כל השיעורים בעמוד אחד

כל 26 השיעורים של סמסטר ב׳ 2026 ברצף אחד — 142 עמודי סיכום ושלושים תמלולים, כפי שהם מופיעים בעמודי השיעורים הנפרדים. העמוד קיים כדי שאפשר יהיה לחפש בכל הסמסטר בבת אחת, ולהדפיס אותו.

תוכן העניינים

1 ממה ניתן לחשב למה ניתן לחשב ביעילות: המודל, המשאבים והמחלקות הבסיסיות

2 חישוב יעיל: מחלקות הזמן והמקום DTime ו-DSpace

3 משפטי היררכיה במקום ובזמן

4 מכונות טיורינג אי-דטרמיניסטיות

5 טיעוני ריפוד ומבוא ל-SAT

6 הגדרה שקולה ל-NP: אימות, עדים ואישורים

7 CLIQUE ו-Independent Set, רדוקציות בזמן פולינומי, NP-קשה ו-NP-שלמה

8 הרדוקציה מ-SAT ל-3SAT

9 משפט קוק–לוין

10 כיסוי בקודקודים, MAXCUT וצביעת גרפים

11 בעיית SUBSET SUM ושלמותה ב-NP

12 PARTITION ו-BIN PACKING, הבעיות ההמילטוניות ו-TSP

13 אלגוריתמי קירוב א׳: 2-קירוב ל-VC, ½-קירוב ל-MAXCUT ואי-קירוב של TSP

14 אלגוריתמי קירוב ב׳: ½-קירוב חמדני ל-MAXCUT, 2-קירוב ל-TSP המטרי ו-2-קירוב לאריזה למכלים

15 אלגוריתמים אקראיים: מבוא, בעיית המזכיר ואלגוריתם Freivalds

16 מכונות טיורינג אקראיות — הגדרה פורמלית, ומחלקות הסיבוכיות RP, coRP ו-BPP

17 העצמת/הקטנת ההסתברות ב-BPP וב-RP

18 בעיית החתך המינימלי: אלגוריתם הכיווץ האקראי, והשיטה ההסתברותית

19 השיטה ההסתברותית, המשך: ניסוי אחיד ל-MAXCUT, חסם 7/8 ל-3ESAT, ובעיית הקבוצה השלטת

20 אלגוריתמים אקראיים לספיקות: אי־שוויון מרקוב, הגברה ודה־רנדומיזציה

21 יחס הקירוב 7/8 ל-MAX-3ECNF, רדוקציה עצמית של SAT, ו-coNP

22 MaxIS — הקבוצה הבלתי תלויה המקסימלית: NP-קשה וגם coNP-קשה

23 חזרה למבחן א׳: פתרון מטלה 1 ושאלה 1 ממבחן 2

24 תרגול חזרה: אפיון מחלקות סיבוכיות ביחס ל-NP (שאלה 3, סעיפים א–ג)

25 חזרה לקראת המבחן: תת-גרף מקסימלי חסר מעגלים, כיסוי בהיפרגרף 3-אחיד, חתך מכוון ואי-קירוב של Bin-Packing

26 חזרה למבחן ד׳: פתרון מטלה 4 — סגירות BPP לחיתוך, וארבעה אפיונים של המחלקות האקראיות

1 ממה ניתן לחשב למה ניתן לחשב ביעילות: המודל, המשאבים והמחלקות הבסיסיות

השיעור מעביר את השאלה המרכזית מ'מה ניתן לחשב' ל'מה ניתן לחשב ביעילות', מקבע את מכונת הטיורינג כסרגל המדידה, מגדיר את משאבי הזמן והמקום, מנתח את מחיר הסימולציות (רב-סרטית והמכונה האוניברסלית), ומוכיח את הקשרים הדו-כיווניים בין זמן למקום ואת ההכלות בין $DTime$ ל-$DSpace$.

ביטחון: high

בקצרה

הקורס הזה הוא המשך ישיר של חישוביות. שם שאלנו **מה ניתן לחשב**; כאן נשאל **מה ניתן לחשב ביעילות** — כלומר אנחנו עושים zoom-in לתוך המחלקה R של הבעיות הכריעות ומחלקים גם אותה. "יעילות" איננה מושג אבסולוטי כמו "ניתן לחשב". צריך לומר יעיל **במה** — זמן, מקום, רוחב פס, ביטים אקראיים, דיוק — ולכן כל הגדרה בקורס תיאמר תמיד ביחס למשאב מסוים ולאורך הקלט.
סרגל המדידה הוא מכונת טיורינג. המשאבים הבסיסיים הם $time_M(x)$ (מספר הפעלות פונקציית המעברים) ו-$space_M(x)$ (מספר התאים **השונים** שהמכונה כותבת בהם).
מעברים בין מודלים עולים כסף, ואנחנו סופרים אותו: סימולציה של מכונה k-סרטית על ידי מכונה חד-סרטית עולה $O(time \cdot space)$ בזמן ואפס בסדר גודל במקום; המכונה האוניברסלית עולה פקטור של $|\langle M\rangle|$ בזמן ופקטור $\lg|\Gamma_M|$ במקום.
הקשר בין זמן למקום אינו סימטרי: תמיד $space_M(x) \le time_M(x)$, אבל בכיוון ההפוך **אין** חסם כלל — אלא אם יודעים שהמכונה עוצרת, ואז $time_M(x) \le 2^{c_M \cdot space_M(x)}$ בעזרת ספירת קונפיגורציות.
מכאן נגזרות שתי המחלקות הבסיסיות $DTime(f)$ ו-$DSpace(f)$ ושתי ההכלות $DTime(f) \subseteq DSpace(f)$ ו-$DSpace(f) \subseteq DTime\left(2^{O(f)}\right)$. אלה הלבנים שמהן ייבנה כל הקורס.

רקע ותלויות

זהו השיעור הראשון בסדרה, ולכן אין כאן הפניות לשיעורים קודמים בקורס. התלות היא כולה בקורס **חישוביות** שקדם לו. מה שצריך לזכור משם — ומה שנשתמש בו כאן ממש, ולכן נכתב במלואו:
1. מכונת טיורינג ופונקציית המעברים. מכונה היא אוסף סופי של מצבים, א"ב קלט/פלט, א"ב עבודה ופונקציית מעברים δ שרואה את המצב הנוכחי ואת התו שהראש הקורא־כותב עומד עליו, ומחליטה למה מצב לעבור, איזה תו לכתוב, ולאן להזיז את הראש. המצב הוא, כדברי המרצה, "כמו שורת קוד". הסרט אינו חסום מאף כיוון.
2. הווריאנט הרב-סרטי ומשפט השקילות. לכל k קבוע מראש (לפני הקלט!) מוגדרת מכונה k-סרטית. משפט השקילות מחישוביות: לכל מכונה רב-סרטית M קיימת מכונה חד-סרטית $\hat{M}$ מעל אותו א"ב קלט/פלט, כך שלכל $x \in \Sigma_M^*$ מתקיים $\hat{M}(x) = M(x)$. בחישוביות זה הספיק; בסיבוכיות נוסיף לזה מימד — כמה זה עולה.

3. המכונה האוניברסלית. קיימת מכונה M_U שמקבלת קידוד של מכונה וקידוד של קלט ומריצה אותם. בחישוביות עניין אותנו רק שהיא קיימת; כאן נשאל כמה זמן ומקום היא צורכת.
4. המחלקות מחישוביות. RE — השפות שניתן לזהות; $coRE$ — המשלימות שלהן; R — השפות שניתן להכריע. בחישוביות R הייתה "הבעיות הקלות", מפני שלא שאלנו כלל כמה משאבים ההכרעה דורשת. כל הקורס הזה מתרחש **בתוך** R.
5. קידודים. כל דטה-טייפ (מספרים, קבוצות, גרפים) ניתן לייצוג כמחרוזת מעל א"ב קבוע, ולהיפך. לכן, כפי שנאמר בהקלטה [00:01:59], הדטה-טייפ פחות מעניין אותנו — מה שמעניין הוא הפונקציות ומודל החישוב.
6. סדר הכמתים. בסיבוכיות זה קריטי פי עשרה מאשר בחישוביות. כשכותבים "לכל M קיים c כך שלכל x", הקבוע c מותר שיהיה תלוי ב-M ואסור שיהיה תלוי ב-x — פשוט מפני ש-x מופיע אחריו.

הגדרות
הגדרה 1: מכונת טיורינג (חד-סרטית)
מכונת טיורינג היא

$$M = (Q, q_{start}, F, \Sigma, \Gamma, \delta),$$

כאשר Q קבוצת מצבים סופית, $q_{start} \in Q$ המצב ההתחלתי, $F \subseteq Q$ קבוצת המצבים הסופיים, Σ א"ב הקלט והפלט, $\Gamma \supseteq \Sigma$ א"ב העבודה, ופונקציית המעברים

$$\delta : Q \times \Gamma \longrightarrow Q \times \Gamma \times \{L, R\}.$$

אינטואיציה. לפי הסיכום, δ "רואה" שני דברים בלבד — המצב הנוכחי והתו שמתחתיו הראש — ומחזירה שלושה: לאן לעבור, מה לכתוב, ולאן לזוז. אין למכונה זיכרון נוסף מעבר לזה: כל מה שהיא רוצה לזכור עליה לכתוב על הסרט או לקודד במצב.
על F. במכונת חישוב מסתפקים במצב סופי אחד, q_H; במכונת הכרעה בשניים בלבד, q_{acc} ו-q_{rej}, והפלט נקבע לפי המצב שבו נעצרה הריצה. לכן בהרבה מקומות (וגם בסיכום) פשוט מוותרים על F כרכיב נפרד בהגדרה. **קונבנציה של הקורס** [00:46:21]: אם לא נאמר אחרת במפורש, "מכונת טיורינג" פירושו מכונה **סטנדרטית — חד-סרטית**, וכל המדדים נמדדים ביחס אליה.
הגדרה 2: מכונת טיורינג k-סרטית
לכל $k \in \mathbb{N}$ הנקבע **מראש, לפני הקלט**, מכונה k-סרטית מוגדרת בדיוק כמו הגדרה 1 פרט לפונקציית המעברים:

$$\delta : Q \times \Gamma^k \longrightarrow Q \times \Gamma^k \times \{L, R\}^k.$$

אינטואיציה. בכל צעד המכונה קוראת תו אחד מכל אחד מ-k הסרטים, ועל סמך k-יית התווים והמצב היא מחליטה מה לכתוב בכל אחד מהסרטים ולאן להזיז כל אחד מ-k הראשים — כל ראש בנפרד. ההדגשה ש-k קבוע מראש חשובה: k אינו רשאי לגדול עם הקלט, ולכן הוא נבלע בקבועים.

דוגמה. מכונה דו-סרטית שמעתיקה את הקלט לסרט השני ואז סורקת את שני הסרטים בכיוונים מנוגדים — נראה אותה בסעיף הדוגמאות. **אי-דוגמה.** "מכונה שמקצה סרט לכל תו בקלט" איננה מכונה k-סרטית לשום k, מפני שמספר הסרטים תלוי בקלט.

הגדרה 3: מדדי הזמן והמקום

בהינתן מכונה M וקלט $x \in \Sigma_M^*$:

$time_M(x)$ — מספר ההפעלות של פונקציית המעברים בריצת M על x.

$space_M(x)$ — מספר התאים **השונים** שבהם M **כותבת** במהלך ריצתה על x.

אינטואיציה והבחנות עדינות. אין דבר כזה "מספר הצעדים של מכונה"; יש רק מספר צעדים של מכונה **על קלט מסוים**. אם המכונה כתבה חמש פעמים באותו תא, זה נספר חמש פעמים בזמן ופעם אחת במקום. שימו לב גם למה **לא** נספר במקום: תאים שהקלט ההתחלתי יושב בהם והמכונה לא כתבה בהם, אינם נספרים [01:05:20]. מכאן שאם M מקבלת מיד את x בלי לקרוא אותו — $time_M(x)$ ו-$space_M(x)$ הם 1 בלבד, גם אם x ארוך.

מוסכמה נוספת [00:19:10]: מדדי היעילות נמדדים תמיד **כפונקציה של אורך הקלט** $|x|$, ואנחנו מתעניינים בסדרי גודל, לא בספירה מדויקת.

הגדרה 4: המכונה האוניברסלית M_U

M_U היא המכונה שהא"ב שלה **בינרי**, המקיימת: לכל מכונה M ולכל $x \in \Sigma_M^*$,

$$M_U(\langle M, x\rangle) = \langle M(x)\rangle.$$

אינטואיציה. M_U יודעת לקבל מכונה מבחוץ ולהריץ אותה. שימו לב שהיא מחזירה את ה**קידוד** של הפלט ולא את הפלט עצמו — ולזה יש סיבה מדויקת. שאלה של סטודנטים [00:35:22]: למה לא להחזיר את הפלט? התשובה: M_U היא מכונה אחת קבועה עם א"ב קבוע (בינרי), והיא צריכה לעבוד עבור מכונות בעלות א"ב שרירותי; אין לה שום דרך לכתוב תו מא"ב שהיא רואה בפעם הראשונה. **במכונת הכרעה** ההערה מתייתרת: שם M_U פשוט מקבלת אם M מקבלת ודוחה אם M דוחה. **המימוש שראינו בחישוביות** — מכונה **רב-סרטית** בעלת חמישה סרטים: סרט קלט, סרט מכונה, סרט עבודה, סרט מצב, וסרט אורך תו.

הגדרה 5: קונפיגורציה

בהינתן מכונה M ומחרוזת $x \in \Sigma_M^*$, **קונפיגורציה** בריצת M על x מורכבת משלושה רכיבים:

המצב הנוכחי;

תוכן הסרט;

מיקום הראש הקורא־כותב.

אינטואיציה. קונפיגורציה היא בדיוק כל המידע שצריך כדי **להמשיך** ריצה מנקודה מסוימת: "אם אני מתחיל ריצה ואני רוצה שאתם תמשיכו אותה, מה עלי לתת לכם?" [01:13:16]. שימו לב מה **אינו** חלק מקונפיגורציה: ההיסטוריה. כיצד הגענו לכאן אינו רלוונטי להמשך, ולמכונה עצמה גם אין דרך לזכור זאת.

דוגמה לגבול ההגדרה (שאלת סטודנטית, [01:23:52]): למה לא די בתו הנוכחי? כי ייתכן שבהמשך הריצה הראש יזוז עשרה תאים ימינה, ואם אין לך את תוכן כל הסרט לא תדעי מה מחכה שם. זה בדיוק כמו להעביר מישהו באמצע ריצה של תוכנית ב-C: לא די בערכי המשתנים של השורה הנוכחית.
אי-דוגמה (שאלת סטודנט, [01:18:35]): מכונה **יכולה** להגיע פעמיים לאותו תוכן סרט בדיוק — למשל מכונה בסגנון אוטומט שסורקת מחרוזת בינרית ובודקת זוגיות של מספר האחדים אינה משנה את הסרט כלל. אבל אלה אינן אותה קונפיגורציה, מפני שהמצב ומיקום הראש שונים.
הגדרה 6: המחלקות $DTime$ ו-$DSpace$
לכל פונקציה $f : \mathbb{N} \to \mathbb{N}$:

$$DTime(f) = \Big\{ A \subseteq \Sigma^* \;\Big|\; \exists M \text{ decider for } A,\ \exists c > 0,\ \forall x :\ time_M(x) \le c \cdot f(|x|) \Big\},$$

$$DSpace(f) = \Big\{ A \subseteq \Sigma^* \;\Big|\; \exists M \text{ decider for } A,\ \exists c > 0,\ \forall x :\ space_M(x) \le c \cdot f(|x|) \Big\}.$$

אינטואיציה. בחישוביות R הייתה "כל הבעיות שקיימת להן מכונה מכריעה". כאן מוסיפים דרישה שנייה על אותה מכונה: לא רק להכריע, אלא להכריע כשמשאב הזמן (או המקום) חסום על ידי f.
סדר הכמתים — נקודת הכישלון הקלאסית [01:22:31]: הקבוע c נבחר **אחרי** המכונה ו**לפני** הקלט. מותר לו להיות תלוי ב-M ובפונקציה, ואסור לו להיות תלוי ב-x. כשכתוב $O(f)$ בהקשר של מדדי סיבוכיות — זו בדיוק המשמעות.
Abuse of notation [01:20:25]: כותבים $DTime(n^2)$ אף שפורמלית צריך להגדיר את הפונקציה $f(n) = n^2$ ואז לכתוב $DTime(f)$. זו הכתיבה המקובלת.
מקרה גבול. אפשר לדבר על $f(n) = \lceil \lg n \rceil$, אבל אז המכונה אפילו לא מספיקה לקרוא את כל הקלט; במכונה דטרמיניסטית שאמורה להכריע נכונה זה נדיר, ויופיע בעיקר בהקשרים מקורבים או הסתברותיים.

משפטים והוכחות
משפט 1: מחיר המעבר ממכונה רב-סרטית למכונה חד-סרטית
לכל מכונה רב-סרטית M קיימת מכונה חד-סרטית $\hat{M}$ מעל אותו א"ב קלט/פלט, כך ש:
הסמנטיקות של M ושל $\hat{M}$ שוות — הן מחשבות בדיוק אותו דבר;
לכל $x \in \Sigma_M^*$ מתקיים

$$time_{\hat{M}}(x) \;\le\; 4 \cdot time_M(x) \cdot \big(space_M(x) + 2\big) \;\le\; O\big(time_M(x) \cdot space_M(x)\big),$$

$$space_{\hat{M}}(x) \;\le\; O\big(space_M(x)\big).$$

הוכחה (הרעיון והחשבון במלואו).
הבנייה. מגדילים את א"ב העבודה כך שכל תא בסרט היחיד של $\hat{M}$ יחזיק k-ייה של תווים — תו אחד עבור כל אחד מ-k סרטי M — ובנוסף סימון של מיקומי k הראשים. כך כל "פרוסה אנכית" של k הסרטים של M מיוצגת בתא אחד של $\hat{M}$.
הסימולציה של צעד בודד. כדי לסמלץ **צעד אחד** של M, המכונה $\hat{M}$ חייבת קודם כול לדעת מה k הראשים קוראים; אך מיקומי הראשים מפוזרים לאורך הסרט, ולכן היא צריכה **לסרוק** את כל התוכן. אחרי שאספה את k התווים היא מפעילה את δ במצב הפנימי שלה, וסורקת שוב כדי לכתוב את k התווים החדשים ולהזיז את k סימוני הראשים. בסך הכול נדרשים **ארבעה סוויפים** על כל התוכן עבור כל צעד של M [00:29:52].
החשבון. אורך התוכן שיש לסרוק חסום על ידי הטווח שהראשים ביקרו בו, כלומר על ידי $space_M(x)$; ה-$+2$ הוא בגלל חריגה של תא אחד לכל צד. לכן כל צעד של M עולה ל-$\hat{M}$ לכל היותר $4 \cdot (space_M(x)+2)$ צעדים, ומכיוון ש-M מבצעת $time_M(x)$ צעדים, סך הכול $4 \cdot time_M(x) \cdot (space_M(x)+2)$.
המקום. $\hat{M}$ כותבת בדיוק על אותו טווח תאים שבו השתמשה M (עד כדי חריגה של תא-שניים), אלא שכל תא "שמן" יותר. השומן הזה נבלע בגודל א"ב העבודה — כלומר בקבוע שאינו תלוי בקלט — ולכן מבחינת **מספר התאים** מדובר באותו סדר גודל: $O(space_M(x))$.

> **הערה:** בהרצאה זה נאמר בקיצור — המרצה הפנה לסרטוני האנימציה מקורס חישוביות ואמר מפורשות שההוכחה שם היא "יותר רעיון מהוכחה פורמלית" [00:31:27]. הפירוט לעיל הוא מה שהיד-מנופפת עומדת מאחוריו.

מה חשוב לקרוא נכון בטענה (שאלה מצוינת של סטודנטית, [00:27:12]). האי-שוויון $time_{\hat{M}} \le O(time_M \cdot space_M)$ **אינו** אומר ש-$\hat{M}$ מהירה יותר. הוא אומר שהיא לא גרועה **בהרבה מדי** — הכפל ב-$space_M$ יכול להיות משמעותי ביותר. הדוגמה: שפת הפלינדרומים נכרעת בזמן ליניארי במכונה דו-סרטית ובזמן ריבועי במכונה חד-סרטית. כלומר המודל הרב-סרטי אינו מחזק אותנו מבחינה **חישובית**, אבל כן מחזק אותנו מבחינת **יעילות**.
מסקנה 1.1. מכיוון ש-$space_M(x) \le time_M(x)$ (משפט 3 להלן), נובע גם

$$time_{\hat{M}}(x) \le O\big(time_M(x)^2\big),$$

כלומר הפער בזמן במעבר לחד-סרטית הוא לכל היותר ריבועי.
משפט 2: יעילות המכונה האוניברסלית הרב-סרטית
תהי M מכונה ויהי $x \in \Sigma_M^*$. אז

$$time_{M_U}(\langle M, x\rangle) = O\Big(|\langle M,x\rangle| + |\langle M\rangle| \cdot time_M(x)\Big) \;\le\; O\Big(|\langle M\rangle| \cdot time_M(x)\Big),$$

$$space_{M_U}(\langle M,x\rangle) \le O\Big(|\langle M,x\rangle| + \lg|\Gamma_M|\cdot space_M(x)\Big) \;\le\; O\Big(\lg|\Gamma_M|\cdot space_M(x)\Big),$$

כאשר האי-שוויון הימני בכל שורה תקף כאשר M קוראת את כל הקלט שלה, וכל הקבועים המוסתרים אינם תלויים לא ב-M ולא ב-x.

הוכחה — חשבון מפורש של הסימולציה.

שלב האתחול. M_U מעתיקה את $\langle M\rangle$ לסרט המכונה, את $\langle x\rangle$ לסרט העבודה, את $\langle q_{start}\rangle$ לסרט המצב, וכותבת סדרת אפסים באורך $1+\lceil\lg|\Gamma_M|\rceil$ בסרט אורך התו. כל זה דורש מעבר אחד על הקלט, כלומר $O(|\langle M,x\rangle|)$ צעדים ו-$O(|\langle M,x\rangle|)$ תאים.

למה בכלל צריך את סרט אורך התו? [00:41:12] בסרט העבודה לא כתוב x אלא **הקידוד הבינרי** של x. כדי לקרוא תו בודד, M_U חייבת לדעת כמה ביטים מרכיבים קידוד של תו אחד; סדרת האפסים משמשת כמונה לאורך זה. (השם "סרט אורך תו" הוא קיצור; מדובר באורך **קידוד** התו.)

הסימולציה. על כל צעד של-M הייתה עושה בריצתה על x, M_U קוראת את התו הנוכחי מסרט העבודה ואת המצב מסרט המצב, ואז **סורקת את כל טבלת** δ הכתובה בסרט המכונה כדי למצוא את המעבר המתאים. במקרה הגרוע היא עוברת על כל הטבלה, כלומר על $O(|\langle M\rangle|)$ תאים. אם M עוצרת — M_U עוצרת.

חשבון הזמן. אתחול פלוס $time_M(x)$ צעדים, שלכל אחד תקורה של $|\langle M\rangle|$:

$$O\big(|\langle M,x\rangle|\big) + time_M(x)\cdot O\big(|\langle M\rangle|\big).$$

מדוע הביטוי השמאלי בדרך כלל נבלע? אם M קוראת את כל הקלט שלה אז $time_M(x)\ge|x|$, ולכן $|\langle M\rangle|+|\langle x\rangle| \;\le\; |\langle M\rangle|\cdot time_M(x)$ עד כדי קבוע. **חשוב:** זה לא תמיד נכון — אצל מכונה שאינה קוראת את כל הקלט הביטוי הראשון עשוי לשלוט. המרצה תיקן את עצמו מפורשות ואמר שהמילה "זניח" כבדה מדי, ושהניסוח הנכון הוא "קטן לעומת השני" [00:45:00].

מדוע $|\langle M\rangle|$ אינו נבלע ב-O? [00:42:52] מפני ש-M היא **חלק מהקלט** של M_U. קבוע מותר שיהיה תלוי במכונה שמריצים — כאן המכונה שמריצים היא M_U, ואילו M משתנה. לכן אסור להסתיר את $|\langle M\rangle|$.

חשבון המקום. M_U נוגעת באותו מספר תאים כמו M, אבל היא כותבת **בביטים**: לכל תו מא"ב Γ_M דרושים $\lceil\lg|\Gamma_M|\rceil$ ביטים (כדי לקודד את כל המספרים מ-1 עד $|\Gamma_M|$). מכאן $\cdot\ \lg|\Gamma_M|$ $space_M(x)$, ובתוספת האתחול מתקבל החסם המבוקש. הערך השלם העליון נבלע בסימון O.

שימו לב שכאן, בניגוד לזמן, **לא באמת הרווחנו** — פשוט בלענו את אורך הקלט בתוך המקום.

מסקנה 2.1: מכונה אוניברסלית חד-סרטית

קיימת מכונה אוניברסלית **חד-סרטית** $\hat{M}_U$ כך שלכל M ולכל $x\in\Sigma_M^*$:

$$time_{\hat{M}_U}(\langle M,x\rangle) \le O\Big(\big(|\langle M,x\rangle|+|\langle M\rangle|\cdot time_M(x)\big)\cdot\big(|\langle M,x\rangle|+\lg|\Gamma_M|\cdot space_M(x)\big)\Big),$$

ובחסם הגס יותר

$$time_{\hat{M}_U}(\langle M, x\rangle) \le O\Big(|\langle M\rangle| \cdot time_M(x) \cdot \lg|\Gamma_M| \cdot space_M(x)\Big),$$

$$space_{\hat{M}_U}(\langle M, x\rangle) \le O\Big(|\langle M, x\rangle| + \lg|\Gamma_M| \cdot space_M(x)\Big).$$

הוכחה. הרכבה של שני המשפטים הקודמים. M_U מומשה כמכונה רב-סרטית; לפי משפט 1, מכונה חד-סרטית שקולה לה רצה בזמן $O(time \cdot space)$ של הרב-סרטית ובאותו סדר גודל של מקום. מציבים את $time_{M_U}$ ואת $space_{M_U}$ ממשפט 2 ומקבלים בדיוק את הביטויים לעיל. ■
למה הקונבנציה הזאת חשובה. בגלל הקונבנציה שכל המדדים נמדדים במכונה סטנדרטית, אנחנו **חייבים** לדעת להחזיר כל בנייה רב-סרטית למכונה חד-סרטית ולשלם את המחיר. זו הסיבה שהמעבר הזה נעשה כאן, בשיעור הראשון, לפני כל דבר אחר.
משפט 3: המקום חסום על ידי הזמן
תהי M מכונה ויהי $x \in \Sigma_M^*$. אז

$$space_M(x) \le time_M(x).$$

הוכחה (מלאה). נסמן $n = time_M(x)$, ונסמן ב-A את קבוצת התאים שהמכונה כותבת בהם בריצתה על x. לפי הגדרה 3, $|A| = space_M(x)$, ובבירור $|\{1, 2, \dots, n\}| = n =$ $time_M(x)$. מדובר, אם כן, באי-שוויון בין גדלים של שתי קבוצות; וכפי שהודגש בהרצאה [01:01:39], מאחורי כל אי-שוויון בין גדלים מסתתרת פונקציה חד-חד-ערכית.
נגדיר $\varphi : A \to \{1, 2, \dots, n\}$ כך: לכל תא $t \in A$, נגדיר $\varphi(t)$ להיות **הצעד הראשון** שבו M כתבה ב-t.
φ מוגדרת היטב: אם $t \in A$ אז לפי הגדרת A קיים צעד שבו המכונה כתבה ב-t; קבוצת הצעדים האלה אינה ריקה וסופית, ולכן יש לה מינימום.
φ חד-חד-ערכית: בכל צעד המכונה כותבת ב**תא אחד בדיוק**. לכן אם $\varphi(t_1) = \varphi(t_2) = j$, אזי בצעד j נכתב גם ב-t_1 וגם ב-t_2, ומכאן $t_1 = t_2$.
קיום פונקציה חד-חד-ערכית מ-A אל $\{1, \dots, n\}$ גורר $|A| \le n$, כלומר $space_M(x) \le$ $time_M(x)$. ■

> **הערה:** בסיכום הצעד "ההתאמה מגדירה פונקציה חד-חד-ערכית" נכתב בשורה אחת. הנימוק שמאחוריו — שבכל צעד נכתב בדיוק תא אחד — הוא בדיוק המקום שבו ההוכחה נשענת על הגדרת $space$ כ"תאים שנכתבו", ולא כ"תאים שבוקרו".

האינטואיציה מאחורי המשפט. כל צעד שהמכונה עושה הוא כתיבה. לפעמים היא כותבת בתא שכבר כתבה בו — וזה נספר לי כצעד אך לא כמקום. לכן המקום אף פעם לא "מדביק" את הזמן.

משפט 4: בכיוון ההפוך אין חסם כלל
טענה. לא ניתן לחסום את זמן הריצה על ידי שום פונקציה של המקום, גם אם ידוע בדיוק כמה מקום המכונה משתמשת.
הוכחה (נגד-דוגמה). נגדיר מכונה M שעל כל קלט רצה לנצח, כאשר הראש הקוראכּותב זז ימינה ושמאלה על אותם שני תאים ללא הפסקה. אז לכל x מתקיים $space_M(x) = 2$ בעוד $time_M(x) = \infty$. אף פונקציה g לא תקיים $\infty \leq g(2)$. ■

> **הערה מהדיון בכיתה** [01:08:31]: תשובה של סטודנט שאמר רק "המכונה עלולה לא לעצור" **אינה מספיקה**. גם במשפט 3 ייתכן שהמכונה לא עוצרת, ושם החסם עדיין נכון (טריוויאלית). מה שהופך את הנגד-דוגמה הזו לתקפה הוא הצירוף: היא לא עוצרת **וגם** משתמשת במספר קבוע של תאים.

משפט 5: אם המכונה עוצרת — הזמן חסום אקספוננציאלית במקום
תהי M מכונת טיורינג. אז קיים קבוע $c_M > 0$ כך שלכל $x \in \Sigma_M^*$: אם M עוצרת על x אז

$$time_M(x) \leq 2^{c_M \cdot space_M(x)}.$$

בכתיב מקוצר: $time_M(x) \leq 2^{O(space_M(x))}$.
שימו לב לסדר הכמתים: תחילה M, אחר כך c_M, ורק אז x. לכן c_M מותר שיהיה תלוי במכונה ואסור שיהיה תלוי בקלט.
הוכחה.
שלב א' — אם המכונה עוצרת, היא לא מבקרת פעמיים באותה קונפיגורציה. המכונה דטרמיניסטית: ברגע שידוע המצב, תוכן הסרט ומיקום הראש — הצעד הבא נקבע ביחידות. נניח בשלילה ש-M בריצתה על x הגיעה לקונפיגורציה C בצעד i ושוב לאותה C בצעד $j > i$.
הקונפיגורציה קובעת את כל ההמשך (ההיסטוריה אינה חלק ממנה, וגם למכונה אין אמצעי לזכור אותה), ולכן מצעד j ואילך תחזור בדיוק אותה סדרת צעדים, ובצעד $j + (j - i)$ נגיע שוב ל-C — וכן הלאה עד אינסוף. מכאן ש-M לא תעצור, בסתירה. לכן:
אם M עוצרת על x, אז M עוברת בכל קונפיגורציה לכל היותר פעם אחת.
שלב ב' — הזמן חסום במספר הקונפיגורציות. נתאים לכל צעד את הקונפיגורציה שבה הריצה נמצאת בסופו. לפי שלב א' זו פונקציה חד-חד-ערכית מקבוצת הצעדים אל קבוצת הקונפיגורציות האפשריות, ולכן

$$time_M(x) \;\leq\; \#\{\text{configurations of } M \text{ on } x\}.$$

שלב ג' — ספירת הקונפיגורציות. קונפיגורציה מורכבת משלושה רכיבים בלתי תלויים:
מצב: $|Q|$ אפשרויות.
תוכן הסרט: אמנם הסרט אינסופי, אך התאים שמחוצה לטווח הריצה נשארים ריקים לנצח. בטווח יש $space_M(x)$ תאים, ולכל תא $|\Gamma|$ אפשרויות בלתי תלויות — מחרוזת באורך s מעל א"ב בגודל g נותנת g^s אפשרויות. סך הכול $|\Gamma|^{space_M(x)}$.

מיקום הראש: הראש אינו יכול לחרוג מהטווח שנכתב בו (בכל צעד הוא כותב), ולכן $space_M(x)$ אפשרויות.
לכן

$$time_M(x) \;\le\; |Q| \cdot |\Gamma|^{space_M(x)} \cdot space_M(x).$$

שלב ד' — האלגברה: העברה לבסיס 2. נסמן $s = space_M(x)$. נשתמש בזהות $a = 2^{\lg a}$ ובכלל $a^b = 2^{b \lg a}$:

$$|Q| \cdot |\Gamma|^{s} \cdot s \;=\; 2^{\lg |Q|} \cdot 2^{s \cdot \lg |\Gamma|} \cdot 2^{\lg s} \;=\; 2^{\lg |Q| + s \cdot \lg |\Gamma| + \lg s}.$$

נוציא את s כגורם משותף בחזקה:

$$= \; 2^{\left(\frac{\lg |Q|}{s} + \lg |\Gamma| + \frac{\lg s}{s}\right) \cdot s}.$$

כעת נחסום מלמעלה. אם $s \ge 1$ אז $\frac{\lg |Q|}{s} \le \lg |Q|$, וכן $\frac{\lg s}{s} \le 1$ מפני ש-$\lg s \le s$ לכל $s \ge 1$.
לכן

$$\le \; 2^{(\lg |Q| + \lg |\Gamma| + 1) \cdot s}.$$

נגדיר $c_M = \lg |Q| + \lg |\Gamma| + 1$ ונקבל בדיוק את הנדרש. ■

> **הערה — התנאי $s \ge 1$ מסומן בסיכום באדום.** החלוקה ב-s בשלב ד' אינה חוקית כאשר $space_M(x) = 0$. המקרה הזה מטופל בנפרד וטריוויאלית: פירושו שהמכונה לא כתבה באף תא, כלומר לא ביצעה אף צעד, ואז $time_M(x) = 0 \le 1 = 2^{c_M \cdot 0}$.
> בכל מקרה אחר המכונה ביצעה לפחות צעד אחד, ובכל צעד היא כותבת בתא, ולכן $space_M(x) \ge 1$.

מה חשוב בביטוי שהתקבל. $c_M = \lg |Q| + \lg |\Gamma| + 1$ תלוי **רק** במכונה — במספר המצבים ובגודל א"ב העבודה — ולא בקלט. זו כל הפואנטה. כמו כן החסם **אינו הדוק**: בשלב ד' העלמנו לתוך המכפלה איברים שיכלו להיות קטנים בהרבה. זה בסדר, מפני שכל מה שרצינו הוא הצורה $2^{O(space)}$.
משפט 6: $DTime(f) \subseteq DSpace(f)$
טענה. לכל $f : \mathbb{N} \to \mathbb{N}$ מתקיים $DTime(f) \subseteq DSpace(f)$.
הוכחה. תהי f כלשהי ותהי $A \in DTime(f)$. לפי ההגדרה קיימת מכונה M וקיים קבוע $c > 0$ כך ש-M מכריעה את A ולכל $x \in \Sigma^*$ מתקיים $time_M(x) \le c \cdot f(|x|)$.
לפי משפט 3, לכל x מתקיים $space_M(x) \le time_M(x)$. בשרשור:

$$space_M(x) \;\le\; time_M(x) \;\le\; c \cdot f(|x|).$$

כלומר **אותה מכונה** M **עצמה** מכריעה את A ומקיימת את מגבלת המקום עם **אותו קבוע** c, שאינו תלוי ב-x. לפי ההגדרה, $A \in DSpace(f)$. ■

מה כדאי לשים לב. ההוכחה אינה בונה מכונה חדשה. כל מה שנדרש הוא לקרוא נכון את שתי ההגדרות ולהשתמש בקשר שכבר הוכחנו. זו הוכחה "לתרגול ההגדרות", אבל היא בדיוק הסוג שנופלים בו במבחן אם מתבלבלים בסדר הכמתים.

משפט 7: $DSpace(f) \subseteq DTime\left(2^{O(f)}\right)$

סימון. הכתיב $DTime\left(2^{O(f)}\right)$ הוא קיצור לאיחוד

$$DTime\left(2^{O(f)}\right) \;=\; \bigcup_{c=1}^{\infty} DTime\left(2^{\,c\cdot f}\right).$$

כלומר: קיים **איזשהו** קבוע c שאינו תלוי בקלט, שעבורו הבעיה נכרעת בזמן $2^{c\cdot f}$. שימו לב שמסתתרים כאן **שני** קבועים — אחד מתוך ה-O שבמעריך ואחד מהגדרת $DTime$ עצמה [01:33:10].

הוכחה. תהי f כלשהי ותהי $A \in DSpace(f)$. לפי ההגדרה קיימת מכונה M וקיים $c > 0$ כך ש-M מכריעה את A ולכל x מתקיים

$$space_M(x) \le c \cdot f(|x|).$$

שלב א' — למה M עוצרת על כל קלט? זו נקודה עדינה שעלתה בכיתה [01:39:00]: חסם על המקום לבדו **אינו** מבטיח עצירה — ראו משפט 4. אבל כאן נתון יותר מזה: M **מכריעה** את A, ומהגדרת ההכרעה, על קלט בשפה היא עוצרת ומקבלת ועל קלט מחוץ לשפה היא עוצרת ודוחה. לכן לכל x, M עוצרת על x.

שלב ב' — הפעלת משפט 5. מכיוון ש-M עוצרת על כל קלט, קיים $c' > 0$ (התלוי ב-M בלבד) כך שלכל x

$$time_M(x) \le 2^{\,c'\cdot space_M(x)}.$$

שלב ג' — שרשור. נציב את חסם המקום בתוך המעריך:

$$time_M(x) \;\le\; 2^{\,c'\cdot space_M(x)} \;\le\; 2^{\,c'\cdot c\cdot f(|x|)}.$$

שלב ד' — הגדרת הקבוע. נגדיר $d = c' \cdot c$. גם c וגם c' הם קבועים התלויים במכונה בלבד ואינם תלויים ב-x, ולכן גם d כזה. קיבלנו מכונה M המכריעה את A, ולכל x מתקיים $time_M(x) \le 2^{\,d\cdot f(|x|)}$. לפי ההגדרה $A \in DTime\left(2^{d\cdot f}\right) \subseteq DTime\left(2^{O(f)}\right)$. ■

דוגמאות ותרגילים מהשיעור

דוגמה 1: שפת הפלינדרומים במכונה חד-סרטית — חשבון מלא

נגדיר

$$PAL = \{x \in \{0,1\}^* \ : \ x = x^R\}.$$

האלגוריתם. המכונה מתחילה מהתו השמאלי ביותר, זוכרת אותו במצב, מוחקת/מסמנת אותו, הולכת ימינה עד התו הימני ביותר שטרם נמחק, ומשווה. אם שונה — דוחה. אם זהה — מוחקת גם אותו, חוזרת שמאלה עד התו השני משמאל, וממשיכה כך פנימה עד שנגמרים התווים.

ספירת הצעדים. נסמן $n = |x|$. המעבר הראשון משמאל לימין עולה בערך n צעדים; החזרה עולה בערך $n-1$; המעבר הבא $n-2$, וכן הלאה עד לצעד בודד. בסך הכול

$$n + (n-1) + (n-2) + \cdots + 1 = \frac{n(n+1)}{2} = O(n^2).$$

זוהי סדרה חשבונית; אפשר לחשב את המספר המדויק, אבל אותנו מעניין סדר הגודל.

ספירת המקום. המכונה כותבת רק בתאים שבתוך הקלט (ואולי חורגת פעם אחת בתא אחד ימינה כדי לזהות את הסוף), ולכן $space = n + O(1) = O(n)$.

מסקנה. $PAL \in DTime(n^2)$ וגם $PAL \in DSpace(n)$. ההוכחה היא בדיוק בדיקת ההגדרה: הצגנו מכונה שמכריעה, ולכל x הזמן שלה $O(|x|^2)$ והמקום שלה $O(|x|)$.

דוגמה 2: אותה שפה במכונה דו-סרטית — הרווח בזמן

האלגוריתם. שני הראשים מתחילים בתו השמאלי ביותר.

מעבר אחד משמאל לימין על שני הסרטים במקביל, שבו מעתיקים את כל x מהסרט הראשון לסרט השני. עלות: n צעדים.

מחזירים את הראש בסרט הראשון לתו השמאלי ביותר. עלות: n צעדים.

מעבר מקבילי: הראש בסרט הראשון הולך **ימינה**, הראש בסרט השני הולך **שמאלה** (מהסוף להתחלה). בכל צעד משווים את שני התווים; אם אי-פעם הם שונים — דוחים. עלות: n צעדים.

החשבון. בסך הכול כ-$3n$ צעדים, כלומר $time = O(n)$ — **ליניארי, לא ריבועי**. במקום, לעומת זאת, אנחנו משלמים קצת יותר: בכל צעד כותבים על שני תאים חדשים (אחד בכל סרט), כלומר בערך $2n+1$; אבל מאחר ש-$k = 2$ קבוע מראש, זה עדיין $O(n)$.

התרגיל שנובע מזה. הריצו את משפט 1 על המכונה הזאת: המעבר לחד-סרטית עולה $O(time \cdot space) = O(n \cdot n) = O(n^2)$ — וקיבלנו בדיוק את המכונה החד-סרטית מדוגמה 1. זה מדגים ששני החסמים תופרים זה לזה בצורה הדוקה במקרה הזה.

דוגמה 3: המכונה שהמקום שלה 2 והזמן שלה אינסוף

מכונה שכל מה שהיא עושה הוא להזיז את הראש ימינה, שמאלה, ימינה, שמאלה לנצח, ולכתוב בכל צעד באחד משני תאים. $space = 2$, $time = \infty$. זו הנגד-דוגמה של משפט 4, והיא גם התשובה לשאלה "האם אי-העצירה היא כל הסיפור?" — התשובה, לפי משפט 5, היא **כן**: ברגע שמניחים עצירה, כן מתקבל חסם.

דוגמה 4 (תרגיל מהכיתה): מכונה שמקבלת מיד
נתונה מכונה שמקבלת כל קלט מיד, בלי לקרוא אותו. מהם המדדים שלה?
פתרון. $time = 1$ ו-$space = 1$. שימו לב שאורך הקלט **אינו** משפיע: התאים שהקלט יושב בהם לא נכתבו על ידי המכונה ולכן אינם נספרים במקום [01:05:20]. זו בדיוק ההבחנה שההגדרה של $space$ היא "תאים שנכתבו" ולא "תאים שקיימים".
תרגיל 5 (ספירה קומבינטורית, מהכיתה)
כמה מחרוזות שונות באורך k יש מעל א"ב בגודל m?
פתרון. לכל אחד מ-k המקומות יש m אפשרויות, והבחירות בלתי תלויות, ולכן m^k. זה בדיוק הרכיב $|\Gamma|^{space_M(x)}$ בספירת הקונפיגורציות — נקודה שבלבלה כמה סטודנטים בשיעור, שחשבו שמדובר ב-$space \cdot |\Gamma|$ במקום בחזקה.
תרגיל 6 (הבנת ההגדרה): לאיזו מחלקה שייכת PAL?
פתרון. לפי דוגמה 1 (מכונה **סטנדרטית**, כמתחייב מהקונבנציה): $PAL \in DTime(n^2)$ ו-$PAL \in DSpace(n)$. מדגישים "סטנדרטית", שכן אילו מדדנו במכונה דו-סרטית היינו מקבלים $O(n)$ בזמן — וזו הסיבה שהקונבנציה נקבעה מראש.
בדיקת עקביות עם משפט 6 ומשפט 7. משפט 6 נותן $DTime(n^2) \subseteq DSpace(n^2)$, ואכן $DSpace(n) \subseteq DTime(2^{O(n)})$ — עקבי, אם כי לא הדוק כאן. משפט 7 נותן $O(n) \subseteq O(n^2)$, וגם זה מתקיים בבירור עבור מכונה שרצה בזמן $O(n^2)$.

הערות מהשיעור
"יעיל" הוא מושג לא אבסולוטי [00:04:06]. בניגוד ל"ניתן/לא ניתן לחשב", שהוא מוחלט, יעילות היא "עניין של אופנה". כשהתחום התחיל בשנות ה-70 של המאה הקודמת, זמן ריצה **פולינומי** בגודל הקלט נחשב יעיל — אף שגם אז ידעו ש-x^{100} אינו באמת יעיל [00:04:37]. היום, בגלל גדלי הנתונים, גם זמן ליניארי לא תמיד נחשב יעיל [00:05:08].
אילו משאבים בכלל ישנ? [00:06:13]–[00:12:42] הדיון בכיתה העלה: זמן, מקום/זיכרון, רוחב פס (כמות הנתונים שצריך להעביר — קריטי באלגוריתמים מודרניים), ביטים אקראיים (יקרים, ו"הרנדום" של המחשב אינו באמת אקראי), ו**נאמנות/דיוק** של האלגוריתם — אלגוריתם אקראי לפעמים טועה, וזה משאב שאני מוכן לסחור בו. בעולם האמיתי משתמשים במשאבים האלה "כמו פלסטלינה": משלמים בזמן כדי לקבל דיוק, משלמים במקום כדי לחסוך בזמן, מחשבים יותר בבית כדי לחסוך ברוחב פס.
מה לא נספור [00:09:31]. זמן קומפילציה, זמן מתכנת, כמות שורות קוד — אלה משאבים אמיתיים בעולם האמיתי, אבל הם **לא תלויים בקלט** והם קורים לפני הריצה. בקורס הזה סופרים רק משאבים שנצרכים ב-run time.
מה הקורס יכסה [00:09:09, בהקלטה השנייה]: (1) מה ניתן לחשב כשהמשאבים מוגבלים; (2) קשרים בין רמות הקושי של בעיות שונות, גם כשלא יודעים להכריע לגבי כל בעיה בנפרד; (3) מה עושים כשבעיה "קשה" — קירוב, אלגוריתמים הסתברותיים. בניגוד לחישוביות, כאן **יודעים הרבה פחות**: יש המון בעיות שלא יודעים לפתור ביעילות וגם לא יודעים להוכיח שאי אפשר.

סימון O מחביא דברים — דעו מה [00:26:08]. במעבר מרב-סרטית לחד-סרטית הקבועים המוסתרים תלויים במספר הסרטים. זה לא תלוי בקלט, אבל צריך להיות ברור מה בדיוק נבלע.
"קטן שווה" אינו "יותר טוב" [00:28:13]. כשכותבים $\leq$ לא אומרים "זה טוב יותר", אלא "זה לא הרבה יותר גרוע".
המשפט הכי חוזר בשיעור [01:30:37], [00:52:11], [01:22:31]: כשאתם רואים $O(\cdot)$ בהקשר של מדדי סיבוכיות, **שאלו את עצמכם במה הקבוע תלוי ובמה אינו תלוי**. הוא אף פעם לא תלוי בקלט. "זה המקום שבו טועים" — נאמר מפורשות שלוש פעמים.
מתי לא נכתוב יותר מכונות טיורינג [00:40:07]. "רוב הזמן בקורס הזה לא נכתוב מכונות טיורינג בצורה מפורשת, אנחנו נכתוב אותן כאלגוריתמים." כתבנו אותן בחישוביות כדי לקבל תחושה של המודל; קיבלנו את התחושה, אפשר להמשיך.
על מספר הסרטים של המכונה האוניברסלית [00:38:33]. המרצה ציין שהוא "נדיב" בסרטים — שלושה או חמישה זה עד כדי קבוע, וקבוע כפלי אינו משחק תפקיד מספיק חשוב בתיאוריה הזאת. בעולם האמיתי ההבדל בין שלושה לחמישה כן חשוב.
שאלת סטודנט ששווה לזכור [01:18:05]: "האם ייתכן שמכונה מיועדת להגיע לאותה קונפיגורציה כמה פעמים ורק אז לעצור?" התשובה — לא. ברגע שהיא לא יודעת את ההיסטוריה, היא לא יודעת שהיא כבר הייתה שם. אבל שימו לב לניסוח: **אותו תוכן סרט** יכול לחזור פעמיים; מה שלא יכול לחזור הוא השלישייה כולה.
על כתיבה ביד [00:22:53]. המרצה מעלה את המחברת ואת ההקלטה, ובכל זאת המליץ לכתוב, לפחות את הטענות המרכזיות וההגדרות — "הזיכרון שלנו עובד יותר טוב כשזה עובר דרך היד", וגם כדי שהחומר יהיה מול העיניים כשמפנים אליו כעבור עשר דקות.
תנאי הלמידה [00:53:37]: השיעור הופסק פעמיים באמצע בגלל אזעקות; הפסקה של רבע שעה. "תשמרו על עצמכם, זה יותר חשוב מסיבוכיות."
המשימה לשיעור הבא [01:32:10]: לחזור על החשבון של שלב ד' במשפט 5 ולוודא שאתם יודעים לבצע אותו לבד — המניפולציות של לוגים וחזקות והמעבר ל-$2^{\lg(\cdot)}$ "צריכים לשבת ממש ממש טוב". זו אלגברה, לא סיבוכיות. בנוסף — למי שלא ראה, לצפות בסרטוני הסימולציה הרב-סרטית מקורס חישוביות.

פערים בין הסיכום להקלטה

מקור: עמוד 1 בסיכום. **הפער:** מכונת טיורינג מוגדרת שם כחמישייה $M = (Q, F, \Sigma, \Gamma, \delta)$, ללא q_{start}; גם בהקלטה הראשונה המרצה התבלבל בהגדרה בזמן אמת [00:15:56] ותיקן את עצמו כמה פעמים. **ההכרעה:** בגוף השיעור כתבתי את ההגדרה עם q_{start}, מפני שהמכונה חייבת מצב התחלתי; ההקלטה השנייה [00:12:48] אכן מונה אותו במפורש כרכיב.
מקור: ההקלטה השנייה בלבד, [01:13:29]–[01:43:19]. **הפער:** הגדרות $DTime(f)$ ו-$DSpace(f)$, שתי ההכלות ביניהן, והפירוק $DTime(2^{O(f)}) = \bigcup_c DTime(2^{cf})$ — כל אלה אינם מופיעים כלל בארבעת עמודי הסיכום. **ההכרעה:** נכללו במלואם, שכן הם נלמדו בשיעור והם התוצר העיקרי שלו.

מקור: ההקלטה הראשונה. **הפער:** ההקלטה הראשונה **אינה** מגיעה למחלקות; היא נעצרת בדיוק אחרי הטענה $time_M(x) \le 2^{c \cdot space_M(x)}$, ככל הנראה בגלל שתי הפסקות האזעקה. **ההכרעה:** שתי ההקלטות סומנו `coverage: full` מפני שיחד הן מכסות את השיעור, והשנייה מכסה גם את מה שהראשונה החמיצה.

מקור: דוגמת הפלינדרומים. **הפער:** מופיעה בשתי ההקלטות (בהרחבה בשנייה, [00:16:32]–[00:20:14]) ואינה מופיעה בסיכום כלל. **ההכרעה:** נכללה בסעיף הדוגמאות עם החשבון המלא, כי היא הדוגמה היחידה בשיעור שבה מדדי הזמן והמקום מחושבים מקצה לקצה.

מקור: עמוד 2 בסיכום מול ההקלטה השנייה [00:43:10]. **הפער:** הסיכום נותן למכונה האוניברסלית החד-סרטית חסם זמן במכפלה $O\big(|\langle M\rangle| \cdot time_M(x) \cdot \lg|\Gamma_M| \cdot space_M(x)\big)$, ואילו בהקלטה השנייה נאמר החסם הגס יותר $O\big(|\langle M\rangle|^2 \cdot time_M(x)^2\big)$. **ההכרעה:** שני החסמים נכונים — השני מתקבל מהראשון על ידי הצבת $space \le time$ ו-$\lg|\Gamma_M| \le |\langle M\rangle|$ — והבאתי את גרסת הסיכום כעיקרית, כי היא ההדוקה יותר, עם המסקנה הריבועית כהערה.

מקור: עמוד 2 בסיכום. **הפער:** חסם הזמן של המכונה האוניברסלית נכתב עם סימן שוויון: $time_{M_U}(\langle M, x\rangle) = O(\dots)$. **ההכרעה:** מדובר בחסם עליון; שמרתי על הסימון של הסיכום בשורה הראשונה, אך ניסחתי את הטענה כחסם.

מקור: עמוד 4 בסיכום, ההערה האדומה. **הפער:** ההערה מסומנת בצבע ובשני סימני קריאה אך ניסוחה המדויק בכתב היד קשה לפענוח מלא; ברור ממנה שהיא נוגעת לצורך להניח משהו על $space$ לפני החלוקה בשלב (*). **ההכרעה:** שוחזרה כתנאי $space_M(x) \ge 1$ (שאחרת החלוקה אינה מוגדרת), והמקרה $space = 0$ טופל בנפרד בגוף ההוכחה. זהו שחזור, לא קריאה מילולית.

מקור: ההקלטה הראשונה, [01:04:19] ו-[01:20:11]. **הפער:** התמלול האוטומטי כותב "פונקציה חד ערכית" במקום "חד-חד-ערכית" (וגם "חדקית", "חדרכית"). **ההכרעה:** תוקן ל-injective; המשמעות המתמטית הנדרשת בשתי ההוכחות היא חד-חד-ערכיות, שהרי בלעדיה אין אי-שוויון בין גדלי הקבוצות.

מקור: ההקלטה הראשונה, [00:24:59] ו-[01:26:32]. **הפער:** התמלול משבש כמעט כל סימון מתמטי — "טיים"/"ט" ל-$time$, "ספייס"/"ספיס"/"SP" ל-$space$, "לוגog"/"לogג" ל-$\lg$, "גמה"/"גם m" ל-Γ_M, "אם כובע" ל-$\hat{M}$. **ההכרעה:** כל הסימונים אוחדו לפי הסיכום, שהוא המקור הסמכותי לנוטציה.

מקור: ההקלטה הראשונה, [00:24:59]. **הפער:** המרצה אמר "בעיקרון זה היה ספייס 2" ומיד תיקן ל"ועוד שתיים, זה בגלל החריגה לשני הצדדים". **ההכרעה:** הסיכום כותב $space_M(x) + 2$, וזה הנוסח שנכלל; ההסבר לתוספת ($+1$ לכל צד) נכלל בגוף ההוכחה.

מקור: משפט 1, שני המקורות. **הפער:** אף מקור אינו נותן הוכחה פורמלית לסימולציה הרב-סרטית; המרצה אמר במפורש שההוכחה בסרטונים "היא לא הוכחה פורמלית, היא יותר מה הרעיון" [00:31:58]. **ההכרעה:** כתבתי את הבנייה ואת חשבון ארבעת הסוויפים במלואם וסימנתי את הקטע בהערת "בהרצאה זה נאמר בקיצור".

סיכום ונקודות למבחן

מה חייבים לדעת בעל פה.

$time_M(x)$ — מספר הפעלות δ. $space_M(x)$ — מספר התאים **השונים שנכתבו**. שתי המחרוזות "השונים" ו"שנכתבו" הן בדיוק הנקודות שנופלים בהן.
רב-סרטית $\to$ חד-סרטית: $time_{\hat{M}} \le 4 \cdot time_M \cdot (space_M + 2) = O(time_M \cdot space_M)$, והמקום נשמר עד כדי סדר גודל.
$\le O(time_M^2)$
מכונה אוניברסלית: פקטור $|\langle M \rangle|$ בזמן, פקטור $\lg |\Gamma_M|$ במקום.
$space_M(x) \le time_M(x)$ — תמיד, ללא הנחות.
אין חסם הפוך בלי הנחת עצירה. **עם** הנחת עצירה: $time_M(x) \le 2^{c_M \cdot space_M(x)}$, כאשר $c_M = \lg |Q| + \lg |\Gamma| + 1$.
מספר הקונפיגורציות $= |Q| \cdot |\Gamma|^{space} \cdot space$.
$DTime(f) \subseteq DSpace(f) \subseteq DTime\left(2^{O(f)}\right)$.
המלכודות הסטנדרטיות.
סדר הכמתים. קבוע התלוי במכונה — מותר. קבוע התלוי בקלט — אסור. אם בהוכחה שלכם הקבוע "נבחר אחרי שראינו את x", ההוכחה שגויה.
לחשוב ש-$\le$ פירושו "טוב יותר". במעבר לחד-סרטית האי-שוויון מבטיח רק ש"לא הרבה יותר גרוע".
לענות "המכונה לא עוצרת" כנימוק שלם במשפט 4. חייבים גם לומר שהיא משתמשת במקום קבוע.
לבלבל $|\Gamma|^{space}$ **עם** $|\Gamma| \cdot space$ בספירת הקונפיגורציות.
לשכוח למה M **עוצרת** בהוכחת משפט 7 — הנימוק אינו חסם המקום אלא העובדה שהיא **מכריעה**.
לספור תאים שהקלט יושב בהם כחלק מה-$space$ כשהמכונה לא כתבה בהם.
לשכוח את הקונבנציה שכל המדדים במכונה סטנדרטית חד-סרטית, אלא אם נאמר אחרת.
צ'ק-ליסט: מה סטודנט אמור לדעת לעשות אחרי השיעור.
לחשב $time$ ו-$space$ של מכונה נתונה על קלט נתון, ולנמק כל אחד מהם.
להוכיח שייכות של שפה ל-$DTime(f)$ או ל-$DSpace(f)$ על ידי הצגת מכונה ובדיקת שני התנאים בהגדרה.
לבצע לבד את כל האלגברה של שלב ד' במשפט 5: $a^b = 2^{b \lg a}$, איחוד חזקות, הוצאת $space$ כגורם משותף, והחסימות $\lg |Q| \le \frac{\lg |Q|}{s}$ ו-$\frac{\lg s}{s} \le 1$.
לספור קונפיגורציות של מכונה נתונה.
לתרגם חסם על מכונה רב-סרטית לחסם על מכונה חד-סרטית ולהיפך.
לזהות, בכל טענה עם O, במה הקבוע תלוי.
הסיכום הכתוב שעליו נשען הקובץ הוא של גיא סופר.

שאלות שנשארו פתוחות

ה-slug שניתן, intro-what-is-computable, מתאים לשיעור הראשון של *חישוביות*; השיעור הזה כבר עוסק ב'מה ניתן לחשב ביעילות' — כלומר במודל, במשאבים ובמחלקות. השארתי את שם הקובץ כפי שהוקצה והכותרת האמיתית נמצאת ב-title_he.

הגדרת מכונת הטיורינג בעמוד 1 בסיכום היא חמישייה $(Q,F,\Sigma,\Gamma,\delta)$ ואינה כוללת את q_{start}. בגוף השיעור כתבתי את ההגדרה המלאה; ייתכן שגיא סופר השמיט את q_{start} בכוונה מפני שהמרצה עצמו התבלבל בהגדרה בהקלטה [00:15:56].

הגדרות $DTime$ ו-$DSpace$ מופיעות רק בהקלטה השנייה ואינן בסיכום של שיעור 1. ייתכן שהן מופיעות בסיכום של שיעור 2 — כדאי שהרכז יוודא שאין כפילות מול הקובץ של שיעור 2.

המרצה אמר [00:21:16] שכדאי לחזור לסרטוני הסימולציה מקורס חישוביות; הסרטונים אינם בין המקורות שלי, ולכן פירוט הסימולציה של מכונה רב-סרטית שוחזר מהתמליל ומהסיכום ולא מהמקור שאליו הפנה.

2 חישוב יעיל: מחלקות הזמן והמקום DTime ו-DSpace

בשיעור הזה מוגדרות מחלקות הסיבוכיות הבסיסיות $\mathrm{DTime}(f)$ ו-$\mathrm{DSpace}(f)$, נגזרים מהן ההכלות הבסיסיות בין זמן למקום, ומוגדרות המחלקות הגסות P, EXP, PSPACE ו-EXPSPACE.

ביטחון: high

בקצרה

מגדירים כאן, לראשונה בקורס, **מחלקות סיבוכיות**: $\mathrm{DTime}(f)$ ו-$\mathrm{DSpace}(f)$ — קבוצות של **שפות** (לא של מכונות) שניתן להכריע בזמן $O(f)$ או במקום $O(f)$ בהתאמה.

מוכיחים שני הקשרים הבסיסיים בין זמן למקום ברמת המחלקות: $\mathrm{DTime}(f) \subseteq \mathrm{DSpace}(f)$ (מקום זול מזמן), ו-$\mathrm{DSpace}(f) \subseteq \bigcup_{d \geq 1} \mathrm{DTime}(2^{d \cdot f})$ (זמן חסום אקספוננציאלית במקום — אבל רק כשהמכונה עוצרת).

מוכיחים שהמחלקות מונוטוניות ביחס לסדר גודל: אם $f = O(g)$ אז $\mathrm{DTime}(f) \subseteq \mathrm{DTime}(g)$ וכן ל-DSpace. זה מה שהופך את הכתיב $\mathrm{DTime}(n^2)$ למשמעותי.

מגדירים את ארבע ה**מחלקות הגסות** של הקורס: P, EXP, PSPACE, $\mathrm{EXPSPACE}$, כאיחודים אינסופיים של מחלקות עדינות.

מוכיחים $P \subseteq \mathrm{PSPACE}$ (פעמיים: הוכחה "ארוכה" שמפרקת את כל הפרמטרים, והוכחה בת שתי שורות מהטענות הקודמות), ובהקלטה השנייה גם $\mathrm{PSPACE} \subseteq \mathrm{EXP}$.

המסר המתודי של השיעור, וכנראה החשוב שבו: בסיבוכיות ההוכחות אינן קשות אלא **עתירות פרמטרים**. כל ההוכחות כאן נבנות באותו מבנה קשיח — פורסים הגדרה כדי לקבל ליד מכונה וקבועים, ואז מרכיבים מהם קבועים חדשים. מי ששולט במבנה הזה לא ייתקע בהוכחות הכבדות של שיעור 3 ואילך.

רקע ותלויות

כל החומר של השיעור הזה נשען על שיעור 1 בלבד (ראו שיעור 1). מה שצריך להיות ביד:

1. גדלי הסיבוכיות של ריצה בודדת. עבור מכונת טיורינג M ומילה $x \in \Sigma_M^*$:

$\mathrm{time}_M(x)$ — מספר הצעדים ש-M מבצעת בריצה על x (ואינסוף אם אינה עוצרת).

$\mathrm{space}_M(x)$ — מספר התאים השונים ש-M כותבת עליהם במהלך הריצה על x.

שימו לב שאלה גדלים של **ריצה בודדת** — הם פונקציה של x, לא של n. בשיעור 1 לא הגדרנו שום מחלקה של שפות; זה בדיוק מה שנעשה היום. (שאלה שנשאלה בשיעור, [00:06:33]: "מה ההבדל בין DSpace למה שעשינו בשיעור הקודם?" — בשיעור הקודם הגדרנו את המקום *של מכונה*, לא מחלקה של שפות המקיימות משהו.)

2. ההסכמה על מודל המכונה. אלא אם נאמר אחרת, "מכונה" בקורס הזה פירושה **מכונת טיורינג דטרמיניסטית חד-סרטית סטנדרטית** — כזו שהראש שלה אינו עוצר במקום ואין בה שום וריאנט מיוחד ([00:43:50]). זה חשוב מאוד: חסמי זמן קונקרטיים (למשל n^2 עבור פלינדרומים) תלויים במודל.

3. הקשר בין זמן למקום ברמת הריצה הבודדת. זו התוצאה המרכזית של שיעור 1, והשיעור הזה נפתח בה (עמוד 1 בסיכום). היא מנוסחת ומוכחת במלואה למטה כ**משפט 1**, כי כל שאר השיעור נשען עליה.

4. סימון O גדול. ההגדרה המקורית: $f = O(g)$ אם קיימים $c > 0$ ו-$n_0 \in \mathbb{N}$ כך שלכל $n > n_0$ מתקיים $f(n) \leq c \cdot g(n)$. ראינו במבנה נתונים שאפשר לוותר על n_0 ולדרוש את החסם **לכל** $n \in \mathbb{N}$, במחיר קבוע אחר ([00:53:05], וגם [00:05:11] בהקלטה השנייה). הגרסה בלי n_0 היא זו שנשתמש בה, והיא זו שמתאימה להגדרת DTime — שדורשת חסם **לכל** x, לא רק מאורך מסוים והלאה.

5. מכריעה $\Rightarrow$ עוצרת. אם M מכריעה שפה A אז M עוצרת על **כל** קלט. זו הנקודה שתאפשר לנו להפעיל את משפט 1 בתוך ההוכחות.

הגדרות

הגדרה 1: $\mathrm{DTime}(f)$

תהא $f : \mathbb{N} \to \mathbb{N}$ פונקציה כלשהי. נגדיר:

$$\mathrm{DTime}(f) = \left\{ A \;\middle|\; \exists M \; \exists c > 0 \;\text{ s.t. }\; M \text{ decides } A \;\wedge\; \forall x : \; \mathrm{time}_M(x) \leq c \cdot f(|x|) \right\}$$

כלומר: $A \in \mathrm{DTime}(f)$ אם ורק אם **קיימת** מכונה M ו**קיים** קבוע $c > 0$ כך ש-M מכריעה את A **וגם** לכל x מתקיים $\mathrm{time}_M(x) \leq c \cdot f(|x|)$.

ה-D הוא קיצור ל-**Deterministic** — בהמשך הקורס יופיעו גם מכונות אי-דטרמיניסטיות, אך כרגע כל המכונות שלנו דטרמיניסטיות.

אינטואיציה. $\mathrm{DTime}(f)$ היא אוסף כל השפות שניתן להכריע בזמן $O(f)$. זו הדרך הנכונה *לחשוב* על המחלקה, אבל **לא** הדרך לעבוד איתה: כשבאים להוכיח משהו חייבים לרדת להגדרה הפורמלית, כי רק היא נותנת ליד את המכונה ואת הקבוע ([00:04:28]).

שלוש נקודות דיוק שחזרו שוב ושוב בשיעור:

סדר הכמתים. $\exists M \; \exists c \; \forall x$ — המכונה והקבוע נבחרים ראשונים, ורק אחר כך רצים על כל הקלטים. קבוע אחד משרת את כל הקלטים.

f מקבלת $|x|$ ולא x. f היא פונקציה מ-$\mathbb{N}$ ל-$\mathbb{N}$, ו-x הוא מחרוזת; $f(x)$ חסר משמעות. סיבוכיות תמיד נמדדת ביחס ל**אורך** הקלט ([00:14:41]).

האיברים של המחלקה הם שפות. A אינה מכונת טיורינג — מחלקות סיבוכיות הן קבוצות שאיבריהן שפות ([00:17:26]).

דוגמה. PAL, שפת הפלינדרומים מעל $\{0,1\}$, מקיימת $PAL \in \mathrm{DTime}(n^2)$ — ראו את הפירוט בסעיף הדוגמאות.

אי-דוגמה שממחישה את הגבול. שפה שאינה כריעה כלל, למשל HALT, אינה שייכת ל-$\mathrm{DTime}(f)$ עבור שום f — ההגדרה דורשת ש-M **תכריע** את A, לא רק תקבל אותה. חסם זמן בלי דרישת הכרעה הוא חסר תוכן כאן.

הגדרה 2: $\mathrm{DSpace}(f)$
תהא $f : \mathbb{N} \to \mathbb{N}$. נגדיר:
$$\mathrm{DSpace}(f) = \left\{ A \;\middle|\; \exists M \; \exists c > 0 \;\text{ s.t. }\; M \text{ decides } A \;\wedge\; \forall x : \; \mathrm{space}_M(x) \leq c \cdot f(|x|) \right\}$$
ההגדרה זהה מילה במילה להגדרה 1, למעט החלפת time ב-space.
אינטואיציה. כל השפות שניתן להכריע במקום $O(f)$.
דוגמה. $PAL \in \mathrm{DSpace}(n)$ — האלגוריתם הנאיבי כותב רק על תאי הקלט עצמו, כלומר $\mathrm{space}_M(x) \leq |x|$, ולכן מתאים $c = 1$ ו-$f(n) = n$.
הגדרה 3: $f = O(g)$ (בגרסה שנשתמש בה)
$f = O(g)$ אם **קיים** $c > 0$ כך ש**לכל** $n \in \mathbb{N}$ מתקיים $f(n) \leq c \cdot g(n)$.
זו גרסה שקולה לגרסה הסטנדרטית (שבה החסם נדרש רק החל מ-n_0 כלשהו), והשקילות נראתה בקורס מבנה נתונים. השקילות אינה מובנת מאליה והיא **הכרחית** כאן: הגדרות 1–2 דורשות את החסם לכל x, גם לקלטים קצרים מאוד, בעוד הגדרת ה-O המקורית "מוותרת" על קלטים קצרים. הרעיון שמאחורי השקילות: יש רק **מספר סופי** של קלטים באורך $\leq n_0$, ולכן אפשר להגדיל את הקבוע c כך שיבלע גם אותם.
הגדרה 4: המחלקות הגסות $P,\ \mathrm{EXP},\ \mathrm{PSPACE},\ \mathrm{EXPSPACE}$
$$P = \bigcup_{c \geq 1} \mathrm{DTime}(n^c) \qquad \mathrm{EXP} = \bigcup_{c \geq 1} \mathrm{DTime}(2^{n^c}) \; \mathrm{PSPACE} = \bigcup_{c \geq 1} \mathrm{DSpace}(n^c) \qquad \mathrm{EXPSPACE} = \bigcup_{c \geq 1} \mathrm{DSpace}(2^{n^c})$$
מינוח. המחלקות $\mathrm{DTime}(f)$ ו-$\mathrm{DSpace}(f)$ נקראות **מחלקות עדינות** (fine), כיוון שכל מחלקה כזו מוגדרת על פי פונקציית חסם **אחת ספציפית**. המחלקות שבהגדרה זו נקראות **מחלקות גסות** (coarse), והן איחודים אינסופיים של מחלקות עדינות.
אינטואיציה. P היא אוסף כל השפות שניתן להכריע בזמן **פולינומי בגודל הקלט**. חשוב לומר "בגודל הקלט" — ל"פולינומי" סתם אין משמעות ([01:06:29]). הנקודה העדינה: החזקה c היא **קבועה** ואינה תלויה בקלט; יש פולינום אחד שחוסם את זמן הריצה על כל הקלטים.
מה הולך לאיבוד באיחוד. שייכות לאיחוד היא **טענת קיום**: $A \in P$ פירושו "קיים $c \geq 1$ כך ש-$A \in \mathrm{DTime}(n^c)$". כשמוכיחים שייכות ל-$P$ חייבים "לקלף" קודם את הקיים הזה, ורק אז מגיעים למכונה ([01:09:40]).
דוגמה. $PAL \in \mathrm{DTime}(n^2) \subseteq P$.
אי-דוגמה שמחדדת את הגבול. $\mathrm{DTime}(n^{100}) \subseteq P$ — למרות שאלגוריתם בזמן n^{100} אינו ישים בפועל בשום צורה. P היא מחלקה רחבה מאוד, והזיהוי שלה עם "יעיל" הוא הסכמה, לא משפט (ראו הערות).

משפטים והוכחות
משפט 1: הקשר בין זמן למקום (תזכורת משיעור 1, עם ההוכחה במלואה)
חלק א'. לכל מכונה M ולכל $x \in \Sigma_M^*$: $\mathrm{space}_M(x) \leq \mathrm{time}_M(x)$.

חלק ב'. לכל מכונה M **קיים** $c>0$ כך **שלכל** $x\in\Sigma_M^*$: אם M עוצרת על x אז $\mathrm{time}_M(x)\ \le\ 2^{\,c\cdot \mathrm{space}_M(x)}$, $\qquad c=\lg|Q|+\lg|\Gamma|+1.$
כאן Q היא קבוצת המצבים של M ו-Γ אלפבית הסרט שלה.

הוכחת חלק א'. בכל צעד יחיד המכונה כותבת על תא אחד לכל היותר. לכן מספר התאים **השונים** שנכתבו לאורך הריצה אינו עולה על מספר הצעדים. $\square$

הוכחת חלק ב'. נסמן $s=\mathrm{space}_M(x)\ge 1$. נספור את מספר הקונפיגורציות השונות האפשריות בריצה של M על x. קונפיגורציה נקבעת על ידי שלושה רכיבים:
המצב הנוכחי — $|Q|$ אפשרויות;
תוכן התאים שנכתבו — כל אחד מ-s התאים מכיל אות מ-Γ, כלומר $|\Gamma|^s$ אפשרויות;
מיקום הראש — s אפשרויות.
לכן מספר הקונפיגורציות השונות חסום על ידי $|Q|\cdot|\Gamma|^s\cdot s\ =\ 2^{\,\lg|Q|\ +\ s\cdot\lg|\Gamma|\ +\ \lg s}$.
כעת נחסום כל אחד משלושת המחוברים במעריך בביטוי שהוא **ליניארי ב-**s, ובכך "נשטח" את המעריך:
$\lg|Q|\le s\cdot\lg|Q|$, כי $s\ge 1$;
$s\cdot\lg|\Gamma|$ — כבר ליניארי ב-s;
$\lg s\le s$, כי $\lg s\le s$ לכל $s\ge 1$.
מכאן שמספר הקונפיגורציות חסום על ידי $2^{c\cdot s}=2^{(\lg|Q|+\lg|\Gamma|+1)\cdot s}$.
לבסוף: M דטרמיניסטית, ולכן אם היא מגיעה פעמיים לאותה קונפיגורציה היא נכנסת ללולאה אינסופית ואינה עוצרת. בהנחה ש-M **עוצרת** על x, כל הקונפיגורציות בריצה שונות זו מזו, ולכן מספר הצעדים אינו עולה על מספר הקונפיגורציות האפשריות: $\mathrm{time}_M(x)\le 2^{c\cdot\mathrm{space}_M(x)}$. $\square$

> **הערה:** בהרצאה זה נאמר בקיצור ("בעזרת טיעון על מספר קונפיגורציות"); הפירוט כאן. במיוחד, המעבר $\lg s\le s$ ו-$\lg|Q|\le s\lg|Q|$ הוא בדיוק המקום שבו הקבוע c מקבל את הצורה $\lg|Q|+\lg|\Gamma|+1$.

שני ההסברים שנוספו בסיכום לצד המשפט (עמוד 1):

① **למה צריך את ההנחה "M עוצרת".** בלעדיה הטענה **שקרית לחלוטין**, ולא רק כי הקבוע לא מספיק: הזמן **אינו חסום על ידי שום פונקציה של המקום**. הדוגמה שניתנה בשיעור ([00:00:35]): מכונה שרצה לנצח על שני תאים בלבד. המקום הוא 2, אבל אין שום פונקציה g שתקיים $\mathrm{time}\le g(2)$, כי הזמן אינסופי. שימו לב שהכיוון ההפוך (חלק א') נכון תמיד, ללא שום הנחה.

② **סדר הכמתים ב-c.** הקבוע c תלוי **אך ורק במכונה** ($|Q|$ ו-$|\Gamma|$ שלה) ואינו תלוי בקלט x — ולכן ניתן "להוציא אותו החוצה" לפני ה-$\forall x$. זו נקודה שתחזור לרדוף אותנו בשיעור 3: כשהמכונה עצמה היא הקלט לבעיה, "קבוע התלוי במכונה" הופך פתאום לקבוע התלוי בקלט, והמשפט הזה כבר לא מספיק ([01:03:25] בהקלטה השנייה).

הערת דיוק חשובה ([00:01:08]): החסם $2^{c\cdot s}$ **אינו הדוק**. השטחנו כאן שלושה מחוברים שונים לאותה צורה. בהמשך הקורס נצטרך לחזור לחישוב מספר הקונפיגורציות ולחסום אותו אחרת — למשל כשה-space גדול מאוד, או כשרוצים חסם שאינו תלוי במכונה כלל.

משפט 2: $\mathrm{DTime}(f) \subseteq \mathrm{DSpace}(f)$
לכל $f : \mathbb{N} \to \mathbb{N}$ מתקיים $\mathrm{DTime}(f) \subseteq \mathrm{DSpace}(f)$.
הוכחה. תהא $f : \mathbb{N} \to \mathbb{N}$. תהא $A \in \mathrm{DTime}(f)$.
מהגדרת $\mathrm{DTime}(f)$: קיימת מכונה M וקיים $c > 0$ כך ש-M מכריעה את A, וגם לכל x מתקיים $\mathrm{time}_M(x) \leq c \cdot f(|x|)$.
נוכיח ש-$A \in \mathrm{DSpace}(f)$, כלומר: נראה שקיימת מכונה M' וקיים $c' > 0$ כך ש-M' מכריעה את A וגם לכל x מתקיים $\mathrm{space}_{M'}(x) \leq c' \cdot f(|x|)$.
נתבונן ב-M (אותה מכונה — אין צורך בבנייה חדשה).
נתבונן ב-c; אכן $c > 0$.
אכן M מכריעה את A (זה בדיוק מה שנתון).
יהי x. לפי משפט 1 חלק א', $\mathrm{space}_M(x) \leq \mathrm{time}_M(x) \leq c \cdot f(|x|)$.
לכן $A \in \mathrm{DSpace}(f)$, ומכיוון ש-A נבחרה שרירותית, $\mathrm{DTime}(f) \subseteq \mathrm{DSpace}(f)$. $\square$
למה ההוכחה נראית "חזרתית" ובכל זאת כתובה כך. המרצה עמד על כך שגם כשההוכחה טריוויאלית, כותבים את **כל** חלקי ההגדרה — כולל "אכן $c > 0$" ו"אכן M מכריעה את A" ([00:11:32], [01:01:32]). הסיבה אינה פדנטיות: המקום שבו כתבנו "M מכריעה את A" כנתון והמקום שבו אנחנו נדרשים לזה כמסקנה הם שני מקומות שונים בהוכחה. בהוכחות הכבדות של הקורס (משפטי ההיררכיה, קוק–לוין) המבנה הזה הוא מה שמונע אובדן פרמטרים.
משפט 3: $\mathrm{DSpace}(f) \subseteq \bigcup_{d \geq 1} \mathrm{DTime}\left(2^{d \cdot f}\right)$
לכל $f : \mathbb{N} \to \mathbb{N}$ מתקיים $\mathrm{DSpace}(f) \subseteq \bigcup_{d \geq 1} \mathrm{DTime}\left(2^{d \cdot f}\right)$.
הכוונה ב-$2^{d \cdot f}$ היא לפונקציה $n \mapsto 2^{d \cdot f(n)}$.
מה בדיוק צריך להוכיח. צריך להראות ש-A שייכת **לאיחוד**, כלומר: **מספיק להראות שקיים** $d \geq 1$ שעבורו $A \in \mathrm{DTime}(2^{d \cdot f})$. זהו הפרמטר הנוסף שנכנס להוכחה, ולכן צריך להיות כאן זהירים יותר מבמשפט 2.
הוכחה. תהא $f : \mathbb{N} \to \mathbb{N}$. תהא $A \in \mathrm{DSpace}(f)$.
מהגדרת $\mathrm{DSpace}(f)$: קיימת מכונה M וקיים $c > 0$ כך ש-M מכריעה את A, וגם לכל x: $\mathrm{space}_M(x) \leq c \cdot f(|x|)$.
מדוע פרסנו כאן את ההגדרה? כי היא **מבטיחה קיום** — היא נותנת לנו ליד את M ואת c, ומהם (ורק מהם) נבנה את הפרמטרים החדשים ([00:23:49]).
נסמן ב-Q, Γ את קבוצת המצבים ואלפבית הסרט של M, ונגדיר: $d = \max\left\{1,\ \left(\lg|Q| + \lg|\Gamma| + 1\right) \cdot c\right\}, \qquad \hat{c} = 1.$
אכן $d \geq 1$ כנדרש. נתבונן ב-M (אותה מכונה) וב-$\hat{c} = 1 > 0$. אכן M מכריעה את A.
יהי x. מכיוון ש-M מכריעה את A, בפרט M **עוצרת** על x — וזה בדיוק התנאי הדרוש כדי להפעיל את משפט 1 חלק ב'. לכן: $\mathrm{time}_M(x) \leq 2^{(\lg|Q| + \lg|\Gamma| + 1) \cdot \mathrm{space}_M(x)} \leq 2^{(\lg|Q| + \lg|\Gamma| + 1) \cdot c \cdot f(|x|)} = 2^{d \cdot f(|x|)} = \hat{c} \cdot 2^{d \cdot f(|x|)}$.
האי-שוויון האמצעי מותר כי הפונקציה $t \mapsto 2^{\alpha t}$ עולה ב-t עבור $\alpha > 0$, והצבנו את החסם $\mathrm{space}_M(x) \leq c \cdot f(|x|)$. האי-שוויון האחרון נובע מכך ש-$d \geq (\lg|Q| + \lg|\Gamma| + 1) \cdot c$.

לכן $A \in \mathrm{DTime}(2^{d\cdot f})$, ומכאן $A \in \bigcup_{d\geq 1}\mathrm{DTime}(2^{d\cdot f})$. $\square$

חשבון הפרמטרים — למה $\hat{c}=1$ ולמה d הוא זה. אחרי הצבת החסם על space, האגף הימני הוא **בדיוק** מהצורה $2^{e\cdot f(|x|)}$ עבור מעריך e כלשהו, בלי שום מקדם כפלי לפניו. הקבוע $\hat{c}$ הוא, לפי ההגדרה, המקדם שכופל את $2^{d\cdot f(|x|)}$ — ומכיוון שאין שם מקדם, $\hat{c}=1$ ([00:32:05]). ו-d הוא כל מה שמוכפל ב-f **בתוך** המעריך ([00:33:09]).

בדיקת שפיות (sanity check) שהמרצה הדגיש ([00:33:39]): ברגע שקובעים d, כל מה שנכנס לביטוי — $|Q|$, $|\Gamma|$, c — כבר "ביד" מהשלב הקודם. אילו היינו נדרשים ל-x או לגודל שתלוי בקלט, ההוכחה הייתה נופלת, כי d נבחר **לפני** ה-$\forall x$.

> **הערה:** הסיכום כותב $d=(\lg|Q|+\lg|\Gamma|+1)\cdot c$ ללא ה-$\max$. זה כמעט תמיד תקין, אבל אינו מובטח: הדרישה באיחוד היא $d\geq 1$, בעוד ההגדרה של DSpace מבטיחה רק $c>0$ — ואם למשל $c=0.1$ ו-$|Q|=|\Gamma|=2$ נקבל $d=0.3<1$. בשיעור עצמו סטודנט העלה בדיוק את הקושי הזה, והמרצה אישר שמותר "לתפור" את הקבוע כרצוננו ([00:24:21]–[00:24:53]). לקיחת $\max\{1,\cdot\}$ פותרת זאת ואינה פוגעת בחסם, כי הגדלת d רק מגדילה את $2^{d\cdot f}$.

משפט 4: מונוטוניות ביחס לסדר גודל

תהיינה $f,g:\mathbb{N}\to\mathbb{N}$ ונניח $f=O(g)$. אז $\mathrm{DTime}(f)\subseteq\mathrm{DTime}(g)$

וגם

$$\mathrm{DSpace}(f)\subseteq\mathrm{DSpace}(g).$$

הוכחה (עבור DTime; המקרה של DSpace זהה מילה במילה עם החלפת time ב-space). תהיינה f,g ונניח $f=O(g)$. לפי הגדרה 3, **קיים** $c>0$ כך שלכל $n\in\mathbb{N}$: $f(n)\leq c\cdot g(n)$. שוב, פרסנו את ההגדרה כי היא מבטיחה קיום של קבוע שנצטרך.

תהא $A\in\mathrm{DTime}(f)$. אז קיימת מכונה M וקיים $\hat{c}>0$ כך ש-M מכריעה את A וגם לכל x: $\mathrm{time}_M(x)\leq\hat{c}\cdot f(|x|)$.

נתבונן ב-M (אין מאיפה להביא מכונה אחרת) ונגדיר $\check{c}=\hat{c}\cdot c$.

אכן $\check{c}>0$ כמכפלת שני מספרים חיוביים, ואכן M מכריעה את A. יהי x; אז $\mathrm{time}_M(x)\leq\hat{c}\cdot f(|x|)\leq\hat{c}\cdot c\cdot g(|x|)=\check{c}\cdot g(|x|)$.

לכן $A\in\mathrm{DTime}(g)$, ומכאן $\mathrm{DTime}(f)\subseteq\mathrm{DTime}(g)$. $\square$

שאלה טובה שנשאלה ([00:10:01] בהקלטה השנייה): "האם $\check{c}=\hat{c}\cdot c$ באמת חיובי? אם שניהם קטנים מ-1, המכפלה קטנה משניהם." התשובה: המכפלה אכן עשויה להיות קטנה משני הגורמים, אבל זה **לא** משנה — ההגדרה דורשת רק $\check{c}>0$, לא $\check{c}\geq 1$ ולא $\check{c}\geq\max$. ומעבר לכך, שרשרת האי-שוויונות למעלה מוכיחה את החסם ישירות, ללא כל הנחה על גודל הקבועים.

למה המשפט הזה חשוב. בלעדיו הכתיב $\mathrm{DTime}(n^2)$ היה שרירותי: הוא מבטיח שהמחלקות "מכבדות" סדרי גודל, ולכן הבחירה בין $f(n)=n^2$ ל-$f(n)=3n^2+5$ אינה משנה את המחלקה. הוא גם הכלי המרכזי בהוכחת $\mathrm{PSPACE}\subseteq\mathrm{EXP}$ (משפט 6).

משפט 5: $P\subseteq\mathrm{PSPACE}$

הוכחה א' (הוכחה "ארוכה", כפי שנעשתה בשיעור). תהא $A\in P$.

מהגדרת P כאיחוד: קיים $c \geq 1$ כך ש-$A \in \mathrm{DTime}(n^c)$. (אי אפשר לקפוץ ישר למכונה — P אינה מוגדרת על ידי מכונות אלא כאיחוד, ולכן קודם מקלפים את ה-"קיים c", [01:09:40].)
מהגדרת $\mathrm{DTime}(n^c)$: קיימת מכונה M וקיים $d > 0$ כך ש-M מכריעה את A וגם לכל x:
$$\mathrm{time}_M(x) \leq d \cdot |x|^c.$$
שימו לב להצבה: הפונקציה כאן היא $n \mapsto n^c$, והמשתנה שאנחנו עובדים איתו הוא $|x|$ — ולכן $d \cdot |x|^c$ ולא "$d \cdot n^c$" ([01:11:26]).
כדי להוכיח $A \in \mathrm{PSPACE}$ צריך להראות שקיים $\alpha \geq 1$ עם $A \in \mathrm{DSpace}(n^\alpha)$. **נתבונן ב-$c$** $\alpha = c$ (הפרמטר היחיד שיש לנו ביד), ואז צריך להראות $A \in \mathrm{DSpace}(n^c)$:
נתבונן ב-M ו**ב-d**; אכן $d > 0$ ואכן M מכריעה את A.
יהי x. לפי משפט 1 חלק א': $\mathrm{space}_M(x) \leq \mathrm{time}_M(x) \leq d \cdot |x|^c$.
לכן $A \in \mathrm{DSpace}(n^c)$, ולכן $A \in \mathrm{PSPACE}$. $\square$
הוכחה ב' (הפתרון האלטרנטיבי, עמוד 4 בסיכום). תהא $A \in P$. אז קיים $c \geq 1$ כך ש-$A \in \mathrm{DTime}(n^c)$. לפי **משפט 2** (עם $f(n) = n^c$), $\mathrm{DTime}(n^c) \subseteq \mathrm{DSpace}(n^c)$, ולכן $A \in \mathrm{DSpace}(n^c)$ ומכאן $A \in \mathrm{PSPACE}$. $\square$

> **הערה:** שתי ההוכחות תקפות לחלוטין, והשנייה קצרה בהרבה. המרצה הסביר במפורש ([01:16:21], [01:17:26]) שהוא פתח דווקא בארוכה מטעם **דידקטי**: היכולת לפרק הגדרה, להוציא את כל הפרמטרים, להשתמש בהם ולהרכיב אותם בחזרה היא המיומנות שכל ההוכחות הכבדות בקורס עומדות עליה. בבחינה — שתיהן מתקבלות.

משפט 6: $\mathrm{PSPACE} \subseteq \mathrm{EXP}$
(מופיע בהקלטה השנייה בלבד, [00:17:29]–[00:33:08]; אינו בסיכום.)
אינטואיציה. אם היחס בין מקום לזמן הוא אקספוננציאלי (משפט 1 חלק ב'), אז מי שנפתר במקום פולינומי חייב להיפתר בזמן אקספוננציאלי. אבל בין האינטואיציה הזו לבין ההגדרה הפורמלית של EXP יש פער טכני אמיתי, וכל עניינה של ההוכחה הוא לגשר עליו.
הוכחה. תהא $A \in \mathrm{PSPACE}$. אז קיים $c \geq 1$ כך ש-$A \in \mathrm{DSpace}(n^c)$, ולכן קיימת מכונה M וקיים $c' > 0$ כך ש-M מכריעה את A וגם לכל x: $\mathrm{space}_M(x) \leq c' \cdot |x|^c$.
M מכריעה את A, ולכן עוצרת על כל קלט. לפי משפט 1 חלק ב' קיים $c'' > 0$ (התלוי רק ב-M) כך שלכל x: $\mathrm{time}_M(x) \leq 2^{c'' \cdot \mathrm{space}_M(x)} \leq 2^{c'' \cdot c' \cdot |x|^c}$.
עד כאן קיבלנו $A \in \mathrm{DTime}\left(2^{c''c' \cdot n^c}\right)$ — וזו **עדיין לא** הגדרת EXP, שדורשת מחלקה מהצורה $\mathrm{DTime}(2^{n^k})$ בדיוק, בלי קבועים בתוך המעריך.
נסמן $g(n) = 2^{c''c' \cdot n^c}$, $\quad h(n) = 2^{n^{c+1}}$.
נטען ש-$g = O(h)$. אכן, לכל $n \geq n_0 := c''c'$ מתקיים $c''c' \cdot n^c \leq n \cdot n^c = n^{c+1}$, ומכיוון ש-$2^t$ עולה ב-t נקבל $g(n) \leq h(n)$ לכל $n \geq n_0$. לפי הגדרת O (ובעזרת השקילות מהגדרה 3, שמאפשרת לוותר על n_0 במחיר קבוע), $g = O(h)$.
לפי **משפט 4**, $\mathrm{DTime}(g) \subseteq \mathrm{DTime}(h)$, ולכן $\square$ $\quad A \in \mathrm{DTime}\left(2^{n^{c+1}}\right) \subseteq \mathrm{EXP}.$

למה זו הדרך הנכונה. אפשר, לחלוטין, לרדוף אחרי הקבוע ולמצוא במפורש D ו-D' כך ש-$\mathrm{time}_M(x) \le D \cdot 2^{|x|^{D'}}$ לכל x — וזה אפילו לא קשה (ראו התרגיל בסעיף הבא). אבל זו עבודה טכנית מיותרת: מכיוון שבסופו של דבר אנחנו מסתכלים על **סדרי גודל**, נכון יותר לשאול מה קורה כשהקלט הולך וגדל, לזהות שמאורך מסוים כל הקבועים "נבלעים" בתוך n, ואז לקבל את המעבר מ-n_0 ל"לכל n" **בחינם** משקילות הגדרות ה-O ([00:28:19]–[00:34:41]).

דוגמאות ותרגילים מהשיעור

דוגמה 1: $PAL \in \mathrm{DTime}(n^2)$, מפורק עד הסוף

$PAL = \{x \in \{0,1\}^* \mid x = x^R\}$ — שפת הפלינדרומים מעל $\{0,1\}$.

האלגוריתם (על מכונה חד-סרטית סטנדרטית): כל עוד נשארו לפחות שני תווים — קרא את התו השמאלי ביותר שלא נמחק, מחק אותו, סע ימינה עד התו הימני ביותר שלא נמחק, השווה, ומחק גם אותו; חזור שמאלה. אם בכל השוואה היה שוויון — קבל; אם הייתה אי-התאמה — דחה.

חשבון הזמן. בסבב מספר i ($i = 1, 2, \ldots$) נותרו $n - 2(i-1)$ תווים, והמכונה עוברת את המרווח הזה הלוך ושוב — כלומר כ-$2\big(n-2(i-1)\big)$ צעדים. סכימה על כל הסבבים, $i = 1, \ldots, \lceil n/2 \rceil$.:

$$\mathrm{time}_M(x) \;\approx\; \sum_{i=1}^{\lceil n/2 \rceil} 2\big(n-2(i-1)\big) \;\le\; 2 \cdot \tfrac{n}{2} \cdot n \;=\; n^2.$$

אם ניקח $f(n) = n^2$ ו-$c = 2$ (כדי לבלוע בנדיבות את צעדי הבקרה), נקבל $\mathrm{time}_M(x) \le c \cdot f(|x|)$ לכל x, ולכן $PAL \in \mathrm{DTime}(f)$.

מופע קונקרטי — $x = 0110$ ($n = 4$): סבב 1 משווה את התו הראשון 0 לתו האחרון 0 — התאמה, שניהם נמחקים; נותר 11. סבב 2 משווה 1 ל-1 — התאמה. לא נותרו תווים $\Longrightarrow$ **קבל**. סה"כ $8 + 4 = 12 \le 2 \cdot 4^2$ צעדים.

אי-מופע — $x = 0100$: סבב 1 משווה 0 ל-0 — התאמה; נותר 10. סבב 2 משווה 1 ל-0 — אי-התאמה $\Longrightarrow$ **דחה**.

על הסימון. פורמלית היינו צריכים לכתוב: "תהא $f : \mathbb{N} \to \mathbb{N}$ המוגדרת על ידי $f(n) = n^2$ לכל $n \in \mathbb{N}$; אז $PAL \in \mathrm{DTime}(f)$." מקובל לקצר ולכתוב פשוט $PAL \in \mathrm{DTime}(n^2)$. שימו לב ש-$n^2$ הוא **מספר**, לא פונקציה — הכתיב הזה הוא קיצור שממנו מובן לאיזו פונקציה התכוונו ([00:45:24]).

אזהרה מהשיעור ([00:43:17]): אל תסיקו מכאן ש"פלינדרומים זה n" מתוך זיכרון של קורס אחר. החסם הריבועי נובע מכך שהמודל הוא **חד-סרטי**. במודל אחר (למשל שני סרטים) המספר משתנה.

תרגיל 1 (נשאל בכיתה, [00:15:49])

אם מספר הצעדים שהמכונה מבצעת נשאר בדיוק אותו דבר, אבל הקלט נעשה ארוך יותר — האם הסיבוכיות גדלה או קטנה?

פתרון. קטנה. סיבוכיות נמדדת **ביחס לאורך הקלט**: אם $\mathrm{time}_M(x)$ קבוע ו-$|x|$ גדל, אז היחס $\mathrm{time}_M(x)/f(|x|)$ קטן, והחסם $c \cdot f(|x|)$ הופך נדיב יותר. האינטואיציה שהוצעה בשיעור: חִשבו על זמן ומקום כעל **מחיר** ועל הקלט כעל **מה שקיבלתם תמורתו** — שילמתם אותו מחיר וקיבלתם קלט גדול יותר, כלומר עשיתם עסקה טובה יותר.

תרגיל 2 (עלה כשאלה, [00:14:08])

למה כתוב $f(|x|)$ ולא $f(x)$?

פתרון. f מוגדרת מ-$\mathbb{N}$ ל-$\mathbb{N}$, ו-x הוא **מחרוזת** מעל אלפבית כלשהו. $f(x)$ הוא ביטוי חסר משמעות — אין ל-f הגדרה על מחרוזות. $|x|$ הוא אורך המחרוזת, שהוא מספר טבעי, ולכן $f(|x|)$ מוגדר היטב. הערכים המוחלטים כאן אינם קידוד ואינם ייצוג — הם פשוט אורך.

תרגיל 3: מציאת הקבוע במפורש ב-$\mathrm{PSPACE} \subseteq \mathrm{EXP}$

במשפט 6 עקפנו את חיפוש הקבוע. מצאו אותו במפורש.

פתרון. נסמן $n_0 = c''c'$. הראינו שלכל x עם $|x| \geq n_0$ מתקיים $\mathrm{time}_M(x) \leq 2^{|x|^{c+1}}$. נותרו קלטים באורך $< n_0$ — ויש **מספר סופי** של קלטים כאלה (האלפבית סופי). M מכריעה את A, ולכן עוצרת על כל אחד מהם; נסמן ב-T את המקסימום של $\mathrm{time}_M(x)$ על פני קבוצה סופית זו. ניקח $D = \max\{1,\ T\}$. אז לכל x: אם $|x| \geq n_0$ אז $\mathrm{time}_M(x) \leq 2^{|x|^{c+1}} \leq D \cdot 2^{|x|^{c+1}}$, ואם $|x| < n_0$ אז $\mathrm{time}_M(x) \leq T \leq D \leq D \cdot 2^{|x|^{c+1}}$. לכן $A \in \mathrm{DTime}(2^{n^{c+1}})$. זהו בדיוק המנגנון שמאחורי השקילות בהגדרה 3 — "בליעת" מספר סופי של קלטים חריגים בתוך הקבוע.

תרגיל 4: קריאת הקיצור $\mathrm{DTime}(2^{O(f)})$

מה הולך לאיבוד בכתיב המקוצר?

פתרון. לפעמים מקצרים $\mathrm{DTime}(2^{d \cdot f})$ ל-$\bigcup_{d \geq 1} \mathrm{DTime}(2^{d \cdot f}) = \mathrm{DTime}(2^{O(f)})$. מה שנעלם הוא **הפרמטר d והכמת שמעליו**. שייכות לאיחוד היא טענת **קיום**, ובלי הפרמטר אין במה "לתפוס" את ההוכחה. הקיצור לגיטימי ואתם חייבים לדעת לקרוא אותו, אבל כשאתם באים להוכיח שייכות — פתחו אותו חזרה ל-"קיים $d \geq 1$ כך ש..." ([00:47:29]–[00:49:02]).

תרגיל 5: $\mathrm{DTime}(n) \subseteq \mathrm{DTime}(n^2)$

פתרון. $f(n) = n$, $g(n) = n^2$. מתקיים $f(n) = n \leq 1 \cdot n^2 = g(n)$ לכל $n \in \mathbb{N}$, ולכן $f = O(g)$ עם $c = 1$ (בגרסה ללא n_0). לפי משפט 4, $\mathrm{DTime}(n) \subseteq \mathrm{DTime}(n^2)$. שימו לב שהמשפט אינו אומר דבר על **הכלה ממש** — השאלה אם ההכלה חזקה היא בדיוק נושא שיעור 3 (משפטי ההיררכיה).

הערות מהשיעור

[00:01:08] החסם על מספר הקונפיגורציות אינו הדוק, וזה יחזור. "לפעמים אנחנו נרצה לחזור לכאן — עם ה-space מאוד גדול, יכול להיות שזה משמעותי." ואכן, בשיעור 3 חוזרים בדיוק לחישוב הזה וחוסמים אותו אחרת כדי לקבל קבוע שאינו תלוי במכונה.

[00:01:40] סדר הכמתים. "תשימו לב לסדר הכמתים, זה מאוד מאוד חשוב." זו האזהרה החוזרת ביותר בשיעור, והיא הנקודה שקורסת בשיעור 3 כשהמכונה עצמה היא הקלט.

[00:04:28] אינטואיציה מול פורמליזם. "בהגדרה האינטואיטיבית הייתי משתמש כשאני רוצה *לחשוב* על המחלקות, אבל לא כשאני צריך לשבת ולהוכיח משהו עליהן." כשמוכיחים — יורדים לפורמליזם, כי רק הוא נותן ליד את המכונה ואת הקבועים.

[00:06:01] שאלת סטודנט: אוטומטים או מכונות טיורינג? מכונות טיורינג. לאוטומט הזמן ידוע מראש והוא ליניארי, ולכן אין בו עניין סיבוכיותי.

[00:08:17] "אני לא מניח שיש איבר — אני לוקח איבר." תיקון ניסוח שהמרצה עמד עליו: בהוכחת הכלה $\forall A \in X \ :\ A \in Y$ אין הנחת קיום; לוקחים איבר שרירותי. הבלבול הזה הוא מקור נפוץ לשגיאות.

[00:09:58] אל תתחילו מהסוף של ההגדרה. טעות נפוצה: מרגישים שכבר "כתבנו את ההתחלה" של ההגדרה בצד הנתון, ולכן קופצים ישר לאי-שוויון בצד שצריך להוכיח. בצד הנתון פרסנו את מה שנובע; בצד שצריך להוכיח צריך להוכיח את **הכול** מחדש.
[00:17:26] מחלקה היא קבוצה שאיבריה שפות. A אינה מכונת טיורינג.
[00:23:49] מתי מצטטים הגדרה? "כשהיא מבטיחה לי קיום של משהו." אם ההגדרה מספקת מכונה או קבוע שאזדקק להם — פורסים אותה. אחרת, בדרך כלל לא.
[00:33:39] בדיקת שפיות. כשקובעים קבוע חדש, ודאו שהוא מורכב **רק** מדברים שכבר יש ביד באותו שלב בהוכחה. שימוש במשתנה שעדיין לא הוצג הוא כמעט תמיד סימן לשגיאה מהותית.
[00:41:06] מדוע "מחלקות עדינות". כי כל פונקציה f מייצרת מחלקה משלה — התאמה חד-חד-ערכית בין פונקציות למחלקות.
[00:49:33] על קיצורים. "כל זמן שזה תלוי בי אני לא אקצר — אבל אתם כן צריכים לדעת לקרוא את זה. מישהו אחר יקצר לכם."
[01:00:30] עבדו בטיוטה. הקבועים ($\check{c}$, $\hat{c}$, d) נמצאים בטיוטה, ולהוכחה מגיעים כשכבר יודעים מה הם. אל תנסו לכתוב הוכחה כזו ב-one pass.
[01:19:36] מה הלאה. "שיעור הבא נגיע למשפט ההיררכיה, ואז תראו מה זו הוכחה מורכבת. קחו אוויר."
[01:20:38] על שינון. ההמלצה: לא לשנן הגדרות. לכתוב את ההגדרה על פתק, לתלות אותה מול העיניים, ולפתור מספיק תרגילים עד שהיא נכנסת דרך שימוש. עד כשלושה ימים לפני המבחן — לעבוד עם החומר פתוח.
[00:14:47] בהקלטה השנייה: P כ"קל" ומחוץ ל-P כ"קשה". מקובל לזהות את P עם הבעיות הפתירות ביעילות. כל מה שנפגשתם בו בקורסי אלגוריתמים היה בתוך P.
[00:15:53] בהקלטה השנייה: הפער בתוך P עצמה. יש תהום בין $\mathrm{DTime}(n)$ ל-$\mathrm{DTime}(n^{100})$ — האחרון אינו ישים בפועל, ועדיין הוא ב-P. ההצדקה האמפירית לזיהוי P ="יעיל": כשמצליחים לפתור בעיה בזמן פולינומי כלשהו, בדרך כלל מוצאים אחר כך גם פולינום קטן.
[00:16:57] בהקלטה השנייה: גם קושי הוא מוצר. שיטת ההצפנה RSA נשענת על ההשערה שפירוק לגורמים ראשוניים **אינו** ניתן לפתרון בזמן פולינומי. לא יודעים להוכיח זאת, אך מסתמכים על כך.

פערים בין הסיכום להקלטה

מקור: עמוד 1 בסיכום. **הפער:** הסיכום נפתח באמצע ניסוח המשפט על הקשר בין זמן למקום ואינו כולל את הוכחתו (היא נעשתה בשיעור 1); ההקלטה מזכירה אותה בשלוש שורות בלבד. **ההכרעה:** שחזרתי את הספירה המלאה של הקונפיגורציות כמשפט 1, כולל הצדקת כל אחד משלושת המעברים שמייצרים את $c = \lg|Q| + \lg|\Gamma| + 1$, בהסתמך על החישוב שנעשה במפורש בהקלטה השנייה ב-[01:13:37]–[01:15:14].

מקור: עמוד 2 בסיכום, הוכחת משפט 3. **הפער:** הסיכום קובע $d = (\lg|Q| + \lg|\Gamma| + 1) \cdot c$, אך האיחוד הוא על $d \geq 1$ בעוד ההגדרה מבטיחה רק $c > 0$ — ולכן ייתכן $d < 1$ (למשל $c = 0.1$, $|Q| = |\Gamma| = 2$). **ההכרעה:** תיקנתי בגוף ל-$d = \max\{1, (\lg|Q| + \lg|\Gamma| + 1) \cdot c\}$. התיקון

אינו פוגע בחסם כי $2^{d \cdot f}$ מונוטונית עולה ב-d. הקושי הזה הועלה בפועל על ידי סטודנט בהקלטה ב-[00:24:21] והמרצה אישר את עקרון "התפירה" של הקבוע.

מקור: ההקלטה השנייה, [00:17:29]–[00:33:08]. **הפער:** המשפט $\mathrm{PSPACE} \subseteq \mathrm{EXP}$ נלמד ולא מופיע בסיכום כלל. **ההכרעה:** הוספתי אותו כמשפט 6, כולל שתי הדרכים (חיפוש הקבוע מול הטיעון האסימפטוטי), כי הוא ההשלמה הטבעית ל-$P \subseteq \mathrm{PSPACE}$ ומדגים את השימוש במשפט 4.

מקור: עמוד 3 בסיכום, ההערה האדומה על הגדרת O. **הפער:** כיוון אי-השוויון בכתב היד ניתן לקריאה כ-$\geq$. **ההכרעה:** ההגדרה הנכונה של $f = O(g)$ היא $f(n) \leq c \cdot g(n)$, וכך גם נאמר במפורש בשתי ההקלטות ([00:52:32] ו-[00:04:10] בהקלטה השנייה). כתבתי $\leq$.

מקור: עמוד 2 בסיכום, שורת ה-PAL. **הפער:** נראה שכתוב "$PAL = \mathrm{DTime}(f)$" במקום "$PAL \in \mathrm{DTime}(f)$". **ההכרעה:** מדובר בשפה בודדת מול מחלקה של שפות, ולכן היחס הוא שייכות; כתבתי $\in$. ההקלטה ([00:44:23]) אומרת "פל ב-DTime f", כלומר שייכות.

מקור: עמוד 3 בסיכום. **הפער:** המחלקה נכתבת "EX". **ההכרעה:** הכוונה ל-EXP (בהקלטה: "אקספ"); כתבתי EXP. באותו אופן, הסיכום כותב $EXSPACE$ ואני כתבתי $\mathrm{EXPSPACE}$ — אותו אובייקט.

מקור: שני המקורות. **הפער:** נושא **חוסן המודל** (מדוע בחירת מודל המכונה אינה משנה את P) אינו נדון בשיעור הזה כלל. ההתייחסות היחידה למודל היא ההסכמה שב-[00:43:50] ש"מכונה" פירושה חד-סרטית סטנדרטית, ואזהרה שחסמים קונקרטיים כמו n^2 עבור PAL **כן** תלויים במודל.

ההכרעה: לא הוספתי דיון בחוסן המודל כדי לא להמציא חומר; ציינתי את הסכמת המודל ואת תלות החסם בו.

מקור: ההקלטה השנייה (video_id ilc7hKBsa1Q). **הפער:** מדקה 36 ואילך ההקלטה עוברת למשפט היררכיית המקום — הגדרת "ישימה במקום", השפה S_f, טענת העזר על $2^{3f(\langle M \rangle)}$ צעדים — שהוא כולו חומר של שיעור 3. **ההכרעה:** סימנתי `coverage: partial` והשארתי את החומר הזה מחוץ לקובץ.

מקור: עמוד 1 בסיכום. **הפער:** הקיצור שליד "לכל מכונה M" אינו קריא בבירור. **ההכרעה:** מההקשר ומההקלטה ([00:01:40] "לכל מכונה") ברור שהכוונה למכונת טיורינג דטרמיניסטית; כתבתי כך.

סיכום ונקודות למבחן

מה חייבים לדעת בעל פה (או, לפי המלצת המרצה, מתוך שימוש חוזר):

$A \in \mathrm{DTime}(f) \iff \exists M\ \exists c > 0:$ M מכריעה את A **וגם** $\forall x:\ \mathrm{time}_M(x) \leq c \cdot f(|x|)$. אותו הדבר ל-DSpace.

$\mathrm{space}_M(x) \leq \mathrm{time}_M(x)$ — **תמיד**, ללא הנחות.

אם M עוצרת על x: $\mathrm{time}_M(x) \leq 2^{c \cdot \mathrm{space}_M(x)}$ עם $c = \lg|Q| + \lg|\Gamma| + 1$ התלוי **רק במכונה**.

$\mathrm{DTime}(f) \subseteq \mathrm{DSpace}(f);\ \mathrm{DSpace}(f) \subseteq \bigcup_{d \geq 1} \mathrm{DTime}(2^{d \cdot f})$.

$f = O(g) \ \Rightarrow\ \mathrm{DTime}(f) \subseteq \mathrm{DTime}(g)$ ו-$\mathrm{DSpace}(f) \subseteq \mathrm{DSpace}(g)$.

$P \subseteq \mathrm{PSPACE} \subseteq \mathrm{EXP}$.

המלכודות הסטנדרטיות:

שכחת הנחת העצירה. כל שימוש בחסם $2^{c\cdot \text{space}}$ מחייב הצדקה מפורשת ש-M עוצרת על הקלט הנדון. בהוכחות שלנו זה תמיד מגיע מ"M מכריעה את A, ולכן עוצרת על כל קלט". בלי ההנחה הזו הטענה **שקרית** — הזמן אינו חסום על ידי שום פונקציה של המקום.
קפיצה מעל האיחוד. כשמוכיחים שייכות ל-$\mathrm{EXP}/\mathrm{PSPACE}/P$ — קודם "קיים $c \geq 1$", ורק אחר כך "קיימת מכונה". אי אפשר לגשת ישר למכונה, כי המחלקה הגסה אינה מוגדרת דרך מכונות.
בלבול $f(x)$ עם $f(|x|)$.
קבוע שנבנה ממשתנה שעדיין לא קיים. כל קבוע חדש חייב להיות מורכב מפרמטרים שכבר "הוצאו" מהגדרות קודמות, ולהיקבע **לפני** ה-$\forall x$.
התעלמות מ-$c \geq 1$ ו-$d \geq 1$ בהגדרות האיחודים. כשהקבוע שהתקבל קטן מ-1 — קחו $\max$.
הנחה ש"פלינדרומים זה ליניארי". לא במודל החד-סרטי.
צ'קליסט — אחרי השיעור הזה אתם אמורים לדעת:
לכתוב מזיכרון את הגדרות $\mathrm{DTime}(f)$ ו-$\mathrm{DSpace}(f)$ עם סדר הכמתים הנכון.
להוכיח שייכות של שפה נתונה למחלקה עדינה על ידי הצגת מכונה, קבוע, וחסם — בכל חמשת חלקי ההגדרה.
להוכיח הכלה בין שתי מחלקות עדינות/גסות במבנה המלא: לקחת איבר, לפרוס את ההגדרה הנתונה, להגדיר את הפרמטרים החדשים מתוך הישנים, ולהרכיב את ההגדרה שצריך להוכיח.
לחשב את מספר הקונפיגורציות של מכונה בריצה שהמקום שלה חסום, ולהסיק ממנו חסם זמן.
לזהות מתי כדאי לרדוף אחרי קבוע מפורש ומתי עדיף לעבור לטיעון אסימפטוטי דרך משפט 4.
לקרוא נכון קיצורים כמו $\mathrm{DTime}(2^{O(f)})$ ו-$\mathrm{DTime}(n^2)$, ולפתוח אותם חזרה לניסוח הפורמלי בעת הצורך.
הסיכום הכתוב הוא של גיא סופר.

שאלות שנשארו פתוחות

עמוד 3 בסיכום: כיוון אי-השוויון בהגדרת O נקרא בכתב היד כ-≲; שתי ההקלטות אומרות ≳, וכך נכתב.

עמוד 1 בסיכום: הקיצור שאחרי 'לכל מכונה M' אינו קריא במלואו; פוענח לפי ההקשר כמכונת טיורינג דטרמיניסטית.

עמידות המודל (model robustness) אינה מכוסה באף אחד מהמקורות ולכן אינה נכתבת כאן; ההערה היחידה בנושא היא מוסכמת הסרט היחיד ב-[00:43:50].

3 משפטי היררכיה במקום ובזמן

יותר משאב נותן ממש יותר כוח: הוכחת משפט ההיררכיה במקום בלכסון על מכונה אוניברסלית עם שני מונים, ניסוח משפט ההיררכיה בזמן, והמסקנה שהמחלקה P מוכלת ממש ב-EXP.

ביטחון: high

בקצרה

זהו השיעור הראשון בקורס שבו מוכיחים **תוצאה שלילית** ברמת הסיבוכיות: לא רק ש"אפשר לעשות משהו בתקציב נתון", אלא ש**אי אפשר** לעשות משהו בתקציב נתון. תוצאות כאלה קשות בהרבה מתוצאות חיוביות ולכן יש מעט מהן.

משפט ההיררכיה במקום: אם $g = o(f)$, אם f ישימה במקום (space-constructible) ואם f סופר־לינארית, אז $\mathrm{DSpace}(g) \subsetneq \mathrm{DSpace}(f)$. כלומר תוספת משמעותית של מקום נותנת ממש יותר כוח חישובי.

משפט ההיררכיה בזמן: באותם תנאים, אבל עם f ישימה בזמן (time-constructible), מקבלים רק $\mathrm{DTime}(g) \subsetneq \mathrm{DTime}(f^2)$. הריבוע הזה אינו קישוט — הוא נובע נקודתית מהמעבר ממכונה רב־סרטית למכונה סטנדרטית, שבמקום עולה קבוע כפלי ובזמן עולה ריבוע.

ההוכחה היא **לכסון** בסגנון חישוביות (השפה של המכונות שדוחות את הקידוד של עצמן), אבל עם רכיב סיבוכיותי שמפצל את עולם המכונות: מי שמשתמשת במעט מקום נופלת במלכודת הלכסון, ומי שמשתמשת בהרבה מקום בורחת ממנה.

שני התנאים הטכניים אינם קישוט: **הישימות** דרושה כדי שהמכונה שבונים תוכל בכלל *לכתוב* את המונים בתוך התקציב, ו**הסופר־לינאריות** דרושה כדי לבלוע את $|\langle M \rangle|$ ואת $\lg f$ בתוך f בחשבון הזמן והמקום.

מסקנה מרכזית: $\mathrm{P} \subsetneq \mathrm{EXP}$. ומכיוון ש-$\mathrm{P} \subseteq \mathrm{PSPACE} \subseteq \mathrm{EXP}$, לפחות אחת משתי ההכלות האלה היא הכלה ממש — **ואף אחד לא יודע איזו**. שתי השאלות פתוחות זה עשרות שנים.

מלכודת שחוזרת: הכלה נשמרת תחת איחוד, **הכלה ממש לא**. לכן אי אפשר להפעיל את משפט ההיררכיה ישירות על מחלקות גסות כמו P ו-EXP; חייבים לעבור דרך שתי מחלקות עדינות באמצע.

רקע ותלויות

השיעור הזה נשען כמעט על כל מה שנבנה עד כה, ולכן נחזור על התוצאות שנשתמש בהן ממש, בניסוח מלא.

מהשיעורים 1–2: המחלקות

$$\mathrm{P} = \bigcup_{c \geq 1} \mathrm{DTime}(n^c), \qquad \mathrm{PSPACE} = \bigcup_{c \geq 1} \mathrm{DSpace}(n^c), \qquad \mathrm{EXP} = \bigcup_{c \geq 1} \mathrm{DTime}\left(2^{n^c}\right).$$

$\mathrm{DTime}(f)$ ו-$\mathrm{DSpace}(f)$ הן מחלקות **עדינות** — לכל פונקציה יש מחלקה משלה. P, PSPACE ו-EXP הן מחלקות **גסות**: הן איחוד אינסופי, והן כבר לא מבחינות בין n^2 ל-n^{10}.
ההבחנה הזו תהיה קריטית בסוף השיעור (ראו שיעור 2).
מהשיעור 2: מונוטוניות במשאב

טענה. לכל $f, g : \mathbb{N} \to \mathbb{N}$: אם $g = O(f)$ אז $\mathrm{DTime}(g) \subseteq \mathrm{DTime}(f)$ וגם $\mathrm{DSpace}(g) \subseteq \mathrm{DSpace}(f)$.

האינטואיציה שהמרצה חזר עליה שוב ושוב: חשבו על המשאב כעל **תקציב**. אם הגדלתי את התקציב, כל מה שיכולתי לעשות קודם אני עדיין יכול לעשות. זו בדיוק המשמעות של הטענה — וזו הסיבה שזו "תוצאה חיובית".

הערה: בהקלטה השנייה המרצה ציין שבשיעור הקודם הטענה נוסחה רק עבור זמן; אותה הוכחה בדיוק עובדת גם למקום, כי אין בה שום דבר שמיוחד לזמן. אנו משתמשים כאן בשתי הגרסאות.

מהשיעור 2: מקום חוסם זמן

טענה. $\mathrm{DSpace}(f) \subseteq \bigcup_{d \geq 1} \mathrm{DTime}\left(2^{d \cdot f}\right)$.

ההוכחה שלה נשענה על ספירת קונפיגורציות, והשורה שנצטרך כאן היא לא התוצאה הסופית אלא **השורה שלפניה**: אם M עוצרת על קלט x אז

$$\mathrm{time}_M(x) \;\leq\; 2^{\lg|Q_M| \,+\, \lg|\Gamma_M| \cdot \mathrm{space}_M(x) \,+\, \lg \mathrm{space}_M(x)}.$$

הביטוי הזה הוא בדיוק מספר הקונפיגורציות האפשריות: $|Q_M|$ בחירות של מצב, $|\Gamma_M|^{\mathrm{space}_M(x)}$ תוכני סרט, ו-$\mathrm{space}_M(x)$ מיקומי ראש. אם המכונה עושה יותר צעדים מזה — קונפיגורציה חוזרת על עצמה והמכונה **לעולם לא תעצור**.
מהשיעור 1: המכונה האוניברסלית והמעבר בין מודלים
שני מדדים של המכונה האוניברסלית M_U על קלט $\langle M, x \rangle$ יופיעו כאן במפורש:

$$\mathrm{space}_{M_U}(\langle M, x \rangle) = O\left(|\langle M, x \rangle| + \lg|\Gamma_M| \cdot \mathrm{space}_M(x)\right), \qquad \mathrm{time}_{M_U}(\langle M, x \rangle) = O\left(|\langle M \rangle| \cdot \mathrm{time}_M(x)\right).$$

ההסבר לפקטור $\lg|\Gamma_M|$: האוניברסלית עובדת מעל קידוד בינרי, ולכן כל תא של M עולה לה $\lg|\Gamma_M|$ תאים. **שימו לב להבדל בין שני המדדים** — במקום משלמים $\lg|\Gamma_M|$, בזמן משלמים $|\langle M \rangle|$. כל ההבדל בין שני משפטי ההיררכיה יצמח מהנקודה הזאת.
וכן, ההמרה בין מודלים:

טענה. לכל מכונה רב־סרטית M קיימת מכונה סטנדרטית (חד־סרטית) $\hat{M}$ השקולה לה סמנטית, כך ש-$\mathrm{space}_{\hat{M}}(x) = O(\mathrm{space}_M(x))$ אבל $\mathrm{time}_{\hat{M}}(x) = O\left(\mathrm{time}_M(x)^2\right)$.

הגדרות

הגדרה 1: ישימות במקום (space-constructible)

תהי $f : \mathbb{N} \to \mathbb{N}$. נאמר ש-$f$ **ישימה במקום** אם קיימת מכונת טיורינג M מעל אלפבית קלט $\{0\}$ (אלפבית של אות אחת) המקיימת, לכל $n \in \mathbb{N}$:

$M(0^n) = 0^{f(n)}$;

$\mathrm{space}_M(0^n) = O(f(n))$.

אינטואיציה. התנאי הראשון לבדו אומר רק ש-f **חשיבה**: נותנים למכונה את המספר n (מקודד באונרית — אורך המחרוזת הוא המספר) והיא מחזירה את $f(n)$ באותו קידוד. התנאי השני מוסיף את הדרישה הסיבוכיותית: המקום שדרוש כדי לחשב את f אינו גדול משמעותית מגודל הפלט עצמו. אפשר לקרוא את זה כך — *אפשר לבנות את f בתוך המקום של עצמה.* שימו לב ש-$O(\cdot)$ ולא שוויון: מותר לצרוך קצת יותר מקום מהפלט, עד כדי קבוע כפלי.

> **הערה על סימונים:** בכתב יד קל להתבלבל בין הספרה 0 בתוך 0^n לבין הסימון $O(\cdot)$. שאלת סטודנט בהקלטה [00:22:10] הייתה בדיוק זו — ב-$M(0^n)$ מדובר בספרה אפס, כלומר מחרוזת של אפסים; אין משמעות ל"O בחזקת n".

מופע. $f(n) = n^2$ ישימה במקום: קל לבנות מכונה שכותבת n^2 אפסים תוך שימוש ב-$O(n^2)$ תאים.

אי־מופע (הבהרת הגבול). פונקציה שאינה חשיבה כלל — למשל $f(n) =$ מספר המכונות בגודל n שעוצרות על הקלט הריק — בוודאות אינה ישימה במקום, כי אפילו התנאי הראשון נכשל. בקורס הזה כמעט לא ניתקל בכאלה: אנחנו כבר לא בעולם של $\mathbb{R}$ ולא בעולם של פונקציות לא חשיבות.

הגדרה 2: ישימות בזמן (time-constructible)

באופן דומה לחלוטין, רק שהתנאי השני מוחלף ב-$\mathrm{time}_M(0^n) = O(f(n))$.

משפט עזר (ללא הוכחה, מותר להשתמש)

> **כל הפונקציות האלמנטריות — פולינומים, אקספוננטים, לוגריתמים והרכבות שלהן — ישימות במקום וישימות בזמן.**

זהו משפט אמיתי שלא מוכיחים בקורס אבל מותר לצטט. בפועל: **כל פונקציה סבירה שתיתקלו בה ישימה בשני המדדים.** זה מה שהופך את התנאי השני של משפט ההיררכיה לתנאי טכני ולא למגבלה אמיתית.

הגדרה 3: סופר־לינאריות

f נקראת **סופר־לינארית** אם $f(n) \geq n$ לכל $n \in \mathbb{N}$.

אינטואיציה. זו הדרישה שהתקציב יספיק לפחות כדי לקרוא את הקלט. היא תשמש אותנו פעמיים בחשבון, שתיהן בצורה "בלע את $|\langle M \rangle|$ בתוך $f(|\langle M \rangle|)$".

הגדרה 4: השפה S_f — האלכסון

תהי $f : \mathbb{N} \to \mathbb{N}$. נגדיר

$$S_f = \left\{ \langle M \rangle \;\middle|\; M \text{ rejects } \langle M \rangle \ \wedge\ \text{space}_M(\langle M \rangle) \leq \frac{f(|\langle M \rangle|)}{\lg |\Gamma_M|} \right\}.$$

במילים: כל הקידודים של מכונות שמקיימות **שני** תנאים — המכונה דוחה את הקידוד של עצמה, וגם המקום שהיא צורכת כשמריצים אותה על הקידוד של עצמה אינו עולה על f של אורך הקידוד, חלקי הלוגריתם של גודל אלפבית הסרט שלה.

> **הערה:** בהרצה הראשונה המרצה אמר במפורש "הנחתי את השפה הזאת — אל תשאלו איך הגעתי אליה, שאלו רק אם ההגדרה ברורה" [00:36:14]. בהרצה המקבילה כן ניתן ההסבר המלא, והוא מובא כאן בשלמותו, כי הוא הדבר החשוב ביותר שאין בסיכום.

מאיפה התנאי הראשון. אם משמיטים לגמרי את תנאי המקום, נשארים עם השפה $\{\langle M \rangle \mid M \text{ rejects } \langle M \rangle\}$. זו בדיוק שפת הלכסון מחישוביות, והיא **אינה כריעה**: אילו הייתה מכונה M' שמכריעה אותה, נשאל מה היא מחזירה על $\langle M' \rangle$. אם היא מקבלת — אז $\langle M' \rangle \in$ השפה, אבל השייכות דורשת שהיא תדחה, סתירה. אם היא דוחה — אז לפי ההגדרה $\langle M' \rangle$ **כן** בשפה, ולכן היא הייתה צריכה לקבל, סתירה. יש קלט אחד — הקידוד של עצמה — שעליו כל מכונה טועה.

מה עושה התנאי השני. תנאי המקום **מפצל את עולם המכונות לשניים**:

מכונה שמשתמשת ב-$O(g)$ מקום: מכיוון ש-g קטנה בסדר גודל מ-f, תנאי המקום מתקיים אצלה אוטומטית (עבור קידודים ארוכים מספיק). ולכן היא נשארת לכודה בדיוק באותה סתירה — היא לא יכולה להכריע את S_f.

מכונה שמשתמשת ביותר מ-$f(|\langle M \rangle|) / \lg |\Gamma_M|$ מקום: אצלה תנאי המקום **נכשל**, ולכן היא יכולה לדחות את הקידוד של עצמה בלי להיכנס לסתירה — היא פשוט אינה שייכת ל-S_f, ולא בגלל תנאי הלכסון אלא בגלל תנאי המקום. מכונות כאלה הן היחידות שיש להן סיכוי להכריע את S_f.

זו התשובה לשאלה המתבקשת ששאל סטודנט [00:09:30]: "אם השפה הזו לא כריעה, איך היא בכלל יכולה להיות ב-$\mathrm{DSpace}(f)$?" — התשובה היא שהיא כן כריעה; תנאי המקום הוא שהופך אותה לכריעה, ולא סתם כריעה, אלא כריעה **בדיוק** על ידי מכונות שמעל הסף.

מאיפה החלוקה ב-$\lg |\Gamma_M|$. זהו הפרט הסיבוכיותי היחיד בהגדרה. כשנכריע את S_f נריץ מכונה אוניברסלית, והמקום שהיא דורשת הוא $O(\text{space}_M(x) \cdot \lg |\Gamma_M|)$. אם נחסום את space_M ב-$f / \lg |\Gamma_M|$, אז ה-$\lg |\Gamma_M|$ **מצטמצם** ונשארים עם $O(f)$ — חסם שאינו תלוי במכונה שמריצים. בלי החלוקה הזו היה נשאר קבוע שתלוי בקלט, ומחלקת DSpace אינה סובלת קבוע כזה. אותו צמצום בדיוק יקרה גם בחשבון הזמן, כי גם שם הפקטור הדומיננטי הוא $2^{\lg |\Gamma_M| \cdot \text{space}_M}$.

משפטים והוכחות

משפט 1 (חימום): $\mathrm{PSPACE} \subseteq \mathrm{EXP}$

הוכחה. תהי $A \in \mathrm{PSPACE}$.

לפי הגדרת PSPACE כאיחוד, קיים $c \geq 1$ כך ש-$A \in \mathrm{DSpace}(n^c)$. (הצעד הראשון תמיד: **לקלף את האיחוד החוצה.**)

מהטענה שהוכחנו בשיעור 2, $\mathrm{DSpace}(f) \subseteq \bigcup_{d\geq 1}\mathrm{DTime}(2^{d\cdot f})$, ולכן $A \in \bigcup_{d\geq 1}\mathrm{DTime}\left(2^{d\cdot n^c}\right)$.
שוב מקלפים את האיחוד: קיים $d \geq 1$ כך ש-$A \in \mathrm{DTime}\left(2^{d\cdot n^c}\right)$.
וכאן נתקעים לרגע — הצורה $2^{d\cdot n^c}$ **אינה** מהצורה $2^{n^{c'}}$ שממנה בנויה EXP.
הנקודה שהמרצה עצר עליה: **קבוע כפלי בתוך החזקה אינו זניח.** קבוע כפלי *מחוץ* לפונקציה תמיד נבלע ב-$O(\cdot)$ ובקבוע של המחלקה, אבל 2^{2n} ו-2^n אינם מאותו סדר גודל בכלל — היחס ביניהם הוא 2^n. אי אפשר "להעיף" את d.
מה כן אפשר? להשתמש בכך ש-EXP הוא איחוד על **כל** החזקות, ולכן מותר לנו לקחת חזקה גדולה יותר. לכל $n \geq d$ מתקיים $d \cdot n^c \leq n \cdot n^c = n^{c+1}$, ולכן

$$2^{d\cdot n^c} = O\left(2^{n^{c+1}}\right).$$

לכן $A \in \mathrm{DTime}\left(2^{n^{c+1}}\right) \subseteq \mathrm{EXP}$. ■
למה בדיוק $c+1$? מפני ש-d קבוע ו-n לא. הגדלת החזקה של n באחד מספיקה כדי לבלוע כל קבוע כפלי, עבור n גדולים מספיק. אם נחזור לדוגמה: 2^{2n} גדול בהרבה מ-2^n, אבל קטן בהרבה מ-2^{n^2}. (גם $c\cdot d$ בחזקה היה עובד — הוא $\geq c$ כי $d \geq 1$ — אבל $c+1$ פשוט יותר.)
משפט 2 (גרסת החלומות — **לא** נכון שיודעים להוכיח)

> תהיינה $f, g : \mathbb{N} \to \mathbb{N}$. אם $g = o(f)$ אז $\mathrm{DSpace}(g) \subsetneq \mathrm{DSpace}(f)$.

זהו הניסוח שמדל את האינטואיציה: הגדלתי משמעותית את התקציב, אז אני יכול עכשיו לעשות דברים שלא יכולתי קודם. **אף אחד אינו יודע להוכיח את זה ואסור להשתמש בו.** צריך תנאים נוספים — וזה בדיוק המשפט הבא.
שימו לב למה קופצים כאן מ-O גדול ל-o קטן: O גדול נותן רק את התוצאה החיובית ($\mathrm{DSpace}(g) \subseteq \mathrm{DSpace}(f)$). o קטן אומר שהתקציב גדל **בסדר גודל**, וזה מה שנדרש כדי לקוות לתוצאה שלילית.
משפט 3: משפט ההיררכיה במקום

> תהיינה $f, g : \mathbb{N} \to \mathbb{N}$. נניח כי
> $g = o(f)$;
> f ישימה במקום;
> $f(n) \geq n$ לכל $n \in \mathbb{N}$ (כלומר f סופר־לינארית).
> אז $\mathrm{DSpace}(g) \subsetneq \mathrm{DSpace}(f)$.

מבנה ההוכחה. "A מוכלת ממש ב-B" פירושו "$A \subseteq B$ **וגם** $B \not\subseteq A$". לכן צריך להוכיח שני דברים נפרדים:
(א) $\mathrm{DSpace}(g) \subseteq \mathrm{DSpace}(f)$;

(ב) $\mathrm{DSpace}(f) \not\subseteq \mathrm{DSpace}(g)$, כלומר **קיימת** שפה $A \in \mathrm{DSpace}(f)$ עם $A \notin \mathrm{DSpace}(g)$.

חלק (ב) הוא טענת קיום, ולכן נציג שפה קונקרטית — את S_f — ונוכיח עליה שני דברים בלתי תלויים: שהיא ב-$\mathrm{DSpace}(f)$, ושהיא לא ב-$\mathrm{DSpace}(g)$.

חלק (א): ההכלה

$g = o(f)$ גורר $g = O(f)$ (אור קטן תמיד גורר אור גדול). לפי הטענה מהשיעור 2, $\mathrm{DSpace}(g) \subseteq \mathrm{DSpace}(f)$. $\square$

זהו — החלק הזה נגמר בשורה אחת, וכל שאר ההוכחה עוסקת בחלק (ב).

חלק (ב1): $S_f \in \mathrm{DSpace}(f)$

לפי ההגדרה, צריך להציג **מכונה** ו**קבוע**, ולהראות שהמכונה מכריעה את S_f ושהיא עושה זאת במקום שאינו עולה על הקבוע כפול f.

בניית המכונה. M_f תהיה מכונה רב־סרטית, מבוססת על המכונה האוניברסלית M_U, **בתוספת שני סרטים**: סרט *מונה מקום* וסרט *מונה זמן*. שימו לב ש-M_f אינה האוניברסלית — היא מחזיקה את האוניברסלית "בבטן", וכן מחזיקה בבטן גם מכונה שמחשבת את f (זה חוקי: f ישימה במקום ובפרט חשיבה, והיא ידועה לנו כבר בזמן הבנייה, כי היא נתונה בניסוח המשפט).

על קלט $\langle M \rangle$ שהוא קידוד של מכונה, M_f פועלת כך:

אתחול מונה המקום. M_f כותבת על סרט מונה המקום $\dfrac{f(|\langle M \rangle|)}{\lg |\Gamma_M|}$ אפסים. את המונה הזה חושבים כמספר **באונרית**.

אתחול מונה הזמן. M_f כותבת על סרט מונה הזמן $3f(|\langle M \rangle|)$ אפסים, ומשמאלם 1. את המונה הזה חושבים כמספר **בבינארית** — כלומר זהו הייצוג הבינארי של $2^{3f(|\langle M \rangle|)}$.

סימולציה. M_f מסמלצת את ריצת M_U על הקלט $\langle M, M \rangle$, כלומר מריצה את M על הקידוד של עצמה, עם שתי תוספות:

בכל צעד ש-M_U מסמלצת בריצה של M על $\langle M \rangle$ — M_f מורידה 1 ממונה הזמן (בבינארית).

בכל פעם ש-M כותבת בתא שעדיין לא כתבה בו — M_f מוחקת אפס אחד ממונה המקום.

אם אחד המונים היה אמור לרדת מתחת לאפס — M_f **דוחה** מיד ועוצרת את הסימולציה.

סיום. אם הסימולציה הסתיימה: אם M **דחתה** את $\langle M \rangle$ אז M_f **מקבלת**; אם M **קיבלה** את $\langle M \rangle$ אז M_f **דוחה**.

הערות טכניות על הבנייה:

מדוע מונה הזמן בבינארית ומונה המקום באונרית? אילו כתבנו את 2^{3f} באונרית היינו צריכים $2^{3f(n)}$ תאים — הרבה מעבר לתקציב. בבינארית זה $3f(n)+1$ תאים בלבד. במונה המקום המספר עצמו הוא כבר בסדר גודל f, ולכן אונרי או בינארי אינו קריטי שם, והאונרי נוח יותר לספירה.

איך יודעים אם M כתבה בתא חדש? מסמנים תאים שכבר נכתב בהם, על ידי שינוי קל של אלפבית הסרט — טכניקה שראינו בחישוביות. אם M כותבת שוב בתא מסומן, לא מורידים מהמונה.

ניתוח סמנטי: M_f מכריעה את S_f.

כיוון ראשון: אם $\langle M \rangle \in S_f$ אז M_f מקבלת. מהשייכות נובעים שני דברים: M דוחה את $\langle M \rangle$ (ובפרט **עוצרת** עליו), וגם $\mathrm{space}_M(\langle M \rangle) \le f(|\langle M \rangle|)/\lg|\Gamma_M|$.

מהתנאי השני נובע מיידית ש**מונה המקום לא ירד מתחת לאפס**, כי הוא אותחל בדיוק לחסם הזה.
לגבי מונה הזמן: מכיוון ש-M עוצרת על $\langle M\rangle$, נשתמש בחסם ספירת הקונפיגורציות מהשיעור 1:

$$\mathrm{time}_M(\langle M\rangle) \;\le\; 2^{\lg|Q_M| + \lg|\Gamma_M|\cdot \mathrm{space}_M(\langle M\rangle) + \lg \mathrm{space}_M(\langle M\rangle)}.$$

נחסום כל אחד משלושת המחוברים בנפרד:
נסמן ב-N את מספר האפשרויות שהקידוד מתאר. אז $\lg|Q_M| \le \lg N \le |\langle M\rangle|$ — מספר המצבים אינו עולה על N, ולוגריתם של מספר אינו עולה על אורך הקידוד שלו. ואז, **מהסופר־לינאריות**, $(|\langle M\rangle|) \le |\langle M\rangle|$.
$\lg|\Gamma_M|\cdot \mathrm{space}_M(\langle M\rangle) \;\le\; \lg|\Gamma_M|\cdot \dfrac{f(|\langle M\rangle|)}{\lg|\Gamma_M|} = f(|\langle M\rangle|)$. **כאן מצטמצם ה-**$\lg|\Gamma_M|$ — זו כל הסיבה שהוא הוכנס להגדרת השפה מלכתחילה.
$(|\langle M\rangle|) \le \mathrm{space}_M(\langle M\rangle) \le f(|\langle M\rangle|)$ — לוגריתם של מספר אינו עולה על המספר, והמקום כבר חסום ב-f (שהרי $\lg|\Gamma_M| \ge 1$).
בסך הכול

$$\mathrm{time}_M(\langle M\rangle) \;\le\; 2^{f(|\langle M\rangle|)+f(|\langle M\rangle|)+f(|\langle M\rangle|)} \;=\; 2^{3f(|\langle M\rangle|)},$$

שזה **בדיוק** המספר שרשום במונה הזמן. לכן גם מונה הזמן לא ירד מתחת לאפס, הסימולציה מסתיימת, M_f מגיעה לשלב 4, מגלה ש-M דחתה את $\langle M\rangle$ — ומקבלת.
כיוון שני: אם $\langle M\rangle \notin S_f$ אז M_f דוחה. שלילת השייכות אומרת: M **אינה דוחה** את $\langle M\rangle$, **או** שהמקום שלה עולה על החסם. נפצל:
מקרה 1: $\mathrm{space}_M(\langle M\rangle) > \dfrac{f(|\langle M\rangle|)}{\lg|\Gamma_M|}$. אז במהלך הסימולציה מונה המקום ירד מתחת לאפס, ולפי שלב 3 M_f דוחה.
מקרה 2: המקום כן חסום, ולכן בהכרח M אינה דוחה את $\langle M\rangle$. שימו לב — "אינה דוחה" **אינו** אותו דבר כמו "מקבלת"; ייתכן גם שהיא לא עוצרת. לכן נפצל שוב:
מקרה 2.1: M אינה עוצרת על $\langle M\rangle$. לפי החסם שלמעלה בקונטרפוזיטיב: אם המקום חסום ב-$f/\lg|\Gamma_M|$ ומספר הצעדים עולה על $2^{3f(|\langle M\rangle|)}$, אז חייבת לחזור קונפיגורציה, ולכן המכונה בלולאה אינסופית. במקרה שלנו המכונה אכן לא עוצרת, ולכן היא בהכרח תעבור את $2^{3f(|\langle M\rangle|)}$ צעדים, מונה הזמן ירד מתחת לאפס, ו-M_f דוחה.
מקרה 2.2: M עוצרת ואינה דוחה, כלומר **מקבלת**. אז המונים לא נגמרים (כמו בחשבון הכיוון הראשון), הסימולציה מסתיימת, M_f מגיעה לשלב 4, מגלה ש-M קיבלה — ודוחה.

> **הערה:** בהרצה הראשונה הכיוון השני הוצג בקיצור, דרך "אם M_f קיבלה אז בהכרח המונים לא ירדו והסימולציה הסתיימה". הפירוט לשלושת המקרים לעיל הוא הגרסה המלאה, כפי שנעשתה בהרצה המקבילה; המלכודת שצריך לשים לב אליה היא בדיוק מקרה 2.1 — "אינה דוחה" מכיל גם "אינה עוצרת".

בשני הכיוונים יחד: M_f מכריעה את S_f.

חשבון המקום. עכשיו צריך לחסום את המקום ש-M_f דורשת. יש שלושה מקורות: כתיבת מונה המקום, כתיבת מונה הזמן, והסימולציה. חשוב: לא מספיק לספור את המקום שהמונה **תופס בסוף**, אלא גם את המקום שנדרש כדי **לחשב** אותו.

קיים $\alpha > 0$ כך שלכל מכונה M ניתן לחשב את $\dfrac{f(|\langle M\rangle|)}{\lg|\Gamma_M|}$ במקום שאינו עולה על $\alpha\cdot f(|\langle M\rangle|)$. זה נובע מכך ש-$f$ **ישימה במקום** (כאן, ורק כאן, נכנס התנאי השני של המשפט): את $\lg|\Gamma_M|$ אפשר לקרוא מיידית מהקידוד — זה פשוט אורך הקידוד של תו בודד — והחילוק הוא פונקציה אלמנטרית, ולכן זול.

קיים $\beta > 0$ כך שלכל M ניתן לחשב את $3f(|\langle M\rangle|)$ במקום שאינו עולה על $3\beta\cdot f(|\langle M\rangle|)$. שוב מהישימות במקום.

קיים $\gamma > 0$ כך שלכל M, המקום שהסימולציה (המבוקרת!) של האוניברסלית דורשת מקיים

$$\begin{aligned}&\mathrm{space}_{M_U}(\langle M, M\rangle) \;\le\\ &\gamma\left(|\langle M, M\rangle| + \lg|\Gamma_M|\cdot\min\left\{\mathrm{space}_M(\langle M\rangle),\ \frac{f(|\langle M\rangle|)}{\lg|\Gamma_M|}\right\}\right).\end{aligned}$$

ה-$\min$ מופיע מפני שאנחנו **קוטעים** את האוניברסלית ברגע שמונה המקום נגמר — היא לעולם לא תעבור את הסף, גם אם M עצמה הייתה זוללת יותר. מכאן, כשבוחרים את האיבר הנוח מתוך ה-$\min$:

$$\le\ \gamma\,(2|\langle M\rangle| + f(|\langle M\rangle|))\ \le\ \gamma\,(2f(|\langle M\rangle|) + f(|\langle M\rangle|))\ =\ 3\gamma\, f(|\langle M\rangle|),$$

כאשר במעבר האמצעי השתמשנו **שוב בסופר־לינאריות** ($|\langle M\rangle| \le f(|\langle M\rangle|)$).

בסך הכול, לכל מכונה M:

$$\mathrm{space}_{M_f}(\langle M\rangle)\ \le\ (\alpha + 3\beta + 3\gamma)\cdot f(|\langle M\rangle|).$$

המרה למכונה סטנדרטית. דקות אחת אחרונה: M_f רב־סרטית, וההגדרה של DSpace מדברת על מכונה סטנדרטית. לפי משפט השקילות בין המודלים קיימת מכונה חד־סרטית $\hat{M}_f$, שקולה סמנטית ל-M_f, וקיים $\hat{c} > 0$ כך שלכל M:

$$\mathrm{space}_{\hat{M}_f}(\langle M\rangle) \le \hat{c}\cdot\mathrm{space}_{M_f}(\langle M\rangle).$$

נגדיר $c = \hat{c}\,(\alpha + 3\beta + 3\gamma)$. אז $\hat{M}_f$ מכריעה את S_f (כי היא שקולה סמנטית ל-M_f), ולכל M:

$$\mathrm{space}_{\hat{M}_f}(\langle M\rangle)\ \le\ \hat{c}\,(\alpha + 3\beta + 3\gamma)\, f(|\langle M\rangle|)\ =\ c\cdot f(|\langle M\rangle|).$$

לכן $S_f \in \mathrm{DSpace}(f)$. $\square$

הערה: במקום המעבר הזה עולה רק קבוע כפלי — וזה בדיוק המקום שבו הזמן יתנהג אחרת. שימו סימנייה.

חלק (ב2): $S_f \notin \mathrm{DSpace}(g)$
זו תוצאה שלילית, ולכן — הוכחה בשלילה. (המרצה הדגיש שהוא בדרך כלל לא אוהב הוכחות בשלילה, אבל כשרוצים להראות ש**משהו לא קורה**, ההוכחה בשלילה שם *for a reason*.)
נניח בשלילה ש-$S_f \in \mathrm{DSpace}(g)$. אז לפי ההגדרה קיימת מכונה M_g וקיים קבוע $c > 0$ כך ש:
M_g מכריעה את S_f;
לכל מכונה M: $\mathrm{space}_{M_g}(\langle M \rangle) \le c \cdot g(|\langle M \rangle|)$.
שימו לב מה יש לנו עכשיו ביד: את M_g ואת c. שניהם קבועים מבחינת ההוכחה מרגע זה ואילך. זו נקודה שתשמש אותנו מיד.
כאן — ורק כאן — נכנס $g = o(f)$. מהגדרת o קטן,

$$\lim_{n\to\infty} \frac{g(n)}{f(n)} = 0.$$

מהגדרת הגבול, לכל $\varepsilon > 0$ קיים n_0 כך שלכל $n \ge n_0$ מתקיים $g(n)/f(n) < \varepsilon$. נבחר

$$\varepsilon = \frac{1}{c \cdot \lg |\Gamma_{M_g}|}.$$

הבחירה חוקית **מפני ש-c ו-M_g כבר ידועים לנו בנקודה הזו** — הם קבועים, לא משתנים שתלויים ב-n. נקבל: קיים $n_0 \in \mathbb{N}$ כך שלכל $n \ge n_0$,

$$\frac{g(n)}{f(n)} < \frac{1}{c \cdot \lg |\Gamma_{M_g}|}.$$

הבעיה שנשארה, והטריק. אנחנו רוצים להפעיל את אי־השוויון הזה על המכונה שביד — אבל M_g היא מכונה ספציפית, ואולי הקידוד שלה קצר מ-n_0. הגבול מבטיח משהו רק עבור קלטים ארוכים מספיק. הפתרון: לנפח את המכונה מבלי לשנות אותה.
נגדיר מכונה $\hat{M}_g$, זהה ל-M_g לחלוטין, אלא שהוספנו לה n_0 **מצבי סרק** — מצבים שלעולם לא נגיע אליהם. אז:
$\hat{M}_g$ פועלת בדיוק כמו M_g על כל קלט (לא שינינו שום דבר במצבים הקיימים ולא בפונקציית המעברים המהותית), ובפרט היא **מכריעה את** S_f;
$|\langle \hat{M}_g \rangle| \ge n_0$ — כי טבלת המעברים גדלה, והקידוד איתה;
הכי חשוב: $\Gamma_{M_g} = \Gamma_{\hat{M}_g}$ — לא נגענו באלפבית. זו הסיבה שניפחנו דווקא במצבים ולא בתווים.
עכשיו נריץ את $\hat{M}_g$ על הקידוד של עצמה. שני מקרים.
מקרה 1: $\hat{M}_g$ מקבלת את $\langle \hat{M}_g \rangle$. מכיוון ש-$\hat{M}_g$ מכריעה את S_f, מהקבלה נובע $\langle \hat{M}_g \rangle \in S_f$. אבל ההגדרה של S_f דורשת, בין השאר, שהמכונה **תדחה** את הקידוד של עצמה. סתירה.

מקרה 2: $\hat{M}_g$ דוחה את $\langle \hat{M}_g \rangle$. מהסמנטיקה, $\langle \hat{M}_g \rangle \notin S_f$. תנאי השייכות ל-$S_f$ הוא "וגם" של שני תנאים; אנחנו יודעים שהתנאי הראשון (דוחה את עצמה) **כן** מתקיים, ולכן בהכרח **התנאי השני נכשל**:

$$\text{space}_{\hat{M}_g}(\langle \hat{M}_g \rangle) \;>\; \frac{f(|\langle \hat{M}_g \rangle|)}{\lg |\Gamma_{\hat{M}_g}|}. \qquad (*)$$

מצד שני נחשב את אותו גודל מלמעלה. ראשית, מכיוון ש-$\hat{M}_g$ פועלת בדיוק כמו M_g (הקלט לא משתנה, רק המכונה שמריצה אותו):

$$\text{space}_{\hat{M}_g}(\langle \hat{M}_g \rangle) = \text{space}_{M_g}(\langle \hat{M}_g \rangle) \le c \cdot g(|\langle \hat{M}_g \rangle|).$$

שנית, מכיוון ש-$|\langle \hat{M}_g \rangle| \ge n_0$ — **וזו בדיוק הסיבה שניפחנו** — מותר להציב באי־שוויון הגבול:

$$\frac{g(|\langle \hat{M}_g \rangle|)}{f(|\langle \hat{M}_g \rangle|)} < \frac{1}{c \cdot \lg |\Gamma_{M_g}|} \quad \Longrightarrow \quad g(|\langle \hat{M}_g \rangle|) < \frac{f(|\langle \hat{M}_g \rangle|)}{c \cdot \lg |\Gamma_{M_g}|} = \frac{f(|\langle \hat{M}_g \rangle|)}{c \cdot \lg |\Gamma_{\hat{M}_g}|},$$

כאשר המעבר האחרון הוא **רק** החלפת Γ_{M_g} ב-$\Gamma_{\hat{M}_g}$ — מותרת כי הם אותו אלפבית בדיוק. נכפיל ב-c:

$$\text{space}_{\hat{M}_g}(\langle \hat{M}_g \rangle) \;\le\; c \cdot g(|\langle \hat{M}_g \rangle|) \;<\; \frac{f(|\langle \hat{M}_g \rangle|)}{\lg |\Gamma_{\hat{M}_g}|}.$$

יחד עם $(*)$ קיבלנו

$$\frac{f(|\langle \hat{M}_g \rangle|)}{\lg |\Gamma_{\hat{M}_g}|} \;<\; \text{space}_{\hat{M}_g}(\langle \hat{M}_g \rangle) \;<\; \frac{f(|\langle \hat{M}_g \rangle|)}{\lg |\Gamma_{\hat{M}_g}|},$$

כלומר גודל גדול ממש מעצמו. **סתירה.**
בשני המקרים הגענו לסתירה, ולכן ההנחה בשלילה בטלה: $S_f \notin \text{DSpace}(g)$. $\square$
יחד עם חלק (ב1), $S_f \in \text{DSpace}(f) \setminus \text{DSpace}(g)$, ועם חלק (א) — $\text{DSpace}(g) \subsetneq \text{DSpace}(f)$. $\blacksquare$
סיכום הרעיון בשורה אחת: כל מכונה שחסומה במקום $O(g)$ מקיימת אוטומטית (אחרי ניפוח) את תנאי המקום של S_f, ולכן נשארת לכודה בסתירת הלכסון הטהורה — היא לא יכולה לא לקבל ולא לדחות את הקידוד של עצמה. מכונות שמעל הסף בורחות, ולכן S_f כן כריעה — רק לא בתקציב g.

משפט 4: משפט ההיררכיה בזמן

תהיינה $f, g : \mathbb{N} \to \mathbb{N}$. נניח כי
$g = o(f)$;
f ישימה בזמן;
f סופר־לינארית.
אז $\mathrm{DTime}(g) \subsetneq \mathrm{DTime}\left(f^2\right)$.

זה משפט חלש יותר, ובמכוון: הייתי רוצה לכתוב $\mathrm{DTime}(f)$ באגף ימין, אבל אנחנו לא יודעים. ההוכחה נמסרה כתרגיל מודרך בשיעורי הבית; המבנה כמעט זהה, ולהלן שתי הנקודות שבהן היא נבדלת — שתיהן נאמרו במפורש בהרצאה, ושתיהן שוות זהב לפני מבחן.

מאיפה צומח הריבוע?

מהמעבר מהמכונה הרב־סרטית למכונה הסטנדרטית. בהוכחה במקום, המכונה M_f שבנינו הייתה רב־סרטית, וההמרה למכונה חד־סרטית עלתה לנו רק בקבוע כפלי במקום — ולכן נשארנו ב-$\mathrm{DSpace}(f)$. בזמן, ההמרה עולה **ריבוע**.

ולמה ההמרה עולה ריבוע? כי המכונה החד־סרטית צריכה לרוץ קדימה ואחורה על פני כל האזור שבו יושבים "הסרטים" הרב־סרטיים המדומים, ולכן כל צעד מדומה עולה כמו רוחב האזור, כלומר כמו המקום. וכיוון שאין לנו שום מידע על המקום, החסם הטוב ביותר שאפשר לתת למקום הוא **הזמן עצמו** — ומכפלת זמן במקום נותנת $O(t^2)$.

הפער השני: אי אפשר לנפח מצבים

בהוכחה במקום, השלב הקריטי היה ניפוח הקידוד **בלי** לשנות את האלפבית, כי המכנה בהגדרת השפה היה $\lg|\Gamma_M|$. בזמן, המדד של האוניברסלית הוא

$$\mathrm{time}_{M_U}(\langle M, x\rangle) = O(|\langle M\rangle| \cdot \mathrm{time}_M(x)),$$

כלומר על כל צעד מסומלץ משלמים לא $\lg|\Gamma_M|$ אלא **את כל אורך הקידוד** $|\langle M\rangle|$. לכן, כדי שהצמצום יעבוד, השפה המקבילה חייבת להיראות כך:

$$\mathrm{time}_M(\langle M\rangle) \;\le\; \frac{f(|\langle M\rangle|)}{|\langle M\rangle|}.$$

ואז נופלת השמיכה הקצרה: כל ניפוח של הקידוד מגדיל **גם את המונה וגם את המכנה**, ולכן טריק מצבי הסרק כבר לא מקדם אותנו.

הפתרון (כפי שנאמר בהרצה כדי לתת כיוון לתרגיל הבית): מגדירים את השפה על קלטים מהצורה $\langle M\rangle\#^k$ — קידוד של מכונה עם ריפוד מלאכותי של סולמיות. עכשיו אפשר להאריך את **הקלט** כרצוננו, ובכך להגדיל את n ולהיכנס לתחום שבו הגבול תופס, **בלי** להגדיל את $|\langle M\rangle|$ שיושב במכנה. ההגדרה המדויקת של השפה המרופדת תינתן בתרגיל.

משפט 5 (מסקנה): $\mathrm{P} \subsetneq \mathrm{EXP}$

המלכודת שצריך לעקוף. משפט ההיררכיה מדבר על מחלקות **עדינות** (DTime של פונקציה בודדת). P ו-EXP הן מחלקות **גסות** — איחודים אינסופיים. אי אפשר להפעיל עליהן את המשפט, והפיתוי לעשות זאת "איבר־איבר" **שגוי**:

> **הכלה נשמרת תחת איחוד. הכלה ממש — לא.**
> נגד־דוגמה: $A_1 = \{1\}$, $A_2 = \{2\}$, $C = \{1, 2\}$. אז $A_1 \subsetneq C$ וגם $A_2 \subsetneq C$, אבל $A_1 \cup A_2 = C$ ואינו מוכל ממש ב-C.

בשפה של המשפטים: מהמשפט קל לקבל "לכל c קיימת שפה $A \in \mathrm{EXP}$ שאינה ב-$\mathrm{DTime}(n^c)$", אבל מה שצריך זה "**קיימת** שפה $A \in \mathrm{EXP}$ שלכל c אינה ב-$\mathrm{DTime}(n^c)$". שני המשפטים אינם שקולים — השני גורר את הראשון, לא להפך.

הפתרון המבני, וזה תמיד יהיה כך: עוברים דרך **שתי מחלקות עדינות באמצע**, מפעילים את משפט ההיררכיה עליהן בלבד, ומשלימים בשתי הכלות רגילות משני הצדדים.

הוכחה.

שלב 1 — ההכלה $\mathrm{P} \subseteq \mathrm{EXP}$. כבר יש: הראינו $\mathrm{P} \subseteq \mathrm{PSPACE}$ (שיעור 2) ו-$\mathrm{PSPACE} \subseteq \mathrm{EXP}$ (משפט 1 לעיל).

שלב 2 — מעבר למחלקה עדינה מלמטה. יהי $c \geq 1$. אז $n^c = O(2^n)$ (למעשה אפילו $o(2^n)$, אבל O מספיק כאן), ולכן $\mathrm{DTime}(n^c) \subseteq \mathrm{DTime}(2^n)$. זה נכון **לכל** c, והכלה רגילה כן נשמרת תחת איחוד, ולכן

$$\mathrm{P} = \bigcup_{c \geq 1} \mathrm{DTime}(n^c) \;\subseteq\; \mathrm{DTime}(2^n).$$

שלב 3 — הפעלת משפט ההיררכיה בזמן. נסמן

$$g(n) = 2^n, \qquad f(n) = 2^{2n}.$$

נבדוק את שלושת התנאים:

- $g = o(f)$: אכן, $\dfrac{2^n}{2^{2n}} = 2^{-n} \xrightarrow[n\to\infty]{} 0$.
- f אלמנטרית ולכן **ישימה בזמן**.
- f סופר־לינארית: $2^{2n} \geq n$ לכל n.

לכן ממשפט ההיררכיה בזמן,

$$\mathrm{DTime}(2^n) \;\subsetneq\; \mathrm{DTime}\big(f^2\big) = \mathrm{DTime}\Big(\big(2^{2n}\big)^2\Big) = \mathrm{DTime}\big(2^{4n}\big)\,.$$

שלב 4 — מעבר למחלקה גסה מלמעלה. $2^{4n} = O\Big(2^{n^2}\Big)$ (כי $4n \leq n^2$ לכל $n \geq 4$), ולכן

$$\mathrm{DTime}\left(2^{4n}\right) \subseteq \mathrm{DTime}\left(2^{n^2}\right) \subseteq \mathrm{EXP}.$$

הצעד האחרון הוא פשוט "לקלף את האיחוד" בכיוון ההפוך: 2^{n^2} הוא מהצורה 2^{n^c} עם $c = 2$.
שלב 5 — הרכבה.

$$\mathrm{P} \;\subseteq\; \mathrm{DTime}(2^n) \;\subsetneq\; \mathrm{DTime}\left(2^{4n}\right) \;\subseteq\; \mathrm{DTime}\left(2^{n^2}\right) \;\subseteq\; \mathrm{EXP}.$$

בשרשרת הכלות שבה **לפחות חוליה אחת היא הכלה ממש**, ההרכבה כולה היא הכלה ממש. לכן $\mathrm{P} \subsetneq \mathrm{EXP}$. ■
משפט 6 (מסקנה מהמסקנה): אחת משתי ההכלות היא ממש — ולא יודעים איזו
אנחנו יודעים:

$$\mathrm{P} \subseteq \mathrm{PSPACE} \subseteq \mathrm{EXP}, \qquad \mathrm{P} \subsetneq \mathrm{EXP}.$$

אילו שתי ההכלות היו שוויונות, היה נובע $\mathrm{P} = \mathrm{EXP}$ — בסתירה למשפט 5. לכן **לפחות אחת** מבין $\mathrm{P} \subseteq \mathrm{PSPACE}$ ו-$\mathrm{PSPACE} \subseteq \mathrm{EXP}$ היא הכלה ממש.
אבל אף אחד לא יודע איזו. שתי השאלות — האם $\mathrm{P} = \mathrm{PSPACE}$ והאם $\mathrm{PSPACE} = \mathrm{EXP}$ — הן בעיות פתוחות. המשפטים האלה ידועים כבר עשרות שנים ולא הצליחו להתקדם. זו טעימה ראשונה מהאופי של התחום: יודעים משהו חלקי, ולא יודעים לחדד אותו.

> **הערה מהשיעור [02:16:59]:** לשאלת סטודנט — לא, מחשבי־על ולא מחשבים קוונטיים לא "יפתרו" את זה. זו שאלה מתמטית על גבולות של מודל חישוב, לא שאלה של כוח חישוב.

דוגמאות ותרגילים מהשיעור
דוגמה 1: מעקב מספרי אחר המונים של M_f
ניקח $f(n) = n^2$ (סופר־לינארית וישימה במקום — פולינום). תהי M מכונה שהקידוד שלה באורך $|\langle M\rangle| = 100$ ואלפבית הסרט שלה בגודל $|\Gamma_M| = 4$, כלומר $\lg|\Gamma_M| = 2$.
מונה המקום מאותחל ל-$\dfrac{f(100)}{2} = \dfrac{10{,}000}{2} = 5{,}000$ אפסים.
מונה הזמן מאותחל ל-$3f(100) = 30{,}000$ אפסים ומשמאלם 1 — כלומר הייצוג הבינארי של $2^{30{,}000}$, ב-$30{,}001$ תאים בלבד. (באונרית זה היה דורש $2^{30{,}000}$ תאים — בלתי אפשרי.)
אם M על $\langle M\rangle$ כותבת ב-$4{,}000$ תאים שונים ועוצרת אחרי 10^9 צעדים: שני המונים שורדים ($4{,}000 \le 5{,}000$ ו-$10^9 \ll 2^{30{,}000}$), ולכן M_f תסמלץ עד הסוף ותהפוך את התשובה.
אם M כותבת ב-$6{,}000$ תאים: מונה המקום נגמר, M_f דוחה — וזה נכון, כי $6{,}000 > 5{,}000$ ולכן $\langle M\rangle \notin S_f$.

אם M נכנסת ללולאה אינסופית תוך שימוש ב-$3{,}000$ תאים בלבד: מספר הקונפיגורציות שלה חסום ב-$2^{3f(100)}$, ולכן היא חייבת לחזור על קונפיגורציה. מונה הזמן יגיע ל-0 ו-M_f תדחה. אכן $\langle M\rangle \notin S_f$, כי מכונה שאינה עוצרת אינה "דוחה".

דוגמה 2: התרגיל שהמרצה נתן לכיתה — לבחור f ו-g נכונות

המרצה ביקש מהכיתה למצוא f, g שיוכיחו $\mathrm{P} \subsetneq \mathrm{EXP}$. הכיתה הציעה שלושה ניסיונות, ושניים מהם נכשלו — ההסבר לכישלון חשוב יותר מהתשובה.

ניסיון א': $f(n) = n^2$**,** $g(n) = n$**.** תקין מתמטית: $g = o(f)$, f ישימה בזמן וסופר־לינארית, ולכן $\mathrm{DTime}(n) \subsetneq \mathrm{DTime}(n^4)$. אבל **חסר תועלת** — שתי המחלקות יושבות עמוק בתוך P ואינן אומרות דבר על EXP.

ניסיון ב': $f(n) = 2^n$**,** $g(n) = n$**.** מקבלים $\mathrm{DTime}(n) \subsetneq \mathrm{DTime}(2^{2n})$. שוב תקין ושוב חסר תועלת: $\mathrm{DTime}(n)$ אינו מכיל את כל P, ולכן לא הוכחנו כלום על P.

ניסיון ג' (הכיוון הנכון): $g(n) = 2^n$**.** קודם מראים ש-$\mathrm{P} \subseteq \mathrm{DTime}(2^n)$ — כי לכל c, $n^c = O(2^n)$, והכלה נשמרת תחת איחוד. עכשיו $\mathrm{DTime}(2^n)$ היא **מחלקה עדינה** שמכילה את כל P, ואפשר להפעיל עליה את המשפט.

תרגיל־בזק שנשאל בכיתה: האם מותר לקחת $f(n) = 2^{n+1}$? **לא.** $\dfrac{g(n)}{f(n)} = \dfrac{2^n}{2^{n+1}} = \dfrac{1}{2}$, שאינו שואף ל-$0$. לכן $g \neq o(f)$ והמשפט אינו חל. צריך פער בסדר גודל, לא פער בקבוע — וזו בדיוק הנקודה שקבוע כפלי בחזקה כן משנה סדר גודל, אבל קבוע כפלי מחוץ לחזקה לא.

דוגמה 3: היכן הטיעון "איבר־איבר" נשבר

ההוכחה השגויה: "לכל $c \geq 1$ מתקיים $n^c = o(2^{n^c})$, ולכן $\mathrm{DTime}(n^c) \subsetneq \mathrm{DTime}(2^{n^c})$; מכיוון שזה נכון לכל c, גם האיחודים מקיימים $\mathrm{P} \subsetneq \mathrm{EXP}$."

מה בדיוק שגוי: מה שהוכחנו הוא "לכל c קיימת $A_c \in \mathrm{EXP}$ שאינה ב-$\mathrm{DTime}(n^c)$". ה-A_c הזו **תלויה ב-**c. ייתכן ש-$A_1 \in \mathrm{DTime}(n^2)$, ש-$A_2 \in \mathrm{DTime}(n^3)$, וכן הלאה — ואז כל אחת מהן בכל זאת נמצאת ב-P, ולא הוכחנו כלום. מה שצריך הוא שפה **אחת** שבורחת מכל המחלקות בבת אחת, וזה בדיוק מה שהמעבר דרך $\mathrm{DTime}(2^n)$ נותן: שפה אחת שאינה ב-P $\supseteq \mathrm{DTime}(2^n)$.

זו הנקודה שהודגמה בכיתה עם $\{1\} \subsetneq \{1,2\}$ ו-$\{2\} \subsetneq \{1,2\}$ אבל $\{1\} \cup \{2\} = \{1,2\}$.

דוגמה 4: יישום ישיר של משפט ההיררכיה במקום

$$\mathrm{DSpace}(n) \subsetneq \mathrm{DSpace}(n^2).$$

בדיקת התנאים: $g(n) = n$, $f(n) = n^2$; $g = o(f)$ ולכן $\dfrac{n}{n^2} = \dfrac{1}{n} \to 0$; f פולינום ולכן ישימה במקום; $f(n) = n^2 \geq n$ ולכן סופר־לינארית. שלושת התנאים מתקיימים, המשפט חל. **שימו לב שבמקום אין ריבוע** — התוצאה היא $\mathrm{DSpace}(f)$ ולא $\mathrm{DSpace}(f^2)$. אילו הייתה זו שאלת זמן, היינו מקבלים רק $\mathrm{DTime}(n) \subsetneq \mathrm{DTime}(n^4)$.

תרגיל בית שניתן בכיתה

להוכיח את משפט ההיררכיה בזמן (משפט 4) כתרגיל מודרך. ההוכחה עוקבת אחרי הוכחת משפט 3 כמעט מילה במילה; שתי הנקודות שמשתנות הן אלה שפורטו לעיל — הריבוע שנולד בהמרה למכונה סטנדרטית, והצורך בריפוד סולמיות במקום ניפוח מצבים.

הערות מהשיעור

[00:13:34] תוצאות חיוביות מול שליליות. עד השיעור הזה כל מה שהוכחנו הן "תוצאות חיוביות" — הכלות, אלגוריתמים, "אני יכול". בחישוביות ראיתם לראשונה תוצאות שליליות (בעיית העצירה). משפט ההיררכיה הוא הפעם הראשונה שרואים תוצאה שלילית **ברמת הסיבוכיות**. תוצאות שליליות קשות בהרבה, ותראו מעט מאוד כאלה בכל התואר. **כלל אצבע שנאמר במפורש:** כשצריך להוכיח תוצאה שלילית — נסו להישען על תוצאה שלילית שכבר יש, במקום לבנות אחת מאפס.

[00:31:45] מה זה "מוכל ממש". $A \subsetneq B$ פירושו $A \subseteq B$ **וגם** $B \not\subseteq A$. שימו לב ש"מוכל ממש" לא אומר "הרבה יותר גדול" — הוא אומר רק "יותר". שאלת סטודנטית שהובילה להבהרה הזו.

[01:15:51] איך קוראים הוכחה בסדר הגודל הזה — טכניקת ה-expand/collapse. בסופו של דבר ההוכחה מצטמצמת ל: "נתבונן ב-$\hat{M}_f$ ובקבוע c; היא מכריעה את S_f במקום $\leq c \cdot f$; לכן $S_f \in \mathrm{DSpace}(f)$." זה המבנה, והוא סטנדרטי לגמרי. אחר כך פותחים בנפרד את "למה היא מכריעה" ואת "למה זה המקום". נכנסים ויוצאים מהרמות כמה פעמים — מפרקים ומרכיבים. **זו ההוכחה הארוכה הראשונה מתוך שתיים בקורס.**

[01:44:47] מה לעשות כשנתקעים. אל תיתקעו על מעבר שלא הבנתם ותעצרו. הניחו שהמעבר נכון, המשיכו הלאה, וסמנו נקודה. בפעם הראשונה יהיו חמש־שש נקודות כאלה; בפעם השנייה שלוש; ובסוף מגיעים לשעת קבלה עם "את המעבר הזה ואת המעבר הזה לא הבנתי" — במקום "לא הבנתי כלום". זו תחושה אחרת לגמרי, ופחות תסכול.

[01:19:37] מתי כן להוכיח בשלילה. המרצה: "אני לא אוהב שמכניסים הוכחה בשלילה לכל מקום סתם. אבל כשאני רוצה להוכיח ש**משהו לא קורה** — זו הוכחה בשלילה par excellence." חלק (ב2) הוא בדיוק המקרה הזה.

[01:55:26] מה נדרש למבחן. לשחזר את כל ההוכחה מאפס — לא. להכיר את ההוכחה ולהגיב לשינויים בה ("אם אשנה את הרכיב הזה, איך ההוכחה משתנה?") — **כן, בהחלט**. זו הצהרה מפורשת: צריך להכיר את ההוכחה הזאת למבחן.

[00:36:14] אל תחפשו מאיפה השפה S_f צצה. בהרצה הראשונה השפה "הונחתה" בכוונה, והמרצה ביקש לשאול רק "האם ההגדרה ברורה" ולא "מאיפה היא באה". ההערה שכן ניתנה: הדבר מריח חישוביות — המכונה שדוחה את הקידוד של עצמה היא בדיוק "הקלקול" שהכנסנו תמיד בלכסון; רכיב המקום הוא מה שקושר את זה לשייכות ל-$\mathrm{DSpace}(f)$. ההסבר המלא (למה השפה הזאת ולמה החלוקה ב-$\lg|\Gamma_M|$) ניתן בהרצה המקבילה ומופיע כאן בסעיף ההגדרות.

[01:02:27] מלכודת בחשבון המקום. כשמחשבים כמה מקום מונה תופס — **לא מספיק** לספור את המקום שהמונה תופס בסוף; צריך לספור גם את המקום שנדרש כדי **לחשב** את הערך שנכתב. זו בדיוק הסיבה לתנאי הישימות במקום, ולכן זו נקודה שקל מאוד להחמיץ.

[01:38:12] למה דווקא מצבי סרק. שאלת סטודנטית: אפשר להוסיף תווים לאלפבית כדי לנפח את הקידוד? **לא** — זה משנה את Γ_M, ואז המכנה $\lg|\Gamma_M|$ בהגדרת השפה זז יחד איתו, וכל הטריק קורס. מצבי סרק מגדילים את טבלת המעברים ולכן את אורך הקידוד, אבל אינם נוגעים באלפבית.
[01:23:22] למה מותר לבחור $\varepsilon = \frac{1}{c\lg|\Gamma_{M_g}|}$. כי בנקודה שבה אנחנו בהוכחה, c ו-M_g **כבר ידועים לנו** — הם התקבלו מההנחה בשלילה. זהו שימוש נכון בסדר של המשתנים: כל פעם שמקבלים משתנה חדש מותר להשתמש בו הלאה.

פערים בין הסיכום להקלטה
מקור: שתי ההקלטות. **הפער:** המשימה תיארה אותן כ"שיעור אחד שפוצל לשני סרטונים", אך למעשה מדובר בשתי מסירות עצמאיות ומלאות של אותו שיעור בידי שני מרצים שונים ומול קהלי סטודנטים שונים (סרטון Eqk3K9frjx8 מול סרטון 2coiPuG7Pe4). הסרטון השני **חוזר מההתחלה** על משפט ההיררכיה במקום, לא ממשיך את הראשון. **ההכרעה:** שתיהן סומנו `coverage: full`; הגוף מאחד את החומר, ומעדיף את ההסבר המפורט יותר בכל נקודה. יש לוודא במניפסט שאין הנחה שגויה שהן חצאים משלימים.
מקור: ההקלטה השנייה. **הפער:** ההסבר האינטואיטיבי המלא — למה בכלל S_f היא השפה הנכונה, איך התנאי השני מפצל את עולם המכונות, ומאיפה בדיוק צומחת החלוקה ב-$\lg|\Gamma_M|$ (מהמדדים של המכונה האוניברסלית) — **אינו מופיע בסיכום כלל**, וגם בהקלטה הראשונה הוא הוזכר בשתי מילים בלבד. **ההכרעה:** שוחזר במלואו והוכנס לסעיף ההגדרות (הגדרה 4), כי בלעדיו ההוכחה נראית שרירותית.
מקור: ההקלטה השנייה. **הפער:** ההסבר על ההבדל בהוכחת משפט ההיררכיה בזמן — שהחלוקה שם היא ב-$|\langle M\rangle|$ ולא ב-$\lg|\Gamma_M|$, ושלכן טריק מצבי הסרק נכשל ויש לרפד את הקלט בסולמיות — אינו בסיכום. **ההכרעה:** הוכנס כתת־סעיף במשפט 4, כי זהו בדיוק תרגיל הבית שניתן.
מקור: ההקלטה הראשונה. **הפער:** הפירוק המלא של הכיוון "$\langle M\rangle \notin S_f \Rightarrow M_f$ דוחה" לשלושה מקרים, ובפרט המקרה שבו M **אינה עוצרת** (ולכן "אינה דוחה" אך גם "אינה מקבלת"), נעשה רק בהקלטה השנייה; ההקלטה הראשונה קיצרה אותו, והסיכום מציג רק את הכיוון ההפוך. **ההכרעה:** הובא הפירוט המלא, כולל השימוש בקונטרפוזיטיב של חסם ספירת הקונפיגורציות.
מקור: הסיכום, עמוד 6. **הפער:** בשרשרת המסקנה נרשם $\mathrm{DTime}(2^n) \subsetneq \mathrm{DTime}(2^{4n})$ ולידו הערה בכחול שמחליפה את $4n$ ב-n^2, כך שקשה לקרוא האם החוליה היא 2^{4n} או 2^{n^2}. **ההכרעה:** מתמטית שתי החוליות נכונות ושתיהן נחוצות — 2^{4n} הוא מה שמשפט ההיררכיה נותן (f^2 עבור $f=2^{2n}$), ו-2^{n^2} הוא הצעד הנוסף שמכניס אותנו ל-EXP. הוצגו שתיהן בנפרד. ההקלטה [02:09:24] מאשרת בדיוק את הסדר הזה.
מקור: התמלול האוטומטי. **הפער:** הכתוביות משבשות באופן שיטתי את הפונקציות: `nב 2` עבור 2^n, `שn 2 n` של `f` עבור $f(n)=2^{2n}$, `גm גם הogסל` עבור $\lg|\Gamma_M|$, `סף / עסף` עבור S_f, `ספ י סdד` עבור DSpace. **ההכרעה:** כל החסמים אומתו מול הסיכום בכתב יד, לא מול הכתוביות; הסיכום הוא הקובע בכל חוסר התאמה נומרי.

מקור: הסיכום, עמוד 1 ועמוד 2. **הפער:** שתי הערות שוליים בכחול אינן קריאות במלואן — האחת ליד תנאי (2) של ההגדרה "ישימה במקום" (משהו בנוסח "המקום שצריך לחשב אותה לא גדול משמעותית מהפלט; הערת O — מותר גם קצת יותר מקום מהפלט"), והשנייה ליד סימן ה-$\leq$ בהגדרת S_f (משהו בנוסח "אולי כדאי לתת למכונה קצת יותר; מותר גם שוויון"). **ההכרעה:** התוכן המהותי של שתיהן שוחזר מההקלטה [00:21:39] ומופיע בגוף; המילה־במילה לא שוחזרה ואינה נדרשת.

מקור: הסיכום, עמוד 7. **הפער:** העמוד כמעט ריק — רק כותרת בכחול (שאותיותיה מטושטשות) ושתי שורות: $\mathrm{P} \subseteq \mathrm{PSPACE} \subseteq \mathrm{EXP}$, $\mathrm{P} \subsetneq \mathrm{EXP}$, והערה "אחת משתי ההכלות היא הכלה ממש. לא יודעים איזו". **ההכרעה:** התוכן ברור ומאושר משתי ההקלטות; נוסח כמשפט 6 עם הצדקה מלאה.

מקור: ההקלטה הראשונה [01:04:09] וההקלטה השנייה [00:49:15]. **הפער:** שמות הקבועים בחשבון המקום שונים בין המסירות (C_1, C_2, C_3 מול α, β, γ), וגם הסידור שונה מעט. **ההכרעה:** אומצה מערכת הסימונים של הסיכום ($\alpha + 3\beta + 3\gamma$, ואז $\hat{c}$ להמרה ו-$c = \hat{c}(\alpha + 3\beta + 3\gamma)$), כדי שהקורא יוכל לעקוב מול הדפים.

מקור: הסיכום. **הפער:** הסיכום אינו כולל את נגד־הדוגמה $\{1\}, \{2\}, \{1, 2\}$ להתנהגות "הכלה ממש" תחת איחוד, ואינו כולל את ההסבר מדוע חייבים לעבור דרך מחלקות עדינות. **ההכרעה:** הוכנס מההקלטות (שתיהן הביאו אותו), כי זו המלכודת המרכזית ביישום המשפט.

סיכום ונקודות למבחן

מה חייבים לזכור בעל־פה

הגדרת ישימות במקום/בזמן: קיימת M מעל $\{0\}$ עם $M(0^n) = 0^{f(n)}$ וגם $\mathrm{space}_M(0^n) = O(f(n))$ (או time).

משפט ההיררכיה במקום: $g = o(f)$, f ישימה במקום, f סופר־לינארית $\Rightarrow \mathrm{DSpace}(g) \subsetneq \mathrm{DSpace}(f)$.

משפט ההיררכיה בזמן: אותם תנאים עם ישימות **בזמן** $\Rightarrow \mathrm{DTime}(g) \subsetneq \mathrm{DTime}(f^2)$. **הריבוע רק בזמן.**

השפה: $S_f = \{\langle M \rangle \mid M \text{ rejects } \langle M \rangle \ \wedge\ \mathrm{space}_M(\langle M \rangle) \leq f(|\langle M \rangle|)/\lg|\Gamma_M|\}$.

חסם הקונפיגורציות: $\mathrm{time}_M(x) \leq 2^{\lg|Q_M| + \lg|\Gamma_M| \cdot \mathrm{space}_M(x) + \lg \mathrm{space}_M(x)}$, ובתנאי השפה זה מצטמצם ל-$2^{3f(|\langle M \rangle|)}$.

המסקנות: $\mathrm{PSPACE} \subseteq \mathrm{EXP}$; $\mathrm{P} \subsetneq \mathrm{EXP}$; ולכן אחת מ-$\mathrm{P} \subseteq \mathrm{PSPACE}$, $\mathrm{PSPACE} \subseteq \mathrm{EXP}$ היא ממש — לא ידוע איזו.

היכן כל תנאי נכנס — טבלת שליטה

התנאי	היכן בדיוק הוא משמש
f ישימה במקום	רק בחשבון המקום: כדי ש-M_f תוכל **לחשב ולכתוב** את שני המונים בתוך $O(f)$ מקום (הקבועים α, β).

התנאי	היכן בדיוק הוא משמש
$f(n) \geq n$ (סופר־לינארית)	פעמיים: לבלוע את $\lVert\langle M\rangle\rVert \leq \lVert Q_M\rVert \lg$ בחשבון הזמן, ולבלוע את $2\lVert\langle M\rangle\rVert$ בחשבון המקום של הסימולציה.
$g = o(f)$	רק בחלק (ב2): כדי לבחור $\varepsilon = \frac{1}{c \lg \lVert\Gamma_{M_g}\rVert}$ ולקבל את n_0 שממנו והלאה אי־השוויון תופס.
$\lVert\Gamma_M\rVert \lg$ במכנה	כדי שהפקטור של האוניברסלית יצטמצם והחסם יהיה $O(f)$ בלתי תלוי ב-M.
מצבי סרק (ולא תווים)	כדי להגדיל את $\lVert\langle M_g\rangle\rVert$ מעל n_0 **בלי** לשנות את Γ שיושב במכנה.

מלכודות סטנדרטיות

קבוע כפלי בחזקה אינו זניח. $2^{2n} \neq \Theta(2^n)$. אי אפשר "להעיף" אותו כמו קבוע כפלי רגיל; מגדילים את החזקה של n באחד ובולעים אותו.

הכלה ממש אינה נשמרת תחת איחוד. לעולם אל תפעילו את משפט ההיררכיה איבר־איבר על מחלקה גסה. עברו דרך שתי מחלקות עדינות באמצע.

"אינה דוחה" $\neq$ "מקבלת". בפיצול המקרים חייבים לטפל גם באפשרות שהמכונה אינה עוצרת.

o קטן ולא O גדול. $f(n) = 2^{n+1}$ מול $g(n) = 2^n$ נכשל, כי היחס שואף ל-$\frac{1}{2}$ ולא ל-0.

המרת מודל. במקום — קבוע כפלי; בזמן — ריבוע. זו הסיבה היחידה ל-f^2 במשפט ההיררכיה בזמן.

גם המקום לחישוב נספר, לא רק המקום שהתוצאה תופסת.

צ׳ק־ליסט: מה סטודנט צריך לדעת לעשות אחרי השיעור

- [ ] לנסח את שני משפטי ההיררכיה במדויק, כולל כל שלושת התנאים ובלי לבלבל בין f ל-f^2.
- [ ] להגדיר את S_f מהזיכרון ולהסביר את התפקיד של כל אחד משני התנאים בהגדרה.
- [ ] לשחזר את בניית M_f (ארבעת השלבים, שני המונים, אונרי מול בינארי) ולהסביר מדוע כל שלב שם.
- [ ] לבצע את חשבון הזמן $\to 2^{3f}$ ואת חשבון המקום $\to (\alpha + 3\beta + 3\gamma)f$, צעד־צעד, בלי לדלג.
- [ ] להסביר היכן בדיוק נכנס כל אחד משלושת התנאים של המשפט (ראו הטבלה).
- [ ] להסביר מדוע מנפחים במצבי סרק ולא באלפבית, ומדוע הטריק הזה נשבר בגרסת הזמן.
- [ ] להוכיח $\mathrm{PSPACE} \subseteq \mathrm{EXP}$ ואת $\mathrm{P} \subsetneq \mathrm{EXP}$ מהתחלה ועד הסוף, כולל השלב שעוקף את בעיית האיחוד.
- [ ] להגיב לשינוי בהוכחה: אם משנים רכיב בהגדרת S_f או בבניית M_f — לזהות איזה שלב בהוכחה נשבר.

שאלות שנשארו פתוחות

עמוד 1 ועמוד 2 בסיכום: שתי הערות שוליים בכחול קריאות רק בחלקן; התוכן שוחזר מן ההקלטות, הניסוח לא.

עמוד 6 בסיכום: בשרשרת המסקנות יש הערה בכחול המחליפה 2^{4n} ב-2^{n²}; שתי החוליות נחוצות ונכונות והובאו בנפרד.

שמות הקבועים שונים בין שתי המסירות (α,β,γ מול C_1,C_2,C_3); אומצה מוסכמת הסיכום.

4 מכונות טיורינג אי-דטרמיניסטיות

מחליפים את פונקציית המעברים בפונקציה לקבוצת החזקה, מגדירים ריצה אפשרית והכרעה אי-דטרמיניסטית (מקבלים אם קיימת ריצה מקבלת, ובלבד שכל הריצות עוצרות), מודדים זמן ומקום כמקסימום על פני הריצות, ומקבלים את המחלקות NTime, NSpace, NP ואת השאלה P מול NP.

ביטחון: high

בקצרה

מוסיפים למודל שינוי **תחבירי אחד בלבד**: פונקציית המעברים מחזירה כעת **קבוצה** של שלשות במקום שלשה יחידה, כלומר $\delta : Q \times \Gamma \to P(Q \times \Gamma \times \{L, R\})$. כל שאר רכיבי המכונה נשארים כשהיו.

השינוי התחבירי הקטן הזה הורס את המושג המרכזי של המודל הקודם: אין יותר "**ה**ריצה של M על x", יש **אוסף הריצות האפשריות** של M על x. כל הסמנטיקה של השיעור נובעת מכך.

תנאי ההכרעה אינו סימטרי, וזו הנקודה שהכי כדאי לזכור: M מכריעה את A באופן אי-דטרמיניסטי אם (א) **בכל** ריצה אפשרית ועל **כל** קלט היא עוצרת, (ב) אם $x \in A$ אז **קיימת** ריצה מקבלת, (ג) אם $x \notin A$ אז **בכל** ריצה היא דוחה. קבלה היא טענת קיום; דחייה ועצירה הן טענות "לכל".

מדדי היעילות הם מקסימום על פני הריצות: $\mathrm{time}_M(x)$ נמדד בריצה אפשרית ארוכה ביותר, ו-$\mathrm{space}_M(x)$ בריצה אפשרית שכותבת בהכי הרבה תאים — **ולא בהכרח באותה ריצה**.

כל הטענות מהמודל הדטרמיניסטי עוברות כמות שהן, וההוכחות משתנות רק ב"מעטפת": קודם "תהא ריצה אפשרית", מוכיחים לגביה, ואז לוקחים מקסימום. המהות של כל הטיעונים — ספירת קונפיגורציות, "בכל צעד כותבים לכל היותר בתא חדש אחד" — לא זזה.

מקבלים את המחלקות $\mathrm{NTime}(f)$, $\mathrm{NSpace}(f)$ ומעליהן NP, NEXP, $NPSPACE$, $NEXPSPACE$, ואת ההכלה הקלה $P \subseteq \mathrm{NP}$ — שנובעת מכך שכל מכונה דטרמיניסטית **היא** מכונה אי-דטרמיניסטית שכל הקבוצות שלה יחידונים.

המודל **אינו** מגדיל את כוח החישוב (מבחינת חישוביות הוא שקול למכונת טיורינג רגילה), אבל הוא עשוי לשנות מהותית את **היעילות** — וכאן נולדת שאלת P מול NP.

אם אתם צריכים רק דבר אחד מהשיעור הזה: המילים "**באופן אי-דטרמיניסטי**" אינן קישוט. הן מסמנות שיש עוד כמת שצריך לטפל בו בכל הוכחה.

רקע ותלויות

השיעור נשען על שיעורים 1–3, ובעיקר על ההגדרות. נחזור על מה שנשתמש בו ממש.

מהשיעור 1: מכונת טיורינג דטרמיניסטית

מכונת טיורינג (חד-סרטית, סטנדרטית) היא

$$M = (Q, q_{start}, F, \Sigma, \Gamma, \delta), \qquad \delta : Q \times \Gamma \longrightarrow Q \times \Gamma \times \{L, R\},$$

כאשר Q קבוצת המצבים הסופית, $q_{start} \in Q$ המצב ההתחלתי, $F \subseteq Q$ קבוצת המצבים הסופיים (במכונת הכרעה $F = \{q_{accept}, q_{reject}\}$), Σ א"ב הקלט, $\Gamma \supseteq \Sigma$ א"ב העבודה הכולל את התו הריק B.

תיקון לסיכום. בעמוד 1 בסיכום נכתב $M = (Q, F, \Sigma, \Gamma, \delta)$ — חמישייה שאין בה מצב התחלתי. בלי q_{start} אי אפשר בכלל לדבר על "הריצה של M על x", ולכן הוספנו אותו. זו אותה השמטה שכבר תוקנה בשיעור 1 (ראו שיעור 1). בהקלטה המקבילה המרצה מנה את הרכיבים ככה: מצב התחלתי, מצב מקבל, מצב דוחה, א"ב, ופונקציית המעברים — כלומר בדיוק אותה הגדרה, בפירוק אחר של F [ב׳ 00:26:23].

מהשיעור 1: מדדי הזמן והמקום

לכל מכונה M וקלט $x \in \Sigma_M^*$:

$\mathrm{time}_M(x)$ — מספר ההפעלות של פונקציית המעברים בריצת M על x;

$\mathrm{space}_M(x)$ — מספר התאים **השונים** שבהם M **כותבת** במהלך הריצה.

שתי ההגדרות האלה מניחות שיש **ריצה אחת**. בדיוק זו ההנחה שתישבר היום.

מהשיעור 2: המחלקות ושתי טענות שנשתמש בהן

$$\mathrm{DTime}(f) = \left\{ A \mid \exists M \, \exists c > 0 : \ M \text{ decides } A \ \wedge \ \forall x : \ \mathrm{time}_M(x) \le c \cdot f(|x|) \right\},$$

ובאותו אופן $\mathrm{DSpace}(f)$ עם space. מעליהן המחלקות הגסות $P = \bigcup_{c \ge 1} \mathrm{DTime}(n^c)$, $\mathrm{EXP} = \bigcup_{c \ge 1} \mathrm{DTime}(2^{n^c})$, $\mathrm{PSPACE} = \bigcup_{c \ge 1} \mathrm{DSpace}(n^c)$.

שתי התוצאות שנשכפל היום:

טענה (מקום חסום בזמן). לכל M ולכל x: $\mathrm{space}_M(x) \le \mathrm{time}_M(x)$. הנימוק: בכל צעד המכונה כותבת בתא אחד לכל היותר, ותא חדש נספר פעם אחת.

טענה (זמן חסום אקספוננציאלית במקום). לכל M קיים $c > 0$ כך שאם M עוצרת על x אז $\mathrm{time}_M(x) \le 2^{c \cdot \mathrm{space}_M(x)}$, עם $c = \lg|Q| + \lg|\Gamma| + 1$.

ההוכחה של השנייה עברה דרך **ספירת קונפיגורציות**: מספר הקונפיגורציות של M שמשתמשות ב-s תאים הוא $|Q| \cdot |\Gamma|^s \cdot s \le 2^{(\lg|Q| + \lg|\Gamma| + 1) \cdot s}$, ומכונה שעושה יותר צעדים מזה חוזרת על קונפיגורציה ולכן אינה עוצרת. **החישוב הזה לא ישתנה היום** — רק העטיפה סביבו (ראו שיעור 2).

מהשיעור 3: משפטי ההיררכיה

$\mathrm{DSpace}(g) \subsetneq \mathrm{DSpace}(f)$ כאשר $g = o(f)$ ו-f ישימה במקום וסופר-לינארית; ובזמן, באותם תנאים, $\mathrm{DTime}(g) \subsetneq \mathrm{DTime}(f^2)$. נשתמש בהם בתרגיל החימום שנפתח בו את סעיף הדוגמאות (ראו שיעור 3).

למה בכלל מודל כזה
השאלה הזאת לא מופיעה בסיכום, אך היא נאמרה במפורש בהקלטה המקבילה [ב׳ 00:24:19]: המחלקה P נתפסת כ"מה שאפשר לפתור ביעילות", ויש **המון** בעיות חשובות שלא יודעים להראות עליהן שהן ב-P. מסתבר שברגע שמרשים למודל להיות אי-דטרמיניסטי, הרבה מאוד מהן פתאום נפתרות בזמן פולינומי. המודל האי-דטרמיניסטי הוא מודל תיאורטי לחלוטין — אף אחד לא בונה מכונה כזאת — אבל הוא בדיוק הכלי שמאפשר לנסח את השאלה "האם הבעיות האלה קשות באמת".

הגדרות
הגדרה 1: מכונת טיורינג אי-דטרמיניסטית
מכונת טיורינג אי-דטרמיניסטית היא בדיוק כמו מכונת טיורינג, פרט לפונקציית המעברים:

$$\delta : Q \times \Gamma \longrightarrow P\big(Q \times \Gamma \times \{L, R\}\big),$$

כאשר $P(\cdot)$ היא **קבוצת החזקה**. כלומר לכל $q \in Q$ ולכל $\alpha \in \Gamma$: בחישוב דטרמיניסטי $\delta(q, \alpha)$ הוא **שלשה אחת**, ובחישוב אי-דטרמיניסטי $\delta(q, \alpha)$ הוא **קבוצה של שלשות**.
אינטואיציה. במצב q כשהראש קורא α, המכונה מסתכלת בקבוצה $\delta(q, \alpha)$ ו"בוחרת" ממנה שלשה אחת ופועלת לפיה. איך היא בוחרת? **אין תשובה** — זה לא חלק מהמודל, ואין פה שום מנגנון פיזיקלי [ב׳ 00:28:25]. המודל רק אומר שכל בחירה כזו היא מהלך לגיטימי.
דוגמה. $\delta(q_1, 1) = \{(q_1, 1, R), (q_2, 1, R)\}$ — שתי אפשרויות: להישאר ב-q_1 או לעבור ל-q_2, בשני המקרים לכתוב 1 ולזוז ימינה.
אי-דוגמה. $\delta(q_1, 1) = \varnothing$ היא לגיטימית לגמרי בהגדרה (הקבוצה הריקה היא איבר של קבוצת החזקה), אבל היא **לא** מתארת "מעבר לדחייה" — היא מתארת מצב שאין ממנו המשך. בקורס הזה נעבוד עם הקונבנציה של הסיכום: תא ריק בטבלה או חץ חסר בסרטוט פירושם מעבר ל-q_{reject} [א׳ 00:15:12], [א׳ 00:41:28].
קונבנציית כתיבה. בטבלת המעברים כותבים בתאים q_{reject} או q_{accept} בקיצור, במקום השלשה המלאה $\{(q_{reject}, \alpha, R)\}$. גם כשכותבים בתא שלשה יחידה בלי סוגריים מסולסלים — זו עדיין קבוצה בת איבר אחד [א׳ 00:14:42].
הגדרה 2: "לא דטרמיניסטי" מול "אי-דטרמיניסטי"
זו הבחנת מינוח שהמרצה הקדיש לה זמן, והיא מופיעה בסיכום בהערה בכתום.
חישוב **דטרמיניסטי**: תוצאת הריצה של האלגוריתם/המכונה היא **פונקציה של הקלט בלבד**. (המרצה עמד על הניסוח "פונקציה של הקלט" ולא "תלויה בקלט" — זה הניסוח המתמטי [א׳ 00:08:49].) שימו לב שמדובר ב"תוצאת ריצה" ולא ב"פלט", כי ייתכן שאין פלט — המכונה עלולה לא לעצור.
not deterministic (בעברית: לא דטרמיניסטי) — כל מודל שבו תוצאת החישוב עשויה להיות תלויה **בגורמים נוספים** מעבר לקלט.
non deterministic (בעברית: אי-דטרמיניסטי) — **המודל הספציפי** שבו בכל צעד בחישוב יכולות להיות מספר אפשרויות למעבר הבא.

דוגמה שמפרידה בין השניים. אלגוריתם אקראי, שזורק מטבע כדי לקבל החלטות, הוא **לא** **דטרמיניסטי** — הפלט תלוי גם בתוצאות המטבע — אבל הוא **אינו** אי-דטרמיניסטי. נלמד מודלים כאלה בהמשך הקורס [א׳ 00:10:57]. כלומר: אי-דטרמיניסטי גורר לא דטרמיניסטי, לא להפך.

הגדרה 3: ריצה אפשרית

בהינתן מכונה אי-דטרמיניסטית M וקלט $x \in \Sigma_M^*$, **ריצה אפשרית** של M על x היא סדרה של שלשות מתוך $Q_M \times \Gamma_M \times \{L, R\}$ ה"מצייתת" לפונקציית המעברים: כל שלשה בסדרה שייכת לקבוצה שפונקציית המעברים מחזירה בצעד המתאים.

באופן מדויק: אם לפני הצעד ה-i המכונה נמצאת במצב q (המצב שברכיב הראשון של השלשה ה-$(i-1)$), ובצעד הראשון (q_{start}) והראש קורא את התו α שנמצא כרגע בתא שמתחתיו, אז השלשה ה-i חייבת להיות איבר של $\delta(q, \alpha)$. הסדרה עשויה להיות סופית — ואז היא מסתיימת במצב סופי — או אינסופית.

> **הערה:** בסיכום נכתב בקיצור "כל שלשה שייכת לקבוצה שפונקציית המעברים מחזירה על השלשה הקודמת". זה קיצור נוח אבל לא מדויק: δ אינה מקבלת שלשה אלא זוג (מצב, תו שמתחת לראש), והתו שמתחת לראש נקבע מתוכן הסרט ומיקום הראש, לא מתוך השלשה הקודמת. הפירוט המדויק כאן.

מינוח נוסף (מההקלטה המקבילה). סדרת הבחירות שהמכונה עושה במהלך הריצה נקראת **תסריט** **ריצה**, וכל תסריט ריצה מתאר ריצה אפשרית אחת [ב׳ 00:31:07]. זה שם נוח לחשוב איתו: הקלט קובע מה המכונה **רואה**, והתסריט קובע מה היא **בוחרת**.

ההבדל הסמנטי המרכזי. במודל הדטרמיניסטי, בהינתן M ו-x, יכולתי לדבר על **הריצה** של M על x — ביידוע. עכשיו אני יכול לדבר רק על **אוסף הריצות האפשריות** של M על x. זה כל ההבדל, וממנו נובע כל השאר [א׳ 00:25:29].

נקודה עדינה. חלק מהריצות האפשריות עוצרות וחלק לא — **על אותו קלט עצמו**. נראה את זה מיד בדוגמה 1.

הגדרה 4: הכרעה באופן אי-דטרמיניסטי

תהא A שפה ותהא M מכונה אי-דטרמיניסטית מעל אותו א"ב, $\Sigma_M = \Sigma_A$. נאמר כי M **מכריעה את A באופן אי-דטרמיניסטי** כאשר:

לכל $x \in \Sigma_M^*$ ובכל ריצה אפשרית של M על x — M עוצרת;

לכל $x \in \Sigma_M^*$: אם $x \in A$ אז **קיימת** ריצה אפשרית של M על x המסתיימת במצב מקבל;

לכל $x \in \Sigma_M^*$: אם $x \notin A$ אז **בכל** ריצה אפשרית של M על x — M דוחה.

ניסוח שקול. בהינתן תנאי 1, אפשר לאחד את 2 ו-3 לכדי

$$x \in A \iff \exists\, \rho \text{ a possible run of } M \text{ on } x \text{ ending in } q_{accept}.$$

הכיוון $\Rightarrow$ הוא תנאי 2; הכיוון $\Leftarrow$ הוא **הקונטרהפוזיציה** של תנאי 3 (אם קיימת ריצה מקבלת, אז לא נכון שכל הריצות דוחות, ולכן $x \in A$) [א׳ 00:32:39], [ב׳ 00:43:09]. בסיכום ובהוכחות נעדיף את הפיצול לשני תנאים, כי ההוכחה ממילא מתפצלת לשני כיוונים.

אינטואיציה. התנאי אינו סימטרי בין קבלה לדחייה, וזה מכוון. קבלה זולה — מספיק **עד אחד** מוצלח מבין כל הריצות. דחייה יקרה — צריך **שכל** העדים ייכשלו. אפשר לחשוב על זה כך: המכונה "מנחשת" מסלול, והשפה היא אוסף הקלטים שעבורם קיים ניחוש מוצלח.

אי-דוגמה חשובה. מכונה שעל קלט אחד יש לה ריצה מקבלת **וגם** ריצה דוחה עדיין יכולה להכריע שפה — ואפילו נראה כזו מיד. מה שאסור זה ריצה שאינה עוצרת. המרצה הדגיש: "קיימת עליו גם ריצה שתסתיים במצב דוחה, אבל לא אכפת לי — זו ההגדרה, ואין מה להתווכח עם הגדרה" [א׳ 00:45:46].

מגבלת המודל. במודל האי-דטרמיניסטי נעסוק **רק במכונות הכרעה**. יש הגדרה גם למכונת חישוב אי-דטרמיניסטית, אבל היא מסובכת יותר ולא נעסוק בה [א׳ 00:24:53], [ב׳ 00:44:13].

הדגשה שהמרצה חזר עליה. תמיד לכתוב "מכריעה באופן אי-דטרמיניסטי", גם אם זה נשמע מיותר (מכונה אי-דטרמיניסטית ממילא לא יכולה להכריע אחרת). זה מזכיר לכם שיש בהגדרה תנאי נוסף שצריך לטפל בו [א׳ 00:27:02].

הגדרה 5: מדדי יעילות במודל האי-דטרמיניסטי

תהא M מכונה אי-דטרמיניסטית ויהי $x \in \Sigma_M^*$. נגדיר:

$\mathrm{time}_M(x)$ — מספר ההפעלות של פונקציית המעברים ב**ריצה אפשרית ארוכה ביותר** של M על x;

$\mathrm{space}_M(x)$ — מספר התאים השונים שבהם M כותבת ב**ריצה אפשרית שבה M כותבת בהכי הרבה תאים**.

למה לא ביידוע. בשתי ההגדרות כתוב "ריצה אפשרית ארוכה ביותר" ולא "הריצה הארוכה ביותר" — ייתכנו כמה ריצות שונות שכולן ארוכות ביותר [א׳ 00:58:30]. המדד עצמו, כמובן, מוגדר היטב: הוא המקסימום.

שתי מלכודות.

אם על x יש ריצה שעוצרת **ויש** ריצה שאינה עוצרת, אז $\mathrm{time}_M(x) = \infty$, כי המקסימום נלקח על פני **כל** הריצות [א׳ 01:00:03].

המקסימום בזמן והמקסימום במקום **אינם בהכרח מושגים באותה ריצה**. ייתכנו ריצה ארוכה שכותבת במעט תאים וריצה קצרה שכותבת בהרבה. אסור להניח שמדובר באותה ריצה [א׳ 01:22:01], [ב׳ 00:53:53].

למה מקסימום ולא ממוצע או מינימום. התשובה הכנה שניתנה בכיתה: כי כך הוגדר, ואנחנו עובדים לפי ההגדרה. הרציונל שמאחורי ההגדרה הוא התפיסה הרווחת במדעי המחשב של **worst case** [א׳ 01:00:34].

הגדרה 6: המחלקות $\mathrm{NTime}(f)$ ו-$\mathrm{NSpace}(f)$

תהא $f : \mathbb{N} \to \mathbb{N}$. נגדיר:

$$\mathrm{NTime}(f) = \Big\{ A \;\Big|\; \exists M \; \exists c > 0 : \; M \text{ decides } A \text{ nondeterministically } \wedge \; \forall x \in \Sigma_M^* : \; \mathrm{time}_M(x) \le c \cdot f(|x|) \Big\}$$

$$\mathrm{NSpace}(f) = \Big\{ A \;\Big|\; \exists M\, \exists c > 0 :\ M \text{ decides } A \text{ nondeterministically } \wedge\ \forall x \in \Sigma_M^* :\ \mathrm{space}_M(x) \le c \cdot f(|x|) \Big\}$$

ה-N הוא קיצור ל-**Non deterministic**, בדיוק כמו ש-D ב-DTime הוא **Deterministic** [ב׳ 01:09:14].

איפה בדיוק ההבדל מההגדרה הדטרמיניסטית. ההגדרה נראית זהה, וזה בסדר — אבל שני דברים משתנים ושניהם מוסתרים [א׳ 01:17:24]:

"מכריעה את A" הוחלף ב"מכריעה את A **באופן אי-דטרמיניסטי**", כלומר שלושת התנאים של הגדרה 4 ולא ההכרעה הדטרמיניסטית;

$\mathrm{time}_M(x)$ ו-$\mathrm{space}_M(x)$ **מחביאים מקסימום** על פני ריצות אפשריות. זה כבר לא מדד של ריצה אחת.

דוגמה. $A = \{x \in \{0,1\}^* \mid \exists y :\ x = 0y1\} \in \mathrm{NTime}(n)$ — נוכיח בהמשך שהמכונה מדוגמה 2 מכריעה אותה באופן אי-דטרמיניסטי, וכל ריצה שלה אורכה $\le |x| + 1$, כלומר $c = 2$ ו-$f(n) = n$ מתאימים.

הגדרה 7: המחלקות הגסות האי-דטרמיניסטיות

$$\mathrm{NP} = \bigcup_{c \ge 1} \mathrm{NTime}(n^c), \qquad \mathrm{NEXP} = \bigcup_{c \ge 1} \mathrm{NTime}\left(2^{n^c}\right),$$

$$NPSPACE = \bigcup_{c \ge 1} \mathrm{NSpace}(n^c), \qquad NEXPSPACE = \bigcup_{c \ge 1} \mathrm{NSpace}\left(2^{n^c}\right).$$

כמו במודל הדטרמיניסטי, שייכות לאיחוד היא **טענת קיום**: $A \in \mathrm{NP}$ פירושו שקיים $c \ge 1$ שעבורו $A \in \mathrm{NTime}(n^c)$, וכשמוכיחים שייכות ל-$\mathrm{NP}$ צריך "לקלף" קודם את הקיים הזה.

משפטים והוכחות

משפט 1: המכונה מדוגמה 1 אינה מכריעה אף שפה

תהא M המכונה מדוגמה 1 (הטבלה המלאה מופיעה בסעיף הדוגמאות; הרכיב הקריטי הוא $\delta(q_2, B) = \{q_{accept}, (q_2, B, R)\}$). אז **אין** שפה A ש-M מכריעה באופן אי-דטרמיניסטי.

הוכחה. די להראות שתנאי 1 בהגדרה 4 נכשל, כלומר:

$$\exists\, x \in \Sigma_M^*\ \exists\, \rho \text{ a possible run of } M \text{ on } x \text{ that never halts.}$$

ניקח $x = 0001$. נתבונן בסדרה האינסופית

$$(q_1, 0, R), (q_1, 0, R), (q_1, 0, R), (q_2, 1, R), (q_2, B, R), (q_2, B, R), (q_2, B, R), \ldots$$

נבדוק שזו אכן ריצה אפשרית: השלשה הראשונה שייכת ל-$\delta(q_{start}, 0) = \{(q_1, 0, R)\}$; שתי הבאות שייכות ל-$\delta(q_1, 0) = \{(q_1, 0, R)\}$; הרביעית שייכת ל-$\delta(q_1, 1) = \{(q_1, 1, R), (q_2, 1, R)\}$; ומכאן ואילך הראש נמצא מימין לקלט וקורא B, והמכונה במצב q_2, ולכן כל שלשה שייכת ל-$\delta(q_2, B) = \{q_{accept}, (q_2, B, R)\}$. אחרי כל צעד כזה הראש זז ימינה וקורא שוב B והמצב נשאר q_2, ולכן אפשר להמשיך כך לנצח.

מצאנו קלט שעליו קיימת ריצה אפשרית שאינה עוצרת, ולכן תנאי 1 אינו מתקיים עבור אף שפה A. ■

> **הערה:** שימו לב לניסוח המדויק, שהמרצה התעכב עליו בכיתה [א׳ 00:34:13]: קודם מציגים את הקלט ורק אחר כך את הריצה. "קיימת ריצה על קלט" בלי להציג את הקלט הוא ניסוח חסר משמעות, כי ריצה מוגדרת רק ביחס לקלט מסוים.

למה זה מעניין. זו בדיוק הסיבה שתנאי 1 קיים בהגדרה. במודל האי-דטרמיניסטי אפשר "לברוח" מהכרעה לא רק בכך שהריצה נתקעת, אלא בכך שיש **ענף אחד** מתוך אינסוף ענפים שלא עוצר — גם אם על אותו קלט יש ענף שעוצר ומקבל.

משפט 2: המכונה המתוקנת מכריעה את $A = \{0y1\}$

תהא M המכונה שמתקבלת מדוגמה 1 על ידי **מחיקת המעבר** (q_2, B, R), כלומר $\delta(q_2, B) = \{q_{accept}\}$. נסמן

$$A = \left\{ x \in \{0,1\}^* \;\middle|\; \exists\, y \in \{0,1\}^* :\; x = 0y1 \right\}$$

— שפת כל המחרוזות מעל $\{0,1\}$ שמתחילות ב-0 ומסתיימות ב-1. אז M מכריעה את A באופן אי-דטרמיניסטי.

הוכחה. נבדוק את שלושת התנאים של הגדרה 4.

תנאי 1 (עצירה בכל ריצה אפשרית). יהי $x \in \Sigma_M^*$ ותהא ρ ריצה אפשרית של M על x. נבחין בשתי עובדות על המכונה:

בכל אחת משלשות המעבר של M הכיוון הוא R, כלומר בכל צעד הראש **זז ימינה**;

כאשר הראש קורא B, בכל אחד משלושת המצבים q_{start}, q_1, q_2 המכונה עוברת למצב סופי: $\delta(q_{start}, B) = \{q_{reject}\}$, $\delta(q_1, B) = \{q_{reject}\}$, $\delta(q_2, B) = \{q_{accept}\}$.

מכיוון שהראש מתחיל בתא הראשון של הקלט וזז ימינה בכל צעד, אחרי $|x|$ צעדים לכל היותר הוא נמצא בתא הראשון שמימין לקלט וקורא B (אם לא עצר קודם), ובצעד שאחריו המכונה נכנסת למצב סופי. לכן ρ עוצרת אחרי **לכל היותר** $|x| + 1$ **צעדים**. מכיוון ש-ρ הייתה ריצה אפשרית שרירותית, בכל ריצה אפשרית M עוצרת.

> **תיקון:** בסיכום נכתב "לא יותר מ-$|x|$ צעדים", וגם בהרצאה נאמר "בדיוק אורך של x צעדים" [א׳ 00:40:57]. זו טעות של אחד: הצעד שבו הראש קורא את התו הריק ועובר למצב סופי הוא הפעלה נוספת של δ. הסיכום עצמו מדגים זאת — הריצה שלו על $x = 0001$ (אפשרות 1) מונה ארבע שלשות ואז q_{reject}, כלומר חמש הפעלות של δ עבור $|x| = 4$. החסם הנכון הוא $|x| + 1$. הוא כמובן אינו משנה דבר במסקנות.

תנאי 2 ($x \in A \Rightarrow$ קיימת ריצה מקבלת). נניח $x \in A$. אז קיים $y \in \{0,1\}^*$ כך ש-$x = 0y1$. נסמן $y = a_1 a_2 \cdots a_n$ כאשר $a_1, \ldots, a_n \in \{0,1\}$ (ייתכן $n = 0$, ואז $x = 01$). נתבונן בסדרת השלשות

$$(q_1, 0, R),\ (q_1, a_1, R),\ (q_1, a_2, R),\ \ldots,\ (q_1, a_n, R),\ (q_2, 1, R),\ q_{accept}.$$

נוודא שזו ריצה אפשרית:
הצעד הראשון: המכונה ב-q_{start} והראש קורא את התו הראשון של x, שהוא 0; ואכן $(q_1, 0, R) \in \delta(q_{start}, 0)$.
הצעדים $2, \ldots, n+1$: המכונה ב-q_1 והראש קורא את a_i. אם $a_i = 0$ אז $(q_1, 0, R) \in \delta(q_1, 0)$; ואם $a_i = 1$ אז $(q_1, 1, R) \in \delta(q_1, 1)$, כי $\delta(q_1, 1)$ מכילה **שתי** שלשות ואנחנו בוחרים את זו שנשארת ב-q_1. כאן, ורק כאן, אנחנו מנצלים את האי-דטרמיניזם.
הצעד $n+2$: המכונה ב-q_1 והראש קורא את התו האחרון של x, שהוא 1; בוחרים את השלשה השנייה, $(q_2, 1, R) \in \delta(q_1, 1)$.
הצעד האחרון: המכונה ב-q_2 והראש נמצא מימין לקלט וקורא B; ואכן $q_{accept} \in \delta(q_2, B)$.
זו ריצה אפשרית של M על x המסתיימת במצב מקבל, כנדרש.
תנאי 3 ($x \notin A \Rightarrow$ כל ריצה דוחה). נניח $x \notin A$. אז x אינו מתחיל ב-0 **או** x אינו מסתיים ב-1. נפצל לשני מקרים (לא בהכרח זרים — די בכך שהם מכסים).
מקרה 1: x אינו מתחיל ב-0. תהא ρ ריצה אפשרית של M על x. בצעד הראשון המכונה נמצאת ב-q_{start} והראש קורא את התו הראשון, שהוא 1 או B (אם $x = \varepsilon$). בשני המקרים $\delta(q_{start}, \cdot) = \{q_{reject}\}$, ולכן כבר בצעד הראשון M דוחה את x.
מקרה 2: x אינו מסתיים ב-1. תהא ρ ריצה אפשרית של M על x (המקרה $x = \varepsilon$ כבר טופל, ולכן נניח $|x| \geq 1$).
אם ρ אינה מגיעה אל q_2: מכיוון שבכל צעד הראש זז ימינה, בסופו של דבר הראש קורא B כשהמכונה נמצאת ב-q_{start} או ב-q_1, ובשני המצבים המעבר על B הוא ל-q_{reject}. לכן ρ מסתיימת במצב דוחה.
אם ρ מגיעה אל q_2: המעבר היחיד שנכנס ל-q_2 הוא $(q_2, 1, R) \in \delta(q_1, 1)$, ולכן בצעד הקודם הראש קרא 1. מכיוון שהנחנו ש-x אינו מסתיים ב-1, אותו 1 אינו התו האחרון של x, ולכן בצעד הבא הראש **אינו** קורא B אלא תו קלט — 0 או 1. מהטבלה, $\delta(q_2, 0) = \delta(q_2, 1) = \{q_{reject}\}$, ולכן ρ מסתיימת במצב דוחה.
בשני המקרים כל ריצה אפשרית של M על x דוחה. משלושת התנאים נובע ש-M מכריעה את A באופן אי-דטרמיניסטי. ■

הערה על מבנה ההוכחה [א׳ 00:48:00], [א׳ 00:53:44]. שני דברים שהמרצה עמד עליהם:
אל תקצרו במקרה 1 בטענה "יש רק ריצה אפשרית אחת ולכן סיימנו". זה נכון אבל זו הליכה על חבל דק: ההגדרה דורשת "לכל ריצה", ולכן פותחים ב"תהא ריצה אפשרית" ומוכיחים לגביה. המבנה הוא מה ששומר עליכם מטעויות.
אל תניחו בשלילה כשאין צורך. סטודנט הציע להניח $x \notin A$ ובשלילה שקיימת ריצה מקבלת; המרצה השיב שאם רוצים ללכת בכיוון הזה, פשוט מוכיחים ישירות את הגרירה "קיימת ריצה מקבלת $x \in A \Rightarrow$" (הניסוח עם "אם ורק אם"), בלי לעטוף אותה בשלילה. שתי הדרכים שקולות לוגית ולגיטימיות לגמרי; בחרו את זו שנוח יותר להוכיח [א׳ 00:46:16].

משפט 3: מקום חסום בזמן במודל האי-דטרמיניסטי
לכל מכונה אי-דטרמיניסטית M ולכל $x \in \Sigma_M^*$ מתקיים

$$\mathrm{space}_M(x) \;\le\; \mathrm{time}_M(x).$$

הוכחה. שני האגפים הם מקסימומים על פני קבוצות ריצות **שונות**, ולכן אי אפשר להשוות ריצה לריצה. הטכניקה: חוסמים כל ריצה בנפרד באגף הימני, ואז לוקחים מקסימום.
תהא ρ ריצה אפשרית כלשהי של M על x. נסמן
t — מספר הצעדים ש-M מבצעת בריצה ρ על x;
s — מספר התאים השונים ש-M כותבת בהם בריצה ρ על x.
(היינו חייבים סימונים חדשים דווקא משום שאי אפשר להשתמש ב-time_M וב-space_M — אלה מדדים של המכונה, לא של ריצה בודדת.)
$s \le t$. בכל צעד בריצה ρ המכונה כותבת בתא אחד לכל היותר, ולכן מספר התאים השונים שנכתבו בהם אינו עולה על מספר הצעדים. זו בדיוק ההבחנה מהמודל הדטרמיניסטי, ללא שינוי.
$t \le \mathrm{time}_M(x)$. לפי הגדרה 5, $\mathrm{time}_M(x)$ הוא המקסימום של מספר הצעדים על פני כל הריצות האפשריות, ו-ρ היא אחת מהן.
משני אלה, $s \le \mathrm{time}_M(x)$.
הראינו זאת עבור ריצה אפשרית שרירותית ρ, כלומר: **בכל** ריצה אפשרית של M על x, מספר התאים השונים שנכתבו בהם חסום על ידי $\mathrm{time}_M(x)$ — שהוא ביטוי **שאינו תלוי ב-**ρ. בפרט זה נכון גם עבור ריצה אפשרית שבה M כותבת בהכי הרבה תאים, ומספר התאים בריצה זו הוא בדיוק $\mathrm{space}_M(x)$. לכן $\mathrm{space}_M(x) \le \mathrm{time}_M(x)$. ■
מה בדיוק השתנה מהמודל הדטרמיניסטי. רק המעטפת [ב׳ 01:03:32]. הליבה — "בכל צעד כותבים בתא אחד לכל היותר" — זהה מילה במילה. מה שנוסף הוא ש**לפני** הליבה כותבים "תהא ריצה אפשרית" ונותנים סימנים למדדים של הריצה הספציפית, ו**אחרי** הליבה לוקחים מקסימום על אי-שוויון שהאגף הימני שלו כבר לא תלוי בריצה. זה התבנית של כל ההוכחות בשיעור הזה.
משפט 4: זמן חסום אקספוננציאלית במקום
לכל מכונה אי-דטרמיניסטית M קיים קבוע $c > 0$ כך שלכל $x \in \Sigma_M^*$:

$$\text{if } M \text{ halts on } x \text{ in every possible run, then} \quad \operatorname{time}_M(x) \;\le\; 2^{c\cdot \operatorname{space}_M(x)}.$$

הקבוע הוא $c = \lg|Q| + \lg|\Gamma| + 1$, כמו במודל הדטרמיניסטי.
איפה ההבדלים מהטענה המקבילה בשיעור 2 [א׳ 01:03:45]. שלושה, אחד גלוי ושניים סמויים:
גלוי: ההנחה היא "M עוצרת בכל ריצה אפשרית" ולא "M עוצרת על x". זו הנחה חזקה יותר, והיא הכרחית — ראו את ההערה בסוף ההוכחה.
סמוי: $\operatorname{time}_M(x)$ הוא מקסימום.
סמוי: $\operatorname{space}_M(x)$ הוא מקסימום — ולא בהכרח באותה ריצה.
הוכחה. תהא ρ ריצה אפשרית כלשהי של M על x. נסמן ב-t את מספר הצעדים ש-M מבצעת ב-ρ, וב-s את מספר התאים השונים ש-M כותבת בהם ב-ρ.
שלב א — ספירת קונפיגורציות. קונפיגורציה של M מורכבת ממצב, מתוכן החלק הרלוונטי של הסרט וממיקום הראש. אם בריצה ρ נכתב ב-s תאים שונים, מספר הקונפיגורציות שיכולות להופיע בריצה זו הוא לכל היותר

$$|Q| \cdot |\Gamma|^{s} \cdot s \;=\; 2^{\lg|Q| + s\cdot\lg|\Gamma| + \lg s} \;\le\; 2^{(\lg|Q| + \lg|\Gamma| + 1)\cdot s},$$

כאשר האי-שוויון האחרון נובע מ-$\lg|Q| \le s\lg|Q|$ ומ-$\lg s \le s$ עבור $s \ge 1$. זהו **בדיוק** החישוב משיעור 2, ללא שינוי כלשהו הנובע מאי-דטרמיניזם [א׳ 01:08:10].
שלב ב — אין חזרה על קונפיגורציה. נטען שבריצה ρ אין שתי קונפיגורציות זהות. נניח בשלילה שיש: הקונפיגורציה C מופיעה ב-ρ בשני זמנים $i < j$. נתבונן בסדרת הבחירות (תסריט הריצה) שהובילה מ-C בזמן i אל C בזמן j. מכיוון שהקונפיגורציה בשני הקצוות זהה, אותה סדרת בחירות עצמה חוקית שוב, ואפשר לחזור עליה שוב ושוב. מתקבלת **ריצה אפשרית אינסופית** של M על x — בסתירה להנחה ש-M עוצרת על x בכל ריצה אפשרית.

> **הערה:** בהרצאה זה נאמר בקיצור, ואף תוקן תוך כדי [א׳ 01:09:13] — המרצה אמר תחילה "אני יודע ש-Q סופית ולכן המכונה אינה חוזרת על אותה קונפיגורציה", עצר ותיקן ל"אני יודע ש-M עוצרת בכל ריצה". הפירוט כאן. שימו לב שזו בדיוק הנקודה שבה ההנחה החזקה יותר משמשת: במודל הדטרמיניסטי חזרה על קונפיגורציה **בריצה שלנו** גוררת מיד שאותה ריצה לא תעצור, כי ההמשך נקבע יחידות. במודל האי-דטרמיניסטי חזרה על קונפיגורציה ב-ρ אינה מונעת מ-ρ עצמה לעצור — היא רק מוכיחה שקיימת **ריצה אחרת** שאינה עוצרת. לכן ההנחה חייבת להיות על **כל** הריצות.

שלב ג — חיבור. מכיוון שכל צעד ב-ρ מוביל לקונפיגורציה חדשה, מספר הצעדים חסום על ידי מספר הקונפיגורציות האפשריות:

$$t \;\le\; 2^{(\lg|Q| + \lg|\Gamma| + 1)\cdot s}.$$

שלב ד — מעבר למדדים. מכיוון ש-s הוא מספר התאים שנכתבו ב-ρ ו-$\operatorname{space}_M(x)$ הוא המקסימום על פני כל הריצות, מתקיים $s \le \operatorname{space}_M(x)$. הפונקציה $u \mapsto 2^{cu}$ עולה, ולכן

$$t \;\le\; 2^{(\lg|Q|+\lg|\Gamma|+1)\cdot \mathrm{space}_M(x)}.$$

שלב ה — מקסימום. האגף הימני אינו תלוי ב-ρ, והאי-שוויון הוכח עבור ריצה אפשרית שרירותית. לכן הוא נכון בפרט עבור ריצה אפשרית ארוכה ביותר, שבה מספר הצעדים הוא $\mathrm{time}_M(x)$:

$$\mathrm{time}_M(x) \;\le\; 2^{(\lg|Q|+\lg|\Gamma|+1)\cdot \mathrm{space}_M(x)}. \qquad \blacksquare$$

מדוע דווקא הכיוון הזה הוכח בכיתה. המרצה בחר בכוונה להוכיח את האי-שוויון הקשה יותר ולהשאיר את $\mathrm{space} \le \mathrm{time}$ כתרגיל [א׳ 01:11:19]; בהקלטה המקבילה הוכח דווקא הקל (משפט 3 כאן), ולכן שני הכיוונים מופיעים בקובץ הזה במלואם.

משפט 5: יחסים בסיסיים בין המחלקות האי-דטרמיניסטיות

תהיינה $f, g : \mathbb{N} \to \mathbb{N}$. אז:

$\mathrm{NTime}(f) \subseteq \mathrm{NSpace}(f)$;

$\mathrm{NSpace}(f) \subseteq \bigcup_{d \ge 1} \mathrm{NTime}\big(2^{d\cdot f}\big)$;

אם $f = O(g)$ אז $\mathrm{NTime}(f) \subseteq \mathrm{NTime}(g)$ וגם $\mathrm{NSpace}(f) \subseteq \mathrm{NSpace}(g)$.

הוכחה של 1. יהי $A \in \mathrm{NTime}(f)$. לפי ההגדרה קיימות מכונה אי-דטרמיניסטית M וקבוע $c > 0$ כך ש-M מכריעה את A באופן אי-דטרמיניסטי ולכל x מתקיים $\mathrm{time}_M(x) \le c \cdot f(|x|)$. לפי משפט 3, לכל x:

$$\mathrm{space}_M(x) \;\le\; \mathrm{time}_M(x) \;\le\; c \cdot f(|x|).$$

אותה מכונה M ואותו קבוע c מעידים ש-$A \in \mathrm{NSpace}(f)$. $\blacksquare$

הוכחה של 2. יהי $A \in \mathrm{NSpace}(f)$, ותהיינה M ו-$c > 0$ המעידות על כך. מכיוון ש-**מכריעה** M את A באופן אי-דטרמיניסטי, מתקיים תנאי 1 של הגדרה 4: לכל x, בכל ריצה אפשרית M עוצרת. לכן תנאי משפט 4 מתקיים, ועם הקבוע $c' = \lg|Q_M| + \lg|\Gamma_M| + 1$ התלוי רק ב-M:

$$\mathrm{time}_M(x) \;\le\; 2^{c'\cdot \mathrm{space}_M(x)} \;\le\; 2^{c'\cdot c\cdot f(|x|)} \;=\; 2^{d\cdot f(|x|)}, \qquad d := \max\{1,\; c'c\}.$$

האי-שוויון האמצעי מותר כי $u \mapsto 2^{c'u}$ עולה והצבנו $\mathrm{space}_M(x) \le c \cdot f(|x|)$. לכן עם הקבוע 1 מעידה ש-$A \in \mathrm{NTime}\big(2^{d\cdot f}\big)$, ובפרט A שייכת לאיחוד. $\blacksquare$

הוכחה של 3. $f = O(g)$ פירושו שקיים $c_0 > 0$ כך שלכל n מתקיים $f(n) \le c_0 \cdot g(n)$. יהי $A \in \mathrm{NTime}(f)$ עם עדים M, c. אז לכל x:

$$\mathrm{time}_M(x) \;\le\; c \cdot f(|x|) \;\le\; (c \cdot c_0) \cdot g(|x|),$$

ולכן M עם הקבוע $c \cdot c_0$ מעידה ש-$A \in \mathrm{NTime}(g)$. ההוכחה למקום זהה מילה במילה עם החלפת time ב-space. $\blacksquare$

משפט 6: כל מכונה דטרמיניסטית היא מכונה אי-דטרמיניסטית, ולכן $\mathrm{DTime}(f) \subseteq \mathrm{NTime}(f)$ לכל $f : \mathbb{N} \to \mathbb{N}$ מתקיים

$$\mathrm{DTime}(f) \subseteq \mathrm{NTime}(f), \qquad \mathrm{DSpace}(f) \subseteq \mathrm{NSpace}(f).$$

הוכחה. יהי $A \in \mathrm{DTime}(f)$, ותהיינה $M = (Q, q_{start}, F, \Sigma, \Gamma, \delta)$ ו-$c > 0$ המעידות על כך. נגדיר מכונה אי-דטרמיניסטית M' עם אותם $Q, q_{start}, F, \Sigma, \Gamma$ ועם

$$\delta'(q, \alpha) = \{\delta(q, \alpha)\} \qquad \text{for all } q \in Q,\ \alpha \in \Gamma.$$

כלומר כל קבוצה בתמונה של δ' היא **יחידון**.
יש בדיוק ריצה אפשרית אחת. באינדוקציה על מספר הצעדים: בכל צעד יש בדיוק שלשה אחת בקבוצה, ולכן אין בחירה. לכן לכל x יש בדיוק ריצה אפשרית אחת של M' על x, והיא זהה לריצת M על x.
M' מכריעה את A באופן אי-דטרמיניסטי. נבדוק את שלושת התנאים; המפתח הוא שכאשר קבוצת הריצות האפשריות היא יחידון, "לכל ריצה" ו"קיימת ריצה" **מתלכדים** [א׳ 01:25:30].
M מכריעה את A, ולכן היא עוצרת על כל קלט; הריצה היחידה של M' היא ריצת M, ולכן M' עוצרת בכל ריצה אפשרית.
אם $x \in A$ אז ריצת M על x מסתיימת ב-q_{accept}; זו ריצה אפשרית של M' המסתיימת במצב מקבל, ולכן **קיימת** ריצה מקבלת.
אם $x \notin A$ אז ריצת M על x מסתיימת ב-q_{reject}; זו הריצה האפשרית היחידה של M', ולכן **בכל** ריצה אפשרית של M' דוחה.
המדדים לא השתנו. $\mathrm{time}_{M'}(x)$ הוא מקסימום על פני קבוצה בת ריצה אחת, ולכן $\mathrm{time}_{M'}(x) = \mathrm{time}_M(x) \le c \cdot f(|x|)$. לכן M' ו-c מעידות ש-$A \in \mathrm{NTime}(f)$.
ההוכחה עבור המקום זהה. ■

מסקנה.

$$P \subseteq \mathrm{NP}.$$

הוכחה. יהי $A \in P$. אז קיים $c \ge 1$ כך ש-$A \in \mathrm{DTime}(n^c)$. לפי משפט 6, $A \in \mathrm{NTime}(n^c) \subseteq \mathrm{NP}$. ■

האינטואיציה בשורה אחת [א׳ 01:24:26]: כל מה שאפשר לעשות בתקציב מסוים באופן דטרמיניסטי — **אותה מכונה** עם **אותו תקציב** עושה באופן אי-דטרמיניסטי. זה מקרה פרטי, לא סימולציה.

השאלה הפתוחה. האם $P = \mathrm{NP}$? באופן שקול (כי כיוון אחד ידוע): האם $\mathrm{NP} \subseteq P$? כלומר, האם כל מה שאפשר להכריע בזמן פולינומי **באופן אי-דטרמיניסטי** אפשר להכריע בזמן פולינומי **באופן דטרמיניסטי**. זו ככל הנראה השאלה הפתוחה המפורסמת ביותר במדעי המחשב, ויש עליה פרס של מיליון דולר. לא יודעים להוכיח שכן ולא יודעים להוכיח שלא [א׳ 01:28:25], [ב׳ 01:21:54].

משפט 7 (ללא הוכחה): שקילות חישובית למודל הדטרמיניסטי
המודל האי-דטרמיניסטי **אינו** מגדיל את כוח החישוב: שפה כלשהי ניתנת להכרעה על ידי מכונה אי-דטרמיניסטית אם ורק אם היא ניתנת להכרעה על ידי מכונת טיורינג רגילה.
הטענה לא הוכחה בכיתה [א׳ 00:55:52]. הרעיון: מכונה דטרמיניסטית יכולה לעבור על **כל** הריצות האפשריות של M על x בסריקה לרוחב של עץ החישוב, ולהכריז "מקבלת" אם מצאה ענף מקבל. אם M מכריעה שפה, כל ענף בעץ סופי והסתעפות העץ סופית (כי δ מחזירה קבוצות סופיות), ולכן העץ כולו סופי והסריקה מסתיימת.
מה כן משתנה — היעילות. בדיוק כמו במעבר בין מכונה רב-סרטית למכונה חד-סרטית: כוח החישוב זהה, המדדים לא. כאן ההפרש עלול להיות אקספוננציאלי, וזה ליבת שאלת P מול NP.
טענות נוספות שעוברות כמות שהן [א׳ 01:14:03], [ב׳ 01:06:39]: מכונה רב-סרטית אי-דטרמיניסטית והקשר בין המדדים שלה למכונה חד-סרטית, מכונה אוניברסלית אי-דטרמיניסטית ומדדי היעילות שלה, ומשפטי ההיררכיה. ההוכחות זהות פרט למעטפת. המרצה המליץ עליהן כתרגול טוב בדיוק משום שהמהות מוכרת וכל מה שנדרש הוא לתרגל את המעטפת.

דוגמאות ותרגילים מהשיעור
דוגמה 1: המכונה מהסיכום, ושלושת הענפים על $x = 0001$
$\Gamma = \{0, 1, B\}$, $\Sigma = \{0, 1\}$, $Q = \{q_{start}, q_1, q_2, q_{accept}, q_{reject}\}$. טבלת המעברים (התאים המסומנים בסיכום בהדגשה הם השורות עם יותר משלשה אחת):

δ	0	1	B
q_{start}	$(q_1, 0, R)$	q_{reject}	q_{reject}
q_1	$(q_1, 0, R)$	$(q_1, 1, R)$, $(q_2, 1, R)$	q_{reject}
q_2	q_{reject}	q_{reject}	q_{accept} , (q_2, B, R)

באותו אופן, כדיאגרמת מצבים (מצב q_{reject} וכל החצים אליו מושמטים לפי הקונבנציה):
$q_{start} \xrightarrow{0/0,R} q_1$
$q_1 \xrightarrow{0/0,R} q_1$ (לולאה עצמית), $q_1 \xrightarrow{1/1,R} q_1$ (לולאה עצמית)
$q_1 \xrightarrow{1/1,R} q_2$
$q_2 \xrightarrow{B/B,R} q_2$ (לולאה עצמית), $q_2 \xrightarrow{B/B,R} q_{accept}$
שלוש ריצות אפשריות על $x = 0001$ (כפי שהן מופיעות בסיכום):
אפשרות 1 — דוחה. $(q_1, 0, R),\ (q_1, 0, R),\ (q_1, 0, R),\ (q_1, 1, R),\ q_{reject}$ המכונה נשארת ב-q_1 גם כשהיא קוראת את ה-1 האחרון, ואז קוראת B ב-q_1 ודוחה.
אפשרות 2 — מקבלת. $(q_1, 0, R),\ (q_1, 0, R),\ (q_1, 0, R),\ (q_2, 1, R),\ (q_2, B, R),\ q_{accept}$ כאן, כשהמכונה קוראת את ה-1 האחרון, היא בוחרת את השלשה השנייה ועוברת ל-q_2; אחר כך היא קוראת B, בוחרת להישאר צעד אחד ב-q_2, ובצעד הבא מקבלת.

אפשרות 3 — אינה עוצרת.
$(q_1, 0, R),\ (q_1, 0, R),\ (q_1, 0, R),\ (q_2, 1, R),\ (q_2, B, R),\ (q_2, B, R),\ (q_2, B, R),\ \ldots$
אותה התחלה, אבל המכונה בוחרת שוב ושוב להישאר ב-q_2 ולזוז ימינה על תווים ריקים — לנצח.

המסקנה. שלוש ריצות אפשריות על **אותו קלט**, עם שלוש תוצאות שונות. לפי משפט 1 המכונה הזאת אינה מכריעה אף שפה, בגלל אפשרות 3.

דוגמה 2: תיקון המכונה — מוחקים מעבר אחד

מוחקים את (q_2, B, R) מהתא $\delta(q_2, B)$. עכשיו כל ריצה עוצרת אחרי $|x| + 1$ צעדים לכל היותר, ולפי משפט 2 המכונה מכריעה באופן אי-דטרמיניסטי את

$$A = \{x \in \{0,1\}^* \mid x \text{ starts with } 0 \text{ and ends with } 1\}.$$

מעקב על שני קלטים קונקרטיים:

$x = 0001$: ריצת אפשרות 2 (בלי שלב ההשהיה ב-q_2) מסתיימת ב-q_{accept} — ואכן x מתחיל ב-0 ומסתיים ב-1. שימו לב שגם אפשרות 1, שדוחה, עדיין קיימת; זה **מותר**, כי לקבלה מספיק עד אחד.

$x = 0010$: כל הריצות דוחות. מי שנשאר ב-q_1 עד הסוף קורא B ב-q_1 ונדחה. מי שעבר ל-q_2 עשה זאת בקריאת ה-1 שבמקום השלישי, ואז קורא 0 ב-q_2 ונדחה מיד. ואכן $x \notin A$.

דוגמה 3: מכונה שנייה (מההקלטה המקבילה) — מחרוזות שמסתיימות ב-0

מכונה אחרת לגמרי, עם שני מצבי עבודה בלבד, $Q = \{q_{start}, q_1, q_{accept}, q_{reject}\}$ ו-$\Gamma = \{0, 1, B\}$:

δ	0	1	B
q_{start}	$(q_{start}, 0, R)$, $(q_1, 0, R)$	$(q_{start}, 1, R)$	q_{reject}
q_1	q_{reject}	q_{reject}	q_{accept}

שלוש ריצות על $x = 000$ [ב׳ 00:34:30]:

$(q_{start}, 0, R), (q_{start}, 0, R), (q_{start}, 0, R), q_{reject}$ — נשארת ב-q_{start} לאורך כל הקלט, ואז קוראת B ב-q_{start} ונדחית.

$(q_1, 0, R), q_{reject}$ — עוברת ל-q_1 כבר בתו הראשון, ואז קוראת 0 ב-q_1 ונדחית.

$(q_{start}, 0, R), (q_{start}, 0, R), (q_1, 0, R), q_{accept}$ — "מנחשת" נכון שה-0 השלישי הוא האחרון, עוברת ל-q_1, קוראת B ומקבלת.

מה המכונה מכריעה. את שפת כל המחרוזות מעל $\{0,1\}$ **שמסתיימות ב-**0. הנימוק: כל ריצה זזה ימינה בכל צעד ולכן מגיעה ל-B ועוצרת. אם x מסתיימת ב-0, יש תסריט שבו המכונה נשארת ב-q_{start} עד התו האחרון ואז עוברת ל-q_1 — ומ-q_1 היא רואה B ומקבלת. אם x אינה מסתיימת ב-0, אז כל ריצה או שנשארה ב-q_{start} עד הסוף (וקוראת B ב-q_{start} ⟵ דוחה), או שעברה ל-q_1 בקריאת 0 שאינו התו האחרון (ואז התו הבא הוא תו קלט, ומ-q_1 כל תו קלט מוביל לדחייה).

וריאציה מקלקלת. אם מוסיפים $\delta(q_1, B) = \{q_{accept}, (q_1, B, R)\}$, המכונה שוב **אינה מכריעה אף שפה**, מאותה סיבה בדיוק כמו במשפט 1 — ההשוואה בין שתי המכונות היא הדרך הכי מהירה לזכור למה תנאי 1 בהגדרה 4 קיים.

תרגיל 1 (תרגיל חימום מתחילת המפגש; חומר חזרה משיעור 3): $\mathrm{DSpace}(n^{1/3}) \subsetneq \mathrm{EXP}$ זהו תרגיל דטרמיניסטי לחלוטין, שנפתר בכיתה לפני המעבר למודל החדש [ב׳ 00:12:20]. הקושי: אגף שמאל הוא מחלקת **מקום** ואגף ימין מחלקת **זמן**, ובנוסף EXP הוא איחוד, וההכלה-ממש אינה נשמרת תחת איחוד.

פתרון א (מקום ⟶ זמן, ואז היררכיית הזמן).

מהקשר בין זמן למקום: $\mathrm{DSpace}(n^{1/3}) \subseteq \bigcup_{c\geq 1} \mathrm{DTime}\left(2^{c\cdot n^{1/3}}\right)$.

להיפטר מהאיחוד: לכל $c \geq 1$ מתקיים $2^{c\cdot n^{1/3}} = O\left(2^{n^4}\right)$ (עבור n גדול מספיק $c\cdot n^{1/3} \leq n^4$),

ולכן כל האיחוד מוכל ב-$\mathrm{DTime}\left(2^{n^4}\right)$. עכשיו יש בידינו **מחלקה עדינה אחת**.

משפט היררכיית הזמן עם $g = 2^{n^4}$ ו-$f = 2^{2n^4}$: מתקיים $g = o(f)$ ו-f ישימה בזמן וסופר-לינארית, ולכן $\mathrm{DTime}\left(2^{n^4}\right) \subsetneq \mathrm{DTime}\left(f^2\right) = \mathrm{DTime}\left(2^{4n^4}\right)$.

לבסוף $2^{4n^4} = O\left(2^{n^5}\right)$, ולכן $\mathrm{DTime}\left(2^{4n^4}\right) \subseteq \mathrm{DTime}\left(2^{n^5}\right) \subseteq \mathrm{EXP}$ לפי הגדרת EXP.

בשרשרת יש הכלה-ממש אחת (שלב 3), ולכן ההכלה הכוללת היא הכלה ממש.

פתרון ב (היררכיית המקום קודם).

$n^{1/3} = o(n^4)$, ו-n^4 ישימה במקום וסופר-לינארית, ולכן ממשפט ההיררכיה המקום:

$\mathrm{DSpace}(n^{1/3}) \subsetneq \mathrm{DSpace}(n^4)$.

$\mathrm{DSpace}(n^4) \subseteq \mathrm{PSPACE}$ לפי הגדרה.

$\mathrm{PSPACE} \subseteq \mathrm{EXP}$ — הוכח בשיעור 3.

גם כאן ההכלה-ממש מגיעה משלב אחד. הפתרון השני קצר יותר משום שהוא מפעיל את משפט ההיררכיה **לפני** המעבר לאיחוד, ואז אין צורך "לתקן" את האיחוד [ב׳ 00:20:41].

תרגיל 2: להוכיח את הניסוח עם "אם ורק אם"

שאלה שנשאלה בכיתה: האם אפשר להחליף את תנאים 2 ו-3 בהגדרה 4 בתנאי יחיד "$x \in A$ אם ורק אם קיימת ריצה אפשרית מקבלת"?

פתרון. כן, בהינתן תנאי 1. תנאי 2 הוא בדיוק הכיוון $x \in A \Rightarrow \exists \rho$ מקבלת. נותר להראות ששני הניסוחים של הכיוון השני שקולים:

תנאי 3 אומר: $x \notin A \Rightarrow$ כל ריצה דוחה.

הקונטרהפוזיציה: אם לא כל ריצה דוחה, אז $x \in A$.

מכיוון שכל ריצה עוצרת (תנאי 1), ריצה שאינה דוחה היא ריצה מקבלת, ולכן "לא כל ריצה דוחה" שקול ל"קיימת ריצה מקבלת".

ולכן תנאי 3 שקול ל: $\exists \rho$ מקבלת $\Rightarrow x \in A$, שהוא בדיוק הכיוון החסר.

שימו לב שתנאי 1 נחוץ כאן: בלעדיו ריצה שאינה דוחה יכולה להיות ריצה שאינה עוצרת, והשקילות נשברת. בהוכחות נעדיף בכל זאת את הפיצול לשני תנאים, כי ההוכחה ממילא מתפצלת [א׳ 00:32:06].

תרגיל 3: תרגילים שהמרצים המליצו עליהם

להוכיח את משפט 4 (הכיוון $\mathrm{time} \leq 2^{c\cdot \mathrm{space}}$) לבד, אחרי שראיתם את משפט 3 — או להפך. שימו לב היכן בדיוק נדרשת ההנחה "עוצרת בכל ריצה אפשרית" [ב׳ 01:06:07].

לנסח ולהוכיח את השקילות בין מכונה רב-סרטית אי-דטרמיניסטית למכונה חד-סרטית אי-דטרמיניסטית, כולל מחיר המדדים.
לנסח את המכונה האוניברסלית האי-דטרמיניסטית ואת מדדי היעילות שלה.
בכל השלושה המהות מוכרת משיעורים 1–2; מה שמתורגל הוא רק המעטפת: "תהא ריצה אפשרית ⟵ סימונים לריצה זו ⟵ טיעון מוכר ⟵ מקסימום" [א׳ 01:15:08].

הערות מהשיעור
חומר השיעור מוקלט בשתי מסירות מקבילות מאותו יום. הפניות מסומנות `[א׳ hh:mm:ss]` להקלטה `ANf62oYXWnM` ו-`[ב׳ hh:mm:ss]` להקלטה `BPaQYss9Qi0`.
"עד עכשיו לא עשינו הרבה יותר מהגדרות" [א׳ 00:01:07]. המרצה פתח בהודאה שהחומר מרגיש עמוס למרות שהוא רדוד: כל הגדרה גוררת המון פרמטרים, ולכן ההוכחות ארוכות ומסורבלות. "ניסיתי לעקוף את זה, אי אפשר." אין כאן עומק — יש כאן הרבה חלקים זזים. ההמלצה המעשית: להיצמד למבנה, כי המבנה מכריח אתכם ללכת במסלול נכון [א׳ 00:55:18].
תחביר לפני סמנטיקה [א׳ 00:12:00]. סטודנט הבחין שהמרצה נתן את ההגדרה של δ אבל עוד לא אמר מה משמעותה. זו הייתה הבחנה נכונה ומכוונת: ההגדרה של המודל היא תחבירית בלבד; הסמנטיקה — ריצה אפשרית והכרעה — מגיעה רק אחר כך.
קונבנציית הסרטוט [א׳ 00:15:12], [א׳ 00:41:28]. את q_{reject} לא מסרטטים, וכל חץ שאינו מופיע פירושו מעבר ל-q_{reject}. בטבלה זה הרבה יותר קל לראות מאשר בסרטוט — ולכן כשמשהו לא ברור בדיאגרמה, חזרו לטבלה.
מצבים סופיים לא השתנו [א׳ 00:21:43]. שאלת סטודנט: האם, כמו במכונה רגילה, מגיעים ל-q_{accept} ופשוט עוצרים? כן. מהמצבים הסופיים לא יוצאים, וזה זהה לחלוטין למודל הקודם.
"אין מה להתווכח עם הגדרה" [א׳ 00:45:46], [א׳ 01:01:36]. המרצה חזר על העיקרון הזה כמה פעמים, כולל בתשובה לשאלה "למה בחרו מקסימום ולא משהו אחר": כשלומדים אפשר לשאול למה הגדירו כך; כשעובדים, עובדים לפי ההגדרה. "זו הגרסה המדעית של because I said so."
תיקון תוך כדי הרצאה [א׳ 01:09:13]. בהוכחת משפט 4 המרצה כתב תחילה "כיוון ש-Q סופית, המכונה אינה חוזרת על אותה קונפיגורציה", עצר ותיקן: מה שנדרש הוא ההנחה שהמכונה עוצרת **בכל ריצה אפשרית**. זו לא קוסמטיקה — ראו את ההערה בהוכחת משפט 4.
המקסימומים אינם באותה ריצה [א׳ 01:22:01]. חזר על כך במפורש: "פה יש לי מקסימום ופה יש לי מקסימום — לא להניח שזו אותה ריצה". שימו לב שבהוכחת משפט 4 באמת לא הנחנו זאת: חסמנו את הקשר בין המדדים **בתוך ריצה אחת**, ורק אחר כך לקחנו מקסימום, כל אחד בנפרד.
שאלת סטודנט שחידדה את ההגדרה [א׳ 00:26:00]. "בחישוביות, באוטומטים אי-דטרמיניסטיים, דיברנו על 'קיימת ריצה'. גם כאן מעניין אותי 'קיימת' או אוסף הריצות?" — התשובה היא ששניהם: **קיימת** לקבלה, ו**כל** הריצות לעצירה ולדחייה.
שאלת סטודנט על מבנה ההוכחה [א׳ 00:52:41]. במקרה 2 של משפט 2, מדוע חוזרים ואומרים "כיוון שזה לא התו האחרון"? כי זו ההנחה של המקרה, ומסתמכים עליה שוב; זו לא טענה חדשה.

קיצורים [א׳ 01:29:03]. המרצה סיים בהערה על כתיבת קיצורים כמו מ"ט במקום "מכונת טיורינג": מתמטית אין בזה שום פסול ולא יורדות עליו נקודות, אבל מניסיונו בבדיקת אלפי תרגילים יש **קורלציה מובהקת** בין כתיבה בראשי תיבות ובין טעויות. המלצה בלבד.
הערת שם [א׳ 01:26:48]. ל-$NEXPSPACE$ אין קיצור מקובל — סימן טוב לכך שלא נשתמש בה הרבה.
מוטיבציה למודל [ב׳ 00:24:50]. "יש הרבה מאוד בעיות חשובות שלא יודעים לפתור בזמן פולינומי, אבל ברגע שמאפשרים למודל להיות אי-דטרמיניסטי — פתאום כן." זו כל הסיבה שהמודל התיאורטי הזה מעניין, וממנה נולדת שאלת P מול NP.
הבטחה להמשך [ב׳ 01:08:12], [ב׳ 01:23:28]. שני המרצים ציינו שדוגמה משמעותית באמת — בעיה שהמודל האי-דטרמיניסטי פותר ביעילות והמודל הדטרמיניסטי לא יודע — תגיע בשיעור הבא. השיעור הזה כולו ברמת ההגדרות.

פערים בין הסיכום להקלטה
מקור: עמוד 1 בסיכום. **הפער:** ההגדרה הדטרמיניסטית נכתבה כחמישייה $M = (Q, F, \Sigma, \Gamma, \delta)$, בלי המצב ההתחלתי. **ההכרעה:** תוקן בגוף ל-$M = (Q, q_{start}, F, \Sigma, \Gamma, \delta)$, בעקבות אותו תיקון שכבר נעשה בשיעור 1; ההקלטה המקבילה מונה במפורש את המצב ההתחלתי כרכיב [ב׳ 00:26:23].
מקור: עמוד 3 בסיכום והקלטה א׳ [00:40:57]. **הפער:** נכתב שהריצה עוצרת אחרי לא יותר מ-$|x|$ צעדים (ובהרצאה: "בדיוק $|x|$"), אך הצעד שבו נקרא התו הריק הוא הפעלה נוספת של δ. **ההכרעה:** תוקן ל-$|x| + 1$; הסיכום עצמו מדגים זאת — הריצה על $x = 0001$ מונה חמש הפעלות של δ. אין לכך השפעה על אף מסקנה.
מקור: עמוד 1 בסיכום. **הפער:** ההגדרה של ריצה אפשרית נוסחה כ"כל שלשה שייכת לקבוצה שפונקציית המעברים מחזירה על השלשה הקודמת", אך δ אינה מקבלת שלשה. **ההכרעה:** נוסח מחדש בגוף באמצעות (מצב נוכחי, תו שמתחת לראש), עם הערה שהניסוח בסיכום הוא קיצור.
מקור: עמוד 4 בסיכום מול שיעור 2. **הפער:** ספירת הקונפיגורציות נכתבה כ-$2^{(\lg|Q|+\lg|\Gamma|+1)\cdot s}$, בעוד הספירה המדויקת היא $s \cdot |\Gamma|^s \cdot |Q|$. **ההכרעה:** נבדק — **אין כאן טעות**. הביטוי בסיכום הוא חסם עליון גס יותר על אותה ספירה, בדיוק כפי שנעשה בשיעור 2, והוא זה שמייצר את הקבוע $c = 1 + \lg|\Gamma| + \lg|Q|$. שני הביטויים מופיעים בגוף.
מקור: הקלטה א׳ [01:09:13] מול עמוד 4 בסיכום. **הפער:** בסיכום נכתב "כיוון ש-M עוצרת בכל ריצה, גם ריצה זו אינה חוזרת על קונפיגורציה" בלי הצדקה. **ההכרעה:** הפירוט נכתב בגוף (חזרה על קונפיגורציה מייצרת ריצה אפשרית אינסופית **אחרת**, ולכן דרושה ההנחה על כל הריצות ולא על הריצה הנתונה).
מקור: הקלטה ב׳. **הפער:** המונח **תסריט ריצה** (סדרת הבחירות של המכונה) והמוטיבציה למודל (בעיות שאין להן פתרון פולינומי ידוע ופתאום יש להן פתרון אי-דטרמיניסטי) אינם מופיעים בסיכום כלל. **ההכרעה:** נוספו לגוף — המונח בהגדרה 3 והמוטיבציה בסעיף הרקע.

מקור: הקלטה ב׳ [00:57:05]–[01:03:32]. **הפער:** הטענה $\text{space}_M(x) \leq \text{time}_M(x)$ מופיעה בסיכום רק ברשימת "טענות נוספות", ובהקלטה א׳ הושארה כתרגיל. **ההכרעה:** ההוכחה המלאה שניתנה בהקלטה ב׳ נכתבה בגוף כמשפט 3, וממנה נגזר סעיף 1 של משפט 5.

מקור: הקלטה ב׳ [00:31:46]–[00:51:11]. **הפער:** המכונה השנייה (השפה של מחרוזות שמסתיימות ב-0) אינה בסיכום. **ההכרעה:** נכללה כדוגמה 3, כולל שלוש ריצות מפורשות והוריאציה שמקלקלת את ההכרעה.

מקור: הקלטה א׳ [01:00:03]. **הפער:** ההבחנה ש-$\text{time}_M(x) = \infty$ כשקיימת ריצה שאינה עוצרת, גם אם ריצות אחרות עוצרות, אינה בסיכום. **ההכרעה:** נוספה כמלכודת בהגדרה 5.

מקור: הקלטה ב׳ [00:00:03]–[00:22:14]. **הפער:** כ-22 הדקות הראשונות של ההקלטה השנייה אינן חומר של שיעור 4 אלא חזרה על שיעור 3 ותרגיל מודרך. **ההכרעה:** התרגיל נכלל כתרגיל 1 עם שני פתרונות מלאים, ומסומן במפורש כחומר חזרה.

מקור: עמוד 1 בסיכום. **הפער:** כותרת העמודה השלישית בטבלת המעברים אינה קריאה בבירור בכתב היד ונראית כספרה. **ההכרעה:** שוחזרה כתו הריק B — זו הפרשנות היחידה שמתיישבת עם תוכן העמודה, עם הדיאגרמה ועם ההקלטה [א׳ 00:13:38].

מקור: עמוד 4 בסיכום. **הפער:** ליד ההגדרה $f : \mathbb{N} \to \mathbb{N}$ מופיעה מילה בסוגריים שאינה קריאה. **ההכרעה:** לא שוחזרה; אין לה השפעה על ההגדרות, שכן ההקלטות מנסחות "תהא f פונקציה מ-$\mathbb{N}$ ל-$\mathbb{N}$" בלי תנאי נוסף.

מקור: הקלטה א׳ [00:55:52]. **הפער:** השקילות החישובית בין המודלים נאמרה ולא הוכחה, ובסיכום אינה מופיעה כלל. **ההכרעה:** נכתבה בגוף כמשפט 7, מסומנת במפורש כטענה שלא הוכחה בכיתה, עם סקיצת הרעיון (סריקת עץ החישוב).

סיכום ונקודות למבחן

מה חייבים לדעת בעל פה.

$\delta : Q \times \Gamma \to P(Q \times \Gamma \times \{L, R\})$ — וזה **כל** ההבדל התחבירי.

שלושת תנאי ההכרעה האי-דטרמיניסטית, עם הכמתים הנכונים: עצירה — לכל ריצה; קבלה — קיימת ריצה; דחייה — לכל ריצה.

$\text{time}_M(x)$ ו-$\text{space}_M(x)$ הם מקסימומים על פני ריצות אפשריות, ולא בהכרח באותה ריצה.

$\text{NTime}(f)$, $\text{NSpace}(f)$, ו-$\text{NP} = \bigcup_{c \geq 1} \text{NTime}(n^c)$.

$\text{NTime}(f) \subseteq \text{NSpace}(f)$, $\text{NSpace}(f) \subseteq \bigcup_{d \geq 1} \text{NTime}(2^{d \cdot f})$, $\text{DTime}(f) \subseteq$

$\text{NTime}(f)$, $\text{DSpace}(f) \subseteq \text{NSpace}(f)$, ולכן $P \subseteq \text{NP}$.

מלכודות סטנדרטיות.

לשכוח את תנאי העצירה. הטעות הכי נפוצה: להראות שקיימת ריצה מקבלת בדיוק על מילות השפה, ולשכוח לבדוק שכל ריצה על כל קלט עוצרת. המכונה מדוגמה 1 היא הדוגמה הנגדית המושלמת — היא "מקבלת בדיוק את מה שצריך" ובכל זאת אינה מכריעה **אף שפה**.

להניח שהמקסימום בזמן ובמקום מושג באותה ריצה. אסור.

להפוך את הכמתים. "לכל ריצה מקבלת" במקום "קיימת ריצה מקבלת" משנה את השפה לגמרי (וכמעט תמיד לשפה הריקה).

לקצר ב"יש רק ריצה אחת אפשרית". גם כשזה נכון, ההגדרה דורשת "לכל ריצה" — פתחו ב"תהא ריצה אפשרית".

לבלבל בין "לא דטרמיניסטי" ל"אי-דטרמיניסטי". אלגוריתם אקראי הוא הראשון ולא השני.

להשתמש במשפט 4 בלי ההנחה החזקה. ההנחה היא "עוצרת בכל ריצה אפשרית", לא "עוצרת".

להפעיל משפט היררכיה על מחלקה גסה. הכלה ממש אינה נשמרת תחת איחוד — צריך לרדת קודם לשתי מחלקות עדינות (תרגיל 1).

צ'קליסט — אחרי השיעור אתם אמורים לדעת:

לתרגם טבלת מעברים אי-דטרמיניסטית לדיאגרמה ולהפך, כולל קונבנציית q_{reject} המושמטת;

בהינתן מכונה וקלט, לכתוב במפורש כמה ריצות אפשריות שונות, ולזהות ריצה שאינה עוצרת;

להוכיח שמכונה נתונה מכריעה שפה נתונה באופן אי-דטרמיניסטי, בשלושת התנאים ובמבנה המלא;

להוכיח שמכונה נתונה **אינה** מכריעה אף שפה, על ידי הצגת קלט ואז ריצה שאינה עוצרת;

להוכיח טענה על מדדי היעילות במודל האי-דטרמיניסטי לפי התבנית "תהא ריצה אפשרית ⟵ סימונים ⟵ טיעון ⟵ מקסימום";

לגזור את היחסים הבסיסיים בין NTime, NSpace, DTime ו-DSpace, ולנסח נכון את שאלת P מול NP.

הסיכום בכתב יד שעליו מבוסס השלד של הקובץ הוא של גיא סופר.

שאלות שנשארו פתוחות

עמוד 4 בסיכום: המילה בסוגריים ליד ההגדרה $f:\mathbb{N}\to\mathbb{N}$ אינה קריאה בבירור ולא שוחזרה.

עמוד 3 בסיכום: החסם על אורך הריצה נכתב $|x|$; ספירת הצעדים בסיכום עצמו נותנת $|x|+1$, ותוקן בגוף.

עמוד 1 בסיכום: כותרת העמודה השלישית בטבלת המעברים מסומנת בכתב יד שנקרא כספרה; שוחזרה כתו הריק B לפי ההקשר.

5 טיעוני ריפוד ומבוא ל-SAT

טכניקת הריפוד: ניפוח מלאכותי של הקלט מאפשר להסיק הכלה בין מחלקות מהכלה נתונה אחרת — ומכאן ש-E≠PSPACE ושאם P=NP אז EXP=NEXP; ובחלק השני, ההגדרות הלוגיות של נוסחת CNF, השפה SAT והטענה SAT∈NP.

ביטחון: high

בקצרה

טיעון ריפוד (padding argument) הוא טכניקה להוכחת הכלה בין מחלקות סיבוכיות **בהינתן הכלה אחרת**. הרעיון: לוקחים שפה קשה, "מנפחים" מלאכותית את הקלטים שלה בזנב ארוך של תו חדש, ומקבלים שפה שהיא בדיוק אותה בעיה — אבל *ביחס לאורך הקלט* היא נראית הרבה יותר קלה, ולכן נופלת למחלקה נמוכה יותר שעליה ההכלה הנתונה כן חלה.

הגרעין של כל הטכניקה הוא תצפית אחת: אם מספר הצעדים של מכונה נשאר קבוע ואורך הקלט גדל, **סיבוכיות הריצה ביחס לאורך הקלט יורדת**. הריפוד לא הופך שום דבר לקל יותר; הוא רק משנה את המכנה שביחס אליו מודדים.

מוכיחים שתי טענות מסוג "אם הכלה אז הכלה": **אם** $\mathrm{E} \subseteq \mathrm{PSPACE}$ **אז** $\hat{\mathrm{E}} \subseteq \mathrm{PSPACE}$, ו**אם** $\mathrm{NP} \subseteq \mathrm{P}$ **אז** $\mathrm{NEXP} \subseteq \mathrm{EXP}$ — כלומר, אם $\mathrm{P} = \mathrm{NP}$ אז $\mathrm{EXP} = \mathrm{NEXP}$, ובניסוח הנגדי־חיובי: **אם** $\mathrm{EXP} \neq \mathrm{NEXP}$ **אז** $\mathrm{P} \neq \mathrm{NP}$.

טענות מותנות כאלה אינן חסרות שיניים: בשילוב עם משפט ההיררכיה בזמן הן נותנות תוצאה **לא מותנית** — $\mathrm{E} \neq \mathrm{PSPACE}$.

מבנה ההוכחה קבוע ואינו משתנה משאלה לשאלה: **ארבע מכונות**, שתיים מקבלים "מהשמיים" מתוך שייכות למחלקה ושתיים בונים בעצמנו. הדבר היחיד שדורש מחשבה הוא **כמה לרפד**, וגם זה נקבע מחשבון פשוט.

החלק השני של השיעור פותח את הפרק החדש, P מול NP: מושגי הלוגיקה (ליטרל, פסוקית, נוסחת CNF, הסמה, ספיקות), הגדרת השפה SAT, והמכונה האי־דטרמיניסטית שמראה $\mathrm{SAT} \in \mathrm{NP}$ — היא "מנחשת" הסמה ומאמתת אותה.

מלכודת שהמרצה הדגיש: $\mathrm{E} \neq \mathrm{PSPACE}$ היא טענה על **שפות**, לא על מכונות. בכל ההכלות הסטנדרטיות שראינו עד כה המכונה נשארה אותה מכונה; כאן, לראשונה, אנחנו מייצרים מכונות חדשות ומשליכים בין מודלים.

רקע ותלויות

השיעור הזה סוגר את הפרק הראשון של הקורס (הקשרים בין מחלקות) ופותח את השני (P מול NP). נזכיר במלואן את התוצאות שנשתמש בהן ממש.

$$\mathrm{P} = \bigcup_{c \geq 1} \mathrm{DTime}(n^c), \qquad \mathrm{PSPACE} = \bigcup_{c \geq 1} \mathrm{DSpace}(n^c), \qquad \mathrm{EXP} = \bigcup_{c \geq 1} \mathrm{DTime}\left(2^{n^c}\right).$$

טענה (מונוטוניות במשאב). אם $g = O(f)$ אז $\mathrm{DTime}(g) \subseteq \mathrm{DTime}(f)$ וגם $\mathrm{DSpace}(g) \subseteq \mathrm{DSpace}(f)$.

נשתמש גם בהבחנה בין מחלקות **עדינות** ($\mathrm{DTime}(f)$, $\mathrm{DSpace}(f)$ — לכל פונקציה מחלקה משלה) למחלקות **גסות** (איחוד אינסופי, כמו P או PSPACE). כל פעם שנקבל שייכות למחלקה גסה, הצעד הראשון יהיה **לקלף את האיחוד החוצה** ולקבל שייכות למחלקה עדינה — ורק ממנה אפשר לחלץ מכונה עם חסם קונקרטי.

מהשיעור 3: משפט ההיררכיה בזמן והישימות

משפט ההיררכיה בזמן. אם f ישימה בזמן (time-constructible), f סופר־לינארית, ו- $g = o(f)$, אז $\mathrm{DTime}(g) \subsetneq \mathrm{DTime}\left(f^2\right)$.

הריבוע שם אינו קישוט — הוא מחיר המעבר ממכונה רב־סרטית למכונה סטנדרטית. נשתמש במשפט הזה פעם אחת בדיוק, בטענה $\mathrm{E} \neq \mathrm{PSPACE}$.

נשתמש גם, שוב ושוב, בשני מושגי הישימות. פונקציה f **ישימה בזמן** אם אפשר לחשב אותה בזמן $O(f)$, ו**ישימה במקום** אם אפשר לחשב אותה במקום $O(f)$. שתי הפונקציות שיופיעו כאן, $n \mapsto n^2$ ו- $n \mapsto d \cdot 2^{n^c}$, הן ישימות בזמן ובמקום. זה **לא** פרט טכני שאפשר לדלג עליו: המכונות שנבנה חייבות *לחשב* את גודל הריפוד, וללא ישימות אין לנו שום מושג כמה זה עולה.

הערה מההקלטה [00:44:21]: סטודנט הציע לחסום את המקום של שלב החישוב באורך הפלט. המרצה עצר על כך במפורש: מכונת טיורינג יכולה להשתמש בהרבה יותר מקום ממה שהיא מוציאה בסוף. הדוגמה הקיצונית שנתן — מכונת הכרעה מוציאה ביט אחד; האם המקום שלה קבוע? ודאי שלא. **בדיוק בשביל זה צריך את הישימות במקום.**

מהשיעור 4: המודל הא־דטרמיניסטי

מכונה א־דטרמיניסטית M **מכריעה** שפה A אם (א) כל ריצה אפשרית של M על כל קלט עוצרת, ו- (ב) $x \in A$ אם ורק אם **קיימת** ריצה של M על x שמסתיימת במצב מקבל. מדד הזמן $\mathrm{time}_M(x)$ הוא המקסימום על פני כל הריצות. מכאן

$$\mathrm{NP} = \bigcup_{c \geq 1} \mathrm{NTime}(n^c), \qquad \mathrm{NEXP} = \bigcup_{c \geq 1} \mathrm{NTime}\left(2^{n^c}\right).$$

הוכחנו בשיעור 4 שכל מחלקה דטרמיניסטית מוכלת במקבילה האי־דטרמיניסטית שלה, ובפרט $\mathrm{P} \subseteq \mathrm{NP}$ ו-$\mathrm{EXP} \subseteq \mathrm{NEXP}$. זו הסיבה שכל טענה על *שוויון* בין הזוגות האלה מצטמצמת להכלה בכיוון אחד בלבד.

הגדרות

הגדרה 1: המחלקה E

$$\mathrm{E} = \bigcup_{c \geq 1} \mathrm{DTime}(2^{cn}) \,.$$

אינטואיציה. זו מחלקת ה"אקספוננציאלי בדיוק" — החזקה היא cn, עם n **בלי חזקות בכלל**. המרצה עצר על כך במפורש: E **אינה** EXP. ב-EXP החזקה היא n^c, ולכן $2^{n^{100}}$ יושב ב-EXP אך לא ב-E.
דוגמה. שפה שמוכרעת בזמן $3 \cdot 2^{5n}$ שייכת ל-E. **אי־דוגמה.** שפה שזמן ההכרעה המינימלי שלה הוא 2^{n^2} אינה ב-E, אך כן ב-EXP. מתקיים $\mathrm{E} \subseteq \mathrm{EXP}$, וההכלה היא הכלה ממש.
הגדרה 2: המחלקה $\hat{\mathrm{E}}$

$$\hat{\mathrm{E}} = \bigcup_{c \geq 1} \mathrm{DTime}\left(2^{cn^2}\right) \,.$$

אינטואיציה. אותו דבר בדיוק, אלא שהמעריך ריבועי במקום לינארי. זו מחלקה **גדולה יותר** מ-E (ובהמשך נוכיח שהיא גדולה ממש), ועדיין מוכלת ב-EXP. ההפרש בין שתי המחלקות הוא בדיוק "ריבוע במעריך" — וזה, כפי שנראה, בדיוק גודל הריפוד שיידרש.
הגדרה 3: שפת ריפוד (padded language)
תהי $A \subseteq \Sigma^*$ שפה, ותהי $p : \mathbb{N} \to \mathbb{N}$ פונקציה ישימה בזמן ובמקום. **שפת הריפוד** של A ביחס ל-p היא

$$B = \left\{ x\#^{\,p(|x|)} \;\middle|\; x \in A \right\},$$

כאשר $\#$ הוא תו **חדש** שאינו באלף־בית Σ של A.
אינטואיציה. B מכילה בדיוק את אותו מידע ש-A מכילה — לכל מילה ב-A מתאימה מילה יחידה ב-B, ולהפך. שום חישוב לא נעשה קל יותר. מה שכן משתנה: הקלט התארך, ולכן אותו מספר צעדים בדיוק נראה עכשיו, *ביחס לאורך הקלט*, זול הרבה יותר. זו כל התחבולה.
למה $\#$ חייב להיות תו חדש? כדי שהפירוק $y = x\#^{\ell}$ יהיה חד־משמעי. אילו $\# \in \Sigma$, לא היינו יכולים לקבוע מהסתכלות ב-y היכן נגמר x ומתחיל הזנב, והשלב הראשון של המכונה שנבנה לא היה מוגדר היטב.
דוגמה. עבור $A = \{\,\texttt{01},\ \texttt{110}\,\}$ ו-$p(n) = n^2$ מקבלים $B = \{\,\texttt{01}\#\#\#\#,\ \texttt{110}\#^{9}\,\}$. **אי־דוגמה.** המילה $\texttt{01}\#\#\#$ אינה ב-B, אף ש-$\texttt{01} \in A$: אורך הזנב אינו $|x|^2$. זו בדיוק הבדיקה שהמכונה תבצע בשלב השני, ובלעדיה B לא הייתה מוגדרת היטב.

הגדרה 4: ליטרל, פסוקית ונוסחת CNF

יהיו $x_1, \ldots, x_n$ **משתנים בוליאניים**.

ליטרל הוא משתנה או שלילה של משתנה. למשל x_2 הוא ליטרל, וגם $\overline{x_4}$.

הֶסְגֵּר (או **פסוקית**, clause) הוא טְפֶל (tuple) סופי של ליטרלים עם $\vee$ ("או") ביניהם. למשל $x_1 \vee \overline{x_2} \vee \overline{x_4}$ היא פסוקית עם שלושה ליטרלים.

נוסחת CNF היא טפל סופי של פסוקיות עם $\wedge$ ("וגם") ביניהן. למשל $\left(x_1 \vee \overline{x_2} \vee x_4\right) \wedge \left(\overline{x_1} \vee \overline{x_3} \vee \overline{x_4} \vee x_5\right)$.

אינטואיציה. CNF (Conjunctive Normal Form) היא "וגם של אואים": רשימת דרישות, שכל אחת מהן מסופקת אם לפחות אחת מהאפשרויות שבה מתקיימת. שימו לב שההגדרה היא **תחבירית בלבד** — עדיין לא נתנו לסימנים האלה שום משמעות.

דוגמה ואי־דוגמה. אין הגבלה על מספר הליטרלים בפסוקית: $\overline{x_2} \vee x_4 \vee x_1 \vee x_5$ היא פסוקית CNF תקינה. לעומת זאת $\left(x_1 \wedge x_2\right) \vee x_3$ **אינה** נוסחת CNF — היא בצורה ההפוכה (DNF).

> **הערה מההקלטה [01:48:51]:** המרצה הוסיף בכוונה משתנה רביעי לדוגמה, "כדי שלא תחשבו שזה חייב להיות עם שלוש". פסוקיות באורך 3 הן מקרה פרטי שיזכה לשם משלו ($3\mathrm{SAT}$), אך אינן ההגדרה.

הגדרה 5: הסמה וספיקות

הסמה היא פונקציה $v : \{x_1, \ldots, x_n\} \to \{0, 1\}$.

לפי הכללים הלוגיים אפשר **להרחיב** את v מן המשתנים לכל נוסחה לוגית: אם $v(x_1) = T$ אז $v(\overline{x_1}) = F$; אם $v(x_1) = T$ ו-$v(x_2) = F$ אז $v(x_1 \vee x_2) = T$ ו-$v(x_1 \wedge x_2) = F$; וכן הלאה.

נוסחה φ נקראת **ספיקה** אם **קיימת** הסמה v המעניקה לה את הערך T; אומרים אז ש-v **מספקת** את φ.

אינטואיציה. ההסמה היא הסמנטיקה — האובייקט החיצוני שנותן משמעות לתחביר. ספיקות אינה תלויה בהסמה מסוימת: היא טענת **קיום**.

דוגמה. ההסמה $v(x_1) = T,\ v(x_2) = F$ מספקת את $x_1 \vee x_2$ ואינה מספקת את $x_1 \wedge x_2$ — אבל $x_1 \wedge x_2$ בכל זאת **ספיקה**, כי הסמה אחרת (שנותנת T לשניהם) כן מספקת אותה. **אי־דוגמה (נוסחה שאינה ספיקה).** $x_1 \wedge \overline{x_1}$. יש כאן משתנה אחד; כל הסמה נותנת F לאחד משני הליטרלים, ולכן נותנת F לנוסחה כולה. לא קיימת הסמה מספקת.

> **הערה מההקלטה [01:56:48]:** "אל תגידו $x_1 = T$ אף פעם. תביאו הסמה ותגידו: ההסמה נותנת T ל-x_1." הרבה טעויות נובעות מהתייחסות למשתנים כאילו יש להם ערכים. למשתנים אין ערכים — כדי לתת להם ערך צריך אובייקט נוסף מבחוץ.

הגדרה 6: השפה SAT

עבור נוסחת CNF φ נסמן ב-$\langle\varphi\rangle$ את הקידוד הבינרי שלה. **מניחים** שכל מחרוזת בינארית מקודדת נוסחת CNF כלשהי (מחרוזת שאינה במבנה התקין מתורגמת לנוסחה קבועה אחת) — בדיוק כפי שעשינו עם קידוד מכונות טיורינג בחישוביות. אז

$$\mathrm{SAT} = \{\, \langle \varphi \rangle \;\mid\; \varphi \text{ CNF},\ \varphi \text{ satisfiable} \,\}.$$

אינטואיציה. שימו את הקידוד בצד; הוא נחוץ רק מפני שמכונת טיורינג מקבלת מחרוזות. במהות, SAT היא אוסף כל נוסחאות ה-CNF שיש להן הסמה מספקת.
דוגמה. $\langle x_1 \vee x_2 \rangle \in \mathrm{SAT}$. **אי־דוגמה.** $\langle x_1 \wedge \overline{x_1} \rangle \notin \mathrm{SAT}$.

משפטים והוכחות
משפט 1: אם $\mathrm{E} \subseteq \mathrm{PSPACE}$ אז $\hat{\mathrm{E}} \subseteq \mathrm{PSPACE}$
הוכחה. נניח $\mathrm{E} \subseteq \mathrm{PSPACE}$, ותהי $A \in \hat{\mathrm{E}}$. עלינו להראות $A \in \mathrm{PSPACE}$.
שלב א' — קבלת המכונה הראשונה. $\hat{\mathrm{E}}$ מוגדרת על ידי איחוד, ולכן נקלף את האיחוד: קיים $c > 0$ כך ש-$A \in \mathrm{DTime}\left(2^{cn^2}\right)$. זו שייכות למחלקה **עדינה**, ומהגדרתה קיימת מכונה M_A וקיים $d > 0$ כך ש-M_A מכריעה את A וכן לכל x:

$$\mathrm{time}_{M_A}(x) \;\le\; d \cdot 2^{\,c|x|^2}.$$

שלב ב' — בניית שפת הריפוד. נגדיר

$$B = \left\{ x\#^{\,|x|^2} \;\middle|\; x \in A \right\},$$

כאשר $\#$ תו חדש שאינו ב-Σ, האלף־בית של A.
למה דווקא $|x|^2$? מפני שההפרש היחיד בין E ל-$\hat{\mathrm{E}}$ הוא ש-n עולה בריבוע במעריך. אם אני מנפח את הקלט כך שאורכו יהיה סדר גודל של $|x|^2$, אז מספר צעדים שהיה $2^{c|x|^2}$ ביחס לקלט הישן נעשה $2^{c|y|}$ ביחס לקלט החדש — בדיוק המעבר מ-$\hat{\mathrm{E}}$ ל-E.
שלב ג' — בניית המכונה השנייה. נגדיר מכונה M_B שעל קלט $y \in (\Sigma \cup \{\#\})^*$ פועלת כך:
נבדוק ש-y מהצורה $x\#^{\ell}$ כאשר $x \in \Sigma^*$; אחרת נדחה.
נחשב את $|x|^2$ ונבדוק ש-$\ell = |x|^2$; אחרת נדחה.
נריץ את M_A על x ונחזיר את תשובתה.
נכונות: M_B מכריעה את B. יהי $y \in (\Sigma \cup \{\#\})^*$.
כיוון ראשון. אם $y \in B$ אז קיים $x \in A$ כך ש-$y = x\#^{|x|^2}$. בהרצת M_B על y: שלב 1 עובר (זהו בדיוק המבנה), שלב 2 עובר (זהו בדיוק האורך), ובשלב 3 המכונה M_A מקבלת את x כי $x \in A$ ו-M_A מכריעה את A. לכן M_B מקבלת את y.
כיוון שני. נניח ש-M_B מקבלת את y. מכיוון שכל שלב שנכשל גורם לדחייה, בהכרח שלושת השלבים עברו: מ-1 נובע ש-$y = x\#^{\ell}$ עבור $x \in \Sigma^*$; מ-2 נובע $\ell = |x|^2$; ומ-3 נובע ש-M_A קיבלה את x, ולכן $x \in A$. מכאן $y = x\#^{|x|^2}$ עם $x \in A$, כלומר $y \in B$.
בנוסף, M_B עוצרת תמיד: שלבים 1–2 הם סריקות סופיות, ו-M_A עוצרת תמיד כי היא מכריעה. לכן M_B מכריעה את B.
שלב ד' — חשבון הזמן של M_B. יהי y שעבר את שלב 1, ונסמן $y = x\#^{\ell}$.

שלב 1 — סריקה אחת של הקלט: מרגע שראינו $\#$ לוודא שלא מופיע עוד תו מ-Σ. עלות: $O(|y|)$ צעדים.
שלב 2 — כאן נדרשת **הישימות בזמן** של $n \mapsto n^2$: היא מבטיחה שחישוב הערך $|x|^2$ אורך $O(|x|^2)$ צעדים. וכיוון ש-$|y| = |x| + |x|^2 \geq |x|^2$, זהו $O(|y|)$.
שלב 3 — מהגדרת M_A, ההרצה על x אורכת לכל היותר $d \cdot 2^{c|x|^2}$ צעדים. שוב $|x|^2 \leq |y|$, ולכן זה חסום ב-$d \cdot 2^{c|y|}$.
סך הכול, לכל y:

$$\mathrm{time}_{M_B}(y) \;\leq\; O(|y|) + O(|y|) + d \cdot 2^{\,c|y|} \;=\; O\Big(2^{\,c|y|}\Big).$$

לכן $B \in \mathrm{DTime}(2^{cn})$, ומכאן $B \in \mathrm{E}$.
שלב ה' — חציית הגשר. מההנחה $\mathrm{E} \subseteq \mathrm{PSPACE}$ נובע $B \in \mathrm{PSPACE}$. נקלף שוב את האיחוד: קיים $\alpha > 0$ כך ש-$B \in \mathrm{DSpace}(n^\alpha)$, ולכן **קיימת המכונה השלישית** $\widetilde{M_B}$ וקיים $\beta > 0$ כך ש-$\widetilde{M_B}$ מכריעה את B ולכל y:

$$\mathrm{space}_{\widetilde{M_B}}(y) \;\leq\; \beta \cdot |y|^\alpha.$$

שלב ו' — בניית המכונה הרביעית. נגדיר $\widetilde{M_A}$ שעל קלט x:
תחשב את $|x|^2$ ותבנה את $y = x\#^{|x|^2}$.
תריץ את $\widetilde{M_B}$ על y ותחזיר את אותה תשובה.
נכונות: $\widetilde{M_A}$ מכריעה את A. יהי $x \in \Sigma^*$. אם $x \in A$ אז לפי הגדרת B מתקיים $x\#^{|x|^2} \in B$, ולכן $\widetilde{M_B}$ מקבלת אותו, ולכן $\widetilde{M_A}$ מקבלת את x. אם $x \notin A$ אז $x\#^{|x|^2} \notin B$ (שוב לפי הגדרת B, שכל איבריה מגיעים מאיברי A), ולכן $\widetilde{M_B}$ דוחה אותו ו-$\widetilde{M_A}$ דוחה את x.
שלב ז' — חשבון המקום של $\widetilde{M_A}$. יהי $x \in \Sigma^*$.
שלב 1 — כאן נדרשת **הישימות במקום** של $n \mapsto n^2$: חישוב הערך $|x|^2$ דורש $O(|x|^2)$ מקום. כתיבת y עצמה תופסת $|x| + |x|^2 = O(|x|^2)$ תאים.
שלב 2 — מהגדרת $\widetilde{M_B}$, ההרצה דורשת לכל היותר $\beta|y|^\alpha$ תאים, וכיוון ש-$|y| = O(|x|^2)$ זהו $O\big(|x|^{2\alpha}\big)$.
סך הכול $\mathrm{space}_{\widetilde{M_A}}(x) = O\big(|x|^{2\alpha}\big)$, כלומר $A \in \mathrm{DSpace}\big(n^{2\alpha}\big)$ ולכן $A \in \mathrm{PSPACE}$. ■
התבנית ב-high level: ארבע מכונות
זהו השלד שחוזר על עצמו בכל טיעון ריפוד, ושווה לזכור אותו לפני הפרטים:

#	מה קורה	מקור
1	$A \in \hat{\mathrm{E}} \longleftarrow$ **מקבלים** את M_A עם חסם **זמן** (כי $\hat{\mathrm{E}}$ מוגדרת בזמן)	מהשמיים
2	בונים שפת ריפוד B, ומעליה **בונים** את M_B שמשתמשת	בנייה

#	מה קורה	מקור
	ב-M_A כקופסה שחורה $\Longleftarrow$ מסיקים $B \in \mathrm{E}$	
3	ההכלה הנתונה $\Longleftarrow$ $B \in \mathrm{PSPACE}$ ⟵ **מקבלים** את $\widetilde{M_B}$ עם חסם **מקום** (כי PSPACE מוגדרת במקום)	מהשמיים
4	**בונים** את $\widetilde{M_A}$ שמכריעה את A בעזרת $\widetilde{M_B}$ $\Longleftarrow$ מסיקים $A \in \mathrm{PSPACE}$	בנייה

הערה מההקלטה [00:40:10]: סטודנט שאל למה בכלל צריך את מכונות ה"גל" ($\sim$) אם כבר יש M_A, M_B. התשובה: על M_A ו-M_B יש לנו מידע על **זמן** בלבד. כדי להסיק שייכות ל-PSPACE אנחנו חייבים מכונה שאנו יודעים לחסום את ה**מקום** שלה — ולכן חייבים לקבל מכונה חדשה. המעבר הזה, ממשאב אחד למשאב אחר או ממודל אחד לאחר, הוא כל תוכן ההוכחה.

משפט 2: $\mathrm{E} \neq \mathrm{PSPACE}$

זו טענה **לא מותנית** — והיא מודגמת כאן כדי להראות שטענות מותנות מסוג משפט 1 אינן חסרות ערך.

כיצד מוכיחים אי־שוויון בין קבוצות? $\mathrm{E} \neq \mathrm{PSPACE}$ פירושו: $\mathrm{E} \not\subseteq \mathrm{PSPACE}$ **או** $\mathrm{PSPACE} \not\subseteq \mathrm{E}$. זו טענת "או", ולכן מוכיחים אותה בהפרדה למקרים: מניחים שהחלק הראשון **אינו** מתקיים ומוכיחים את השני. (המרצה הדגיש: לטענת "או" מספיק צד אחד, ואין צורך בהוכחה בשלילה.)

הוכחה. אם $\mathrm{E} \not\subseteq \mathrm{PSPACE}$ — סיימנו. נניח אפוא $\mathrm{E} \subseteq \mathrm{PSPACE}$; נראה $\mathrm{PSPACE} \not\subseteq \mathrm{E}$. ממשפט 1 נובע $\hat{\mathrm{E}} \subseteq \mathrm{PSPACE}$.

לכל $c > 0$ מתקיים $2^{cn} = O\left(2^{n^2}\right)$ (שכן $cn \le n^2$ לכל $n \ge c$). לפי מונוטוניות במשאב, $\mathrm{DTime}(2^{cn}) \subseteq \mathrm{DTime}\left(2^{n^2}\right)$. הכלה נשמרת תחת איחוד, ולכן

$$\mathrm{E} \;\subseteq\; \mathrm{DTime}\left(2^{n^2}\right).$$

עכשיו נפעיל את משפט ההיררכיה בזמן על שתי **מחלקות עדינות**. נסמן

$$g(n) = 2^{n^2}, \qquad f(n) = 2^{2n^2}, \qquad \text{so} \qquad f^2(n) = \left(2^{2n^2}\right)^2 = 2^{4n^2}.$$

f סופר־לינארית וישימה בזמן, ומתקיים $g = o(f)$ שכן $g(n)/f(n) = 2^{-n^2} \xrightarrow[n\to\infty]{} 0$. לכן

$$\mathrm{DTime}\left(2^{n^2}\right) \subsetneq \mathrm{DTime}\left(2^{4n^2}\right).$$

מהגדרת $\hat{\mathrm{E}}$ (עם $c = 4$) מתקיים $\mathrm{DTime}\left(2^{4n^2}\right) \subseteq \hat{\mathrm{E}}$.
נשרשר: $\mathrm{E} \subseteq \mathrm{DTime}\left(2^{n^2}\right) \subsetneq \mathrm{DTime}\left(2^{4n^2}\right) \subseteq \hat{\mathrm{E}} \subseteq \mathrm{PSPACE}$. בשרשרת הכלות שאחת מהן ממש, ההכלה בין הקצוות היא ממש, ולכן

$$\mathrm{E} \subsetneq \mathrm{PSPACE}.$$

מהכלה ממש נובע $\mathrm{PSPACE} \not\subseteq \mathrm{E}$, ובפרט $\mathrm{E} \neq \mathrm{PSPACE}$. ■

> **הערה:** המרצה ציין ש"בדרך הזו" השתמשנו במשפט 1 בצורה חזקה מאוד — בלעדיו לא היה לנו מסלול מ-E אל $\hat{\mathrm{E}}$ בתוך PSPACE. וכן: **הכלה** נשמרת תחת איחוד, **הכלה ממש** לא — ולכן שלב 3 נעשה על מחלקות עדינות דווקא.

משפט 3: אם $\mathrm{P} = \mathrm{NP}$ אז $\mathrm{EXP} = \mathrm{NEXP}$
בניסוח שהוצג בכיתה: **הראו כי אם $\mathrm{EXP} \neq \mathrm{NEXP}$ אז $\mathrm{P} \neq \mathrm{NP}$.**
צמצום הניסוח. ראשית מעיפים את השלילות במעבר לנגדי־חיובי: הטענה שקולה ל"אם $\mathrm{P} = \mathrm{NP}$ אז $\mathrm{EXP} = \mathrm{NEXP}$". שנית, כבר ידוע (שיעור 4) ש-$\mathrm{P} \subseteq \mathrm{NP}$ ו-$\mathrm{EXP} \subseteq \mathrm{NEXP}$; לכן כל מה שהטענה מחדשת הוא ההכלה בכיוון השני, ומספיק להוכיח:

> אם $\mathrm{NP} \subseteq \mathrm{P}$ אז $\mathrm{NEXP} \subseteq \mathrm{EXP}$.

וזו כבר טענה מן הצורה "אם הכלה אז הכלה" — מועמדת מובהקת לריפוד.
הוכחה. נניח $\mathrm{NP} \subseteq \mathrm{P}$, ותהי $A \in \mathrm{NEXP}$.
מכונה 1. קיים $c \geq 1$ כך ש-$A \in \mathrm{NTime}\left(2^{n^c}\right)$, ולכן קיימת מכונה **א־דטרמיניסטית** M_A וקיים $d > 0$ כך ש-M_A מכריעה את A באופן א־דטרמיניסטי ולכל x:

$$\mathrm{time}_{M_A}(x) \;\leq\; d \cdot 2^{\,|x|^c}.$$

(ההדגשה "א־דטרמיניסטית" חיונית: ללא ציון אחר, "מכונה" פירושה מכונה דטרמיניסטית סטנדרטית.)
כמה לרפד? זה החישוב היחיד שדורש מחשבה, והמרצה עשה אותו בקול. אני רוצה ש-B תהיה ב-NP, כלומר שזמן הריצה יהיה **פולינומי ב-$|y|$**. אבל הזמן היקר הוא הרצת M_A, שהוא **מעריכי ב-$|x|$**. כדי שאותו מספר צעדים ייראה פולינומי, $|y|$ חייב להיות מעריכי ב-$|x|$. לכן הריפוד יהיה מעריכי — וניקח מיד את הקבוע d פנימה, כדי שהחשבון יֵצא נוח:

$$B = \left\{ \, x\#^{\,d\cdot 2^{|x|^c}} \;\middle|\; x \in A \, \right\}, \qquad \# \notin \Sigma.$$

מכונה 2. נגדיר מכונה א־דטרמיניסטית M_B, שעל קלט $y \in (\Sigma \cup \{\#\})^*$:

תוודא ש-y מהצורה $x\#^{\ell}$ עם $x \in \Sigma^*$; אחרת תדחה.
תחשב את $d \cdot 2^{|x|^c}$ ותוודא ש-$\ell = d \cdot 2^{|x|^c}$; אחרת תדחה.
תריץ את M_A על x ותחזיר את תשובתה.

שימו לב: **שלבים 1 ו-2 דטרמיניסטיים לחלוטין**; כל האי־דטרמיניזם של M_B יושב בתוך הרצת M_A בשלב 3. M_B "מחזיקה את M_A בבטן" ומריצה אותה, ולכן היא יורשת ממנה את האי־דטרמיניזם. (אין כאן שימוש במכונה אוניברסלית: כשאנו בונים את M_B אנו כבר מכירים את M_A וקובעים אותה בתוך המכונה.)

נכונות — בטרמינולוגיה של אי־דטרמיניזם.

כיוון ראשון. נניח $y \in B$, כלומר $y = x\#^{d\cdot 2^{|x|^c}}$ עבור $x \in A$. שלבים 1 ו-2 דטרמיניסטיים ויעברו בכל ריצה. כיוון ש-$x \in A$ ו-M_A מכריעה את A א־דטרמיניסטית, **קיימת** ריצה של M_A על x שמסתיימת במצב מקבל. לכן **קיימת** ריצה של M_B על y שמסתיימת במצב מקבל — זו שבה M_B בוחרת בשלב 3 את הבחירות של אותה ריצה מקבלת.

כיוון שני. נניח שקיימת ריצה של M_B על y המסתיימת במצב מקבל. בריצה זו שלבים 1 ו-2 עברו, ולכן קיים $x \in \Sigma^*$ עם $y = x\#^{d\cdot 2^{|x|^c}}$. כמו כן, בריצה זו ההרצה של M_A על x הסתיימה במצב מקבל, ולכן $x \in A$. מכאן $y \in B$.

בנוסף, כל ריצה של M_B עוצרת, כי שלבים 1–2 סופיים וכל ריצה של M_A עוצרת. לכן M_B מכריעה את B באופן א־דטרמיניסטי.

חשבון הזמן של M_B. נסמן $y = x\#^{\ell}$.

שלב 1: סריקה אחת, $O(|y|)$ צעדים.

שלב 2: מהישימות בזמן של $n \mapsto d \cdot 2^{n^c}$, החישוב עולה $O\big(2^{|x|^c}\big)$ צעדים. וכיוון ש-$|y| \geq d \cdot 2^{|x|^c}$, זהו $O(|y|)$.

שלב 3: מהגדרת M_A, לכל היותר $d \cdot 2^{|x|^c}$ צעדים — שהם, שוב, לכל היותר $|y|$.

סך הכול $\mathrm{time}_{M_B}(y) = O(|y|)$, כלומר $B \in \mathrm{NTime}(n) \subseteq \mathrm{NP}$. הריפוד הוריד את הסיבוכיות ממעריכית ללינארית — לא מפני שהחישוב התייעל, אלא מפני שהמכנה גדל.

מכונה 3. מההנחה $\mathrm{NP} \subseteq \mathrm{P}$ נובע $B \in \mathrm{P}$, ולכן קיים $\alpha > 0$ כך ש-$B \in \mathrm{DTime}(n^{\alpha})$, ולכן קיימת מכונה **דטרמיניסטית** $\widetilde{M_B}$ וקיים $\beta > 0$ כך ש-$\widetilde{M_B}$ מכריעה את B ולכל y:

$$\mathrm{time}_{\widetilde{M_B}}(y) \;\leq\; \beta \cdot |y|^{\alpha}.$$

מכונה 4. נגדיר מכונה דטרמיניסטית $\widetilde{M_A}$ שעל קלט x:
תחשב את $d \cdot 2^{|x|^c}$ ותבנה את $y = x\#^{\,d\cdot 2^{|x|^c}}$.
תריץ את $\widetilde{M_B}$ על y ותחזיר את אותה תשובה.

ההוכחה ש-$\widetilde{M_A}$ מכריעה את A זהה מילה במילה לזו שבמשפט 1: $x \in A \iff x\#^{d\cdot 2^{|x|^c}} \in \widetilde{M_B}$ מקבלת אותו.

הערה: בהרצאה השלב הזה נאמר במשפט אחד ("תשלימו בדיוק אותה הוכחה"); הפירוט המלא: אם $x \in A$ אז לפי הגדרת B מתקיים $y \in B$, ו-$\widetilde{M_B}$ מכריעה את B ולכן מקבלת. אם $x \notin A$, אז אף איבר של B אינו מהצורה $x\#^{d\cdot 2^{|x|^c}}$ עבור x זה, ולכן $y \notin B$ ו-$\widetilde{M_B}$ דוחה. בשני המקרים $\widetilde{M_A}$ מחזירה את התשובה הנכונה, והיא עוצרת תמיד.

חשבון הזמן של $\widetilde{M_A}$. יהי $x \in \Sigma^*$.

שלב 1: מהישימות בזמן של $d \cdot 2^{n^c}$, החישוב עולה $O\left(2^{|x|^c}\right)$; כתיבת y עולה עוד $|x| + d \cdot 2^{|x|^c} = O\left(2^{|x|^c}\right)$ צעדים.

שלב 2: לכל היותר $\beta|y|^\alpha = \beta\left(|x| + d\cdot 2^{|x|^c}\right)^\alpha$ צעדים.

הגורם הדומיננטי הוא השני, והעלאה בחזקת α מכניסה את α כמקדם במעריך:

$$\mathrm{time}_{\widetilde{M_A}}(x) \;\le\; O\left(2^{|x|^c}\right) + \beta\left(|x| + d\cdot 2^{|x|^c}\right)^{\alpha} \;=\; O\left(2^{\,\alpha|x|^c}\right) \;=\; O\left(2^{\,|x|^{c+1}}\right),$$

כאשר המעבר האחרון תקף כי $\alpha|x|^c \le |x|^{c+1}$ לכל $|x| \ge \alpha$, וקלטים קצרים יותר נבלעים בקבוע. לכן

$$A \in \mathrm{DTime}\left(2^{\,n^{c+1}}\right) \subseteq \mathrm{EXP}. \qquad \blacksquare$$

הערה מההקלטה [01:10:09]: אודליה שאלה אם המעבר בריפוד תמיד יהיה "זמן $\leftrightarrow$ מקום". התשובה: לא. כאן זה **מזמן לזמן**, אבל **מא־דטרמיניסטי לדטרמיניסטי**. תמיד יש איזשהו מעבר בין משהו למשהו, אך הוא לא תמיד זמן ומקום — ומבחינת מבנה ההוכחה זה שקוף לחלוטין.

משפט 4: $\mathrm{SAT} \in \mathrm{NP}$

הוכחה. נבנה מכונת טיורינג א־דטרמיניסטית **דו־סרטית** M, שעל קלט $\langle\varphi\rangle$:

נספור את מספר המשתנים ב-φ (בפועל: האינדקס הגדול ביותר המופיע בנוסחה) ונסמנו n.

נכתוב n ביטים **באופן א־דטרמיניסטי** על הסרט השני.

נתייחס לביטים כאל הסמה v (הביט ה-i הוא $v(x_i)$) ונבדוק אם v מספקת את φ; נקבל אם כן, ונדחה אחרת.

נכונות. אם φ ספיקה, קיימת הסמה v המספקת אותה; קיימת ריצה של M שבשלב 2 כותבת בדיוק את מחרוזת הביטים המתאימה ל-v, ובריצה זו שלב 3 מוצא שהנוסחה מסופקת ומקבל. לכן קיימת ריצה מקבלת. להפך, אם קיימת ריצה מקבלת, אז המחרוזת שנכתבה בה בשלב 2 מגדירה הסמה שעברה את הבדיקה בשלב 3, כלומר הסמה שמספקת את φ — ולכן φ ספיקה. בנוסף כל ריצה עוצרת: שלב 2 כותב בדיוק n ביטים, ושלבים 1 ו-3 דטרמיניסטיים וסופיים. לכן M מכריעה את SAT באופן א־דטרמיניסטי.

הערה: בהרצאה נאמר "אם הנוסחה ספיקה קיימת אפשרות לכתוב הסמה מספקת על הסרט השני" ותו לא; הנימוק המפורט לשני הכיוונים הוא הפירוט שלנו. המרצה השאיר במפורש את המשך ההוכחה כשיעורי בית לשיעור הבא [02:05:32].

חשבון הזמן. נסמן $m = |\langle\varphi\rangle|$ ו-$n \le m$ את מספר המשתנים.
שלב 1: סריקה של הקידוד תוך שמירת האינדקס המרבי — $O(m^2)$ צעדים בגבול העליון הגס (סריקה אחת לכל השוואה); בוודאי פולינומי.
שלב 2: כתיבת $n \le m$ ביטים — $O(m)$ צעדים.
שלב 3: עוברים על הנוסחה ליטרל־ליטרל; לכל ליטרל ניגשים לביט המתאים בסרט השני, מה שעולה לכל היותר $O(m)$ צעדי הזזה. מספר הליטרלים חסום ב-m, ולכן $O(m^2)$ צעדים.
סך הכול $\mathrm{time}_M(\langle\varphi\rangle) = O(m^2)$ — פולינומי.
מעבר למכונה סטנדרטית. המחלקות מוגדרות באמצעות מכונות **חד־סרטיות**, ולכן נותר לתרגם. מהשקילות בין המודלים (שיעור 1), סימולציה של מכונה רב־סרטית במכונה חד־סרטית עולה לכל היותר ריבוע בזמן; לכן קיימת מכונה א־דטרמיניסטית חד־סרטית $\widehat{M}$ שמכריעה את SAT בזמן $O(m^4)$. מכאן

$$\mathrm{SAT} \in \mathrm{NTime}\big(n^4\big) \subseteq \mathrm{NP}. \qquad \blacksquare$$

הערה מההקלטה [02:03:54]: "לכתוב באופן א־דטרמיניסטי" **אינו** "לכתוב באקראי". אין כאן שום הסתברות: פונקציית המעברים פשוט מאפשרת גם לכתוב 0 וגם לכתוב 1, ואנחנו שואלים אם **קיימת** בחירה נכונה. לא בכל ריצה המכונה תבחר נכון — אבל קיימת לה אפשרות כזו. הסתברות היא מודל אחר לגמרי.

דוגמאות ותרגילים מהשיעור
דוגמה 1: מעקב אחרי מילה קונקרטית בריפוד הריבועי
ניקח $\Sigma = \{0,1\}$ ונניח ש-$x = \mathtt{101} \in A$, כאשר $A \in \hat{\mathrm{E}}$ עם $c = 1$ ו-$d = 1$, כלומר רצה על x לכל היותר $2^{|x|^2} = 2^9 = 512$ צעדים.
קדימה (מ-A ל-B): $|x| = 3$, ולכן $|x|^2 = 9$ ו-

$$y = \mathtt{101}\#\#\#\#\#\#\#\#\#, \qquad |y| = 3 + 9 = 12.$$

M_B על y: שלב 1 סורק 12 תווים ומוודא שאחרי ה-$\#$ הראשון אין תו מ-Σ — עובר. שלב 2 מחשב $3^2 = 9$ ומשווה ל-9 — עובר. שלב 3 מריץ את M_A על $\mathtt{101}$ ב-≤ 512 צעדים. סך הצעדים $\le 2^{c|y|}$ ואכן ההרצה נכנסת בתקציב $12 + 9 + 512 < 2^{1\cdot 12} = 4096$.
אחורה (מ-B ל-A): $\widetilde{M_A}$ על $\mathtt{101}$ מחשבת 9, כותבת את אותו y באורך 12, ומריצה עליו את $\widetilde{M_B}$ במקום $\le \beta \cdot 12^\alpha$ — שהוא $O\big(3^{2\alpha}\big)$, כלומר פולינומי ב-$|x|$.

היכן זה נשבר בכוונה: המילה $y' = 101\#\#\#\#$ (זנב באורך 4) תיפול בשלב 2, וזה נכון — היא באמת אינה ב-B. וזו הסיבה ששלב 2 אינו מותרות: בלעדיו M_B הייתה מקבלת מילים קצרות מדי, וחשבון הזמן שנשען על $|x|^2 \le |y|$ היה קורס.

דוגמה 2: מעקב בריפוד המעריכי

נניח $A \in \mathrm{NTime}\left(2^{n^2}\right)$ (כלומר $c = 2$), $d = 1$, ו-$x = 10$. גודל הריפוד: $|x| = 2$, ולכן $|y| = 2 + 16 = 18$. $d \cdot 2^{|x|^c} = 2^4 = 16$.

M_A על x רצה לכל היותר 16 צעדים. ביחס ל-y זה $18 \le$ צעדים — **לינארי**. אותו מספר צעדים בדיוק, מכנה גדול פי תשעה. זה, בשורה אחת, כל טיעון הריפוד.

דוגמה 3: הבדיקה שהנוסחה מסופקת (הדוגמה מהסיכום)

נתונה הנוסחה

$$\varphi = (x_1 \vee \overline{x_2} \vee x_3) \wedge (x_2 \vee x_3 \vee \overline{x_4}).$$

יש בה ארבעה משתנים (הם חוזרים על עצמם, אך המשתנים הם x_1, x_2, x_3, x_4), ולכן M תכתוב בשלב 2 מחרוזת באורך **4**.

ריצה שנכשלת: נניח שנכתב 0100, כלומר $v(x_1) = 0,\ v(x_2) = 1,\ v(x_3) = 0,\ v(x_4) = 0$. הפסוקית הראשונה: $v(x_1) = 0$, $v(\overline{x_2}) = 0$, $v(x_3) = 0$ — כולם F, ולכן הפסוקית אינה מסופקת, ולכן v אינה מספקת את φ. הריצה הזו דוחה.

ריצה שמצליחה: לו נכתב 1101, כלומר $v(x_1) = 1,\ v(x_2) = 1,\ v(x_3) = 0,\ v(x_4) = 1$. הפסוקית הראשונה: $v(x_1) = 1$ — מסופקת. הפסוקית השנייה: $v(x_2) = 1$ — מסופקת. לכן v מספקת את φ והריצה מקבלת.

המסקנה: קיימת ריצה מקבלת, ולכן M מקבלת את $\langle \varphi \rangle$ — כנדרש, שכן φ אכן ספיקה. שימו לב שהריצה הדוחה אינה סתירה: בהכרעה א־דטרמיניסטית מספיק ש**קיימת** ריצה מקבלת.

תרגיל 1 (נשאל בכיתה): הנוסחה שאינה ספיקה

שאלה: לפי ההגדרה מרגיש כאילו כל נוסחה ספיקה. תנו דוגמה לנוסחה שאינה ספיקה.

פתרון: $\varphi = x_1 \wedge \overline{x_1}$. יש כאן משתנה יחיד, ולכן שתי הסמות אפשריות בלבד. אם $v(x_1) = T$ אז $v(\overline{x_1}) = F$ ולכן $v(\varphi) = F$; אם $v(x_1) = F$ אז $v(\varphi) = F$. בשני המקרים F, ולכן לא קיימת הסמה מספקת ו-$\langle \varphi \rangle \notin \mathrm{SAT}$.

תרגיל 2 (השאלה המכינה מהשיעור הקודם)

שאלה: מכונה רצה מיליון צעדים. מכניסים לה קלט **גדול יותר** והיא רצה את אותו מספר צעדים. סיבוכיות הריצה עלתה או ירדה?

פתרון: **ירדה.** סיבוכיות נמדדת תמיד ביחס לאורך הקלט. אם מספר הצעדים לא השתנה (או השתנה עד כדי קבוע) והקלט התארך, אז אני "משלם את אותו מחיר על קלט גדול יותר". זו בדיוק ההצדקה לריפוד: לא מייעלים כלום, רק מגדילים את המכנה.

תרגיל 3 (הכיוון של הריפוד — כמה לרפד?)

שאלה: בטענה על NEXP, מדוע לא הספיק ריפוד ריבועי כמו במשפט 1?

פתרון: מטרתנו הייתה $B \in \mathrm{NP}$, כלומר זמן פולינומי ב-$|y|$. הצוואר הוא הרצת M_A, שעולה $d \cdot 2^{|x|^c}$ — מעריכי ב-$|x|$. ריפוד ריבועי נותן $|y| = O\big(|x|^2\big)$, ואז $d \cdot 2^{|x|^c}$ **אינו** פולינומי ב-$|y|$. רק ריפוד **מעריכי** מביא את $|y|$ לאותו סדר גודל כמו מספר הצעדים, ואז אותו מספר צעדים נעשה לינארי ב-$|y|$. הכלל האצבע שהמרצה נתן: כתבו את החסם הרצוי, כתבו את החסם שיש, וראו איזה $|y|$ מגשר; אם חורגים — הקטינו או הגדילו את הריפוד ונסו שוב.

תרגיל 4 (האינטואיציה מההקלטה המקבילה, [02:07:54]–[02:13:14])

שאלה: קחו את השפה $A = \{x \mid x \text{ is a composite number in binary}\}$ ואת האלגוריתם הנאיבי שעובר על כל המספרים מ-1 עד x ומנסה לחלק. מה זמן הריצה שלו, ומה קורה אם משנים את הקידוד לאונרי?

פתרון: בקידוד **בינרי**, אורך הקלט הוא $\Theta(\log x)$ בעוד שמספר הפעולות הוא $\Theta(x)$ (ואף יותר, בגלל עלות כל חילוק). לכן ביחס לאורך הקלט זמן הריצה הוא $2^{\Theta(|x|)}$ — מעריכי. בקידוד **אונרי**, אורך הקלט הוא בדיוק x; **אותו אלגוריתם בדיוק**, ללא שינוי של תו אחד, רץ עכשיו בזמן פולינומי (סדר גודל $|x|^2$) ביחס לאורך הקלט.

המסקנה: שינוי מלאכותי של אורך הקלט משנה את הסיווג הסיבוכיותי של אותו אלגוריתם. הריפוד הוא בדיוק המהלך הזה, מנוסח כשפה חדשה במקום כקידוד חדש.

הערות מהשיעור

[00:09:20] "בדרך תהיינה ארבע מכונות." שתיים מקבלים משייכות למחלקה, שתיים בונים. שווה לכתוב את הספירה הזו בשוליים לפני שמתחילים — היא מונעת אבדן דרך באמצע.

[00:19:31] שאלת סטודנט: איך M_A מכירה את התו $\#$, הרי הוא לא באלף־בית של A? *תשובה:* היא אינה מכירה אותו, ואינה צריכה — M_A מורצת **רק על** x, לא על הזנב. בעקבות השאלה המרצה חידד את הכתיבה והוסיף במפורש "כאשר $x \in \Sigma^*$", וסימן Σ = האלף־בית של A.

[00:21:04] מוסכמה: אחרי כל שלב אפשר לכתוב "אחרת נדחה", במקום שלב מסכם רביעי. שתי הכתיבות שקולות; בסיכום מופיע שלב 4 מפורש, בהקלטה הוא נבלע בשלבים.

[00:33:10] הניסוח המדויק של הרווח: "מספר הצעדים לא השתנה, אבל הכול גדל, אז פתאום אני משלם פחות **ביחס לקלט**."

[00:45:28] הישימות אינה טכניקליות. בכל טיעון ריפוד יש לומר במפורש שפונקציית הריפוד ישימה (בזמן, במקום, או בשניהם — לפי מה שחוסמים). "היא תמיד תהיה חשובה בריפוד, אז תמיד צריך להגיד את זה" [01:34:30].

[00:59:45] מלכודת מושגית: $\mathrm{E} = \mathrm{PSPACE}$ היא טענה על **שפות**. אין טענה שמכונה שרצה בזמן כזה תרוץ במקום כזה; הטענה היא שאם קיימת מכונה אחת, קיימת מכונה אחרת. בכל ההכלות הסטנדרטיות שראינו עד כה המכונה נשארה אותה מכונה — כאן, לראשונה, החלפנו מכונות.

[01:00:17] טכניקה לטענת "או": מוכיחים בהפרדה למקרים — מניחים שהחלק הראשון אינו מתקיים ומוכיחים את השני. אין צורך להוכיח את שני הצדדים, ואין צורך בהוכחה בשלילה.

[01:05:46] שאלת סטודנט: מאיפה הופיעה פתאום הכלה **ממש**? *תשובה:* היא הגיעה ממשפט ההיררכיה בזמן, והיא נשמרת: בשרשרת הכלות שאחת מהן ממש, ההכלה בין הקצוות היא ממש.

[01:38:48] כלל עבודה: ריפוד מוכיח **הכלה**. אם רוצים הכלה **ממש**, מפרקים לשתיים — הכלה בכיוון אחד, ואי־הכלה בכיוון השני. לא מערבבים את שני המהלכים.
[01:06:25] הערת מבחן/תרגיל: "תקבלו תרגיל ממש ממש דומה בשיעורי הבית. תעקבו אחד לאחד וזה מסתדר." המבנה קבוע; הדבר היחיד שמשתנה בין שאלה לשאלה הוא **גודל הריפוד**.
[01:25:06] שאלת סטודנט: האם M_B היא מכונה א־דטרמיניסטית מפני ש"משכנו" אליה את האי־דטרמיניזם של M_A? *תשובה:* כן בדיוק. היא מחזיקה את M_A בתוכה ומריצה אותה, ולכן יורשת את האי־דטרמיניזם.
[01:45:45] טרמינולוגיה: "טפל" (tuple) ולא "סדרה" — סדרה מרמזת על אינסופיות, ופסוקית היא סופית תמיד. "הסגר" ו"פסוקית" הם שני שמות לאותו מושג.
[02:06:05] מה נשאר פתוח לשיעור הבא: להוכיח פורמלית ש-M מכריעה את SAT באופן א־דטרמיניסטי, לחשב את זמן הריצה, ולעבור למכונה חד־סרטית ("לא לשכוח שהמחלקות מוגדרות על ידי מכונה חד־סרטית"). הפירוט המלא הוזן כאן לתוך משפט 4.

פערים בין הסיכום להקלטה
מקור: עמוד 6 בסיכום. **הפער:** כתוב "$B \in \mathrm{NSpace}(n) \subseteq \mathrm{NP}$" מיד אחרי שחושב חסם **זמן** $\mathrm{time}_{M_B}(y) \le O(|y|)$. **ההכרעה:** זו פליטת קולמוס; הנכון הוא $\mathrm{NTime}(n) \subseteq \mathrm{NP}$ (ואכן $\mathrm{NSpace}(n) \subseteq \mathrm{NP}$ אינה טענה נכונה כלל). ההקלטה [01:28:57] מאשרת: "B הוא אפילו בזמן ליניארי, אבל זה מוכל ב-NP". תוקן בגוף.
מקור: עמוד 6 בסיכום. **הפער:** כתוב "קיים $\alpha > 0$ כך ש-$B \in \mathrm{DSpace}(n^\alpha)$" — אף שההנחה היא $B \in \mathrm{P}$, ואף שהשורה הבאה בסיכום עצמו נוקבת בחסם **זמן** $\mathrm{time}_{\widetilde{M_B}} \le \beta|y|^\alpha$. **ההכרעה:** אותה פליטת קולמוס (Space במקום Time). הנכון הוא $B \in \mathrm{DTime}(n^\alpha)$. תוקן בגוף.
מקור: עמוד 5 בסיכום. **הפער:** מספור השלבים של M_B במקרה ה-NEXP הוא ①,③,④ — שלב ② חסר. **ההכרעה:** מספור בלבד, ללא חוסר מתמטי; מוספרו כאן 1,2,3 בעקביות עם ההוכחה הראשונה.
מקור: ההקלטה. **הפער:** בהקלטה מופיעה שאלה מכינה ("מכונה שרצה מיליון צעדים על קלט גדול יותר — הסיבוכיות עלתה או ירדה?") שהיא הגרעין האינטואיטיבי של כל הטכניקה, ואינה מופיעה בסיכום כלל. **ההכרעה:** נכללה כתרגיל 2 וכהערה.
מקור: ההקלטה [00:42:15]–[00:45:28]. **הפער:** דיון ארוך ומהותי מדוע אי אפשר לחסום את המקום באורך הפלט, ומדוע דווקא הישימות במקום היא שמצילה — אין לו זכר בסיכום. **ההכרעה:** נכלל כהערה בסעיף הרקע.
מקור: ההקלטה [01:14:30]–[01:16:02]. **הפער:** ההסבר *כיצד בוחרים את גודל הריפוד* (כותבים את החסם הרצוי, את החסם הקיים, ומגשרים; ואם חורגים — מנסים שוב) הוא הדבר היחיד שדורש מחשבה בהוכחה, והסיכום מציג רק את התוצאה. **ההכרעה:** נכלל בגוף משפט 3 ובתרגיל 3.
מקור: ההקלטה השנייה (zcCQY3oT40Y). **הפער:** ההקלטה כולה, פרט לשבע הדקות האחרונות, עוסקת בחומר של שיעור אחר (המודל הא־דטרמיניסטי, דוגמת המספרים הפריקים, ואפיון NP באמצעות מוודא ועדות והוכחת השקילות). **ההכרעה:** סומנה `partial` ; מתוכה נלקחה רק

ההקדמה המוטיבציונית לריפוד (בינרי מול אונרי), שנכללה כתרגיל 4. אין בה גרסה שנייה של ההוכחות, ולכן הצלבת החסמים נעשתה מול הסיכום בלבד.

מקור: ההקלטה [02:01:15] מול עמוד 8 בסיכום. **הפער:** בכתוביות האוטומטיות הפסוקית השנייה בדוגמה נשמעת "$x_2 \vee x_3 \vee x_4$" ללא שלילה, ובסיכום היא $(x_2 \vee x_3 \vee \overline{x_4})$. **ההכרעה:** הסיכום מנצח (וממילא ההסמה 1101 מספקת את שתי הגרסאות). כמו כן, מחרוזות ההסמה בכתוביות מקוטעות ("$1\,0\,1$", "$1\,0\,1$"); הסיכום נוקב ב-0100 ו-1101, ואלו נבדקו ונמצאו נכונות.

מקור: ההקלטה [02:05:32] והסיכום עמוד 8. **הפער:** שני המקורות עוצרים אחרי תיאור המכונה ל-SAT ולפני חשבון זמן הריצה והמעבר למכונה חד־סרטית. **ההכרעה:** ההשלמה נכתבה כאן במלואה וסומנה כהשלמה בהערה; ראו גם `open_questions` .

מקור: עמוד 3 בסיכום. **הפער:** הערה סגולה בשוליים השמאליים, שנראה שהיא מסבירה מדוע הריפוד הוא בגודל n^2, קריאה רק חלקית. **ההכרעה:** שוחזרה מתוך ההסבר המקביל בהקלטה [00:50:55] ("מכיוון שההבדל בין E ל-$\hat{\mathrm{E}}$ היה רק שה-n עולה בריבוע, ריפדתי בריבוע").

סיכום ונקודות למבחן

מה לזכור בעל פה

$$\mathrm{E} = \bigcup_{c \geq 1} \mathrm{DTime}(2^{cn}), \qquad \hat{\mathrm{E}} = \bigcup_{c \geq 1} \mathrm{DTime}\left(2^{cn^2}\right), \qquad B = \left\{ x \#^{p(|x|)} \mid x \in A \right\}.$$

התבנית של ארבע המכונות: מקבלים–בונים–מקבלים–בונים. שני ה"מקבלים" באים משייכות למחלקה (אחרי קילוף האיחוד), שני ה"בונים" הם עבודה שלכם.

שלושת השלבים של מכונת הריפוד: בדיקת צורה → חישוב הריפוד ובדיקת אורך → הרצת המכונה הישנה כקופסה שחורה. אף פעם לא יותר מזה.

הכיוון של שתי הטענות: אם $\mathrm{E} \subseteq \mathrm{PSPACE}$ אז $\hat{\mathrm{E}} \subseteq \mathrm{PSPACE}$ (מהקטנה לגדולה!); אם $\mathrm{NP} \subseteq \mathrm{P}$ אז $\mathrm{NEXP} \subseteq \mathrm{EXP}$, כלומר $\mathrm{EXP} \neq \mathrm{NEXP} \Rightarrow \mathrm{P} \neq \mathrm{NP}$ — ולא ההפך.

התוצאה הלא מותנית: $\mathrm{E} \neq \mathrm{PSPACE}$, ולמעשה בכל מקרה $\mathrm{PSPACE} \not\subseteq \mathrm{E}$ או $\mathrm{E} \not\subseteq \mathrm{PSPACE}$.

$\mathrm{SAT} = \{\langle \varphi \rangle \mid \varphi$ **CNF satisfiable**$\}$**,** ו-$\mathrm{SAT} \in \mathrm{NP}$ באמצעות "ניחוש" הסמה ואימותה.

מלכודות סטנדרטיות

לרפד בכיוון הלא נכון. הריפוד תמיד מוסיף אורך; הוא מוריד סיבוכיות **יחסית**, לעולם לא מוריד מספר צעדים. אם החשבון שלכם "חוסך צעדים" — טעיתם.

לשכוח את בדיקת אורך הזנב. בלי שלב 2, השפה B מכילה מילים שלא התכוונתם אליהן וכל חשבון הזמן קורס.

לשכוח לומר "ישימה בזמן / במקום". זה נקודות במבחן, וזה גם באמת נחוץ.

לערבב הכלה עם הכלה ממש. הכלה נשמרת תחת איחוד; הכלה ממש לא. משפט ההיררכיה חל על מחלקות **עדינות** בלבד.

לבלבל אי־דטרמיניזם עם אקראיות. "קיימת ריצה מקבלת" אינו "בהסתברות גבוהה".

לכתוב $x_1 = T$. משתנה אינו ערך; רק הסמה נותנת ערך.
להניח שמכונה נשארת אותה מכונה בין שתי מחלקות. טענות ההכלה הן על שפות.
צ'ק־ליסט: מה צריך לדעת לעשות אחרי השיעור

- [ ] בהינתן שתי מחלקות וטענה מותנית מסוג "אם הכלה אז הכלה", לקבוע **מה גודל הריפוד** מתוך חשבון של החסם הרצוי מול החסם הקיים.
- [ ] לכתוב מכונת ריפוד בשלושת שלביה ולהוכיח שהיא מכריעה את השפה המרופדת, בשני הכיוונים — ובמקרה הא־דטרמיניסטי, בטרמינולוגיה של "קיימת ריצה מקבלת".
- [ ] לבצע את שני חשבונות המשאב (של M_B ושל $\widetilde{M_A}$) עד הסוף, כולל המעבר מ-$|x|$ ל-$|y|$ ובחזרה.
- [ ] לשלב ריפוד עם משפט ההיררכיה כדי לקבל תוצאה לא מותנית, כולל ההפרדה למקרים בהוכחת טענת "או".
- [ ] להגדיר ליטרל, פסוקית, נוסחת CNF, הסמה וספיקות במדויק, ולהבחין בין תחביר לסמנטיקה.
- [ ] לתאר את המכונה הא־דטרמיניסטית עבור SAT, לנתח את זמן ריצתה, ולהסביר את המעבר למכונה חד־סרטית.

שאלות שנשארו פתוחות

עמוד 3 בסיכום: הערה סגולה בשוליים השמאליים על הסיבה לבחירת ריפוד בגודל n^2 קריאה רק חלקית; שוחזרה לפי ההסבר המקביל בהקלטה [00:50:55].

מספרי השיעורים שאליהם מפנה סעיף הרקע (3 למשפטי ההיררכיה, 4 למודל הא־דטרמיניסטי) נגזרו מתיאור המרצה בפתיחת ההקלטה ולא מקובץ שיעור קיים; כדאי לאמת מול המניפסט.

ההוכחה ש-$\mathrm{SAT} \in \mathrm{NP}$ נותרה חלקית בהקלטה: המרצה השאיר את חשבון זמן הריצה ואת המעבר למכונה חד־סרטית כשיעורי בית לשיעור הבא; הפירוט כאן הוא השלמה שלנו ואינו מופיע בסיכום.

6 הגדרה שקולה ל-NP: אימות, עדים ואישורים

מוכיחים שהמחלקה NP, שהוגדרה באמצעות מכונות אי-דטרמיניסטיות פולינומיות, שקולה בדיוק למחלקת השפות שעבורן קיים עד (certificate) באורך פולינומי שניתן לאמת בזמן פולינומי — ומראים איך כל אחת משתי ההגדרות נבנית מהשנייה.

ביטחון: high

בקצרה

מסיימים את הטיפול במכונה האי-דטרמיניסטית שמכריעה את SAT: היא אכן מכריעה את SAT באופן אי-דטרמיניסטי, וכמכונה **חד-סרטית** זמן הריצה שלה חסום ב-$O(|\langle\varphi\rangle|^3)$.

עושים את אותו תרגיל מקצה לקצה על שפת **המספרים הפריקים**: אלגוריתם דטרמיניסטי נאיבי דורש זמן אקספוננציאלי באורך הקלט, ואילו מכונה אי-דטרמיניסטית מכריעה אותה ב-$O(|x|^3)$ — הדגמה חדה של מה הכוח האי-דטרמיניסטי קונה לנו.

שתי המכונות האלה חולקות מבנה אחד: **האי-דטרמיניזם מרוכז כולו בשלב אחד** — כתיבת ההשמה, או כתיבת שני הגורמים. אם מישהו חיצוני היה נותן לנו את האובייקט הזה, כל השאר היה דטרמיניסטי ופולינומי.

המשפט המרכזי: $A \in \mathrm{NP}$ **אם ורק אם** קיימים פולינומים p, q ומכונה **דטרמיניסטית** M הרצה בזמן p, כך שלכל x מתקיים $x \in A \iff \exists w \in \{0,1\}^{q(|x|)}$ שעבורו M מקבלת את (x, w).

המרצה בהקלטה המקבילה קורא למחלקה המוגדרת כך NP', ומוכיח $\mathrm{NP} = \mathrm{NP}'$.

ה-w נקרא **עד (witness)** או **אישור (certificate)**, והמכונה M נקראת **מוודא (verifier)**. שימו לב: M **אינה** מכריעה את A — היא אפילו לא מקבלת את x לבדו כקלט.

ההוכחה דו-כיוונית ובנייתית: מ-verifier בונים NTM שכותבת את w באופן אי-דטרמיניסטי ואז מריצה את M; מ-NTM בונים verifier שהעד שלו הוא **רצף הבחירות האי-דטרמיניסטיות** לאורך ענף מקבל. בדרך מוכיחים למת עזר: אפשר להניח שלכל מעבר יש **לכל היותר שתי** אפשרויות, ואז די בביט אחד לכל צעד.

שני החסמים הכרחיים: אורך העד חייב להיות פולינומי, **וגם** זמן האימות חייב להיות פולינומי. ויתור על הראשון מוריד את ההגדרה עד כדי אפיון של RE מקורס החישוביות; ויתור על השני מנפח את המחלקה מעל EXP.

המשמעות שכדאי לקחת: x הוא **טענה**, w הוא **הוכחה**, M הוא **בודק ההוכחות**. השאלה P מול NP הופכת לשאלה "האם קשה יותר להוכיח מאשר לבדוק הוכחה" — או, בניסוח של ההרצאה, האם קל יותר לפתור מבחן או לבדוק אותו.

רקע ותלויות

מהשיעורים הקודמים בסדרה נדרשים חמישה דברים, ונחזור עליהם במלואם כדי שלא תצטרכו לקפוץ.

(א) מודל המכונה (ראו שיעורים 1–2). מכונת טיורינג נכתבת כרביעייה-שישייה $M = (Q, q_{start}, F, \Sigma, \Gamma, \delta)$, כאשר Q קבוצת המצבים, q_{start} מצב ההתחלה, $F \subseteq Q$ קבוצת המצבים המקבלים, Σ אלפבית הקלט, $\Gamma \supseteq \Sigma$ אלפבית הסרט, ו-δ פונקציית (או יחס) המעברים. במכונה **דטרמיניסטית** $\delta(q,\alpha)$ הוא איבר יחיד; במכונה **אי-דטרמיניסטית** $\delta(q,\alpha) \subseteq Q \times \Gamma \times \{L, R\}$ היא קבוצה, ובכל צעד המכונה בוחרת אחד מאיבריה.

(ב) מעבר בין מספר סרטים (ראו שיעורים 1–2). עבור מכונה **רב-סרטית** M קיימת מכונה חד-סרטית שקולה סמנטית $\hat{M}$ שעבורה $\mathrm{time}_{\hat{M}}(x) \le O\big(\mathrm{time}_M(x) \cdot \mathrm{space}_M(x)\big)$. מכיוון שתמיד $\mathrm{space} \le \mathrm{time}$, נובע מכאן גם החסם המוכר $O(\mathrm{time}^2)$ — אבל כשידוע לנו משהו על המקום, הגרסה הראשונה הדוקה יותר. שתי המסירות של השיעור משתמשות בדיוק בנקודה הזו, וכל אחת מקבלת בזכותה חסם $O(n^3)$ במקום $O(n^4)$.

(ג) הכרעה באופן אי-דטרמיניסטי (ראו שיעור 4). מכונה אי-דטרמיניסטית N **מכריעה** שפה A באופן אי-דטרמיניסטי אם מתקיימים שני תנאים: (i) לכל x, **כל** ריצה אפשרית של N על x עוצרת — אין ריצות אינסופיות; (ii) $x \in A$ אם ורק אם **קיימת** ריצה אפשרית של N על x שבה היא מקבלת. שקול לנסח את (ii) כשני תנאים נפרדים: אם $x \in A$ אז קיימת ריצה מקבלת, ואם $x \notin A$ אז בכל ריצה אפשרית N דוחה. שימו לב לאסימטריה: קבלה נקבעת על ידי כמת "קיים", דחייה על ידי כמת "לכל". בפרט ייתכן בהחלט שעל קלט **ששייך** לשפה נריץ את המכונה ונקבל דחייה — הדרישה היא רק שתהיה אפשרות לבחור נכון.

(ד) מדדי יעילות אי-דטרמיניסטיים והמחלקות (ראו שיעור 4). $\mathrm{time}_N(x)$ מוגדר כמספר הצעדים ב**ריצה הארוכה ביותר** מבין כל הריצות האפשריות על x; $\mathrm{space}_N(x)$ הוא מספר התאים השונים שנכתבים ב**ריצה הבזבזנית ביותר** — ולא בהכרח באותה ריצה. $\mathrm{NTime}(f)$ היא מחלקת השפות שניתן להכריע אי-דטרמיניסטית בזמן $O(f)$, ובאופן דומה $\mathrm{NSpace}(f)$. המחלקה שמעניינת אותנו היא $\mathrm{NP} = \bigcup_{c \ge 1} \mathrm{NTime}(n^c)$.

(ה) SAT ו-CNF (ראו שיעור 5). נוסחת CNF היא קוניונקציה של פסוקיות, וכל פסוקית היא דיסיונקציה של ליטרלים. $\mathrm{SAT} = \{\langle \varphi \rangle \mid \varphi \text{ CNF, satisfiable}\}$. בסוף שיעור 5 הוגדרה מכונה דו-סרטית אי-דטרמיניסטית M שעל קלט $\langle\varphi\rangle$:

סורקת את φ וסופרת את מספר המשתנים n — באופן **דטרמיניסטי**;

כותבת על הסרט השני מחרוזת $v \in \{0,1\}^n$ — באופן **אי-דטרמיניסטי**;

בודקת האם ההשמה המקודדת ב-v מספקת את φ, ומקבלת אם ורק אם כן — באופן **דטרמיניסטי**.

הפרשנות של שלב 2: כל מחרוזת בינרית באורך מספר המשתנים נחשבת לתיאור של השמה — הביט ה-i הוא הערך שההשמה נותנת למשתנה x_i. זו התשובה לשאלה של סטודנט: ההשמה v אמנם מוגדרת פורמלית כפונקציה שמקבלת משתנה יחיד ומחזירה $\mathrm{true}/\mathrm{false}$, אבל **הקידוד** שלה על הסרט הוא מחרוזת אחת באורך n ([00:07:39], מסירה 11).

> **על ציטוט המקורות בקובץ זה.** לשיעור יש שתי הקלטות של שתי מסירות מקבילות לשתי קוהורטות. חותמות זמן מסומנות כאן `[hh:mm:ss]` עם ציון המסירה: **מסירה 10** = `zcCQY3oT40Y` (הקוהורטה שעבדה על המספרים הפריקים), **מסירה 11** = `U3Sy9Qr1Me0` (הקוהורטה שהמשיכה מ-SAT).

הגדרות

הגדרה 1: מוודא (verifier), עד (witness / certificate), והמחלקה NP'

תהא A שפה. נאמר ש-$A \in \mathrm{NP}'$ אם קיימים פולינומים p, q ומכונת טיורינג **דטרמיניסטית** M כך ש:

לכל קלט a מתקיים $\mathrm{time}_M(a) \le p(|a|)$;

לכל x מתקיים $x \in A \iff \exists\, w \in \{0,1\}^{q(|x|)}$ s.t. M accepts (x, w).

המחרוזת w נקראת **עד (witness)** או **אישור (certificate)** לשייכות $x \in A$, והמכונה M נקראת **מוודא (verifier)**. באופן שקול: $A = \left\{ x \in \Sigma^* \;\middle|\; \exists w \in \{0,1\}^{q(|x|)} :\ M \text{ accepts } (x,w) \right\}$.

השם NP' הוא הסימון שבו השתמש המרצה במסירה 10 ([00:39:10]) כדי להדגיש שזו לכאורה מחלקה **אחרת**, שהוגדרה בלי שום התייחסות לאי-דטרמיניזם; משפט 4 יוכיח ש-$\mathrm{NP} = \mathrm{NP}'$.

אינטואיציה. חשבו על x בתור **טענה** ועל w בתור **הוכחה** לטענה. המוודא אינו מנסה להוכיח בעצמו — הוא מקבל טענה והוכחה, וכל תפקידו הוא להגיד אם ההוכחה משכנעת ([00:42:22]–[00:43:23], מסירה 10). זה ההבדל בין לפתור מבחן לבין לבדוק מבחן ([00:16:07], מסירה 11; [00:46:01], מסירה 10). ותנאי (2) הוא בדיוק הדרישה שהמערכת תהיה **נאותה ושלמה**: לכל טענה נכונה יש הוכחה משכנעת, ולשום טענה שגויה אין הוכחה משכנעת.

בגלל זה חשוב להדגיש: M **אינה מכריעה את** A, ולא רק מסיבה חישובית אלא כבר מסיבה תחבירית — הקלט שלה הוא הזוג (x, w) ולא x ([00:20:28], מסירה 11; [00:41:50], מסירה 10). לכן היא נקראת מוודא ולא מכונת הכרעה.

שני הפרמטרים בהגדרה הם שני חסמים **נפרדים**: q חוסם את **אורך העזרה** שמותר לקבל מבחוץ, ו-p חוסם את **זמן הבדיקה**. כדברי המרצה במסירה 10 ([00:16:57]): "אני רוצה להימנע ממקרה שיש איזו עדות, אבל היא כל כך ארוכה שרק לקרוא אותה ייקח לי זמן אקספוננציאלי". במשפט 5 נראה שאף אחד מהחסמים אינו מיותר.

מופע. $A = \mathrm{SAT}$. העד ל-$\langle \varphi \rangle \in \mathrm{SAT}$ הוא השמה מספקת, מקודדת כמחרוזת בינרית באורך מספר המשתנים; האימות הוא הצבה וחישוב ערך אמת — פולינומי.

מופע נוסף. $\mathrm{COMPOSITES} = \{x \in \{0,1\}^* \mid x \text{ encodes a composite number in binary}\}$. אם אני טוען בפניכם ש-8 פריק, אתם לא מוכנים להאמין לי סתם — פירוק לגורמים הוא יקר. אבל אם אני מוסר לכם את הזוג $(2, 4)$, כל מה שנשאר לכם הוא **כפל**, שהוא זול חישובית. העד הוא הזוג, האימות הוא הכפל ([00:23:14], מסירה 11; [00:48:41], מסירה 10).

אי-מופע — למה זו לא סתם "כל שפה". קחו את $\overline{\mathrm{SAT}}$ (נוסחאות CNF שאינן ספיקות). מהו העד? השמה בודדת אינה עוזרת — כדי לשכנע ש-φ אינה ספיקה צריך משהו שמכסה את **כל** ההשמות, ולא ידוע לאיש עד קצר כזה. ההגדרה אינה מספקת את עצמה אוטומטית.

הגדרה 2: תסריט ריצה (run script)

תהא N מכונה אי-דטרמיניסטית. בכל צעד N מחליטה על שלושה דברים: המצב הבא, התו שייכתב, וכיוון הזזת הראש. לכן כל ריצה של N על קלט x ניתנת לתיאור על ידי **סדרה סופית של שלשות** $(q, \beta, d) \in Q \times \Gamma \times \{L, R\}$, באורך מספר הצעדים בריצה. מחרוזת המקודדת סדרה כזו

נקראת **תסריט ריצה** של N על x. מספר הביטים לתיאור שלשה אחת הוא $\lceil \lg |Q| \rceil + \lceil \lg |\Gamma| \rceil + 1$, כי לציון אחד מ-$|Q|$ מצבים דרושים $\lceil \lg |Q| \rceil$ ביטים, לציון אחד מ-$|\Gamma|$ תווים דרושים $\lceil \lg |\Gamma| \rceil$ ביטים, וכיוון ההזזה הוא ביט יחיד. $|Q|$ ו-$|\Gamma|$ הם **קבועים** של המכונה ואינם תלויים בקלט.

אינטואיציה — המבוך ([00:40:43]–[00:43:31], מסירה 11). חשבו על מכונה אי-דטרמיניסטית כעל מי שפותר מבוך: בכל התפצלות הוא בוחר לאן לפנות, והמבוך "פתיר" אם ורק אם **קיימת** סדרת בחירות שמוציאה החוצה. איזו עזרה מינימלית אני צריך לקבל *לפני* הכניסה כדי לוודא שאפשר לצאת? לא מצפן — אני לא יודע איפה היציאה. לא שלטים — הם כבר בפנים. **מפה** תספיק, אבל היא נותנת יותר מדי: היא מאפשרת לי לפתור את המבוך, לא רק לוודא פתרון. המינימום הנדרש הוא **רשימת הפניות**: "בצומת הראשון שמאלה, בשני ישר, בשלישי ימינה...". תסריט ריצה הוא בדיוק רשימת הפניות הזו.

הגדרה 3: מכונה אי-דטרמיניסטית מנורמלת (בינארית)

מכונה אי-דטרמיניסטית N תיקרא **מנורמלת** אם לכל $q \in Q$ ולכל $\alpha \in \Gamma$ מתקיים $|\delta(q,\alpha)| \le 2$ — כלומר בכל מעבר יש לכל היותר שתי אפשרויות בחירה.

למה זה שימושי. במכונה מנורמלת, **ביט אחד** לכל צעד מספיק כדי לקבוע איזו בחירה בוצעה. זה מצמצם את תיאור הריצה מרצף שלשות לרצף ביטים, ומייתר את הצורך לוודא שהתסריט "חוקי" — כל מחרוזת ביטים מתארת ריצה חוקית כלשהי. משפט 3 יראה שאפשר תמיד להניח נרמול, במחיר קבוע כפלי בזמן הריצה.

מופע. המכונה למספרים פריקים (משפט 2) כפי שנכתבה במסירה 10 היא כמעט מנורמלת: בשלב כתיבת המספר יש לה בדיוק שלוש אפשרויות בכל צעד — לכתוב 0, לכתוב 1, או לסיים ולעבור לשלב הבא. **אי-מופע:** מכונה שבמעבר מסוים מפצלת ל-10 אפשרויות אינה מנורמלת; משפט 3 מראה איך להחליף אותה בשקולה מנורמלת.

משפטים והוכחות

משפט 1: המכונה מכריעה את SAT באופן אי-דטרמיניסטי, בזמן $O(|\langle\varphi\rangle|^3)$

טענה. המכונה M שתוארה בסעיף (ה) של הרקע מכריעה את SAT באופן אי-דטרמיניסטי.

הוכחה. תהא φ נוסחה מצורת CNF.

מקרה $\langle\varphi\rangle \in \mathrm{SAT}$. אזי קיימת השמה v המספקת את φ. נסמן ב-n את מספר המשתנים; v מקודדת כמחרוזת בת n ביטים. בשלב 2 המכונה כותבת מחרוזת שרירותית באורך n באופן אי-דטרמיניסטי, ולכן **קיימת ריצה אפשרית** של M שבה היא כותבת בדיוק את הקידוד של v. בריצה זו שלב 3 — דטרמיניסטי — בודק את v על φ, מוצא שהיא מספקת, ולכן M מקבלת.

מקרה $\langle\varphi\rangle \notin \mathrm{SAT}$. אזי אף השמה אינה מספקת את φ. תהא ריצה אפשרית כלשהי, ותהא v ההשמה שנכתבה בה בשלב 2. מכיוון ש-v אינה מספקת, שלב 3 מסיים בדחייה. זה נכון **לכל** ריצה אפשרית.

לפי הגדרת ההכרעה האי-דטרמיניסטית, M מכריעה את SAT באופן אי-דטרמיניסטי. ■

הרעיון בלב ההוכחה ([00:04:20], מסירה 11). בכל הוכחת הכרעה אי-דטרמיניסטית התבנית זהה: בכיוון החיובי מספיק להצביע על **אפשרות אחת** לבחור נכון; בכיוון השלילי צריך לכסות את **כל** האפשרויות.

ניתוח סיבוכיות זמן ומקום
בהינתן $\langle\varphi\rangle$, על המכונה הדו-סרטית:
ספירת המשתנים — מעבר ליניארי אחד: $O(|\langle\varphi\rangle|)$ צעדים.
כתיבת ההשמה — $n \le |\langle\varphi\rangle|$ ביטים: $O(|\langle\varphi\rangle|)$ צעדים.
בדיקת הסיפוק — $O(|\langle\varphi\rangle|^2)$. הנימוק: עוברים על הנוסחה ליטרל אחר ליטרל, ולכל מופע של משתנה יש לגשת לתא המתאים בהשמה שעל הסרט השני. במקרה הגרוע המופעים מסודרים כך שהראש נאלץ לחצות את כל ההשמה בין מופע למופע (מופע של המשתנה הראשון, אחריו של האחרון, אחריו שוב של הראשון). מכפלת מספר המופעים ב-אורך ההשמה נותנת $O(n^2)$.
סך הכל $\mathrm{time}_M(\langle\varphi\rangle) = O(|\langle\varphi\rangle|^2)$, ו-$\mathrm{space}_M(\langle\varphi\rangle) = O(|\langle\varphi\rangle|)$ — המכונה כותבת רק את ההשמה.
מעבר לחד-סרטית. למה בכלל חישבנו מקום? כי אנחנו רוצים חסם על מכונה **חד-סרטית**, ולפי סעיף (ב) ברקע ([00:10:47], מסירה 11): $\mathrm{time}_{\hat{M}} \le O\big(\mathrm{time}_M \cdot \mathrm{space}_M\big) = O\big(|\langle\varphi\rangle|^2 \cdot |\langle\varphi\rangle|\big) = O\big(|\langle\varphi\rangle|^3\big)$.
מסקנה. קיימת מכונה חד-סרטית אי-דטרמיניסטית $\hat{M}$ המכריעה את SAT באופן אי-דטרמיניסטי, ולכל נוסחת CNF φ מתקיים $\mathrm{time}_{\hat{M}}(\langle\varphi\rangle) \le O(|\langle\varphi\rangle|^3)$. בפרט $\mathrm{SAT} \in \mathrm{NTime}(n^3) \subseteq \mathrm{NP}$. ■

> **הערה:** בהרצאה החסם נאמר בקיצור ("זה מגיע מזה שזה הספייס כפול הטיים"). הפירוט: אילו היינו משתמשים בחסם הגס $\mathrm{time}_{\hat{M}} = O(\mathrm{time}_M^2)$ היינו מקבלים $O(|\langle\varphi\rangle|^4)$. החסם דרך המקום הדוק יותר משום שהמכונה חסכנית במקום.

משפט 2: $\mathrm{COMPOSITES} \in \mathrm{NP}$ — ומה הכוח האי-דטרמיניסטי קונה
זהו המהלך המקביל שנעשה במסירה 10 ([00:04:49]–[00:34:29]) במקום SAT. הוא מובא כאן במלואו, גם מפני שהוא דוגמה שנייה בלתי תלויה לאותה תבנית, וגם מפני שהוא המקום היחיד בקורס שבו פונקציית המעברים של מכונה אי-דטרמיניסטית נכתבת במפורש.
נגדיר $A = \{x \in \{0,1\}^* \mid x \text{ is a binary encoding of a composite number}\}$.
נקודת המוצא: כמה עולה הפתרון הדטרמיניסטי הנאיבי? האלגוריתם המתבקש עובר על כל המספרים בין 2 ל-$x-1$ ומנסה לחלק. מספר המחלקים שיש לנסות הוא בסדר גודל x עצמו — אבל x **מתקבל בקידוד בינרי**, כלומר $x \approx 2^{|x|}$. לכן ביחס לאורך הקלט זמן הריצה הוא $O(2^{|x|})$, ואם מוסיפים גם את עלות כל חילוק ($O(|x|^2)$ בכפל/חילוק ארוך) — עוד יותר. זה **אקספוננציאלי באורך הקלט**, לא פולינומי.

> **הערה:** שני סטודנטים חידדו כאן נקודות אמיתיות ([00:11:41] ו-[00:12:11], מסירה 10).
> הראשון שאל למה זה $2^{|x|}$ ולא x — התשובה היא שהמדד תמיד נמדד ביחס ל**אורך הקלט**: כדי לכתוב מיליון די בכ-20 ביטים, ולכן מיליון פעולות הן 2^{20} פעולות ביחס לקלט באורך 20.
> השני שאל מה עם עלות החילוק עצמו — ואכן צריך להוסיף אותה, אך היא זניחה ביחס למספר האיטרציות ואינה משנה את המסקנה. המרצה ציין גם ([00:08:00]) שקיים אלגוריתם **דטרמיניסטי פולינומי** לבעיה, תוצאה מלפני כ-20 שנה, אך הוא מסובך מאוד ואינו הנושא כאן.

המכונה האי-דטרמיניסטית. נגדיר מכונה אי-דטרמיניסטית N בעלת ארבעה סרטים. על קלט x (על הסרט הראשון):

כתוב באופן אי-דטרמיניסטי על הסרט השני מספר a באורך **לכל היותר** $|x|$.

כתוב באופן אי-דטרמיניסטי על הסרט השלישי מספר b באורך לכל היותר $|x|$.

אם $a \leq 1$ או $a \geq x$ או $b \leq 1$ או $b \geq x$ — דחה.

חשב את $a \cdot b$ על הסרט הרביעי.

אם $a \cdot b = x$ — קבל; אחרת — דחה.

שוב, כמו במכונה של SAT: שלבים 1–2 אי-דטרמיניסטיים, שלבים 3–5 דטרמיניסטיים לחלוטין ([00:24:22], מסירה 10).

איך נראה שלב 1 ברמת δ? זהו הפירוט שהמרצה נתן פעם אחת ואמר שלא נחזור עליו ([00:20:04]–[00:23:49], מסירה 10). נניח שהמכונה במצב q_1 והראש על הסרט הראשון קורא 0 או 1. אז ל-$\delta(q_1, \cdot)$ יש **שלוש** אפשרויות:

לכתוב 0 על הסרט השני, להישאר ב-q_1, ולהזיז את שני הראשים ימינה;

לכתוב 1 על הסרט השני, להישאר ב-q_1, ולהזיז את שני הראשים ימינה;

להחליט שסיימנו לכתוב, ולעבור ל-q_2 (שם הראשים מוחזרים לתחילת הסרטים ומתחיל שלב 2).

ואם הראש על הסרט הראשון קורא את התו הריק — כלומר עברנו את אורך הקלט — המכונה **חייבת** לעבור ל-q_2. זה בדיוק המימוש של "מספר באורך לכל היותר $|x|$", וזה גם מה שמבטיח שאין ריצות אינסופיות: התנאי הראשון בהגדרת ההכרעה האי-דטרמיניסטית.

נכונות. ננסח כשרשרת של "אם ורק אם" ([00:29:41]–[00:31:17], מסירה 10): $x \in A \iff$

$$x \text{ is composite} \iff \exists a, b \text{ with } 1 < a, b < x \text{ and } a \cdot b = x \iff$$

$\exists$ an accepting run of N on x. השוויון האחרון הוא בדיוק בנייתה של N: היא בוחרת שני מספרים בטווח ובודקת את המכפלה, וזה המקרה היחיד שבו היא מקבלת. בכיוון אחד: אם x פריק, קיימים a, b כאלה, ולכן קיימת ריצה שבה N בוחרת בדיוק אותם ומקבלת. בכיוון השני: אם קיימת ריצה מקבלת, אז בריצה זו נכתבו a, b שעברו את בדיקת שלב 3 ומקיימים $ab = x$, ולכן x פריק.

> **הערה מתודית מההרצאה ([00:31:17], מסירה 10):** כשהשקילות נובעת ישירות מההגדרה מותר לכתוב אותה כשרשרת "אם ורק אם" כזו; בבעיות מורכבות יותר עדיף לפצל ולהוכיח כל כיוון בנפרד. שימו לב שגם כאן, כמו במשפט 4 בהמשך, **שני** הכיוונים נחוצים.

ניתוח זמן ומקום. יהי x קלט, $n = |x|$.

שלב 1: לכל היותר n צעדים (חסמנו את אורך a ב-n).

שלב 2: לכל היותר n צעדים, ובנוסף החזרת הראשים — $O(n)$.

שלב 3: השוואות בין מספרים באורך $\leq n$ — $O(n)$.

שלב 4: כפל ארוך של שני מספרים בני n ביטים — $O(n^2)$: צריך להכפיל כל ספרה בכל אחת מהאחרות ולסכום.

שלב 5: השוואה אחת — $O(n)$.

סך הכל $\mathrm{time}_N(x) = O(n^2)$. המקום: הסרטים מחזיקים את x, את a, את b ואת המכפלה שאורכה $\leq 2n$ — לכן $\mathrm{space}_N(x) = O(n)$.

מכיוון ש-$\mathrm{time}_N(x)$ חסום, בפרט **כל** ריצה עוצרת — התנאי הראשון בהגדרת ההכרעה מתקיים "בחינם" מתוך חסם הזמן ([00:29:10], מסירה 10).

מעבר לחד-סרטית. N היא רב-סרטית, ואילו הגדרת NTime נוסחה למכונה סטנדרטית. לפי סעיף (ב) ברקע: $\mathrm{time}_{\hat{N}}(x) \;\le\; O\big(\mathrm{space}_N(x)\cdot \mathrm{time}_N(x)\big) = O(n\cdot n^2) = O(n^3)$.

מסקנה. $A \in \mathrm{NTime}(n^3) \subseteq \mathrm{NP}$. ■

מה הרווחנו. דטרמיניסטית-נאיבית: $2^{\Theta(n)}$. אי-דטרמיניסטית: $O(n^3)$. במקום לעבור על כל המחלקים האפשריים, המכונה **בוחרת אחד** ובודקת רק אותו; מספיק שתהיה אפשרות לבחור נכון ([00:13:14], מסירה 10).

> **אזהרה מהמרצה ([00:37:36], מסירה 10):** המודל האי-דטרמיניסטי הוא **מודל פיקטיבי**. אין דבר כזה מכונה אי-דטרמיניסטית במציאות; זהו כלי להבנת הקושי של בעיות. ההגדרה השקולה שנוכיח מיד היא זו שנותנת ל-NP משמעות ממשית.

משפט 3 (למת נרמול): אפשר להניח שתי אפשרויות בכל מעבר

טענה. לכל מכונה אי-דטרמיניסטית N קיימת מכונה אי-דטרמיניסטית **מנורמלת** $\hat{N}$ (כלומר $|\hat{\delta}(q,\alpha)| \le 2$ לכל q,α) כך ש:

לכל x: קיימת ריצה מקבלת של N על x אם ורק אם קיימת ריצה מקבלת של $\hat{N}$ על x (שקילות סמנטית);

לכל x: $\mathrm{time}_{\hat{N}}(x) = O\big(\mathrm{time}_N(x)\big)$.

הבנייה ([00:57:43]–[01:07:23], מסירה 10). נתבונן במעבר של N שבו יש k אפשרויות: $\delta(q,\alpha) = \big\{(q_{i_1},\beta_1,d_1),\ (q_{i_2},\beta_2,d_2),\ \ldots,\ (q_{i_k},\beta_k,d_k)\big\}$. נחליף אותו ב-$k$ מעברים בינאריים, בעזרת מצבי עזר חדשים $q^{(2)}, q^{(3)}, \ldots, q^{(k)}$:

$$\hat{\delta}(q,\alpha) = \big\{(q_{i_1},\beta_1,d_1),\ (q^{(2)},\alpha,S)\big\},\quad \hat{\delta}(q^{(2)},\alpha) = \big\{(q_{i_2},\beta_2,d_2),\ (q^{(3)},\alpha,S)\big\},\quad \ldots\quad \hat{\delta}(q^{(k)},\alpha) = \big\{(q_{i_k},\beta_k,d_k)\big\}.$$

כאן S פירושו "אל תזיז את הראש ואל תשנה את התו" — מעבר שמטרתו היחידה היא לדחות את ההחלטה. במילים: בכל שלב המכונה נשאלת שאלה **בינרית** — "לבצע את האפשרות הנוכחית, או לעבור למצב שאומר 'עכשיו תבחר מבין הנותרות'?" — וכך מצטמצם מספר האפשרויות באחת בכל פעם, עד שבמצב האחרון נותרת אפשרות יחידה.

נכונות (סעיף 1). לכל q,α ולכל $j \le k$: $(q_{i_j},\beta_j,d_j) \in \delta(q,\alpha) \iff$ there is a choice sequence in $\hat{N}$ from q ending in (q_{i_j},β_j,d_j), כלומר הסדרה $(q^{(2)},\alpha,S),(q^{(3)},\alpha,S),\ldots,(q^{(j)},\alpha,S)$ ואז (q_{i_j},β_j,d_j). מכיוון שמצבי העזר אינם משנים את הסרט ואינם מזיזים את הראש, הקונפיגורציה בסוף השרשרת הזו זהה לקונפיגורציה שאליה N מגיעה בצעד יחיד. באינדוקציה על מספר הצעדים: לכל ריצה של N על x מתאימה ריצה של $\hat{N}$ העוברת באותן קונפיגורציות (עם קונפיגורציות ביניים), ולהפך. בפרט קיימת ריצה מקבלת ב-N אם ורק אם קיימת ב-$\hat{N}$.

חשבון הזמן (סעיף 2). על כל צעד יחיד של N, המכונה $\hat{N}$ מבצעת לכל היותר k צעדים, כאשר $k = |\delta(q,\alpha)|$. נחסום את k: כל אפשרות היא שלשה מתוך $Q \times \Gamma \times \{L,R\}$, ולכן $k \le 2\cdot|Q|\cdot|\Gamma|$. זהו **קבוע** התלוי רק ב-N ולא ב-x ([01:08:28]–[01:10:40], מסירה 10). לכן

$$\mathrm{time}_{\hat{N}}(x) \;\le\; 2|Q||\Gamma|\cdot \mathrm{time}_N(x) \;=\; O\big(\mathrm{time}_N(x)\big).$$ ■

הערה: בהרצאה נאמר במפורש שזו אינה הוכחה פורמלית מלאה אלא בנייה מלווה בהסבר ([01:04:09] ו-[01:11:42], מסירה 10). הפירוט כאן — הניסוח המדויק של $\hat{\delta}$, טענת ההתאמה בין סדרות בחירה, האינדוקציה, וחסם $k \leq 2|Q||\Gamma|$ — הוא ההשלמה. הבנייה עצמה, כולל מצבי העזר וחסם מספר השלשות, נאמרה בהרצאה.

מדוע זה משתלם. אחרי הנרמול, כדי לתאר ריצה מספיק **ביט אחד לכל צעד**, ולא שלשה שלמה. זה מה שמאפשר במשפט 4 לקחת $|w| = p(|x|) \cdot (1 + \lceil \lg |Q| \rceil + \lceil \lg |\Gamma| \rceil)$ בדיוק, ולא $p(|x|)$. חשוב מכך: בקידוד הביטים, **כל** מחרוזת w מתארת ריצה חוקית, ולכן המוודא אינו צריך כלל לבדוק חוקיות — הוא רק מריץ.

משפט 4 (המשפט המרכזי): $\mathrm{NP} = \mathrm{NP}'$

ניסוח. תהא A שפה. אזי $A \in \mathrm{NP}$ אם ורק אם קיימים פולינומים p, q ומכונה **דטרמיניסטית** M כך ש:

לכל קלט a: $\mathrm{time}_M(a) \leq p(|a|)$;

לכל x: $x \in A \iff \exists w \in \{0,1\}^{q(|x|)}$ שעבורו M מקבלת את (x, w).

הערה מקדימה. ב-(1)–(2) המכונה M היא **דטרמיניסטית**, בניגוד להגדרה המקורית של NP שבה המכונה אי-דטרמיניסטית. זה כל העניין: המשפט מחליף אי-דטרמיניזם בעזרה חיצונית קצרה. (בסיכום זו הערה בכחול בשולי עמוד 2.) שימו לב גם ש-(1) חוסם את זמן הריצה באורך הקלט ה**מלא** של M — כלומר $|x| + |w|$ — ולא ב-$|x|$ ([01:14:20], מסירה 10).

כיוון א': מ-verifier ל-NP (אם קיימים p, q, M כנ"ל, אז $A \in \mathrm{NP}$)

הבנייה. נניח שקיימים p, q, M המקיימים (1) ו-(2). נבנה מכונה אי-דטרמיניסטית $\hat{M}$. שימו לב ש-$\hat{M}$ "מחזיקה את M בבטן" — M ידועה בזמן הבנייה ואינה חלק מהקלט ([00:30:03], מסירה 11).

על קלט x:

$\hat{M}$ **מחשבת** את $q(|x|)$.

$\hat{M}$ **כותבת מחרוזת** $w \in \{0,1\}^{q(|x|)}$ **באופן אי-דטרמיניסטי**, על הסרט מיד אחרי x.

$\hat{M}$ **מריצה את** M **על** (x, w) **ומחזירה את אותה תשובה.**

זה בדיוק מה שעשו שתי המכונות שראינו: ג'נרוט אובייקט באופן אי-דטרמיניסטי, ואחריו בדיקה דטרמיניסטית ([00:28:30], מסירה 11; [01:24:07], מסירה 10). שלב 3 חוקי משום שמכונה אי-דטרמיניסטית תמיד יכולה להריץ מכונה דטרמיניסטית — כל מכונה דטרמיניסטית היא בפרט אי-דטרמיניסטית עם אפשרות יחידה בכל מעבר ([01:22:00], מסירה 10).

נכונות: $\hat{M}$ **מכריעה את** A **באופן אי-דטרמיניסטי.** יהי x.

אם $x \in A$: מתנאי (2), בכיוון "רק אם", קיימת $w \in \{0,1\}^{q(|x|)}$ כך ש-M מקבלת את (x, w). מכיוון ששלב 2 כותב מחרוזת שרירותית באורך $q(|x|)$, **קיימת ריצה אפשרית** של $\hat{M}$ על x שבה נכתבת בדיוק אותה w. בריצה זו שלב 3 מריץ את M על (x, w), מקבל "קבל", ולכן $\hat{M}$ מקבלת.

אם $x \notin A$: מתנאי (2), בכיוון "אם", **אף** $w \in \{0,1\}^{q(|x|)}$ אינה גורמת ל-M לקבל את (x, w) — כלומר לכל w המכונה M דוחה. תהא ריצה אפשרית כלשהי של $\hat{M}$ על x, ותהא w המחרוזת שנכתבה בה בשלב 2. שלב 3 מריץ את M על (x, w), מקבל "דחה", ומחזיר אותה תשובה. לכן **כל** ריצה אפשרית של $\hat{M}$ דוחה.

הערה: כאן הנקודה שהמרצה עצר עליה במפורש ([00:32:17]–[00:33:49], מסירה 11): תנאי (2) הוא **אם ורק אם**, ובהוכחה משתמשים *בשני* הכיוונים שלו — באחד כדי לייצר ריצה מקבלת כש-$x \in A$, ובשני כדי לשלול ריצה מקבלת כש-$x \notin A$. אילו (2) היה גרירה חד-כיוונית בלבד, $\hat{M}$ הייתה עלולה לקבל קלטים שאינם ב-A. שתי המסירות מנסחות את הכיוון השני אחרת: מסירה 11 עושה זאת בשלילה (נניח שקיימת ריצה מקבלת, ונגיע לסתירה), ומסירה 10 ישירות ([01:33:36]). שתי הגרסאות תקפות; הגרסה הישירה מובאת למעלה, וגרסת השלילה שקולה לה.

לכן $\hat{M}$ מכריעה את A באופן אי-דטרמיניסטי.

ניתוח יעילות. יהי x, ונסמן $n = |x|$.

שלב 1 דורש $O(q(n))$ צעדים. הנימוק: q הוא פולינום, וכל פונקציה אלמנטרית כזו היא **ישימה בזמן** — ניתנת לחישוב בזמן מסדר הגודל של ערכה ([00:35:56], מסירה 11; [01:26:09], מסירה 10).

שלב 2 דורש בדיוק $q(n)$ צעדים: המכונה רק רושמת $q(n)$ ביטים, ביט אחד לצעד.

שלב 3 דורש $\mathrm{time}_M\big((x,w)\big) \le p\big(|(x,w)|\big)$ לפי תנאי (1). הקידוד של הזוג הוא שרשור של x ואחריו w (עד כדי תו מפריד קבוע), ולכן $|(x,w)| = |x| + |w| = n + q(n)$, ומכאן $\mathrm{time}_M\big((x,w)\big) \;\le\; p\big(n + q(n)\big)$.

סך הכל, אם נגדיר $\tilde{p}(n) = O(q(n)) + q(n) + p\big(n+q(n)\big)$, אז $\mathrm{time}_{\hat{M}}(x) \le \tilde{p}(n)$.

פולינומים סגורים תחת **סכום, מכפלה והרכבה** ([00:38:03], מסירה 11; [01:28:51], מסירה 10) — ולכן $\tilde{p}$ הוא פולינום ב-$n = |x|$. קיבלנו מכונה אי-דטרמיניסטית המכריעה את A בזמן פולינומי, כלומר $A \in \mathrm{NP}$. ■

למה סגירות הפולינומים היא לב העניין ([01:29:21], מסירה 10). זו אחת הסיבות שמסתכלים דווקא על P ו-NP: אלגוריתם פולינומי שמריץ אלגוריתם פולינומי אחר נשאר פולינומי. אין דבר כזה בזמן ליניארי — אלגוריתם ליניארי שמריץ אלגוריתם ליניארי בתוך לולאה כבר ריבועי. כאן זה קריטי: שלב 3 של $\hat{M}$ הוא בדיוק "הרצת אלגוריתם בתוך אלגוריתם".

למה החישוב עובד רק בגלל ששני החסמים פולינומיים. אילו q היה, נניח, 2^n — שלב 2 לבדו היה דורש 2^n צעדים. ואילו p לא היה פולינומי — שלב 3 היה הורג אותנו. שני החסמים נכנסים לחישוב, כל אחד במקומו.

כיוון ב': מ-NP ל-verifier (אם $A \in \mathrm{NP}$ אז קיימים p, q, M כנ"ל)

נתון. $A \in \mathrm{NP}$: קיימת מכונה אי-דטרמיניסטית N ופולינום p_0 כך ש-N מכריעה את A באופן אי-דטרמיניסטי, ולכל x מתקיים $\mathrm{time}_N(x) \le p_0(|x|)$. איננו יודעים דבר על אופן פעולתה של N — רק את שתי העובדות האלה ([01:38:49], מסירה 10).

מה חסר ל-verifier? הבעיה במכונה אי-דטרמיניסטית היא בדיוק שהיא עושה בחירות עצמאיות. מכונה דטרמיניסטית שרוצה לדעת אם קיימת ריצה מקבלת חייבת, בלי עזרה, לסרוק עץ ריצות שגודלו אקספוננציאלי. העזרה המינימלית שתפתור לה את הבעיה היא **רשימת הבחירות** (הגדרה 2, אנלוגיית

המבוך). בניסוח של מסירה 10 ([01:40:26]): זהו "להוציא את האי-דטרמיניזם אל מחוץ למכונה" — במקום שהמכונה תבצע בחירות תוך כדי ריצה, היא מקבלת את כל הבחירות מראש, ומאותו רגע היא דטרמיניסטית לחלוטין.

יש שתי דרכים לממש את הרעיון, ושתי המסירות בחרו בשתיהן. נביא את שתיהן, כי ההבדל ביניהן מלמד.

דרך I — העד הוא תסריט ריצה מלא (מסירה 11 והסיכום)

אורך התסריט. מספר הצעדים בכל ריצה של N על x חסום ב-$p_0(|x|)$, ולכן מספר ההחלטות חסום גם הוא ב-$p_0(|x|)$. כל החלטה היא שלשה (q, β, d) הנתונה ב-$\lceil \lg |Q| \rceil + \lceil \lg |\Gamma| \rceil + 1$ ביטים. נסמן $q(n) = \left(\lceil \lg |Q| \rceil + \lceil \lg |\Gamma| \rceil + 1\right) \cdot p_0(n)$, שכן הגורם הראשון פולינום ב-n, קבוע התלוי רק ב-N.

הבנייה. מכונה **דטרמיניסטית** M; על קלט (x, w):

M מפרשת את w כרשימת שלשות, ומוודאת ש-w מתאר ריצה **חוקית ומקבלת** של N על x.

אם כן — קבל; אחרת — דחה.

מה נבדק בשלב 1? M מסמלצת: מחזיקה את הקונפיגורציה הנוכחית (מצב, תוכן סרט, מיקום ראש), מתחילה מהקונפיגורציה ההתחלתית של N על x, וקוראת את השלשות בזו אחר זו. לכל שלשה היא בודקת מול δ_N שהמעבר המבוקש הוא באמת אחת מהאפשרויות המותרות מהקונפיגורציה הנוכחית, ואם כן — מעדכנת. בסיום היא בודקת שהמצב הסופי ב-F ([00:49:55]–[00:50:25], מסירה 11).

דרך II — העד הוא רצף ביטי בחירה (מסירה 10)

לפי משפט 3 נניח ש-N **מנורמלת**: בכל מעבר לכל היותר שתי אפשרויות. (אם לא — נחליף אותה ב-$\hat{N}$ מהמשפט, שזמן ריצתה $O(p_0)$, ונקרא לפולינום החדש p_0.) כעת די בביט אחד לכל צעד, ולכן נסמן פשוט $q(n) = p_0(n)$.

הבנייה. מכונה **דטרמיניסטית** M בעלת שני סרטים; על קלט (x, w):

אתחול: העתק את w אל הסרט השני ומחק אותו מהסרט הראשון, כך שעל הסרט הראשון נשאר רק x.

סימולציה: סמלץ את ריצת N על x; בכל צעד שבו ל-N יש בחירה בין שתי אפשרויות — אם הראש שעל הסרט השני קורא 0, בצע את האפשרות הראשונה; אם הוא קורא 1, בצע את השנייה. בסוף כל צעד הזז את הראש שעל הסרט השני ימינה. החזר את התשובה שאליה הגיעה הסימולציה.

למה זה חוקי. מכונה דטרמיניסטית אינה יכולה "להריץ" מכונה אי-דטרמיניסטית — הכיוון ההפוך אפשרי, לא זה ([01:45:08], מסירה 10). הפתרון: בבנייה הזו אין ל-M שום בחירה, כי כל בחירה **נקבעת מראש** על ידי הביט הנוכחי שעל הסרט השני. פורמלית, במקום מעבר אחד עם שתי אפשרויות יש ל-M שני מעברים דטרמיניסטיים נפרדים, המובחנים לפי התו הנקרא על הסרט השני.

ההבדל המהותי בין שתי הדרכים. בדרך I יש מחרוזות w שאינן מתארות ריצה חוקית כלל, ולכן המוודא חייב לבדוק חוקיות מול δ_N. בדרך II **כל** $w \in \{0,1\}^{q(|x|)}$ מתארת ריצה חוקית של N — פשוט מפני שכל ביט בוחר בין שתי אפשרויות שקיימות ממילא — ולכן אין מה לבדוק, רק להריץ. זה מה שהלמה של משפט 3 קונה לנו.

נכונות (משותפת לשתי הדרכים)

יהי x.

אם $x \in A$: מכיוון ש-N מכריעה את A אי-דטרמיניסטית, קיימת ריצה מקבלת של N על x. נתבונן בריצה כזו. **ראשית נחסום את אורכה:** נתון ש-$\mathrm{time}_N(x) \le p_0(|x|)$, וזהו חסם על הריצה הארוכה ביותר; בפרט מספר הצעדים בריצה המקבלת הספציפית הזו הוא $\le p_0(|x|)$ ([01:50:59]–[01:51:34], מסירה 10). לכן מספר הבחירות בה $\le p_0(|x|)$, ורצף הבחירות מתקודד ב-w באורך $\le q(|x|)$: בדרך I כרצף שלשות, בדרך II כרצף ביטים שבו הביט ה-i מתאים לבחירה שביצעה N בצעד ה-i (0 לאפשרות הראשונה, 1 לשנייה). על הקלט (x, w) הסימולציה של M עוברת בדיוק לאורך הריצה הזו ומסתיימת במצב מקבל, ולכן M מקבלת.

אם $x \notin A$: אזי **אין** ריצה מקבלת של N על x כלל. תהא w כלשהי. בדרך II, w מגדירה ריצה יחידה של N על x, ומכיוון שאין ריצה מקבלת — הריצה הזו דוחה, ולכן M דוחה את (x, w). בדרך I, אם w אינה חוקית M תגלה זאת מול δ_N ותדחה; ואם היא חוקית, היא מתארת ריצה של N, שאינה מקבלת, ולכן M תדחה בסוף. בשני המקרים: לכל w, המכונה M דוחה.

קיבלנו בדיוק את תנאי (2): $x \in A \iff \exists w \in \{0,1\}^{q(|x|)}$ שעבורה M מקבלת את (x, w).

> **הערה:** המרצה במסירה 10 עצר כאן באמצע ותיקן את עצמו בקול ([01:56:24]–[01:57:25]): הוא הוכיח את שני הכיוונים אך לא סגר במפורש את המסקנה "ולכן $x \in A$", ואמר "אולי צריך להוסיף — זה מקור הבלבול". הניסוח שלמעלה סוגר את השרשרת במפורש.

שאלה מהכיתה: מה מבטיח שהסימולציה תסתיים לפני ש-w ייגמר? ([01:59:30]–[02:01:38], מסירה 10)

זו השאלה הטובה ביותר שנשאלה בשיעור. אם M מתקדמת ביט אחד לכל צעד סימולציה, מה מונע מצב שבו הריצה המסומלצת עוד לא הסתיימה ו-w כבר אזל?

התשובה: החסם $\mathrm{time}_N(x) \le p_0(|x|)$ הוא חסם על **הריצה הארוכה ביותר** של N על x — כלומר על כל ריצה, ולא משנה אילו בחירות בוצעו. לכן, יהיה w אשר יהיה, הסימולציה עוצרת אחרי $\le p_0(|x|)$ צעדים, וזה בדיוק אורך w. שימו לב שהתשובה אינה נשענת על כך ש-M מקבלת, ואינה נשענת על מבנה כלשהו של N — היא נובעת אך ורק מהנתון על זמן הריצה. (סטודנטית אחרת הציעה שהדבר נובע מכך שהמכונה עוצרת במצב מקבל; זו אינה התשובה, כי היא לא הייתה מכסה ריצות דוחות.)

ניתוח יעילות

נעשה אותו לפי דרך II, שבה הוא נקי יותר. יהיו x ו-w.

שלב 1 (העתקת w לסרט השני): מעבר אחד על הקלט — $O(|x| + |w|)$ צעדים.

שלב 2 (הסימולציה): לכל היותר $\mathrm{time}_N(x) \le p_0(|x|)$ צעדי סימולציה, וכל צעד עולה מספר קבוע של פעולות (קריאת ביט, התייעצות בטבלת δ_N, עדכון, הזזת שני הראשים).

נגדיר $Q(n) = n + p_0(n)$ — פולינום. אז $\mathrm{time}_M\big((x,w)\big) \le O\big(|x| + |w|\big) + O\big(Q(|x| + |w|)\big)$, כאשר המעבר האחרון הוא חסם מלמעלה גס אך תקף: החלפנו $p_0(|x|)$ ב-$p_0(|x| + |w|)$, מה שרק מגדיל ([02:03:43]–[02:04:13], מסירה 10). כלומר זמן הריצה של M פולינומי ב**אורך הקלט שלה**, כנדרש בתנאי (1).

לבסוף, M היא דו-סרטית; לפי סעיף (ב) ברקע קיימת חד-סרטית שקולה שזמן ריצתה חסום ב-$O(Q^2)$ — עדיין פולינום. לכן קיימים p (נניח $p = O(Q^2)$) ו-q ומכונה דטרמיניסטית המקיימים (1) ו-(2), כלומר $A \in \mathrm{NP}'$. ■

סיכום הכיוון. בהינתן מכונה אי-דטרמיניסטית המכריעה את A, בנינו **מוודא** — מכונה שאינה מכריעה את A אך יודעת לוודא אותה — שהעד שהיא מצפה לו הוא רצף הבחירות שיש לבצע כדי להגיע למצב מקבל.

מכיוון ששני הכיוונים הוכחו, $\mathrm{NP} = \mathrm{NP}'$. ■

מבט לאחור: SAT ו-$\mathrm{COMPOSITES}$ כמקרים פרטיים. אם מפעילים את כיוון ב' על המכונה של SAT ממשפט 1, מקבלים verifier שהעד שלו הוא תסריט הריצה המלא. אבל למכונה ההיא מבנה מיוחד — האי-דטרמיניזם מרוכז כולו בשלב 2 — ולכן כל הבחירות שמחוץ לשלב 2 נקבעות ביחידות ואפשר להשמיטן. מה שנשאר מהתסריט הוא בדיוק n הביטים של ההשמה. באותו אופן בדיוק, במכונה של $\mathrm{COMPOSITES}$ נשארים מהתסריט רק הביטים של a ושל b. זו הסיבה שהעד ה"טבעי" הוא ההשמה או זוג הגורמים, ולא היסטוריית החישוב: התסריט הוא הבנייה הכללית, וההשמה היא הדחיסה שלה במקרה הפרטי.

משפט 5: שני החסמים הכרחיים

(א) ויתור על החסם q על אורך העד מוריד את ההגדרה ל-RE. נגדיר: $A \in \mathcal{C}$ אם קיימת מכונה דטרמיניסטית M הרצה בזמן פולינומי באורך **כל** הקלט שלה, כך ש- $A = \{x \mid \exists w \in \{0,1\}^* :\ M \text{ accepts } (x, w)\}$, ללא כל חסם על $|w|$. אזי $\mathcal{C} = \mathrm{RE}$.

הוכחה. ($\subseteq$) בהינתן M כזו, המכונה שעל x עוברת על כל $w \in \{0,1\}^*$ בסדר לקסיקוגרפי ומריצה את $M(x,w)$, עוצרת ומקבלת ברגע שנמצאה w מקבלת, מזהה את A; לכן $A \in \mathrm{RE}$. ($\supseteq$) תהא $A \in \mathrm{RE}$ ותהא N מכונה המזהה אותה. נגדיר $M(x,w)$ שמקבלת אם ורק אם w מקודדת חישוב מקבל של N על x — בדיקה פולינומית באורך $|x| + |w|$, בדיוק כמו בכיוון ב'. אם $x \in A$ אז N עוצרת ומקבלת ולכן קיים w כזה; אם $x \notin A$ אין חישוב מקבל ולכן אין w. ■

זהו בדיוק המשפט מקורס החישוביות: $A \in \mathrm{RE}$ אם ורק אם קיים פרדיקט דו-מקומי כריע f כך ש-$A = \{x \mid \exists t :\ f(x,t) = 1\}$. **הקשר הזה עלה בשתי המסירות באופן בלתי תלוי** — במסירה 11 המרצה הצביע עליו מיוזמתו ([00:22:11]), ובמסירה 10 סטודנט שאל עליו ישירות ([00:43:55]). התשובה שם: "זה בדיוק אותו משפט אפיון, עד כדי כך ששם לא דיברנו על זמן ריצה… ב-RE הייתה לנו עדות לא מוגבלת באורך; כאן אורך העדות צריך להיות פולינומי, כי אני לא מאפשר הוכחות ארוכות מדי — אם כן, רק לקרוא אותה היה לוקח זמן אקספוננציאלי" ([00:44:26], מסירה 10). כלומר ההבדל היחיד בין האפיון של RE לבין האפיון של NP הוא **שני החסמים הפולינומיים**.

(ב) ויתור על החסם p על זמן האימות מנפח את המחלקה. אם נדרוש $|w| = q(|x|)$ פולינומי אך נרשה ל-M לרוץ בזמן $2^{|x|^k}$, המחלקה המתקבלת מכילה את EXP במלואה: קחו $q \equiv 0$ (עד ריק) והריצו את המכריע האקספוננציאלי ישירות. מכיוון ש-$\mathrm{P} \subsetneq \mathrm{EXP}$ ממשפט היררכיית הזמן, זו בבירור אינה המחלקה שביקשנו לאפיין.

המסקנה. ההגדרה חייבת את **שני** החסמים בו-זמנית: העד קצר, והבדיקה מהירה.

דוגמאות ותרגילים מהשיעור

דוגמה 1: מעקב מלא אחרי המכונה של SAT

תהא הנוסחה (משוחזרת; המרצה שרטט נוסחה בת חמישה משתנים על הלוח, [00:06:34], מסירה 11) $\varphi = (x_1 \vee \neg x_2 \vee x_3) \wedge (\neg x_1 \vee x_4) \wedge (x_2 \vee \neg x_5) \wedge (x_3 \vee x_5)$.

שלב 1 (דטרמיניסטי). סריקה וספירה: חמישה משתנים, $n = 5$.

שלב 2 (אי-דטרמיניסטי). כתיבת חמישה ביטים על הסרט השני. יש $2^5 = 32$ ריצות אפשריות.

ריצה מקבלת. נניח שנכתב $w = 01101$, כלומר $x_1 = 0,\ x_2 = 1,\ x_3 = 1,\ x_4 = 0,\ x_5 = 1$ — הביט ה-i הוא הערך של x_i ([00:07:06], מסירה 11).

פסוקית 1: $x_1 = 0$, $\neg x_2 = 0$, $x_3 = 1$ ⟶ מסופקת.

פסוקית 2: $\neg x_1 = 1$ ⟶ מסופקת.

פסוקית 3: $x_2 = 1$ ⟶ מסופקת.

פסוקית 4: $x_3 = 1$ ⟶ מסופקת.

כל הפסוקיות מסופקות, ולכן בריצה זו המכונה **מקבלת**, ומכאן $\langle \varphi \rangle \in \mathrm{SAT}$.

ריצה דוחה. בריצה שבה נכתב $w = 00000$: פסוקית 4 היא $x_3 \vee x_5 = 0 \vee 0 = 0$ — אינה מסופקת, ולכן בריצה זו המכונה **דוחה**. זה אינו סותר את ההכרעה: להכרעה אי-דטרמיניסטית מספיקה ריצה מקבלת אחת.

העד. בשפת משפט 4: $w = 01101$ הוא העד לשייכות $\langle \varphi \rangle \in \mathrm{SAT}$, והמוודא הוא "הצב את w ב-φ וחשב".

דוגמה 2: אותו מופע דרך תסריט ריצה (הכיוון ההפוך)

נפעיל את דרך I של כיוון ב' על המכונה של SAT ועל אותו φ. תסריט הריצה של הענף המקבל הוא רצף השלשות (q, β, d) של כל הצעדים: ראשית $O(|\langle\varphi\rangle|)$ שלשות של שלב הספירה — כולן **קבועות**, כי השלב דטרמיניסטי; אחריהן חמש שלשות שבהן התו הנכתב הוא $0, 1, 1, 0, 1$ בהתאמה — אלה השלשות היחידות שבהן הייתה בחירה; ואחריהן $O(|\langle\varphi\rangle|^2)$ שלשות של שלב הבדיקה, גם הן קבועות. המוודא מקבל את השרשור כ-w, מסמלץ שלשה-שלשה מול δ, ורואה שהריצה חוקית ומסתיימת במצב מקבל.

בדרך II התמונה נקייה יותר: אחרי הנרמול, הביטים היחידים שיש בהם אינפורמציה הם חמשת הביטים 01101 — בדיוק העד מדוגמה 1. שאר הצעדים דטרמיניסטיים ולכן הביט שלהם נקבע ביחידות.

דוגמה 3: 8 הוא פריק — מקצה לקצה בשני המודלים

במודל האי-דטרמיניסטי (משפט 2). קלט $x = 1000_2$ (כלומר 8), $|x| = 4$.

שלב 1: המכונה כותבת באופן אי-דטרמיניסטי מספר באורך ≤ 4. באחת הריצות היא כותבת $a = 10_2 = 2$.

שלב 2: באותה ריצה היא כותבת $b = 100_2 = 4$.

שלב 3: בדיקה — $2 > 1$, $2 < 8$, $4 > 1$, $4 < 8$: עוברת.

שלב 4: כפל ארוך — $2 \cdot 4 = 8 = 1000_2$.

שלב 5: השוואה ל-x: שווה ⟶ **קבל**.

בריצה אחרת המכונה כותבת $a=3, b=5$: שלב 5 מגלה $8 \neq 15 \longrightarrow$ דוחה. בריצה שלישית $a=1$: שלב 3 דוחה מיד. אין בכך פגם — קיימת ריצה מקבלת, ולכן $8 \in A$.
לעומת זאת עבור $x=7$: כל זוג a, b עם $1 < a, b < 7$ מקיים $ab \neq 7$, ולכן **כל** ריצה דוחה, ובצדק $7 \notin A$.
במודל המוודא (הגדרה 1). העד הוא w באורך $2|x|$, המפורש כשני מספרים a, b בני $|x|$ ביטים כל אחד. עבור $x=8$: $w = 0010\,0100$, כלומר $a=2, b=4$. המוודא (1) בודק ש-$1 < a < x$ ו-$1 < b < x$; (2) מחשב $a \cdot b$; (3) משווה ל-x. שתיים ראשונות $O(|x|)$, הכפל $O(|x|^2)$ — פולינומי. הפולינום שמגביל את אורך העד הוא $q(n) = 2n$ ([00:50:45], מסירה 10). לכן $A \in \mathrm{NP}'$, וממשפט 4 גם $A \in \mathrm{NP}$ — הפעם בלי לבנות NTM כלל.

> **תיקון:** בהקלטה, בגרסת המוודא, המרצה תיאר רק את הכפל וההשוואה והשמיט את בדיקת הטווח $1 < a, b < x$ ([00:49:43]–[00:50:15], מסירה 10). בלעדיה העד $w = (1, x)$ היה מתקבל עבור **כל** x, וכל מספר היה נראה פריק. הבדיקה כן מופיעה בגרסת ה-NTM של אותה הרצאה (שלב 3, [00:17:29]), ולכן ברור שמדובר בהשמטה בעל פה. הוחזרה כאן.

דוגמה 4 (תוספת עורך): CLIQUE
$\mathrm{CLIQUE} = \{\langle G, k\rangle \mid G \text{ contains a clique of size } k\}$. העד הוא רשימת k קודקודים; אורכה $O(k \log |V|)$ — פולינומי בקלט. האימות: לוודא שכל הקודקודים שונים, שיש בדיוק k מהם, ושכל אחד מ-$\binom{k}{2}$ הזוגות הוא קשת ב-G — $O(k^2)$ בדיקות. לכן $\mathrm{CLIQUE} \in \mathrm{NP}$. הדוגמה מובאת כתרגול נוסף לתבנית "עד + אימות" ולא נאמרה באף אחת מהמסירות.
תרגיל: המבוך כמודל ([00:41:16], מסירה 11)
השאלה שהמרצה שאל את הכיתה: נתון מבוך, ומכונה שבכל התפצלות בוחרת לאן לפנות. המבוך "פתיר" אם ורק אם קיימת סדרת בחירות שמוציאה החוצה. איזו עזרה מינימלית תספיק לי, לפני הכניסה, כדי לוודא שאפשר לצאת?
הפתרון המלא. *לא* מצפן — הוא מצביע צפונה, ואיני יודע היכן היציאה. *לא* שלטים — הם בתוך המבוך ולא אצלי. *מפה* מספיקה, אך נותנת יותר מדי: היא מאפשרת לי לפתור את המבוך, לא רק לוודא פתרון. העזרה המינימלית היא **רשימת פניות** באורך מספר הצמתים שאעבור: "שמאלה, ימינה, ישר, ישר, שמאלה…". איתה אני נכנס, ממלא אחר ההוראות, ורואה אם יצאתי — בלי לקבל אף החלטה בעצמי. התרגום: הרשימה היא תסריט הריצה, וכל "פנייה" היא בחירה ב-δ. אחרי משפט 3 אפשר לומר יותר: אם בכל צומת יש בדיוק שתי אפשרויות, הרשימה היא מחרוזת ביטים באורך מספר הצמתים.
תרגיל: נרמול מכונה עם 10 אפשרויות ([00:58:15]–[01:00:22], מסירה 10)
השאלה שהמרצה שאל את הכיתה: נתון מעבר של מכונה אי-דטרמיניסטית שבו יש 10 אפשרויות. איך מגדירים מכונה שקולה שבה לכל מעבר לכל היותר שתי אפשרויות?
הצעת סטודנט: "לעשות את מה שהמכונה עושה, או לא לעשות". זה הכיוון הנכון, אך צריך לוודא ששקילות נשמרת: אם למכונה המקורית 10 אפשרויות, המכונה החדשה חייבת לאפשר להגיע לכל אחת מהן.

הפתרון המלא. מפצלים את השאלה "בחר אחת מתוך 10" ל-10 שאלות בינאריות שרשוריות: "האם לבצע את האפשרות הראשונה, או לעבור למצב שאומר 'בחר אחת מתוך התשע הנותרות'?" — וכן הלאה, עד שבמצב האחרון נשארת אפשרות יחידה. זו בדיוק הבנייה של משפט 3. המחיר: על כל צעד מקורי מבצעים לכל היותר $k \leq 2|Q||\Gamma|$ צעדים — קבוע שאינו תלוי בקלט, ולכן זמן הריצה גדל לכל היותר בגורם קבוע.

שאלה מהכיתה: האם זה כמו fixer? ([00:33:49], מסירה 11)

השאלה: תנאי (2) נראה כמו הפעלת מכונה על שני ארגומנטים, כמו העיקרון של נקודת שבת.

התשובה: לא. במשפט נקודת השבת הפואנטה היא שמתקבלת אותה תשובה עבור אובייקט מקובע. כאן M **אינה מחויבת** להחזיר את אותה תשובה על כל w — להפך, זה כל העניין: על w אחת היא מקבלת ועל אחרת דוחה. השאלה שאנחנו שואלים אינה "מה M מחזירה" אלא "**האם קיימת** w שעבורה היא מקבלת".

הערות מהשיעור

[00:00:34] מסירה 11 / [00:19:33] מסירה 10 — אל תגידו "מגרילה". שני המרצים, בנפרד, הזהירו מפני המונח. האי-דטרמיניזם אינו הגרלה, אינו דגימה ואינו אקראיות. המונח "מנחשת" נפוץ אך שניהם ממליצים להימנע ממנו: "הוא עצמו לא טעות, אבל הוא מקרב אתכם לטעות". במסירה 10 סטודנט שאל במפורש "האם זה אומר שהיא לוקחת מספר אקראי?", והתשובה: לא בדיוק — כשמדברים על אקראיות יש גם התפלגות הסתברות על התוצאות, וכאן אין. הניסוח המדויק: המכונה **בוחרת** או **כותבת מחרוזת באופן אי-דטרמיניסטי**.

[00:01:04] מסירה 11 / [00:24:22] מסירה 10 — איפה בדיוק האי-דטרמיניזם. בשתי המכונות שראינו הוא מרוכז בשלב אחד בלבד; כל השאר דטרמיניסטי. זו התובנה שממנה נולד כל השיעור.

[00:02:45] מסירה 11 — $\langle\varphi\rangle$ מול φ. פורמלית עובדים עם הקידוד, כי שפה היא קבוצת מחרוזות; בראש חושבים על הנוסחה.

[00:14:17] מסירה 10 — עד כמה מפורט לכתוב מכונה. המרצה כתב את δ במפורש **פעם אחת** בכוונה, והדגיש: מכאן והלאה כותבים מכונות ברמת high level ("כתוב באופן אי-דטרמיניסטי מספר באורך…"), ולא תראו את הכתיבה המפורטת בשום מקום אחר. אבל חשוב לראות אותה פעם אחת כדי להבין שההגדרות באמת עומדות מאחורי הניסוח המקוצר.

[00:15:35] מסירה 11 — למה זו לא מכונת הכרעה. מכונה שמכריעה את SAT מקבלת נוסחת CNF ומחזירה true/false. כאן שינינו את צורת הקלט — הוא הפך לזוג — ולכן זו כבר לא מכונת הכרעה אלא מוודא.

[00:17:43] מסירה 11 / [00:39:10] מסירה 10 — "הגדרה שקולה" היא בעצם משפט. ברגע שמוסרים הגדרה שנייה לאותה מחלקה כבר טוענים טענה. במסירה 10 המרצה נזהר במיוחד וקרא למחלקה החדשה NP' עד שהוכיח את השוויון.

[00:26:23] מסירה 11 — ההברקה שמחברת בין שתי ההגדרות. ה"קיים w" בהגדרת ה-verifier מתחבר בדיוק ל"קיימת ריצה אפשרית מקבלת" שבהגדרת ההכרעה האי-דטרמיניסטית. שני כמתי הקיום הם אותו כמת.

[00:27:27] מסירה 11 — מה המכונה "מחזיקה בבטן". $\hat{M}$ מקבלת כקלט רק את x; את M היא אינה מקבלת כקלט — היא מקודדת בתוך הגדרתה. הדבר היחיד שחסר לה הוא w.
[00:37:36] מסירה 10 — המודל האי-דטרמיניסטי פיקטיבי. אין מכונות אי-דטרמיניסטיות במציאות. ההגדרה עם המוודא היא זו שנותנת ל-NP משמעות.
[00:45:28]–[00:46:32] מסירה 10 — המשמעות הפילוסופית של P מול NP. NP היא מחלקת הבעיות שבהן לקלטים **בפנים** יש עדות משכנעת, ולקלטים **בחוץ** אין אף עדות — כלומר "אי אפשר להוכיח טענות לא נכונות". לכן השאלה P מול NP היא השאלה: האם יש משמעות להוכחות? האם כל דבר שאני יודע לבדוק הוכחה עבורו, אני גם יודע להוכיח בעצמי? האינטואיציה מהעולם היום-יומי אומרת שקל יותר לבדוק הוכחה מאשר לכתוב אותה — כלומר שמשערים $\mathrm{P} \neq \mathrm{NP}$ — אבל אין לכך הוכחה.
[01:19:11] מסירה 10 — כיוון הבנייה. סטודנט הציע להפוך כל מצב אי-דטרמיניסטי ל"סינגלטון". המרצה הבהיר שבכיוון הזה **נתונה** מכונה דטרמיניסטית ומבקשים לבנות אי-דטרמיניסטית — ולכן אין מה "לצמצם"; מה שחסר הוא לייצר את w. הבלבול טבעי, ושווה לשים לב לו: בכל אחד משני הכיוונים המכונה הנתונה והמכונה הנבנית מתחלפות בתפקידיהן.
[01:45:08] מסירה 10 — אסימטריה שכדאי לזכור. מכונה אי-דטרמיניסטית יכולה להריץ מכונה דטרמיניסטית (כל מכונה דטרמיניסטית היא בפרט אי-דטרמיניסטית). ההפך אינו נכון — ולכן בכיוון ב' חייבים לספק את הבחירות מבחוץ.
[00:38:34] מסירה 11 / [01:29:21] מסירה 10 — מה נדרש על פולינומים. סכום, מכפלה והרכבה של פולינומים הם פולינום. במסירה 10 המרצה הוסיף שזו אחת הסיבות שמסתכלים דווקא על P ו-NP: אלגוריתם פולינומי שמריץ אלגוריתם פולינומי נשאר פולינומי — תכונה שאינה מתקיימת בזמן ליניארי.
[00:52:39] מסירה 11 — לגבי המבחן והתרגיל. הכיוון $\mathrm{NP} \Rightarrow$ verifier לא נכתב במלואו במסירה 11, והמרצה אמר שיחזרו עליו. הוא ציין שיש שאלה בתרגיל הבית הנשענת על החומר, ושכדי לפתור אותה **אין צורך בהוכחה עצמה** — צריך את הרעיון של תסריט ריצה ואת ניסוח הטענה. במסירה 10 ([02:13:45]) נאמר שבסוף אותו תרגיל יש שתי שאלות שאי אפשר לפתור עד שיילמד הנושא הבא (טכניקת הריפוד).

פערים בין הסיכום להקלטה

מקור: הקלטה 12 (`0_fFIUnWa4g`). **הפער:** אינה שייכת לשיעור זה כלל — כולה טכניקת הריפוד: $\mathrm{P} = \mathrm{NP} \Rightarrow \mathrm{EXP} = \mathrm{NEXP}$, $E \subseteq \mathrm{PSPACE} \Rightarrow E^2 \subseteq \mathrm{PSPACE}$, והמסקנה $E \neq \mathrm{PSPACE}$. **ההכרעה:** סומנה `coverage: none` ; החומר שייך לשיעור אחר בסדרה.
מקור: הקלטה 10 (`zcCQY3oT40Y`) מול הקלטה 11. **הפער:** שתי המסירות בונות את אותו משפט על שתי דוגמאות שונות לגמרי — מסירה 11 על SAT (בהמשך לשיעור 5), מסירה 10 על $\mathrm{COMPOSITES}$. אף אחת אינה מזכירה את הדוגמה של השנייה. **ההכרעה:** שתיהן נכללו במלואן (משפט 1 ומשפט 2), כי כל אחת מדגימה את אותה תבנית בהקשר אחר. הן מאשרות זו את זו: שתיהן מגיעות ל-$O(n^3)$ באמצעות $\mathrm{time} \cdot \mathrm{space}$, בשתיהן האי-דטרמיניזם מרוכז בשלב אחד.

מקור: הקלטה 10, [00:54:26]–[01:11:42]. **הפער:** למת הנרמול (לכל היותר שתי אפשרויות בכל מעבר, במחיר גורם קבוע) אינה מופיעה בסיכום ואינה מופיעה בהקלטה 11 כלל. **ההכרעה:** נוספה כמשפט 3 עם הבנייה המלאה, טענת ההתאמה, וחסם $k \le 2|Q||\Gamma|$. היא משנה את חשבון אורך העד בכיוון ב' — ראו הבא.

מקור: שתי המסירות. **הפער:** חשבון אורך העד בכיוון NP verifier $\Rightarrow$ שונה. מסירה 11 והסיכום (עמוד 3): העד הוא תסריט שלשות, $q(n) = (\lg|Q| + \lg|\Gamma| + 1) \cdot p_0(n)$. מסירה 10: אחרי נרמול העד הוא ביט אחד לצעד, $q(n) = p_0(n)$. **ההכרעה:** שתיהן נכונות. הצגנו את שתיהן כ"דרך I" ו"דרך II", כאשר דרך I שומרת על סימון הסיכום ודרך II היא הטיפול העשיר יותר; ההבדל המהותי — שבדרך II כל w מתארת ריצה חוקית ולכן אין מה לוודא — נכתב במפורש.

מקור: עמוד 3 בסיכום. **הפער:** נכתב $\lg|Q| + \lg|\Gamma| + 1$ ללא חלקים עליונים. **ההכרעה:** תוקן ל-$\lceil\lg|Q|\rceil + \lceil\lg|\Gamma|\rceil + 1$; מספר ביטים חייב להיות שלם. אין השפעה על הפולינומיות.

מקור: הקלטה 10, [00:49:43]–[00:50:15]. **הפער:** בגרסת המוודא ל-$\mathrm{COMPOSITES}$ המרצה השמיט את בדיקת $1 < a, b < x$, ותיאר רק כפל והשוואה. זו שגיאה מתמטית: בלעדיה $w = (1, x)$ מתקבל לכל x, וכל מספר נראה פריק. **ההכרעה:** הבדיקה הוחזרה בגוף הדוגמה. היא מופיעה בגרסת ה-NTM של אותה הרצאה ([00:17:29]), ולכן ברור שמדובר בהשמטה בעל פה.

מקור: עמוד 2 בסיכום מול הקלטה 10. **הפער:** בגוף ההגדרה בסיכום נכתב $w \in \{0,1\}^{q(|x|)}$ (אורך מדויק), ואילו בהערה הכחולה בצד נכתב $A = \{x \mid \exists w \in \{0,1\}^* \dots\}$ (אורך כלשהו). ההבדל אינו קוסמטי: בלי חסם אורך המחלקה היא RE ולא NP. **ההכרעה:** הוכרע לטובת האורך המדויק — מסירה 10 מנסחת גם היא "מחרוזת בינרית באורך $p(|x|)$" ([00:40:15]), כלומר שני מקורות בלתי תלויים נגד ההערה הכחולה, שהיא קיצור בלתי-פורמלי. הנקודה עצמה הפכה למשפט 5(א).

מקור: שתי המסירות. **הפער:** שמות שני הפולינומים הפוכים. הסיכום ומסירה 11: p = זמן הריצה, q = אורך העד. מסירה 10: t = זמן הריצה, p = אורך העד. **ההכרעה:** אומץ סימון הסיכום לאורך כל הקובץ; ההבדל מתועד כאן וב-`open_questions` כדי שקורא שיאזין להקלטה 10 לא יתבלבל.

מקור: הקלטה 11, [00:51:00]. **הפער:** הכיוון NP verifier $\Rightarrow$ נמסר שם כ"רעיון הוכחה" בלבד. **ההכרעה:** הפער נסגר לגמרי על ידי מסירה 10, שמוסרת את הכיוון הזה במלואו — הבנייה הדו-סרטית, שני כיווני הנכונות, וניתוח הזמן ([01:37:48]–[02:05:50]). מה שהיה בגרסה הקודמת של הקובץ שחזור עורך הוא כעת חומר מוקלט.

מקור: שני המקורות. **הפער:** בדרך I אף אחד מהם אינו מטפל בפער שבין "ריצה מקבלת עשויה להיות קצרה מ-$p_0(|x|)$" לבין הדרישה $|w| = q(|x|)$ **בדיוק**. **ההכרעה:** בדרך II הבעיה נעלמת — הסימולציה פשוט עוצרת, והביטים הנותרים אינם נקראים, וזו בדיוק תשובת המרצה לשאלת הסטודנט ב-[01:59:30]. בדרך I מרפדים את התסריט לאורך $q(|x|)$ ומגדירים את המוודא לעצור ולקבל ברגע שהסימולציה הגיעה למצב מקבל. הניסוח $|w| \le q(|x|)$ שקול.

מקור: הקלטה 11, [00:06:34]. **הפער:** הנוסחה הקונקרטית בת חמישה המשתנים נכתבה על הלוח ואינה נשמעת. **ההכרעה:** נבדק גם מול מסירה 10 — שאינה עוסקת ב-SAT כלל ולכן אינה יכולה לסייע. הנוסחה נותרת שחזור: נבחרה נוסחת CNF בת חמישה משתנים שההשמה 01101 שנאמרה בהקלטה אכן מספקת אותה.

מקור: משפט 5, סעיף (א). **הפער:** בגרסה הקודמת של הקובץ סומן כתוספת עורך. **ההכרעה:** מסירה 10 מאשרת אותו — סטודנט שאל ישירות על הקשר לאפיון RE והמרצה אישר שזה "בדיוק אותו משפט אפיון", והסביר במפורש שחסם אורך העד הוא ההבדל ([00:43:55]–[00:44:56]). התיוג שונה מ"תוספת" ל"מבוסס מקור". סעיף (ב) נותר הרחבת עורך.

מקור: כל מקורות השיעור. **הפער:** רביעיית המכונה אינה נכתבת במפורש באף אחד מהם, ובפרט מצב ההתחלה אינו מופיע. **ההכרעה:** אומצה הצורה המחייבת של הסדרה, $M = (Q, q_{start}, F, \Sigma, \Gamma, \delta)$, והמצבים המקבלים מסומנים F במקום q_{acc}.

מקור: עמוד 4 בסיכום. **הפער:** העמוד מכיל חמש שורות בלבד (סיום ההוכחה) וכותרת כחולה קצרה ומעט מטושטשת. **ההכרעה:** תוכן השורות ברור ושולב במלואו בכיוון ב'; הכותרת אינה נושאת מידע מתמטי ולא שוחזרה.

מקור: תוספת עורך. **הפער:** דוגמת CLIQUE ומשפט 5(ב) אינם מופיעים באף מקור. **ההכרעה:** נכללו כתוספת מסומנת, כתרגול נוסף וכהשלמת התמונה "למה ההגדרה נראית כך".

סיכום ונקודות למבחן

מה חייבים לזכור בעל פה

הניסוח המדויק של האפיון. $A \in \mathrm{NP} \iff$ קיימים פולינומים p, q ומכונה **דטרמיניסטית** M הרצה בזמן $p(|a|)$ על כל קלט a, כך שלכל x: $x \in A \iff \exists w \in \{0,1\}^{q(|x|)}$ ש-M מקבלת את (x, w). אם שכחתם אחד מהשלושה — "דטרמיניסטית", "q פולינומי", "אם ורק אם" — הניסוח שגוי.

שתי הבניות. NTM ⟶ verifier: כתוב w באופן אי-דטרמיניסטי, הרץ M. verifier ⟶ NTM: העד הוא רצף הבחירות; או $q(n) = (\lceil \lg |Q| \rceil + \lceil \lg |\Gamma| \rceil + 1) \cdot p_0(n)$ עם תסריט שלשות ובדיקת חוקיות, או — אחרי נרמול — $q(n) = p_0(n)$ עם ביט לצעד ובלי בדיקת חוקיות.

למת הנרמול. לכל NTM יש שקולה שבכל מעבר לכל היותר שתי אפשרויות, בעלות גורם קבוע $\leq |Q||\Gamma|$ בזמן.

חשבון הזמן בכיוון א'. $O(q(n)) + q(n) + p(n + q(n))$, וסגירות פולינומים לסכום והרכבה.

שתי הדוגמאות עם החסם המספרי: $\mathrm{SAT} \in \mathrm{NTime}(n^3)$ ו-$\mathrm{COMPOSITES} \in \mathrm{NTime}(n^3)$, בשניהם מ-$\mathrm{time} \cdot \mathrm{space} = O(n^2) \cdot O(n)$.

מלכודות סטנדרטיות

לומר ש-M מכריעה את A. לא — M מקבלת (x, w), לא x. היא מוודא.

להשתמש רק בכיוון אחד של ה"אם ורק אם" בתנאי (2). בלי הכיוון "אם קיים w אז $x \in A$" לא ניתן לשלול ריצה מקבלת עבור $x \notin A$.

לשכוח את החסם על אורך העד. בלי q מקבלים RE, לא NP.

לחסום את זמן האימות ב-$p(|x|)$ במקום ב-$p(|x| + |w|)$. ההגדרה חוסמת את זמן הריצה באורך **הקלט המלא** של M, שהוא הזוג.

לשכוח למה הסימולציה עוצרת. בכיוון ב' העצירה נובעת מ-$\mathrm{time}_N(x) \leq p_0(|x|)$ — חסם על הריצה **הארוכה ביותר**, ולכן על כל ריצה — ולא מכך שהמכונה מקבלת.

למדוד את הזמן ביחס למספר ולא לאורך הקידוד שלו. זו הטעות שהפילה את האלגוריתם הנאיבי ל-$\mathrm{COMPOSITES}$: איטרציות הן $2^{|x|}$ ביחס לאורך הקלט.

לומר "מגרילה" / "בוחרת אקראית". אין אקראיות במודל האי-דטרמיניסטי.
לבלבל בין העד לבין המפה. העד הוא המידע המינימלי המספיק לאימות, לא פתרון מלא.
צ'ק-ליסט: מה סטודנט אמור לדעת לעשות אחרי השיעור
לנסח את שתי ההגדרות של NP ולהסביר איזו מכונה דטרמיניסטית ואיזו לא.
בהינתן שפה חדשה, להציע עד, להוכיח שאורכו פולינומי, לתאר את אלגוריתם האימות ולחסום את זמנו — ובכך להוכיח שייכות ל-NP בלי לבנות NTM כלל.
בהינתן NTM פולינומית, לבנות ממנה verifier ולחשב את $q(n)$ במפורש — בשתי הדרכים.
בהינתן verifier, לבנות ממנה NTM ולהראות שזמן הריצה פולינומי, תוך ציון היכן נכנסת סגירות הפולינומים.
לנרמל מכונה אי-דטרמיניסטית לשתי אפשרויות למעבר ולחסום את מחיר הנרמול.
לכתוב פעם אחת את δ של שלב אי-דטרמיניסטי במפורש, ולהסביר איך "כתוב מחרוזת באופן אי-דטרמיניסטי" מתורגם למעברים.
להסביר מה קורה לכל אחת מההגדרות אם מסירים את החסם על אורך העד או על זמן האימות.
הסיכום הכתוב שעליו נשען הקובץ: גיא סופר.

שאלות שנשארו פתוחות

הנוסחה הקונקרטית בת חמישה המשתנים שהמרצה שרטט על הלוח אינה נשמעת באף אחת מהמסירות; שוחזרה נוסחה תואמת שההשמה 01101 מספקת אותה.

שתי המסירות מסמנות את שני הפולינומים בשמות הפוכים; נקטנו בסימון הסיכום (p לזמן, q לאורך העד).

עמוד 2–3 בסיכום: סימוני החצים ⇐/⇒ ליד שני כיווני ההוכחה כתובים לפי כיוון הקריאה מימין לשמאל; בגוף הקובץ סימנו כל כיוון לפי תוכנו ולא לפי החץ.

רביעיית המכונה אינה נכתבת במפורש באף אחד ממקורות השיעור; אימצנו את הצורה המחייבת של הסדרה, כולל מצב ההתחלה.

7 CLIQUE ו-Independent Set, רדוקציות בזמן פולינומי, NP-קשה ו-NP-שלמה

בשיעור זה מוסיפים שתי שפות גרפים ל-NP (CLIQUE ו-IS), מגדירים את הרדוקציה בזמן פולינומי $\le_p$ ואת המושגים NP-קשה ו-NP-שלמה, ומוכיחים את הרדוקציה בין IS ל-CLIQUE דרך הגרף המשלים — הכלי שיאפשר בהמשך להעשיר את משפחת הבעיות הקשות בלי לחזור להגדרה בכל פעם.

ביטחון: high

בקצרה

מרחיבים את אוסף השפות שאנחנו יודעים שהן ב-NP בשתי בעיות גרפים: **CLIQUE** (קיימת קליקה בגודל K?) ו-Independent Set = **IS** (קיימת קבוצה בלתי תלויה בגודל K?). כל אחת מוכחת בדרך אחרת — האחת דרך מכונה אי-דטרמיניסטית, השנייה דרך verifier — כך שנראה את שתי ההגדרות השקולות של NP בפעולה.

מוכיחים שמותר מכאן ואילך לכתוב **פסאודו-קוד** במקום מכונת טיורינג: זמן על מכונת טיורינג שקול פולינומית לזמן על מכונת RAM, והרזולוציה שמעניינת אותנו ("פולינומי / לא פולינומי") גסה מספיק כדי לא להבחין בהפרש.

מגדירים את הכלי המרכזי של כל שארית הקורס: **רדוקציה בזמן פולינומי** $A \le_p B$. הכיוון קריטי — $A \le_p B$ אומר ש-B היא *לפחות* קשה כמו A, כי אלגוריתם ל-B פותר גם את A.

מוכיחים $\mathrm{CLIQUE} \le_p \mathrm{IS}$ (ובאותה רדוקציה גם $\mathrm{IS} \le_p \mathrm{CLIQUE}$) על ידי מעבר ל**גרף המשלים**, כולל הנימוק למה ניסיונות נאיביים יותר — למחוק את כל הקשתות או להוסיף את כל הקשתות — נכשלים.

מגדירים **NP-קשה** ("כל שפה ב-NP נרדקת אליי") ו-**NP-שלמה** ("NP-קשה **וגם** שייכת ל-NP"). זהו בדיוק ההבדל בין שני המושגים, והוא נבדק במבחנים.

מוכיחים את משפט ההעברה: אם A היא NP-קשה ו-$A \le_p B$ אז גם B היא NP-קשה. זהו המשפט שהופך את החיים לאפשריים — בלעדיו כל הוכחת NP-קושי הייתה מחייבת לטפל בכל שפה ב-NP מחדש.

רקע ותלויות

השיעור הזה יושב כולו על ההגדרות שנבנו בשיעורים 4–6, ומשתמש בהן בלי לחזור עליהן. לכן נציג אותן כאן במלואן.

מחלקות הזמן (ראו שיעור 4). לכל פונקציה f, המחלקה $\mathrm{DTime}(f(n))$ היא אוסף השפות שניתן להכריע במכונת טיורינג דטרמיניסטית בזמן $O(f(n))$, ומכאן $P = \bigcup_{c \in \mathbb{N}} \mathrm{DTime}(n^c)$.

NP — ההגדרה הבסיסית (ראו שיעור 6). באופן מקביל, $\mathrm{NTime}(f(n))$ היא אוסף השפות שמכונה אי-דטרמיניסטית מכריעה בזמן $O(f(n))$, ו- $\mathrm{NP} = \bigcup_{c \in \mathbb{N}} \mathrm{NTime}(n^c)$. "מכריעה" עבור מכונה אי-דטרמיניסטית M פירושו: $x \in L$ אם ורק אם **קיימת** ריצה של M על x שמקבלת; אם $x \notin L$ אז **כל** הריצות דוחות; וכל ריצה אפשרית עוצרת, ובזמן פולינומי באורך הקלט.

NP — ההגדרה השקולה עם verifier (ראו שיעור 6). $A \in \mathrm{NP}$ אם ורק אם קיימת מכונת טיורינג **דטרמיניסטית** M שרצה בזמן פולינומי, וקיים פולינום p, כך שלכל x: $x \in A \iff \exists\, w \in \{0,1\}^{\leq p(|x|)} \text{ s.t. } M \text{ accepts } \langle x, w\rangle$. המכונה M נקראת **מוודא בזמן פולינומי (polynomial-time verifier)** עבור A. שימו לב לניסוח המדויק: M אינה מכריעה את A — היא מכריעה שפה של *זוגות*. שני התנאים שהיא צריכה לקיים הם "לקלטים בקבוצה יש עדות קצרה שמשכנעת אותה" ו"קלטים שאינם בקבוצה — אי אפשר לרמות אותה עליהם". שתי ההגדרות הוכחו שקולות בשיעור 6.

רדוקציות מחישוביות. בחישוביות אמרנו ש-A נרדקת ל-B אם קיימת פונקציה f חשיבה־מלאה כך ש-$x \in A \iff f(x) \in B$; שקול לכך, קיימת מכונת טיורינג M שעוצרת על כל קלט ומקיימת את התכונה הזו. גם ראינו שם ש-R ו-RE סגורות כלפי מטה תחת רדוקציות, ושהיחס טרנזיטיבי (ההוכחה: שרשור מכונות / הרכבת פונקציות). כל מה שנעשה כאן הוא להוסיף לדרישה הסמנטית הזו דרישת **יעילות**.

מודל החישוב — למה מותר לעבור לפסאודו-קוד. ניתן להוכיח כי הזמן על מכונת טיורינג שקול פולינומית לזמן על **מכונת RAM** (Random Access Memory) — המודל שבו מותר לגשת ישירות לתא בזיכרון בלי לצעוד אליו, כלומר בדיוק המודל שבו נכתב פסאודו-קוד בקורסי מבני נתונים ואלגוריתמים. בחישוביות עניינה אותנו שקילות סמנטית ("מה אפשר לחשב"); בסיבוכיות אנחנו מוסיפים על הסמנטיקה גם את היעילות, ואומרים שהמודלים שקולים **עד כדי פולינום**. מכאן:

> כל עוד הרזולוציה שמעניינת אותנו היא "האם הסיבוכיות היא n^c עבור c כלשהו", כלומר "פולינומי או לא פולינומי", אפשר לעבוד בפסאודו-קוד.

אם פתרתי בעיה בזמן פולינומי בפסאודו-קוד, אני יכול לפתור אותה בזמן פולינומי גם במכונת טיורינג. ייתכן שהפולינום יגדל — אבל הפולינום עצמו לא מעניין אותנו, רק היותו פולינום. המסננת שדרכה אנחנו עובדים גסה מאוד, ולכן אפשר לעבוד באיזה מודל שנוח. מכאן ואילך רוב הקורס ייכתב בשפה של אלגוריתמים, לא של מכונות.

מוסכמה על גרפים. מכאן ואילך "גרף" פירושו תמיד גרף **פשוט ולא מכוון**, אלא אם נאמר אחרת. גרף נכתב $G = (V, E)$, וקשת בין x ל-y נסמן xy. כשמדובר בקלט לבעיית הכרעה, G הוא כמובן קידוד של הגרף; לא נעסוק בקידוד עצמו, רק נדרוש שיהיה סביר (כלומר שהגודל שלו יהיה פולינומי במספר הקדקודים והקשתות).

הגדרות

הגדרה 1: קליקה

יהי $G = (V, E)$ גרף. קבוצה $U \subseteq V$ נקראת **קליקה (clique)** כאשר לכל $x, y \in U$ שונים מתקיים $xy \in E$.

אינטואיציה. קליקה היא קבוצת קדקודים ש"כולם מחוברים לכולם" — תת-גרף שלם. חשבו על קבוצת אנשים ברשת חברתית שכל שניים בה מכירים זה את זה.

מופע. בגרף P_5 עם $V = \{a, b, c, d, e\}$ ו-$E = \{ab, bc, cd, de\}$, הקבוצה $\{a, b\}$ היא קליקה (בגודל 2), וכך גם כל קשת בודדת. הקבוצה $\{a\}$ היא קליקה טריוויאלית, וגם $\varnothing$.

אי-מופע. באותו גרף, $\{a,b,c\}$ **אינה** קליקה: $ac \notin E$. שימו לב שדי בזוג אחד חסר כדי להרוס את התכונה.

הגדרה 2: השפה CLIQUE

$$\mathrm{CLIQUE} = \Big\{ \langle G, K \rangle \;\Big|\; G=(V,E) \text{ graph},\ K \in \mathbb{N},\ \exists U \subseteq V:\ |U| = K \text{ and } U \text{ is a clique in } G \Big\}.$$

כלומר, הקלט הוא זוג $\langle G, K \rangle$ ואנחנו צריכים להכריע האם בגרף G קיימת קליקה בגודל K.

מופע. בגרף שהודגם בשיעור — משולש שאליו מחוברים עוד קדקודים — הזוג $\langle G, 3 \rangle$ שייך ל-CLIQUE, כי שלושת קדקודי המשולש הם קליקה בגודל 3.

אי-מופע. עבור אותו גרף בדיוק, $\langle G, 4 \rangle \notin \mathrm{CLIQUE}$: כל ארבעה קדקודים שנבחר — יימצאו בהם שניים שאין ביניהם קשת.

הגדרה 3: קבוצה בלתי תלויה

יהי $G=(V,E)$ גרף ותהי $U \subseteq V$. הקבוצה U נקראת **בלתי תלויה (independent set)** כאשר לכל $x,y \in U$ שונים מתקיים $xy \notin E$.

אינטואיציה. זו קבוצת קדקודים שאין ביניהם אף קשת. חשבו על קבוצת משימות שאף שתיים מהן אינן מתנגשות.

> **הערה:** זה **לא** בדיוק "ההפך מקליקה", והלקטור עצר על כך במפורש. ההגדרה של קליקה היא "לכל שני איברים **יש** קשת"; השלילה הלוגית שלה היא "**קיימים** שניים שאין ביניהם קשת". לעומת זאת ההגדרה כאן היא "לכל שניים **אין** קשת" — טענה חזקה בהרבה. אי אפשר לשלול "לכל" ולקבל "לכל". הקשר האמיתי בין שני המושגים אינו שלילה אלא מעבר לגרף המשלים, וזה בדיוק תוכן משפט 3.

מופע. ב-P_5 שלמעלה, $\{a,c,e\}$ בלתי תלויה: $ac, ae, ce \notin E$.

אי-מופע. $\{a,b\}$ אינה בלתי תלויה, כי $ab \in E$.

הגדרה 4: השפה IS

$$\mathrm{IS} = \Big\{ \langle G, K \rangle \;\Big|\; G=(V,E) \text{ graph},\ K \in \mathbb{N},\ \exists U \subseteq V:\ |U| = K \text{ and } U \text{ is independent in } G \Big\}.$$

השפה מזכירה מאוד את CLIQUE — רק שבמקום "יש קשת" נדרש "אין קשת".

הגדרה 5: רדוקציה בזמן פולינומי

תהיינה A, B שפות. **רדוקציה בזמן פולינומי מ-A ל-B** היא מכונת טיורינג (דטרמיניסטית, חד-סרטית סטנדרטית) M המקיימת:

M רצה בזמן פולינומי בגודל הקלט;

לכל קלט x:

אם $x \in A$ אז $M(x) \in B$, **וגם**

אם $x \notin A$ אז $M(x) \notin B$.

אם קיימת רדוקציה כזו נסמן $A \le_p B$.

אינטואיציה, וזה החלק שחייבים לא להתבלבל בו. תנאי 2 שקול ל-$x \in A \iff M(x) \in B$ — הרדוקציה **ממירה** קלטים של A לקלטים של B תוך שימור התשובה. המשמעות המעשית: אם יש בידי מכונה שמכריעה את B, אני יכול להכריע את A — בהינתן x אריץ את הרדוקציה (זמן פולינומי), אקבל $M(x)$, ואשאל את המכריע של B. לכן

אם $A \leq_p B$, אז A "אינה קשה מ-" B עד כדי פולינום.

כלומר B **היא הבעיה הקשה יותר**, ולא להפך. הסימון $\leq$ נבחר בדיוק כדי לקודד את זה, וה-p הקטנה מציינת שההמרה עצמה חסומה בפולינום. זו נקודת הכשל הנפוצה ביותר בשיעור הזה ובכל מה שבא אחריו.

מה רדוקציה איננה. רדוקציה **אינה** פותרת אף אחת מהבעיות. בזמן בניית הרדוקציה איני יודע — ואיני יכול לדעת בזמן פולינומי — האם הקלט שקיבלתי שייך ל-A או לא. ההמרה חייבת לעבוד "בעיוורון". רק בשלב ההוכחה, שהוא לא-אלגוריתמי, אני מרשה לעצמי להניח "נניח $x \in A$, אז **קיימת**...".

הבדל מחישוביות. בחישוביות דרשנו רק את תנאי 2 (הסמנטיקה); זמן הריצה לא עניין אותנו כלל, רק שהמכונה תעצור. כאן אנחנו מוסיפים על הסמנטיקה גם את היעילות.

הגדרה 6: NP-קשה

תהי A שפה. A נקראת **NP-קשה (NP-hard)** כאשר לכל שפה $B \in \mathrm{NP}$ מתקיים $B \leq_p A$.

אינטואיציה. A קשה לפחות כמו כל בעיה ב-NP: לו ידענו לפתור את A בזמן פולינומי, היינו יודעים לפתור בזמן פולינומי כל בעיה ב-NP, ומקבלים $P = \mathrm{NP}$. שימו לב לכיוון: הרדוקציות מגיעות **מ**כל שפה ב-NP **אל** A.

הערה על ההגדרה. A עצמה אינה נדרשת להיות ב-NP. שפה NP-קשה יכולה להיות קשה הרבה יותר — למשל בלתי כריעה לחלוטין.

הגדרה 7: NP-שלמה

תהי A שפה. A נקראת **NP-שלמה (NP-complete)** כאשר:

A היא NP-קשה, **וגם**

$A \in \mathrm{NP}$.

ההבדל בין השתיים בשורה אחת. NP-קשה = "לפחות קשה כמו כל דבר ב-NP". NP-שלמה = NP-קשה **ובנוסף** שייכת בעצמה ל-NP, כלומר היא הבעיה הקשה ביותר **בתוך** NP. תנאי (2) הוא שהופך את A לנציגה של המחלקה ולא רק לחסם עליון עליה.

> **הערה:** מי שלמד חישוביות בקורס שבו לא ניתן שם למושג "RE-קושי" — למד בדיוק את התכונה הזו, פשוט בלי לתת לה שם: במקום להגדיר "RE-קשה" בנפרד, נכתב תנאי הרדוקציה ישירות בתוך הגדרת ה-RE-שלמות. אין כאן שום הבדל מהותי, רק פירוק ההגדרה לשני מרכיבים.

משפטים והוכחות

משפט 1: $\mathrm{CLIQUE} \in \mathrm{NP}$

ההוכחה מתבצעת לפי ההגדרה הבסיסית של NP, באמצעות מכונה אי-דטרמיניסטית. כפי שהוסבר ברקע, מותר לנו לתאר אלגוריתם ולא מכונה.

האלגוריתם. על קלט $\langle G, K\rangle$, כאשר $G=(V,E)$ גרף ו-$K \in \mathbb{N}$:
באופן אי-דטרמיניסטי בחר קבוצה $U \subseteq V$ כך ש-$|U| = K$.
לכל $x, y \in U$ שונים: אם $xy \notin E$ — **דחה**.
קבל.

שימו לב שרק שלב 1 אי-דטרמיניסטי; שלבים 2–3 הם לולאה דטרמיניסטית לגמרי. מכונה אי-דטרמיניסטית רשאית להכיל חלקים דטרמיניסטיים, וגם רשאית לפזר את הבחירות האי-דטרמיניסטיות שלה לאורך הריצה ולא לרכז את כולן בהתחלה.

נכונות — כיוון ראשון. יהי $G=(V,E)$ גרף ויהי $K \in \mathbb{N}$. נניח $\langle G, K\rangle \in \mathrm{CLIQUE}$. אזי, לפי ההגדרה, **קיימת** $U \subseteq V$ כך ש-$|U| = K$ וגם U קליקה ב-G. חשוב לתת שם לאובייקט הזה כדי שנוכל להתייחס אליו בהמשך. כעת, קיימת עבור האלגוריתם ריצה אפשרית שבה הוא בוחר בשלב 1 **בדיוק** את U. בריצה זו, לכל $x, y \in U$ שונים מתקיים $xy \in E$ (כי U קליקה), ולכן התנאי בשלב 2 לעולם אינו מתקיים, האלגוריתם אינו דוחה, ומגיע לשלב 3 ומקבל. לכן קיימת ריצה מקבלת.

נכונות — כיוון שני. נניח $\langle G, K\rangle \notin \mathrm{CLIQUE}$. את המשמעות של זה יש לנסח **על הזוג** לפני שמדברים על האלגוריתם: $\forall U \subseteq V: \quad |U| = K \implies U \text{ is not a clique in } G.$ כעת: בכל ריצה אפשרית של האלגוריתם הוא בוחר בשלב 1 קבוצה $U \subseteq V$ בגודל K; לפי הנוסח שלמעלה U אינה קליקה ב-G, כלומר קיימים $x, y \in U$ שונים עם $xy \notin E$; כשהלולאה בשלב 2 תגיע לזוג הזה היא תדחה. לכן **כל** ריצה אפשרית דוחה.

> **הערה:** בהרצאה נאמר בקצרה "לכל ריצה אפשרית לא יימצא U מתאים", והמרצה עצר את הכיתה ודרש קודם את האפיון של הזוג עצמו. זה לא קפדנות לשמה: אם מדלגים על השלב הזה, קל להחליק בין "האלגוריתם לא מצא" (טענה על האלגוריתם) לבין "לא קיים" (טענה על הקלט), וזו בדיוק השגיאה שהופכת הוכחות מסוג זה למעגליות.

ניתוח זמן ריצה. על קלט $\langle G, K\rangle$:
בחירת U דורשת $O(|V|)$ צעדים: במקרה הגרוע צריך לעבור על כל קדקוד ולהחליט אם הוא בקבוצה או לא.
הלולאה בשלב 2 עוברת על כל הזוגות מתוך U, כלומר $\binom{K}{2} = O(K^2)$ זוגות.
בלי הגבלת הכלליות $K \le |V|$: אם $K > |V|$ אפשר לדחות מיד (אין $|V|+1$ קדקודים). לכן $O(K^2) \subseteq O(|V|^2)$.
סך הכול $O\big(|\langle G, K\rangle|^2\big)$, ובפרט פולינומי בגודל הקלט. לכן $\mathrm{CLIQUE} \in \mathrm{NP}$. ■

> **הערה על החסם $K \le |V|$ — נקודה עדינה שעלתה בשתי המסירות.** המספר K מקודד בבינארית ותופס $\Theta(\log K)$ ביטים. לכן אלגוריתם שעושה K צעדים עושה מספר צעדים **מעריכי** בגודל הקידוד של K! אם K היה מגיע לבדו כקלט, שום דבר כאן לא היה פולינומי. מה שמציל אותנו הוא שלצד K מגיע גם הגרף: אחרי הצמצום $K \le |V|$, כל חסם ב-K הופך לחסם ב-$|V|$, ו-$|V|$ הוא **כן** לינארי בגודל הקידוד של הקלט. במילים אחרות — "הגרף משלם את המחיר של K". בכל ניתוח זמן ריצה של בעיות מהסוג הזה חייבים לבטא את הכול כפונקציה של **גודל הקלט**, ולא של הפרמטרים המספריים שבתוכו.

הערה על עצירה: בשיעור נשאל אם לא היינו צריכים להוכיח בנפרד שהאלגוריתם עוצר בכל ריצה. המרצה תחילה הסכים, ובהמשך חזר בו והבהיר: מאחר שניתחנו את זמן הריצה **לכל ריצה אפשרית** והראינו שהוא חסום בפולינום, העצירה נובעת מכך ואין צורך בטיעון נפרד.

משפט 2: $\mathrm{IS} \in \mathrm{NP}$

הפעם נוכיח דרך **ההגדרה השקולה**, עם verifier. אפשר היה כמובן להעתיק את הוכחת משפט 1 ולהחליף בשלב 2 את התנאי $xy \in E$ ב-$xy \notin E$; אנחנו בוחרים בדרך השנייה כדי לתרגל את שתי ההגדרות.

המוודא. על קלט $\langle G, K \rangle$ עם $G = (V, E)$ גרף, $K \in \mathbb{N}$, ועדות $U \subseteq V$:

ודא ש-$|U| = K$ (אחרת דחה).

לכל $x, y \in U$ שונים: אם $xy \in E$ — **דחה**.

קבל.

האלגוריתם דטרמיניסטי לחלוטין. אין בו שום בחירה: הקבוצה U מגיעה מבחוץ. זהו בדיוק ההבדל בין שתי ההגדרות — האם *אני* עושה את הבחירה באופן אי-דטרמיניסטי, או שמישהו חיצוני (שיש לו "כוחות על") עושה אותה ומגיש לי את התוצאה, ואני רק מוודא. אם קיימת בחירה נכונה, אותו מישהו יבחר נכון.

נכונות. נראה שלכל גרף $G = (V, E)$ ולכל $K \in \mathbb{N}$: $\langle G, K \rangle \in \mathrm{IS} \iff$ $\exists\, w \text{ of size polynomial in } |\langle G, K \rangle| \text{ s.t. the algorithm accepts } \langle G, K \rangle, w.$

($\Rightarrow$) נניח $\langle G, K \rangle \in \mathrm{IS}$. אזי קיימת $U \subseteq V$ כך ש-$|U| = K$ ו-U בלתי תלויה ב-G. את U ניתן לקודד במחרוזת של $|V|$ ביטים — ביט לכל קדקוד, "בפנים / בחוץ" — וזה **פולינומי (ואף לינארי) בגודל הקלט**. על העדות הזו האלגוריתם עובר את שלב 1 (הגודל נכון), ואינו דוחה בשלב 2 (כי לכל שני קדקודים שונים ב-U אין קשת), ולכן מקבל.

($\Leftarrow$) נראה את הניגוד: נניח $\langle G, K \rangle \notin \mathrm{IS}$. אז לכל $U \subseteq V$, אם $|U| = K$ אז U אינה בלתי תלויה ב-G, כלומר קיימים בה x, y שונים עם $xy \in E$, והאלגוריתם דוחה בשלב 2. ואם $|U| \neq K$ האלגוריתם דוחה כבר בשלב 1. לכן לכל עדות w כלשהי האלגוריתם דוחה, ובפרט אין עדות מקבלת.

הערה — למה בכלל טרחנו לומר "פולינומי בגודל הקלט" על העדות? זו לא פדנטיות. תנאי אורך העדות הוא חלק בלתי נפרד מהגדרת ה-verifier, והוא מה שמונע רמאות. דוגמה נגדית שניתנה בשיעור: אפשר לבנות "מוודא" ל-SAT שמקבל נוסחה **יחד עם טבלת האמת המלאה שלה**, ופשוט קורא את התשובה מהטבלה. המוודא הזה אכן מוודא נכון — אבל טבלת האמת היא **מעריכית** בגודל הנוסחה, ולכן הבנייה חסרת ערך ואינה מוכיחה $\mathrm{SAT} \in \mathrm{NP}$. הדרישה "עדות באורך $p(|x|)$" היא בדיוק מה שפוסל אותה. אצלנו העדות היא $|V|$ ביטים בלבד — לינארי — ולכן הכול תקין.

ניתוח זמן ריצה. על קלט $\langle \langle G, K \rangle, U \rangle$:

הבדיקה $|U| = K$ דורשת $O(|V|)$ צעדים (פשוט ספירת האיברים).

הלולאה דורשת $O(|V|^2) \subseteq O(K^2)$ צעדים, שוב לפי $K \leq |V|$.

סך הכול $O\left(|\langle \langle G, K \rangle, U \rangle|^2\right)$ — פולינומי. לכן $\mathrm{IS} \in \mathrm{NP}$. ■

משפט 3: $\mathrm{IS} \leq_p \mathrm{CLIQUE}$

כיוון הטענה. אנחנו טוענים שאלגוריתם ל-CLIQUE פותר גם את IS. איננו טוענים דבר על הקושי של אף אחת מהן בפני עצמה, ואיננו מכריעים כאן אף אחת מהן.

איך מגיעים לרדוקציה — הניסיונות שנכשלו. הקלט של IS הוא זוג $\langle G, K\rangle$, והפלט צריך להיות גם הוא זוג "גרף ומספר", כי זה הפורמט של קלטי CLIQUE. השאלה היא איזה גרף.

הצעה ראשונה בכיתה: "נמחק את קשתות הקליקה". נפסלה מיד — אני לא יודע למצוא קליקה. כל העניין הוא שאיני יודע לפתור את הבעיה; אם הייתי יודע, לא הייתי צריך רדוקציה. (אותה מלכודת הופיעה בחישוביות: ברדוקציה מ-HALT ל-HALT_0 לא יכולנו לבדוק אם הקלט ב-HALT; היינו צריכים להעביר את התכונה **בלי לדעת**.)

הצעה שנייה: "נמחק את כל הקשתות מהגרף". אז הפלט לעולם אינו ב-CLIQUE (עבור $K \geq 2$) — לא משנה מה היה הקלט. זה הורס את כיוון ה"אם".

ההצעה המשלימה: "נוסיף את כל הקשתות". אז הפלט **תמיד** ב-CLIQUE, ללא קשר לקלט. זה הורס את הכיוון השני.

המסקנה שהוציא מכך המרצה היא הלב של השיעור: **הרדוקציה חייבת לקיים אם ורק אם**, ולכן כל פעולה שמייצרת פלט קבוע-מראש מקלקלת אחד הכיוונים. צריך פעולה שמשמרת את המבנה — לא מוסיפה הכול ולא מוחקת הכול, אלא **מחליפה**: איפה שהייתה קשת נוריד, ואיפה שלא הייתה נוסיף. זהו **הגרף המשלים**.

הרדוקציה. על קלט $\langle G, K\rangle$ כאשר $G = (V, E)$ גרף ו-$K \in \mathbb{N}$:

בנה את הגרף המשלים $\bar{G} = (V, \bar{E})$ של G, כאשר $\bar{E} = \left\{ xy \;\middle|\; x, y \in V,\ x \neq y \right\} \setminus E = \binom{V}{2} \setminus E$.

החזר $\langle \bar{G}, K\rangle$.

K נשאר ללא שינוי.

ניתוח זמן ריצה. על קלט $\langle G, K\rangle$: בניית הגרף המשלים דורשת $O(|V|^2)$ צעדים — עוברים על כל זוג קדקודים (יש $\binom{|V|}{2}$ כאלה), בודקים אם הקשת קיימת ומכניסים ל-$\bar{E}$ בהתאם. סך הכול $O\big(|\langle G, K\rangle|^2\big)$, ובפרט פולינומי. (בהחלט לא ניסינו להיות יעילים; לצורך הרדוקציה מספיק "פולינומי".)

נכונות — כיוון ראשון: $\langle G, K\rangle \in \mathrm{IS} \Rightarrow \langle \bar{G}, K\rangle \in \mathrm{CLIQUE}$.

יהי $G = (V, E)$ גרף ויהי $K \in \mathbb{N}$. נניח $\langle G, K\rangle \in \mathrm{IS}$. אזי קיימת $U \subseteq V$ כך ש-$|U| = K$ וגם U בלתי תלויה ב-G.

נתבונן **באותה** U בתוך $\bar{G}$ (מותר — לשני הגרפים אותה קבוצת קדקודים V). אז $U \subseteq V$ וגם $|U| = K$. נותר להראות ש-U קליקה ב-$\bar{G}$. יהיו $x, y \in U$ שונים. מכיוון ש-U בלתי תלויה ב-G, מתקיים $xy \notin E$. לפי הגדרת המשלים, כל זוג קדקודים שונים שאינו קשת ב-E הוא קשת ב-$\bar{E}$; לכן $xy \in \bar{E}$. מכאן ש-U קליקה ב-$\bar{G}$, ולכן $\langle \bar{G}, K\rangle \in \mathrm{CLIQUE}$.

נכונות — כיוון שני: $\langle \bar{G}, K\rangle \in \mathrm{CLIQUE} \Rightarrow \langle G, K\rangle \in \mathrm{IS}$.

נניח $\langle \bar{G}, K\rangle \in \mathrm{CLIQUE}$. אזי קיימת $U \subseteq V$ כך ש-$|U| = K$ וגם U קליקה ב-$\bar{G}$ (שימו לב: חייבים לומר "ב-$\bar{G}$" ולא סתם "קליקה" — יש כאן שני גרפים).

נתבונן באותה U בתוך G. אז $U \subseteq V$ וגם $|U| = K$. יהיו $x, y \in U$ שונים. מכיוון ש-U קליקה ב-$\bar{G}$ מתקיים $xy \in \bar{E}$, ולפי הגדרת המשלים $xy \notin E$. מכאן ש-U בלתי תלויה ב-G, ולכן $\langle G, K \rangle \in \text{IS}$.

סיכום. האלגוריתם רץ בזמן פולינומי ומקיים $x \in \text{IS} \iff M(x) \in \text{CLIQUE}$, ולכן הוא רדוקציה בזמן פולינומי, כלומר $\text{IS} \leq_p \text{CLIQUE}$. ■

> **הערה על מבנה ההוכחה.** ההגדרה של רדוקציה דורשת שני תנאים ($x \in A \Rightarrow M(x) \in B$ ו-$x \notin A \Rightarrow M(x) \notin B$). מותר, ולרוב נוח יותר, להוכיח במקום התנאי השני את **הניגוד** שלו: $M(x) \in B \Rightarrow x \in A$. זה מה שעשינו. שני הניסוחים שקולים. תמיד לעבוד עם השלד של ההגדרה — "מה הנחתי, מה אני צריך להוכיח" — לפני שמפרקים את ההגדרות; השלד הוא המעקה ששומר על ההוכחה.

משפט 4: $\text{CLIQUE} \leq_p \text{IS}$

טענה. אותה רדוקציה בדיוק — המעבר לגרף המשלים — היא גם רדוקציה בכיוון ההפוך.

הרדוקציה. על קלט $\langle H, K \rangle$ עם $H = (V, F)$ גרף: החזר $\langle \bar{H}, K \rangle$.

זמן ריצה. זהה: $O(|V|^2) \subseteq O(|\langle H, K \rangle|^2)$.

נכונות. המפתח הוא ש**המשלים הוא אינוולוציה**: $\overline{\bar{H}} = H$, כי $\binom{V}{2} \setminus \left(\binom{V}{2} \setminus F \right) = F$.

($\Rightarrow$) נניח $\langle H, K \rangle \in \text{CLIQUE}$, כלומר קיימת $U \subseteq V$ בגודל K שהיא קליקה ב-H. יהיו $x, y \in U$ שונים; אז $xy \in F$, ולכן $xy \notin \bar{F}$, כלומר U בלתי תלויה ב-$\bar{H}$. לכן $\langle \bar{H}, K \rangle \in \text{IS}$.

($\Leftarrow$) נניח $\langle \bar{H}, K \rangle \in \text{IS}$, כלומר קיימת $U \subseteq V$ בגודל K בלתי תלויה ב-$\bar{H}$. יהיו $x, y \in U$ שונים; אז $xy \notin \bar{F}$, ולכן $xy \in F$, כלומר U קליקה ב-H. לכן $\langle H, K \rangle \in \text{CLIQUE}$. ■

> **הערה:** בהרצאה זה נאמר בקיצור — "באופן דומה אפשר להראות רדוקציה בכיוון ההפוך; למעשה אותה רדוקציה עצמה" — והפירוט כאן. המסקנה: שתי הבעיות **שקולות** תחת $\leq_p$. אחת מהן ב-P אם ורק אם השנייה ב-P; אחת מהן NP-שלמה אם ורק אם השנייה NP-שלמה.

משפט 5: טרנזיטיביות של $\leq_p$

טענה. לכל שלוש שפות A, B, C: אם $A \leq_p B$ וגם $B \leq_p C$ אז $A \leq_p C$.

הוכחה. תהיינה M_1 רדוקציה בזמן פולינומי מ-A ל-B ו-M_2 רדוקציה בזמן פולינומי מ-B ל-C. יהיו p_1, p_2 פולינומים החוסמים את זמני הריצה שלהן בהתאמה; בלי הגבלת הכלליות שניהם מונוטוניים עולים. נגדיר את M כשרשור: על קלט x, הרץ M_1 על x, קבל $y = M_1(x)$, הרץ M_2 על y והחזר $M_2(y)$. (במונחי פונקציות: הרכבה, $f = f_2 \circ f_1$.)

סמנטיקה. לכל x: $x \in A \iff M_1(x) \in B \iff M_2(M_1(x)) \in C$, כאשר השקילות הראשונה היא נכונות M_1 והשנייה נכונות M_2 (מופעלת על הקלט $M_1(x)$). לכן $x \in A \iff M(x) \in C$.

זמן ריצה — כאן נמצא כל החידוש לעומת חישוביות. השלב הראשון עולה $p_1(|x|)$. השלב השני עולה $p_2(|y|)$, ולכן צריך לחסום את $|y|$. מכונה שרצה t צעדים אינה יכולה לכתוב יותר מ-t תווים, ולכן $|y| = |M_1(x)| \leq p_1(|x|)$ (עד כדי תוספת $|x|$, אם נספור גם את הקלט ההתחלתי — עדיין

פולינומי). מכאן שסך זמן הריצה חסום על ידי $p_1(|x|) + p_2\big(p_1(|x|)\big)$, וזהו פולינום ב-$|x|$, כי **הרכבה של פולינומים היא פולינום** וסכום של פולינומים הוא פולינום. לכן M היא רדוקציה בזמן פולינומי מ-A ל-C. ■

> **הערה:** בהרצאה הוכרז שהמשפט יוכח בשיעור הבא, וניתנה רק תמצית הרעיון ("הניתוח הסמנטי בדיוק כמו בחישוביות; זמן הריצה נובע מכך שהרכבת פולינומים היא פולינום"); הפירוט המלא כאן. הסיכום מציין את הטענה כתרגיל.

משפט 6: סגירות כלפי מטה תחת $\leq_p$

טענה. המחלקות P, NP ו-PSPACE סגורות כלפי מטה תחת רדוקציות בזמן פולינומי. במפורש, עבור P: $\forall A, B: \quad A \in P \text{ and } B \leq_p A \implies B \in P$. ובאותו אופן עבור NP ועבור PSPACE.

שימו לב לכיוון. הרדוקציה היא **מ-B אל-A**, ומה שמסיקים הוא על B — הבעיה ה"קלה" יותר. זהו בדיוק תוכן ההגדרה: אם היעד קל, גם המקור קל. הכיוון ההפוך ("$B \in P \Rightarrow A \leq_p B$ ו-$A \in P$") **שגוי**, ואם הוא היה נכון היינו מקבלים ש-$P = \mathrm{NP}$ טריוויאלית.

הוכחה עבור P. נניח $A \in P$ ו-$B \leq_p A$. תהי M_A מכונה דטרמיניסטית המכריעה את A בזמן $q(n)$ פולינומי, ותהי R רדוקציה מ-B ל-A בזמן $p(n)$ פולינומי. נגדיר מכונה M_B: על קלט x, חשב $y = R(x)$, ואז הרץ את M_A על y והחזר את תשובתה.

נכונות. $x \in B \iff R(x) \in A \iff M_B$ מקבלת את x. M_A מקבלת את $R(x)$.

זמן ריצה. $|y| \leq p(|x|)$ (מכונה שרצה $p(|x|)$ צעדים אינה יכולה לכתוב פלט ארוך יותר), ולכן הזמן הכולל חסום על ידי $p(|x|) + q\big(p(|x|)\big)$ — פולינום. לכן $B \in P$.

עבור NP ההוכחה זהה מילה במילה, למעט ש-M_A היא מכונה אי-דטרמיניסטית פולינומית; M_B יורשת ממנה את האי-דטרמיניזם, וכל ריצה שלה נמשכת $p(|x|) + q(p(|x|))$ צעדים לכל היותר. $x \in B$ אם ורק אם $R(x) \in A$ אם ורק אם קיימת ריצה מקבלת של M_A על $R(x)$ אם ורק אם קיימת ריצה מקבלת של M_B על x.

עבור PSPACE אותו שרשור, אלא שכעת סופרים מקום: הרדוקציה רצה בזמן פולינומי ולכן צורכת גם מקום פולינומי ומייצרת פלט באורך פולינומי, ו-M_A צורכת מקום פולינומי באורך הפלט הזה — כלומר פולינומי ב-$|x|$. ■

> **הערה:** גם משפט זה הוכרז בהרצאה כדחוי לשיעור הבא, והסיכום מציין אותו כטענה "ללא הוכחה" ומפנה לתרגיל. הרעיון המרכזי שנאמר בעל פה — "הרכבה של פולינומים היא פולינום" — הוא בדיוק מה שכתוב כאן במלואו. הרשימה $\{P, \mathrm{NP}, \mathrm{PSPACE}\}$ אינה ממצה; אלו המחלקות שיעניינו אותנו.

משפט 7: משפט ההעברה של NP-קושי

טענה. תהיינה A, B שפות. אם A היא NP-קשה וגם $A \leq_p B$, אז B היא NP-קשה.

הוכחה. נניח ש-A היא NP-קשה וגם $A \leq_p B$. לפי הגדרה 6, כדי להוכיח ש-B היא NP-קשה עלינו להראות שלכל $C \in \mathrm{NP}$ מתקיים $C \leq_p B$.

תהי $C \in \mathrm{NP}$ (חייבים לתת לה שם, כדי שנוכל להתייחס אליה בהמשך).

A היא NP-קשה, ולכן — לפי ההגדרה, מופעלת על C — מתקיים $C \le_p A$. (שימו לב לכיוון: **מ-**C **אל-**A, לא להפך.)
נתון $A \le_p B$.
ממשפט 5 (טרנזיטיביות היחס $\le_p$) נקבל $C \le_p B$.
מאחר ש-$C \in \mathrm{NP}$ הייתה שרירותית, הראינו שלכל שפה ב-NP קיימת רדוקציה בזמן פולינומי **ממנה אל** B. זו בדיוק הגדרה 6, ולכן B היא NP-קשה. ■
למה המשפט הזה חיוני. להוכיח מאפס שבעיה A היא NP-קשה זה מורכב: ההוכחה חייבת להתחיל ב"תהי $B \in \mathrm{NP}$" — ואני **לא יודע כלום** על B. היא יכולה להיות בעיה בגרפים, בעיה על נוסחאות CNF, בעיה על מספרים, כל דבר. ועליי לבנות רדוקציה ממנה אל A, בלי לדעת עליה דבר. משפט 7 אומר: **מספיק לעשות את זה פעם אחת.** ברגע שיש בידי בעיה אחת שידוע שהיא NP-קשה, כדי להראות ש-B נוספת היא NP-קשה מספיק להראות רדוקציה **מהבעיה שכבר יש לי אליה** — ואין צורך לחזור להגדרה.
זו בדיוק התוכנית להמשך: בשיעור הבא נוכיח את **משפט Cook–Levin**, שאומר ש-SAT היא NP-קשה — זו ה"בעיה הראשונה" שנעבוד קשה כדי להשיג. משם והלאה נעשה רדוקציות מ-SAT אל בעיות נוספות, ומהן אל בעיות נוספות, וכל בעיה חדשה מצטרפת למאגר ומותר להשתמש גם בה כנקודת מוצא. כך "מעשירים את עולם הבעיות ה-NP-קשות".

דוגמאות ותרגילים מהשיעור
דוגמה 1: הכרעה ידנית ב-CLIQUE
בשיעור הוצג גרף ונשאלו שתי שאלות עליו. נשחזר את הרעיון על גרף קונקרטי: $V = \{1,2,3,4,5\}$, $E = \{12, 13, 23, 34, 45\}$ — משולש על $\{1,2,3\}$, ואליו נגררת שרשרת $3-4-5$.
$\langle G, 3\rangle \in \mathrm{CLIQUE}$? **כן.** $U = \{1,2,3\}$: $12, 13, 23 \in E$, ו-$|U| = 3$.
$\langle G, 4\rangle \in \mathrm{CLIQUE}$? **לא.** יש רק 5 קדקודים, כלומר $\binom{5}{4} = 5$ קבוצות אפשריות; בכל אחת מהן נמצא זוג לא-מחובר. למשל ב-$\{1,2,3,4\}$ חסרה 14; ב-$\{1,2,3,5\}$ חסרה 15; ב-$\{2,3,4,5\}$ חסרה 25; ב-$\{1,3,4,5\}$ חסרה 14; ב-$\{1,2,4,5\}$ חסרה 14.
שימו לב שאותו גרף בדיוק נותן קלט חיובי ושלילי בהתאם ל-K — K הוא חלק מהקלט, וזה בדיוק מה שיהפוך את הניתוח לרגיש בהמשך.
דוגמה 2: מעקב מלא אחרי הרדוקציה, בשני הכיוונים
זהו התרגיל המרכזי. ניקח את המסלול P_5: $V = \{a,b,c,d,e\}$, $E = \{ab,\ bc,\ cd,\ de\}$.
חישוב הגרף המשלים. כל הזוגות האפשריים הם $\binom{V}{2} = \binom{5}{2} = 10$: $\{ab, ac, ad, ae, bc, bd, be, cd, ce, de\}$. מחסרים את E ומקבלים $\bar{E} = \{ac,\ ad,\ ae,\ bd,\ be,\ ce\}$.
כיוון $\mathrm{CLIQUE} \to \mathrm{IS}$**.** נבדוק את הקלט $\langle G, 3\rangle$ עבור IS.
הקלט אכן ב-IS: הקבוצה $U = \{a,c,e\}$ מקיימת $|U| = 3$, ו-$ac \notin E$, $ae \notin E$, $ce \notin E$. לכן $\langle G, 3\rangle \in \mathrm{IS}$.
מפעילים את הרדוקציה: $f(\langle G, 3\rangle) = \langle \bar{G}, 3\rangle$ עם $\bar{E}$ שלמעלה. K לא השתנה.

בודקים את הפלט: **אותה** $U = \{a, c, e\}$ — $ac \in \bar{E}$, $ae \in \bar{E}$, $ce \in \bar{E}$, ולכן U קליקה ב-$\bar{G}$ ו-$\langle \bar{G}, 3 \rangle \in \mathrm{CLIQUE}$. ✓

כיוון $\mathrm{CLIQUE} \to \mathrm{IS}$ (הכיוון השני של אותה רדוקציה, ובו זמנית הדגמה של משפט 4). ניקח כעת את $\bar{G}$ כקלט ל-CLIQUE.

הקלט ב-CLIQUE: $\{a, c, e\}$ היא קליקה ב-$\bar{G}$ כפי שראינו. למעשה זו הקליקה היחידה בגודל 3 ב-$\bar{G}$: לזוג $\{a, d\}$ אין קדקוד שלישי משותף ($ac \in \bar{E}$ אבל $cd \notin \bar{E}$; $ae \in \bar{E}$ אבל $de \notin \bar{E}$; $ab \notin \bar{E}$), ולזוג $\{b, d\}$ חסר de.

מפעילים את הרדוקציה: $f(\langle \bar{G}, 3 \rangle) = \langle \overline{\bar{G}}, 3 \rangle = \langle G, 3 \rangle$ — חוזרים בדיוק ל-G המקורי, כי המשלים הוא אינוולוציה.

בודקים: $\{a, c, e\}$ בלתי תלויה ב-G. ✓

בדיקת קלט שלילי (חובה — אחרת לא הראינו "אם ורק אם"). ניקח $K = 4$.

$\langle G, 4 \rangle \notin \mathrm{IS}$: הקבוצה הבלתי תלויה המקסימלית ב-P_5 היא בגודל 3. כל קבוצה של 4 קדקודים מתוך 5 חייבת להכיל שני קדקודים סמוכים במסלול (למשל $\{a, b, c, d\}$ מכילה את ab; $\{a, c, d, e\}$ מכילה את cd; וכן הלאה).

והפלט: $\langle \bar{G}, 4 \rangle \notin \mathrm{CLIQUE}$ — הקליקה המקסימלית ב-$\bar{G}$ היא בגודל 3, כפי שספרנו בשלב 1 למעלה.

שני הצדדים "לא", כנדרש. הרדוקציה שומרת גם על תשובות שליליות — וזו בדיוק הדרישה שהצעות "מחק הכול / הוסף הכול" נכשלו בה.

תרגיל 3 (מהשיעור): למה האלגוריתם הנאיבי ל-CLIQUE אינו פולינומי?

השאלה. נניח שאני מכריע את CLIQUE דטרמיניסטית על ידי מעבר על כל תת-הקבוצות בגודל K. מה זמן הריצה, ולמה אין די בכך?

פתרון. מספר הקבוצות הוא $\binom{|V|}{K}$, ולכן זמן הריצה הוא $\Omega\left(\binom{|V|}{K}\right)$. נחסום מלמטה: $\binom{|V|}{K} = \frac{|V|(|V|-1)\cdots(|V|-K+1)}{K!} \geq \left(\frac{|V|}{K}\right)^K$, כי מדובר במכפלה של K גורמים מהצורה $\frac{|V|-i}{K-i}$, וכל אחד מהם לפחות $\frac{|V|}{K}$.

למה זה לא פולינום? פולינום הוא "משתנה בחזקת **קבוע**". כאן המעריך הוא K — ו-K **מגיע כחלק מהקלט**, כלומר אינו קבוע. אין שום c קבוע שעבורו הביטוי הזה חסום על ידי $|\langle G, K \rangle|^c$, כי החזקה עצמה גדלה עם הקלט.

הערה חשובה: מכאן **לא** נובע ש-$\mathrm{CLIQUE} \notin P$. נובע רק שהאלגוריתם **הספציפי** הזה אינו פולינומי. השאלה אם CLIQUE ב-P פתוחה, ושקולה (כפי שיתברר) לשאלת P מול NP.

תרגיל 4 (מהשיעור): מימוש הבחירה האי-דטרמיניסטית ברמת המכונה

בשלב 1 של האלגוריתם במשפט 1 כתבנו "בחר באופן אי-דטרמיניסטי קבוצה U בגודל K". איך זה נראה בפועל?

פתרון (מהמסירה השנייה). אפשר לנסות בדרך "מתוחכמת" — לבחור קדקוד, אחר כך קדקוד שלא נבחר, וכך K איטרציות — אבל אז צריך לנהל את הזיכרון של מי כבר נבחר. הרבה יותר פשוט לבחור באופן הכי גס, ולתקן אחר כך. מכונה עם שני סרטים:

כתוב באופן אי-דטרמיניסטי K מספרים, כל אחד בין 1 ל-$|V|$, על הסרט השני.

התייחס אליהם כאל קדקודים ב-G.
אם קיים קדקוד שנבחר יותר מפעם אחת — **דחה** (הבחירה לא ייצרה קבוצה בגודל K).
אם קיימים שני קדקודים מבין הנבחרים שאין ביניהם קשת ב-E — **דחה**.
אחרת — **קבל**.

ניתוח. שלב 1: כתיבת K מספרים בין 1 ל-$|V|$ עולה $O(K \cdot |V|) \subseteq O(|V|^2)$, שוב **תוך שימוש ב-**$K \leq |V|$ — וכאן זה קריטי, כי אחרת מספר הצעדים היה מעריכי באורך הקידוד הבינארי של K. שלב 3: לכל אחד מ-K המספרים סורקים את השאר, $O(K^2) \subseteq O(|V|^2)$. שלב 4: עוברים על כל זוג נבחרים ולכל זוג סורקים את רשימת הקשתות, $O(K^2 \cdot |E|) \subseteq O(|V|^2 \cdot |E|) \subseteq O(|G|^3)$. סך הכול חסום ב-$O(|\langle G, K \rangle|^3)$ — לא הפולינום הטוב ביותר, אבל פולינום, וזה כל מה שנדרש.

בהמשך הקורס לא נרד לרמת פירוט זו; נכתוב "ננחש קבוצת קדקודים" ונמשיך. אבל כדאי שהמימוש יישאר ברקע כדי לדעת שהוא באמת אפשרי ויעיל.

תרגיל 5: ניתוח זמן ריצה חלופי לרדוקציה

בסיכום נכתב שבניית הגרף המשלים עולה $O(|V|^2)$; במסירה השנייה נאמר $O(|V|^2 \cdot |E|)$. מי צודק?

פתרון: שניהם, וההבדל הוא בייצוג. אם הגרף נתון במטריצת שכנויות, בדיקת "האם $xy \in E$" עולה $O(1)$, ולכן מעבר על כל $\binom{|V|}{2}$ הזוגות עולה $O(|V|^2)$. אם הגרף נתון ברשימת קשתות ואנחנו סורקים אותה עבור כל זוג, נשלם $O(|V|^2 \cdot |E|)$. שניהם פולינומיים, ולכן לצורך הטענה $\text{IS} \leq_p \text{CLIQUE}$ אין הבדל — וזו בדיוק הסיבה שמותר לנו להתרשל בפרטי המימוש. זהו יישום ישיר של "המסננת גסה מאוד".

תרגיל 6 (מהסיכום): הוכיחו את טענת הסגירות ואת הטרנזיטיביות

התרגיל מופיע בסיכום כשורה אחת; הפתרונות המלאים כתובים למעלה — משפט 5 (טרנזיטיביות) ומשפט 6 (סגירות). בשני המקרים הרעיון הסמנטי מועתק מהוכחות החישוביות המקבילות (שרשור מכונות / הרכבת פונקציות), והחלק **החדש** היחיד הוא ניתוח זמן הריצה, שנשען על שתי עובדות: (א) מכונה שרצה t צעדים כותבת פלט באורך $O(t)$ לכל היותר, ולכן אורך הביניים חסום פולינומית; (ב) הרכבה של פולינומים היא פולינום. מומלץ לחזור על הוכחות אלו מקורס החישוביות לפני השיעור הבא.

הערות מהשיעור

[00:10:08] המעבר לפסאודו-קוד הוא היתר, לא ויתור. "כל זמן שהרזולוציה שמעניינת אותנו היא זמן ריצה פולינומי — אפשר לעבור לפסאודו-קוד." הפולינום עצמו יכול לגדול במעבר בין המודלים, אבל מכיוון שמה שמעניין אותנו הוא רק "פולינומי או לא", זה לא משנה באיזה מודל עובדים. זה יהיה נכון כמעט לכל שארית הקורס.

[00:16:00] הקידוד נעלם מהתמונה — בכוונה. מכאן ואילך נכתוב "קלט: זוג $\langle G, K \rangle$" בלי לפרט את הקידוד. עדיין מדובר בקידוד, ועדיין הוא חייב להיות סביר, אבל הוא לא מעניין אותנו יותר.

[00:28:49] המלכודת של K. נשאלה שאלה מצוינת מהכיתה: הקלט מכיל גם את K, וכדי לקודד את K צריך רק $\log_2 K$ ביטים — אז איך $O(K^2)$ נחשב פולינומי? התשובה: K עצמו גדול מאוד ביחס לגודל הקידוד שלו, אבל **בגלל שהגרף נמצא לידו בקלט, הגרף "משלם את המחיר"**. יחד עם

ההנחה $K \leq |V|$, הכול חוזר להיות פולינומי בגודל הקלט. אם K היה מגיע לבדו — הניתוח היה קורס. שווה לזכור: כשמספר מופיע כפרמטר בקלט, תמיד לשאול אם החסם מבוטא ביחידות הנכונות.

[00:31:27] → [00:46:25] חזרה מהצהרה. נשאל אם צריך להוכיח בנפרד שהאלגוריתם עוצר בכל ריצה. תחילה נאמר "אתה צודק ב-100%", ולאחר מכן המרצה חזר בו: "ברגע שזמן הריצה הוא פולינומי בכל ריצה, אני לא צריך את זה בנפרד." שתי התשובות אינן שגויות — הראשונה זהירה מדי. במבחן: אם ניתחתם זמן ריצה **לכל ריצה אפשרית**, אין צורך בטיעון עצירה נפרד.

[00:33:34] "זה לא בדיוק ההפך מקליקה." אזהרה מפורשת נגד הטעות הנפוצה ביותר בהגדרות: השלילה של "לכל שניים יש קשת" היא "קיימים שניים שאין ביניהם קשת", ולא "לכל שניים אין קשת". שלילת כמת "לכל" אינה משאירה "לכל".

[00:49:04] העדות חייבת להיות קצרה, וזה לא טכני. "אני רוצה להימנע מדברים כמו: הנה מוודא, והוא באמת מוודא — אבל הוא קיבל witness גדול מדי." הדוגמה שניתנה: מוודא ל-SAT שמקבל את טבלת האמת המלאה של הנוסחה, שגודלה מעריכי. חסם האורך הפולינומי הוא מה שמונע מההגדרה להתמוטט.

[00:58:20] → [01:00:25] הדרך אל הגרף המשלים. ההצעות "נמחק את כל הקשתות" ו"נוסיף את כל הקשתות" נדחו לא כי הן טיפשות, אלא כי כל אחת מהן שוברת בדיוק כיוון אחד של ה"אם ורק אם". זו הדגמה מדויקת של מה שרדוקציה צריכה: לא פונקציה שמייצרת פלט "טוב", אלא פונקציה ש**משמרת מבנה**. שווה לחשוב על כך בכל פעם שנתקעים בבניית רדוקציה: איזה כיוון ההצעה שלי שוברת?

[00:58:50] הקבלה לחישוביות. "כשעשינו רדוקציה מ-HALT ל-HALT_0 לא יכולנו לבדוק אם הקלט ב-HALT; היינו צריכים להעביר את התכונה בלי לדעת." אותה מחשבה בדיוק חלה כאן — הרדוקציה עיוורת לתשובה.

[01:03:35] "פה הקבוצה לא נתונה לנו." בלבול שעלה בכיתה: בהוכחת הרדוקציה תלמידה חיפשה את הקבוצה U כאילו היא חלק מהקלט, כמו ב-verifier של משפט 2. ההבהרה: **בהוכחה** מותר לומר "קיימת U" ולעבוד איתה — זו טענה מתמטית, לא שלב אלגוריתמי. ההבחנה בין "מה האלגוריתם עושה" ל"מה אני מוכיח" היא המקור השכיח ביותר לבלבול בשיעור הזה. במסירה השנייה [01:25:54] נאמר אותו דבר במפורש: "בזמן בניית הרדוקציה לא ידעתי אם זה שייך או לא שייך; בזמן ההוכחה אני מניח כיוון אחד ומראה את השני."

[01:05:48] "תמיד לעבוד עם השלד של ההוכחה — זה המעקה ששומר עליכם." לפני שמפרקים הגדרות: מה הנחתי? מה בדיוק אני צריך להוכיח? רק אז לפתוח את ההגדרות. בהמשך אותה הוכחה נאמר לתלמידה שהתחילה מהפירוק: "זה כבר ה'איך אני מוכיח', לא 'מה אני רוצה להוכיח'."

[01:07:24] כשיש שני גרפים — חובה לציין באיזה. לא "קליקה", אלא "קליקה ב-$\bar{G}$"; לא "קבוצת הקשתות", אלא "$\bar{E}$". בהוכחת רדוקציה בין בעיות גרפים זהו מקור קבוע לשגיאות.

[01:22:29] ההבדל בין הקורסים. למי שלמד חישוביות במסלול שבו לא הוגדר "RE-קשה": את התכונה למדתם, פשוט לא נתתם לה שם. אין הבדל מהותי.

[01:26:48] למה בכלל צריך את משפט 7. להוכיח NP-קושי לפי ההגדרה מחייב לטפל בשפה **שרירותית** ב-NP — "אני לא יודע כלום על ה-B הזאת" — ולכן זה מורכב. משפט 7 מאפשר לעשות את העבודה הקשה פעם אחת (Cook–Levin, שיעור הבא) ואז להתקדם ברדוקציות. "ברגע שיש לי

פערים בין הסיכום להקלטה

מקור: עמוד 2 בסיכום. **הפער:** בהגדרת קבוצה בלתי תלויה נכתב ככל הנראה "לכל $x, y \in V$ שונים מתקיים $xy \notin E$", בעוד שההגדרה של קליקה בעמוד 1 משתמשת נכון ב-$x, y \in U$. הניסוח עם V היה אומר שאין בגרף אף קשת כלל. **ההכרעה:** תוקן ל-$x, y \in U$ בהגדרה 3; זו ההגדרה שנאמרה בשתי ההקלטות. ייתכן גם שמדובר בשגיאת קריאה שלי בכתב היד — לכן נרשם ב- `open_questions` .

מקור: הקלטה 13, [00:33:00]. **הפער:** התמלול האוטומטי מוריד את השלילה וכותב "U תיקרא בלתי תלויה כאשר לכל $x, y \in U$ שונים הקשת xy **בגרף**". **ההכרעה:** ארטיפקט תמלול. במשפט הבא המרצה עצמו אומר "פה אני דורש שלכל שניים **אין** קשת", והסיכום מסכים. נכתב $xy \notin E$.

מקור: הסיכום מול הקלטה 13. **הפער:** הסיכום מציג את טענות הסגירות והטרנזיטיביות כ"טענה ללא הוכחה" ומוסיף "תרגיל: להוכיח"; בהקלטה נאמר שהן יוכחו בשיעור הבא, וניתן רק הרעיון המרכזי ("הרכבה של פולינומים היא פולינום"). **ההכרעה:** ההוכחות נכתבו כאן במלואן (משפטים 5 ו-6), עם סימון מפורש שבהרצאה הן נדחו.

מקור: הקלטה 13, [01:15:16]. **הפער:** הכיוון $\mathrm{CLIQUE} \leq_p \mathrm{IS}$ מוזכר במשפט אחד — "אותה רדוקציה למעשה היא רדוקציה גם בכיוון ההפוך" — ואינו מופיע כלל בסיכום. **ההכרעה:** נכתב כמשפט 4 עם הוכחה מלאה, כולל האינוולוציה $\overline{\overline{H}} = H$ שהמשפט נשען עליה; מסומן כשחזור.

מקור: הסיכום (עמ' 4) מול הקלטה 14 ([01:19:52]). **הפער:** הסיכום מעריך את בניית הגרף המשלים ב-$O(|V|^2)$; המסירה השנייה מעריכה $O(|G|^3) \subseteq O(|V|^2 \cdot |E|)$. **ההכרעה:** אין סתירה — ההבדל הוא בייצוג הגרף (מטריצת שכנויות מול רשימת קשתות). שני החסמים פולינומיים, ולכן שניהם מספיקים; שניהם מובאים, עם ההסבר, בתרגיל 5.

מקור: הקלטה 14 בלבד ([00:44:46]–[00:49:07]). **הפער:** ניתוח החסם התחתון $\binom{|V|}{K} \geq (|V|/K)^K$ לאלגוריתם הנאיבי, וההסבר מדוע "משתנה בחזקת משתנה" אינו פולינום, אינם מופיעים בסיכום ולא במסירה השנייה. **ההכרעה:** נכללו כתרגיל 3, כולל האזהרה שמכאן לא נובע $\mathrm{CLIQUE} \notin P$.

מקור: הקלטה 14 בלבד ([00:50:14]–[00:59:31]). **הפער:** המימוש המפורש של הבחירה האי-דטרמיניסטית (כתיבת K מספרים ואז פסילת חזרות) והניתוח שלו אינם בסיכום. **ההכרעה:** נכללו כתרגיל 4.

מקור: הקלטה 13 בלבד ([00:57:50]–[01:00:25], [00:28:49], [00:49:04]). **הפער:** הדיון בניסיונות הכושלים לבניית הרדוקציה, מלכודת הקידוד הבינארי של K, והדוגמה הנגדית של טבלת האמת כ-witness — כולם חסרים בסיכום ובמסירה השנייה. **ההכרעה:** נכללו, כי הם ההסבר ל**מה עומד מאחורי** ההגדרות, ולא רק להגדרות עצמן.

מקור: הקלטה 14, [00:00:00]–[00:39:20]. **הפער:** כשליש מהקובץ עוסק בהגדרת SAT ובהוכחה ש-$\mathrm{SAT} \in \mathrm{NP}$ (בשתי הגרסאות), כולל דיון טכני באורך העדות (n מול $p(|\varphi|)$). זהו חומר של שיעור 6. **ההכרעה:** לא נכלל כאן; רק ההערה הכללית על אורך העדות שימשה כדוגמה נגדית בהערה שאחרי משפט 2. סומן ב- `coverage: partial` .

מקור: הגדרת הרדוקציה. **הפער:** הסיכום והקלטה 13 מגדירים רדוקציה כ**מכונה** M; הקלטה 14 מגדירה אותה כ**פונקציה** f הניתנת לחישוב בזמן פולינומי. **ההכרעה:** ההגדרות שקולות (פונקציה חשיבה = קיימת מכונה שמחשבת אותה); הובאה גרסת הסיכום, עם ההסבר של המסירה השנייה מדוע לרוב נוח יותר להגדיר את הפונקציה ישירות דרך המכונה ולא בשני שלבים.

סיכום ונקודות למבחן

מה חייבים לדעת בעל פה

מושג	ההגדרה, בשורה
קליקה	$U \subseteq V$ שלכל $x \neq y$ בה $xy \in E$
קבוצה בלתי תלויה	$U \subseteq V$ שלכל $x \neq y$ בה $xy \notin E$
CLIQUE	$\{\langle G, K\rangle : \exists U \subseteq V,\ \lvert U\rvert = K,\ U \text{ clique in } G\}$
IS	$\{\langle G, K\rangle : \exists U \subseteq V,\ \lvert U\rvert = K,\ U \text{ independent in } G\}$
$A \leq_p B$	קיימת TM דטרמיניסטית פולינומית M עם $x \in A \iff M(x) \in B$
NP-קשה	$\forall B \in \mathrm{NP}:\ B \leq_p A$
NP-שלמה	NP-קשה **וגם** $A \in \mathrm{NP}$

התוצאות

$\mathrm{CLIQUE} \in \mathrm{NP},\ \mathrm{IS} \in \mathrm{NP}$.

$\mathrm{IS} \leq_p \mathrm{CLIQUE}$ ו-$\mathrm{CLIQUE} \leq_p \mathrm{IS}$, שתיהן על ידי $\langle G, K\rangle \mapsto \langle \bar{G}, K\rangle$.

$\leq_p$ טרנזיטיבי.

P, NP, PSPACE סגורות כלפי מטה תחת $\leq_p$.

A NP-קשה ו-$A \leq_p B$ $\Rightarrow$ B NP-קשה.

מלכודות סטנדרטיות

הפיכת כיוון הרדוקציה. $A \leq_p B$ אומר ש-B קשה **לפחות** כמו A. הסגירות היא "$A \in P$ ו-$B \leq_p A$ $\Longrightarrow$ $B \in P$" — הרדוקציה נכנסת **אל** הקלה. אם כתבתם את זה הפוך, קיבלתם $P = \mathrm{NP}$, וזה סימן אזהרה.

NP-קשה ≠ NP-שלמה. שפה NP-קשה אינה חייבת להיות ב-NP, ואפילו לא כריעה. תמיד לבדוק את שני התנאים.

"ההפך מקליקה". קבוצה בלתי תלויה אינה שלילת קליקה. הקשר הוא הגרף המשלים.

רדוקציה שפותרת את הבעיה. אם בתיאור הרדוקציה שלכם מופיע "נמצא את הקליקה" או "נבדוק אם הקלט בשפה" — הרדוקציה לא חוקית. היא חייבת לפעול בלי לדעת את התשובה.

הוכחת כיוון אחד בלבד. רדוקציה דורשת אם ורק אם. הוכחה שרק "כן $\Longrightarrow$ כן" חסרה חצי.

חסמים בפרמטרים במקום בגודל הקלט. $O(K^2)$ אינו תשובה; צריך להסביר למה זה $O(|\langle G, K\rangle|^2)$, ולשם כך צריך את $K \leq |V|$.

witness ארוך מדי. אם העדות אינה חסומה פולינומית באורך הקלט, ההוכחה ש-$A \in \mathrm{NP}$ אינה תקפה.

צ'ק-ליסט: אחרי השיעור הזה סטודנט צריך לדעת

להוכיח שבעיית גרפים נתונה שייכת ל-NP, בשתי הדרכים (מכונה אי-דטרמיניסטית / verifier), כולל ניתוח זמן ריצה מלא כפונקציה של גודל הקלט.

לנסח רדוקציה בזמן פולינומי בשלושה חלקים: תיאור האלגוריתם, ניתוח זמן הריצה, והוכחת נכונות בשני הכיוונים.

להסביר מדוע הרדוקציה $\mathrm{IS} \leq_p \mathrm{CLIQUE}$ עובדת, ומדוע ניסיונות נאיביים (מחיקת/הוספת כל הקשתות) נכשלים.

לקבוע נכון, בהינתן $A \leq_p B$, מי הבעיה הקשה יותר ומה נובע ממה.

להבחין בין NP-קשה ל-NP-שלמה, ולהסביר את התפקיד של משפט 7 בהעשרת אוסף הבעיות ה-NP-קשות.

לעקוב אחרי גרף קונקרטי קטן דרך הרדוקציה, בשני הכיוונים, כולל קלט שלילי.

לקראת השיעור הבא. נוכיח את משפט Cook–Levin: SAT היא NP-קשה (ולמעשה NP-שלמה, שכן $\mathrm{SAT} \in \mathrm{NP}$ הוכח בשיעור 6). זו תהיה "הבעיה הראשונה", והיא נקודת המוצא לכל הרדוקציות שיבואו. מומלץ לחזור לפני כן על הוכחת משפט הרדוקציה ועל הוכחת הטרנזיטיביות מקורס החישוביות — ההוכחות כאן בנויות עליהן, בתוספת ניתוח הזמן.

הסיכום המקורי בכתב יד: גיא סופר.

שאלות שנשארו פתוחות

עמוד 2 בסיכום: בהגדרת קבוצה בלתי תלויה נכתב ככל הנראה x,y∈V במקום x,y∈U; בגוף השיעור נכתבה הגרסה הנכונה.

ה-slug מפרק ל-CLIQUE, IS, NP-hard, NP-complete; חשוב לוודא שלא ייקרא כאילו הוכח כאן ש-CLIQUE היא NP-קשה — הוכחה זו מגיעה רק אחרי משפט Cook–Levin.

המסירה בהקלטה 13 מזכירה CLIQUE ≤p IS באמירה קצרה בלבד ('אותה רדוקציה עובדת גם בכיוון ההפוך'); ההוכחה המלאה כאן היא שחזור.

8 הרדוקציה מ-SAT ל-3SAT

בשיעור מוכיחים 3SAT ≤p SAT על ידי חיתוך כל פסוקית ארוכה לפסוקיות באורך 3 בעזרת משתני עזר חדשים, ומסיקים ש-3SAT היא NP-שלמה.

ביטחון: medium | ללא הקלטה

בקצרה

מוכיחים את הרדוקציה $\mathrm{SAT} \leq_p \mathrm{3SAT}$: כל נוסחת CNF ניתנת לתרגום, בזמן פולינומי, לנוסחת 3CNF **שקולת-ספיקות** לה.

הכיוון ההפוך, $\mathrm{3SAT} \leq_p \mathrm{SAT}$, הוא רדוקציית הזהות — ומכאן ש-$\mathrm{3SAT} \in \mathrm{NP}$.

בשילוב עם משפט קוק–לוין (SAT היא NP-קשה; ראו שיעור 9) מתקבל ש-$\mathrm{3SAT}$ היא **NP-שלמה**. זו הבעיה הנוחה ביותר להתחיל ממנה רדוקציות, כי מבנה הקלט שלה נוקשה — בדיוק 3 ליטרלים לפסוקית לכל היותר.

לב הבנייה: פסוקית באורך $k > 3$ נחתכת לשתי פסוקיות באורכים 3 ו-$k-1$ בעזרת **משתנה עזר חדש** z שמשמש כמתג. חוזרים על הצעד עד שכל הפסוקיות קצרות.

החצי העדין הוא הכיוון ההפוך של הנכונות: להראות שמשתני העזר **אינם יכולים לרמות** — כל השמה שמספקת את $\hat{\varphi}$ מצטמצמת להשמה שמספקת את φ. זה מוכח כאן במלואו.

בנוסף: השיעור פותח בשלוש טענות תשתית ($\mathrm{NP} \subseteq \mathrm{PSPACE}$, סגירות P תחת רדוקציות, ומשמעות NP-שלמות), ונחתם בהדגמת **כוח הביטוי של CNF** — קידוד "בדיוק אחד", "לא ריק ולא מלא", ובעיית 8 המלכות כנוסחת CNF.

רקע ותלויות

השיעור הזה נשען כמעט כולו על שלושה דברים שכבר נלמדו. כדי לא לשלוח את הקורא אחורה, הנה הם במלואם.

1. המחלקה NP — שתי ההגדרות השקולות (שיעור 5–6). בהגדרה הראשונה, $A \in \mathrm{NP}$ אם קיימת מכונת טיורינג אי-דטרמיניסטית N שמכריעה את A וזמן הריצה של כל ריצה שלה חסום בפולינום באורך הקלט. בהגדרה השנייה (הגדרת ה-verifier), $A \in \mathrm{NP}$ אם קיימות מכונה **דטרמיניסטית** M בזמן פולינומי ופולינום q כך שלכל x: $x \in A \iff \exists\, w \in \{0,1\}^{q(|x|)} \ \text{s.t.}\ M \text{ accepts } (x, w)$. המחרוזת w נקראת עדות (witness). בשיעור 6 הוכח ששתי ההגדרות שקולות. בהוכחות כאן נוח לעבוד עם הגדרת ה-verifier, וכך נעשה גם בשיעור 9 — כדברי המרצה, "דטרמיניזם תמיד יותר נוח לי, כי אני יודע כל צעד מה קורה בצעד הבא" [00:02:41, תמלול 15].

> **הערה על סימון המכונה:** מכונת טיורינג נכתבת כאן כ-$M = (Q, q_{start}, F, \Sigma, \Gamma, \delta)$, כולל מצב ההתחלה. בכמה עמודי סיכום בקורס מושמט q_{start}; זו החלקה ידועה במקור והתיקון נעשה כאן במכוון.

2. הבעיה SAT (נלמדה בשיעור 7, ומופיעה בהקלטה [00:06:24]–[00:16:14]). SAT היא בעיית ההכרעה שקלטיה הם נוסחאות CNF, והשאלה היא האם הנוסחה ספיקה. בשיעור 7 הוכח $\mathrm{SAT} \in \mathrm{NP}$: המכונה האי-דטרמיניסטית כותבת על סרט שני ביטים (n = מספר המשתנים בנוסחה), מתייחסת אליהם כהשמה, ובודקת האם ההשמה מספקת. זמן הריצה $O(|\varphi|^2)$ [00:25:26].

3. רדוקציית זמן פולינומי (שיעור 7, [01:04:14]–[01:08:34]). $f : \Sigma^* \to \Sigma^*$ היא רדוקציית זמן פולינומי מ-A ל-B אם היא ניתנת לחישוב בזמן פולינומי ולכל x מתקיים $x \in A \iff f(x) \in B$. מסמנים $A \leq_p B$.

> **כיוון הרדוקציה — קראו את זה לאט.** $A \leq_p B$ פירושו ש-B **היא הבעיה הקשה יותר**: מי שיודע לפתור את B יודע לפתור גם את A (מתרגמים את הקלט ופותרים). הכיוון הזה מתהפך כל הזמן בדיבור, ולכן בכל פעם שנכתוב $\leq_p$ נאמר גם במילים מי הקשה. בשיעור הזה נוכיח $\mathrm{SAT} \leq_p 3\mathrm{SAT}$ — כלומר **3SAT היא לפחות קשה כמו SAT**, וזו בדיוק המטרה: להעביר את הקושי של SAT אל 3SAT.

4. שתי הערות מתודיות שחזרו בהקלטה ושייכות גם כאן.

ברדוקציה **אין פתרון של אף בעיה**: "אני לא מכריע פה את IS ולא מכריע פה את CLIQUE, כל מה שאני עושה זה להמיר קלט" [01:11:50, 01:22:33].

יש שני שלבים נפרדים לגמרי: בניית המכונה (שנעשית **בלי לדעת** אם הקלט בשפה — אם היינו יודעים, היינו מכריעים בזמן פולינומי), ורק אחר כך הוכחת הנכונות, שבה מותר להניח שהקלט בשפה [01:25:54].

הגדרות

הגדרה 1: משתנים, ליטרלים, פסוקיות ונוסחת CNF

יהיו $x_1, \ldots, x_n$ **משתנים בוליאניים**, כלומר משתנים שיכולים לקבל את הערכים true ו-false (נסמן גם 1 ו-0).

ליטרל הוא משתנה או שלילתו: x_i או $\bar{x}_i$.

פסוקית (clause) היא "או" בין ליטרלים: $\ell_1 \vee \ell_2 \vee \cdots \vee \ell_k$.

נוסחת (conjunctive normal form) **CNF** היא "וגם" בין פסוקיות.

אינטואיציה. CNF היא נוסחה בוליאנית שנכפתה עליה צורה נוקשה מאוד: שתי שכבות בלבד, "או" בפנים ו"וגם" בחוץ. הנוקשות הזו היא בדיוק מה שהופך את SAT לבעיה נוחה לרדוקציות — קלט של SAT הוא אובייקט פשוט לתיאור, ולכן קל "לכתוב לתוכו" בעיות אחרות. כדי לספק נוסחת CNF צריך לספק את **כל** הפסוקיות, אבל בכל פסוקית מספיק ליטרל **אחד** מסופק [00:14:32].

דוגמה. $\varphi = (x_1 \vee \bar{x}_2) \wedge (\bar{x}_1 \vee x_3 \vee x_4 \vee \bar{x}_5)$ היא נוסחת CNF בת שתי פסוקיות.

אי-דוגמה. $(x_1 \wedge x_2) \vee x_3$ אינה CNF — כאן ה"וגם" נמצא בפנים וה"או" בחוץ (זו צורת DNF). היא כמובן שקולה לנוסחת CNF כלשהי, אבל בתור מחרוזת קלט היא אינה חוקית עבור SAT.

הגדרה 2: השמה וסיפוק

השמה היא פונקציה v שנותנת לכל אחד מהמשתנים $x_1, \ldots, x_n$ ערך ב-$\{0,1\}$. עבור ליטרל מסמנים $v(\bar{x}) = 1 - v(x)$. ההשמה **מספקת** פסוקית אם לפחות ליטרל אחד בה מקבל 1, ומספקת נוסחת CNF אם היא מספקת כל אחת מפסוקיותיה. נוסחה נקראת **ספיקה** אם קיימת השמה שמספקת אותה.

דוגמה (מההרצאה, [00:12:20]–[00:13:56]). עבור $\varphi = (x_1 \vee x_3 \vee x_4) \wedge (\bar{x}_1 \vee x_2) \wedge (\bar{x}_2 \vee x_3 \vee \bar{x}_4)$ וההשמה $v(x_1)=1,\ v(x_2)=1,\ v(x_3)=0,\ v(x_4)=1$: הפסוקית הראשונה מסופקת על ידי x_1, השנייה על ידי x_2, אך בשלישית $\bar{x}_2 = 0,\ x_3 = 0,\ \bar{x}_4 = 0$ — ולכן v **אינה** מספקת את φ. אם משנים ל-$v(x_3) = 1$ ההשמה כן מספקת. שימו לב: הנוסחה ספיקה, אך ההשמה הספציפית אינה מספקת — אלה שני דברים שונים.

הגדרה 3: נוסחת 3CNF

נוסחת CNF φ נקראת **נוסחת 3CNF** אם כל פסוקית שלה מכילה **לא יותר מ-3 ליטרלים**.

אינטואיציה ואי-דוגמה. הנוסחה $(x_1 \vee \bar{x}_2) \wedge (\bar{x}_1 \vee x_3 \vee x_4 \vee \bar{x}_5)$ היא CNF ואף 5CNF ו-4CNF, אבל **אינה** 3CNF, בגלל הפסוקית השנייה שאורכה 4. לעומת זאת $(x_1 \vee \bar{x}_2) \wedge (x_3)$ היא 3CNF — פסוקיות באורך 2 ו-1 מותרות, כי הדרישה היא "לכל היותר 3".

> **הערה חשובה על הגדרה זו.** יש ספרים שמגדירים 3CNF כ"בדיוק 3 ליטרלים בכל פסוקית". ההבדל אינו מהותי (ראו משפט 7), אבל הוא משנה את פרטי הבנייה. **בקורס הזה ההגדרה היא "לכל היותר 3"**, וזו ההגדרה שממנה נגזר האלגוריתם שלהלן — לכן אין בו טיפול נפרד בפסוקיות באורך 1 או 2.

הגדרה 4: הבעיות SAT ו-3SAT

$$\mathrm{SAT} = \{\langle \varphi \rangle \ :\ \varphi \text{ is a satisfiable CNF formula}\}$$
$$3\mathrm{SAT} = \{\langle \varphi \rangle \ :\ \varphi \text{ is a satisfiable 3CNF formula}\}$$

כמו בהרצאה, לא נעסוק בפרטי הקידוד $\langle \cdot \rangle$: מניחים שהקלט מתקבל כמחרוזת תקינה שמתארת נוסחה, ואם אינו תקין — בודקים זאת בזמן פולינומי ודוחים [00:17:52]. נחזור לנקודה הזו כשנבנה את הרדוקציה, כי שם היא דורשת טיפול קטן אך אמיתי.

הגדרה 5: NP-קשה ו-NP-שלמה

שפה B נקראת **NP-קשה** (NP-hard) אם לכל $A \in \mathrm{NP}$ מתקיים $A \le_p B$. שפה B נקראת **NP-שלמה** (NP-complete) אם B NP-קשה **וגם** $B \in \mathrm{NP}$.

אינטואיציה. NP-קשה = "לפחות קשה כמו כל דבר ב-NP", ולאו דווקא שייכת ל-NP בעצמה. NP-שלמה = "הכי קשה ב-NP, ובתוך NP". סדר הכמתים קריטי: לכל שפה ב-NP קיימת רדוקציה — **לא** קיימת רדוקציה אחת שמתאימה לכולן [00:01:08, תמלול 15].

משפטים והוכחות

משפט 1: $\mathrm{NP} \subseteq \mathrm{PSPACE}$

טענה. כל שפה ב-NP ניתנת להכרעה במקום פולינומי.

הוכחה. תהא $A \in \mathrm{NP}$. לפי הגדרת ה-verifier קיימות מכונה דטרמיניסטית M שזמן ריצתה פולינומי — נסמן את הפולינום p — ופולינום q, כך שלכל x: $x \in A \iff \exists\, w \in \{0,1\}^{q(|x|)} \text{ s.t. } M \text{ accepts } (x,w)$.

נגדיר מכונה דטרמיניסטית M_A, על קלט x:

חשב את $q(|x|)$.

לכל $w \in \{0,1\}^{q(|x|)}$ בסדר לקסיקוגרפי (יש $2^{q(|x|)}$ אפשרויות):

2.1 הרץ את M על (x,w).

2.2 אם M קיבלה — קבל.

דחה.

הנקודה שכל ההוכחה תלויה בה: בונים את M_A כך שכל איטרציה של הלולאה תשתמש **באותם תאים** — לפני מעבר ל-w הבא מוחקים את סרט העבודה. מספר האיטרציות אקספוננציאלי, אבל המקום לא מצטבר.

נכונות. אם $x \in A$ אז קיים w שעבורו M מקבלת את (x,w); מכיוון ש-M_A עוברת על כל המחרוזות באורך $q(|x|)$, היא תגיע ל-w הזה, שלב 2.2 יופעל, ו-M_A תקבל. אם $x \notin A$ אז לכל $w \in \{0,1\}^{q(|x|)}$ המכונה M דוחה את (x,w), לכן שלב 2.2 לא מופעל לעולם ו-M_A דוחה בשלב 3.

ניתוח מקום. q פולינום, ולכן כתיבת w ומונה הלולאה דורשות $O(q(|x|))$ תאים. הרצת M על (x,w): זמן הריצה של M פולינומי ב-$|(x,w)| \le |x| + |w| = |x| + q(|x|)$, ומכונה אינה יכולה לבקר ביותר תאים ממספר הצעדים שעשתה, ולכן המקום שהיא דורשת חסום ב-$p(|x| + q(|x|))$. בסך הכול, $\mathrm{space}_{M_A}(x) = O\big(q(|x|) + p(|x| + q(|x|))\big)$ וזהו פולינום ב-$|x|$ — הרכבה וסכום של פולינומים הם פולינום. לכן $A \in \mathrm{PSPACE}$. ■

> **הערה:** ההוכחה הזו היא הסיבה שלא ניתן לקוות ל"הפרדה בזול" בין P ל-NP דרך מקום: כל NP יושבת בתוך PSPACE, כלומר החיפוש האקספוננציאלי עולה הרבה זמן אך מעט מקום.

משפט 2: P סגורה כלפי רדוקציות פולינומיות

טענה. אם $A \le_p B$ ו-$B \in \mathrm{P}$, אז $A \in \mathrm{P}$.

הוכחה. נניח $A \le_p B$. אז קיימת מכונה M_{AB} שמחשבת את הרדוקציה, עם פולינום P כך שלכל x מתקיים $\mathrm{time}_{M_{AB}}(x) \le P(|x|)$, ולכל x: $x \in A \iff M_{AB}(x) \in B$. אז נניח $B \in \mathrm{P}$ קיימת מכונה M_B שמכריעה את B עם פולינום q כך שלכל y מתקיים $\mathrm{time}_{M_B}(y) \le q(|y|)$.

נגדיר מכונה M_A, על קלט x:

חשב את $M_{AB}(x)$.

הרץ את M_B על $M_{AB}(x)$ והחזר את אותה תשובה.

נכונות. אם $x \in A$ אז $M_{AB}(x) \in B$, לכן M_B מקבלת את $M_{AB}(x)$, לכן M_A מקבלת את x. אם $x \notin A$ אז $M_{AB}(x) \notin B$, לכן M_B דוחה, לכן M_A דוחה.

ניתוח זמן. שלב 1 לוקח לכל היותר $P(|x|)$ צעדים. לשלב 2 דרוש $q(|M_{AB}(x)|)$, ולכן צריך לחסום את **אורך הפלט**. מכונה שרצה t צעדים אינה יכולה להאריך את הקלט ביותר מ-t תווים, ולכן $|M_{AB}(x)| \le \mathrm{time}_{M_{AB}}(x) + |x| \le P(|x|) + |x|$, ומכאן ששלב 2 עולה לכל היותר

$q\big(P(|x|)+|x|\big)$. סכום שני הביטויים הוא סכום והרכבה של פולינומים — ולכן פולינום. לכן M_A מכריעה את A בזמן פולינומי, כלומר $A \in \mathrm{P}$. ■

> **הערה:** החסם על אורך הפלט הוא בדיוק הצעד ש"נבלע" בדרך כלל. בלעדיו לא הייתה סיבה ש-q מופעל על ארגומנט קטן, וההרכבה יכלה להתפוצץ. זו הסיבה שכדאי תמיד לכתוב $|f(x)| \le P(|x|)+|x|$ במפורש.

מסקנות (עמוד 3 בסיכום).

באותו אופן בדיוק — מחליפים את P במחלקה המתאימה ואת חסם הזמן בחסם המתאים — מקבלים ש-NP, PSPACE, $\mathrm{NPSPACE}$, EXP ו-NEXP כולן סגורות כלפי רדוקציות זמן פולינומי.

היחס $\le_p$ **טרנזיטיבי**: אם $A \le_p B$ דרך f ו-$B \le_p C$ דרך g, אז $g \circ f$ היא רדוקציה מ-A ל-C; היא ניתנת לחישוב בזמן פולינומי כי $|f(x)|$ פולינומי ב-$|x|$ (אותו חישוב בדיוק כמו למעלה), והנכונות היא שרשור של שתי שקילויות.

מכאן המסקנה המבצעית של כל התחום: **מספיק למצוא בעיה קשה אחת.** אם A NP-קשה ו-$A \le_p B$, אז B NP-קשה — כי לכל $C \in \mathrm{NP}$ מתקיים $C \le_p A \le_p B$ ולפי הטרנזיטיביות $C \le_p B$.

משפט 3: משמעות NP-שלמות

טענה. תהא A שפה NP-שלמה. אז $A \in \mathrm{P}$ אם ורק אם $\mathrm{P}=\mathrm{NP}$.

הוכחה. ($\Leftarrow$) אם $\mathrm{P}=\mathrm{NP}$: מכיוון ש-A NP-שלמה בפרט $A \in \mathrm{NP}=\mathrm{P}$. ($\Rightarrow$) נניח $A \in \mathrm{P}$. ההכלה $\mathrm{P} \subseteq \mathrm{NP}$ ידועה. לכיוון השני, תהא $B \in \mathrm{NP}$ שרירותית. מכיוון ש-A NP-קשה מתקיים $B \le_p A$, ומכיוון ש-$A \in \mathrm{P}$, לפי משפט 2 מתקבל $B \in \mathrm{P}$. מכאן $\mathrm{NP} \subseteq \mathrm{P}$, ובסך הכול $\mathrm{P}=\mathrm{NP}$. ■

זו הסיבה שכל התחום מתעניין בבעיות NP-שלמות: אלגוריתם פולינומי לאחת מהן מפיל את כולן.

הצעד הבא — קיומה של בעיה NP-קשה ראשונה — הוא משפט קוק–לוין: **SAT היא NP-קשה** (שיעור 9). כל מה שנעשה כאן מתבסס עליו כקופסה שחורה.

משפט 4: $3\mathrm{SAT} \le_p \mathrm{SAT}$, ומכאן $3\mathrm{SAT} \in \mathrm{NP}$

טענה. $3\mathrm{SAT} \le_p \mathrm{SAT}$.

הוכחה. הרדוקציה היא **פונקציית הזהות**: בהינתן $\langle\varphi\rangle$ מחזירים $\langle\varphi\rangle$. זמן החישוב הוא זמן ההעתקה, כלומר $O(|\langle\varphi\rangle|)$ — פולינומי. הנכונות: אם φ נוסחת 3CNF ספיקה, אז בפרט φ נוסחת CNF ספיקה (כל 3CNF היא CNF), כלומר $\langle\varphi\rangle \in \mathrm{SAT}$. ולהפך, אם $\langle\varphi\rangle \in \mathrm{SAT}$, אז $\langle\varphi\rangle$ הוא קידוד של 3CNF φ ו-$\langle\varphi\rangle \in 3\mathrm{SAT}$ לפי ההגדרה. (קלט שאינו 3CNF תקין נדחה על ידי שתי הבעיות ולכן אינו מפר את השקילות.) ■

מסקנה: $3\mathrm{SAT} \in \mathrm{NP}$. נובע ממשפט 4, מ-$\mathrm{SAT} \in \mathrm{NP}$ (שיעור 7) ומסגירות NP תחת רדוקציות פולינומיות (מסקנה 1 למשפט 2). לחלופין ישירות: מנחשים השמה ובודקים.

הערה: בהקלטה של השיעור העוקב המרצה מזכיר בדיוק את זה: "הראנו גם את הרדוקציה בכיוון השני, שהיא כמעט הייתה טריוויאלית — הרדוקציה מחזירה לכל נוסחה את עצמה" [00:00:00, תמלול 15].

משפט 5 (הלמה המרכזית): נכונות צעד הפיצול

זהו הלב המתמטי של השיעור. נגדיר תחילה את הצעד הבודד.

אלגוריתם 1. על קלט φ, נוסחה מצורת CNF:

אם φ היא כבר נוסחת 3CNF — החזר את φ.

אחרת, נסמן ב-C את **הפסוקית הראשונה** ב-φ שיש בה יותר מ-3 ליטרלים, ונכתוב $C = \ell_1 \vee \ell_2 \vee \cdots \vee \ell_k$ ($k > 3$). נגדיר $C' = \ell_1 \vee \ell_2 \vee z$ (3 literals) $C'' = \ell_3 \vee \ell_4 \vee \cdots \vee \ell_k \vee \bar{z}$ $(k-1 \text{ literals})$ כאשר z הוא **משתנה חדש שאינו מופיע ב-φ**.

נגדיר את $\hat{\varphi}$ כנוסחה המתקבלת מ-φ על ידי החלפת C ב-$C' \wedge C''$ (במקומה, כך ש-C'' נשארת הפסוקית הארוכה הראשונה).

החזר את $\hat{\varphi}$.

האינטואיציה — מה z עושה. z הוא מתג שאומר "הליטרלים הראשונים לא סיפקו את C, מישהו מאוחר יותר יסדר את זה". אם $z = 1$ אז C' מסופקת בזכות z בלבד, ואז $\bar{z} = 0$ ולכן C'' **חייבת** להיות מסופקת על ידי אחד מ-$\ell_3, \ldots, \ell_k$. אם $z = 0$ אז C'' מסופקת בזכות $\bar{z}$ בלבד, ואז C' **חייבת** להיות מסופקת על ידי ℓ_1 או ℓ_2. בשני המקרים "מישהו אמיתי" מתוך $\ell_1, \ldots, \ell_k$ חייב להיות אמיתי — וזו בדיוק C.

בניסוח קומפקטי: לכל השמה v למשתני φ, $v(C) = 1 \iff \exists\, b \in \{0,1\} : \; v[z \mapsto b](C' \wedge C'') = 1$. כלומר $C' \wedge C''$ **אינה שקולה** ל-C — היא שקולה לה רק אחרי שמכמתים קיומית את z. השקילות שאנחנו צריכים היא **שקילות ספיקות** (equisatisfiability), לא שקילות לוגית. זו נקודה שנופלים עליה במבחן.

טענה (משפט 5). תהא φ נוסחת CNF, ונסמן ב-$\hat{\varphi}$ את פלט אלגוריתם 1 על φ. אז φ ספיקה $\iff$ $\hat{\varphi}$ ספיקה.

הוכחה. נפריד לשני מקרים.

מקרה A: $\varphi = \hat{\varphi}$. זה קורה בדיוק כאשר φ כבר 3CNF, ואז הטענה טריוויאלית.

מקרה B: $\varphi \neq \hat{\varphi}$. נסמן כמו באלגוריתם: $C = \ell_1 \vee \cdots \vee \ell_k$ היא הפסוקית הראשונה באורך > 3, ו-$C' = \ell_1 \vee \ell_2 \vee z$, $C'' = \ell_3 \vee \cdots \vee \ell_k \vee \bar{z}$, כאשר z חדש. שימו לב לעובדה שתשמש שוב ושוב: **פסוקיות φ ו-$\hat{\varphi}$ זהות פרט לכך ש-C הוחלפה ב-C', C'', ו-z אינו מופיע באף פסוקית אחרת.**

כיוון ראשון: φ ספיקה $\Rightarrow$ $\hat{\varphi}$ ספיקה.

תהא v השמה המספקת את φ. מכיוון ש-v מספקת את φ היא בפרט מספקת את C, ולכן קיים $1 \leq i \leq k$ עם $v(\ell_i) = 1$. נפריד לשני תת-מקרים לפי מה שקורה בשני הליטרלים הראשונים.

מקרה B.1: $v(\ell_1) = 0$ וגם $v(\ell_2) = 0$. נגדיר השמה $\hat{v}$ עבור $\hat{\varphi}$: $\hat{v}(x) = \begin{cases} v(x) & x \neq z \\ 1 & x = z \end{cases}$

כל פסוקית D של $\hat{\varphi}$ שאינה C' ואינה C'': D היא גם פסוקית של φ, ולכן v מספקת אותה.
המשתנה z אינו מופיע ב-D, ולכן $\hat{v}$ ו-v נותנות את אותם ערכים לכל משתני D. מכאן ש-$\hat{v}$ מספקת את D.
C': מכיוון ש-$\hat{v}(z) = 1$, הליטרל z מספק את C'.
C'': v מספקת את C ומתקיים $v(\ell_1) = v(\ell_2) = 0$, ולכן קיים $3 \le j \le k$ כך ש-$v(\ell_j) = 1$.
הליטרל ℓ_j הוא מעל משתנה של φ, כלומר משתנה ששונה מ-z, ולכן מהגדרת $\hat{v}$ מתקיים $\hat{v}(\ell_j) = v(\ell_j) = 1$. לכן $\hat{v}$ מספקת את C''.
מכאן ש-$\hat{v}$ מספקת את כל פסוקיות $\hat{\varphi}$, כלומר $\hat{\varphi}$ ספיקה.

מקרה B.2: $v(\ell_1) = 1$ **או** $v(\ell_2) = 1$**.** נגדיר השמה $\hat{v}$ עבור $\hat{\varphi}$: $\hat{v}(x) = \begin{cases} v(x) & x \neq z \\ 0 & x = z \end{cases}$

> **הערה:** בסיכום הכתוב, המקרה הזה מסוכם במילים "באופן דומה $\hat{v}$ מספקת את $\hat{\varphi}$". הנה הפירוט המלא.

כל פסוקית D שאינה C', C'': בדיוק כמו קודם — D פסוקית של φ, z אינו מופיע בה, $\hat{v}$ מסכימה עם v על משתניה, ו-v מספקת אותה. לכן $\hat{v}$ מספקת את D.
C': הליטרלים ℓ_1, ℓ_2 הם מעל משתנים של φ, ולכן $\hat{v}(\ell_1) = v(\ell_1)$ ו-$\hat{v}(\ell_2) = v(\ell_2)$. לפי ההנחה אחד מהם שווה 1, ולכן $\hat{v}$ מספקת את C'.
C'': מכיוון ש-$\hat{v}(z) = 0$ מתקיים $\hat{v}(\bar{z}) = 1$, והליטרל $\bar{z}$ מספק את C''.
לכן $\hat{v}$ מספקת את $\hat{\varphi}$, ו-$\hat{\varphi}$ ספיקה. הכיוון הזה הושלם.

כיוון שני (החצי העדין): $\hat{\varphi}$ ספיקה $\Rightarrow$ φ ספיקה.
כאן צריך להראות שמשתנה העזר **אינו יכול לרמות** — שאי אפשר "לספק" את $\hat{\varphi}$ בזכות z בלבד ולהשאיר את φ בלתי מסופקת. שימו לב שכאן אין לנו חופש בבחירת ההשמה: היא נתונה לנו, ולעומת זאת בכיוון הראשון אנחנו אלה שבנינו אותה.
תהא $\hat{v}$ השמה המספקת את $\hat{\varphi}$. נגדיר השמה v עבור φ על ידי **צמצום**: לכל משתנה x המופיע ב-φ נגדיר $v(x) = \hat{v}(x)$. (זה מוגדר היטב, כי כל משתני φ הם משתני $\hat{\varphi}$.)
כל פסוקית D של φ שאינה C: D היא גם פסוקית של $\hat{\varphi}$, ולכן $\hat{v}$ מספקת אותה; v נותנת אותם ערכים כמו $\hat{v}$ לכל משתני D, ולכן v מספקת את D.
נותר להראות ש-v מספקת את C. נפריד לשני מקרים לפי הערך ש-$\hat{v}$ נתנה למשתנה החדש.
מקרה B.3: $\hat{v}(z) = 1$**.** $\hat{v}$ מספקת את $\hat{\varphi}$ ובפרט את $C'' = \ell_3 \vee \cdots \vee \ell_k \vee \bar{z}$. אבל $\hat{v}(\bar{z}) = 0$, ולכן הליטרל $\bar{z}$ אינו זה שמספק את C''; לכן **חייב** להתקיים שקיים $3 \le j \le k$ עם $\hat{v}(\ell_j) = 1$.
הליטרל ℓ_j הוא מעל משתנה של φ, ולכן $v(\ell_j) = \hat{v}(\ell_j) = 1$. מכאן ש-$v$ מספקת את C.
מקרה B.4: $\hat{v}(z) = 0$**.** $\hat{v}$ מספקת בפרט את $C' = \ell_1 \vee \ell_2 \vee z$. אבל $\hat{v}(z) = 0$, ולכן הליטרל z אינו מספק את C'; לכן $\hat{v}(\ell_1) = 1$ או $\hat{v}(\ell_2) = 1$. שוב ℓ_1, ℓ_2 מעל משתנים של φ, ולכן $v(\ell_1) = 1$ או $v(\ell_2) = 1$, ומכאן ש-v מספקת את C.
בשני המקרים v מספקת את כל פסוקיות φ, ולכן φ ספיקה. ■

למה הוכחה כזו לא יכולה להיות "ברורה מאליה": ההוכחה בכיוון השני נשענת על שתי עובדות שאינן אוטומטיות — (א) שהמשתנה z מופיע **בדיוק בשתי פסוקיות**, פעם חיובית ופעם שלילית; (ב) שהוא **חדש**. אם אחת מהן נופלת, הטענה נופלת. בסעיף הדוגמאות מובאות שתי דוגמאות נגדיות מפורשות בדיוק לשני הכשלים האלה.

למה לא בנייה נאיבית? שווה לראות מה נשבר:
ניסיון א' — לחתוך את C לבלוקים: $C = \ell_1 \vee \cdots \vee \ell_6$ מוחלפת ב- $(\ell_1 \vee \ell_2 \vee \ell_3) \wedge (\ell_4 \vee \ell_5 \vee \ell_6)$. זה **שגוי לחלוטין**: הבנייה דורשת שכל בלוק יסופק, כלומר היא חזקה מדי — עם $\ell_1 = 1$ וכל השאר 0 מסופקת, בעוד הנוסחה החדשה אינה מסופקת.
ניסיון ב' — פשוט לזרוק ליטרלים: מחליפים את C ב-$(\ell_1 \vee \ell_2 \vee \ell_3)$. גם זה שגוי, מאותה סיבה בכיוון ההפוך — נוסחה ספיקה יכולה להיות ספיקה רק בזכות ℓ_5.
מה שחסר בשני הניסיונות הוא בדיוק אמצעי להעביר את המידע "כבר סיפקתי" מבלוק לבלוק.
משתנה עזר חדש z הוא בדיוק אמצעי כזה — ולכן הוא הכרחי, ולכן הבנייה יוצרת נוסחה שאינה שקולה ללוגית ל-φ אלא רק שקולת-ספיקות.
משפט 6: $\mathrm{SAT} \leq_p \mathrm{3SAT}$
טענה. קיימת רדוקציית זמן פולינומי מ-SAT ל-$\mathrm{3SAT}$. במילים: **3SAT היא לפחות קשה כמו SAT.**
הוכחה. נתבונן באלגוריתם הבא. על קלט φ, נוסחה מצורת CNF:
כל עוד φ אינה נוסחה מצורת 3CNF:
1.1 הרץ את אלגוריתם 1 על φ ונסמן את הפלט $\hat{\varphi}$ (בכל הפעלה נבחר משתנה עזר **חדש**, שלא הופיע באף שלב קודם).
1.2 $\varphi \leftarrow \hat{\varphi}$.
החזר את φ.
בנוסף, אם הקלט אינו קידוד תקין של נוסחת CNF — נדחה אותו, כלומר נחזיר נוסחת 3CNF קבועה ובלתי-ספיקה, למשל $(y) \wedge (\bar{y})$. בדיקת התקינות והפלט הקבוע נעשים בזמן לינארי. (בהרצאה הנקודה הזו נאמרה כהנחה: "אני מניח שקיבלתי נוסחה בצורת CNF... אפשר לבדוק תקינות ולדחות" [00:17:52].)
עצירה. בכל איטרציה, פסוקית באורך $k > 3$ מוחלפת בפסוקיות באורכים 3 ו-$k-1$; פסוקיות באורך ≤ 3 אינן משתנות לעולם. לכן הסכום $\sum_{C \in \varphi,\ |C|>3} (|C| - 3)$ יורד בדיוק ב-1 בכל איטרציה, והוא מספר טבעי אי-שלילי — אז הלולאה עוצרת, ובפלט כל הפסוקיות באורך ≤ 3, כלומר הפלט הוא 3CNF.
נכונות. נסמן ב-$\varphi_0 = \varphi$ את הקלט, וב-$\varphi_1, \ldots, \varphi_m$ את הנוסחאות אחרי כל איטרציה, כאשר φ_m הוא הפלט. לפי משפט 5, לכל $0 \leq t < m$ מתקיים "φ_t ספיקה $\iff$ φ_{t+1} ספיקה". באינדוקציה על t מתקבל φ satisfiable $\iff$ φ_m satisfiable. מכיוון ש-φ_m היא 3CNF, זה בדיוק $\langle \varphi \rangle \in \mathrm{SAT} \iff \langle \varphi_m \rangle \in \mathrm{3SAT}$.

הערה על תנאי הרעננות בלולאה: משפט 5 דורש ש-z לא יופיע ב-φ **הנוכחית**, כלומר גם לא במשתני העזר שנוספו באיטרציות קודמות. לכן מקצים משתנה עזר חדש לכל איטרציה. הדבר גם מבטיח שהאינדוקציה למעלה חוקית: בכל צעד תנאי משפט 5 מתקיימים.

ניתוח זמן ריצה (במפורש). נסמן ב-L את מספר מופעי הליטרלים בנוסחת הקלט; ברור ש- $L \le |\varphi|$.

מספר האיטרציות. כפי שראינו בהוכחת העצירה, מספר האיטרציות שווה בדיוק ל- $\sum_{|C|>3}(|C|-3)$, כלומר $L \le |\varphi|$. (בסיכום כתוב לצד זה בכחול: כל הפעלה מקטינה את הפסוקית הארוכה ב-1 — זו בדיוק הסיבה.)

גידול אורך הנוסחה. בכל איטרציה פסוקית באורך k מוחלפת בשתי פסוקיות באורכים 3 ו-$k-1$, כלומר מספר מופעי הליטרלים גדל ב-2 בדיוק, ומספר הפסוקיות ב-1. לכן אחרי כל האיטרציות $L_{\text{final}} \le L + 2 \cdot (\text{number of iterations}) \le 3L = O(|\varphi|)$, **הנוסחה אינה מתנפחת** — היא נשארת לינארית באורך הקלט. בפרט לכל אורך הריצה כל נוסחת ביניים היא בגודל $O(|\varphi|)$.

מחיר איטרציה בודדת. סריקת הנוסחה הנוכחית כדי לאתר את הפסוקית הארוכה הראשונה, והעתקתה עם הפיצול, עולים $O(|\varphi|) = O(|\varphi_t|)$.

סך הכול. $O(|\varphi|) \cdot O(|\varphi|) = O(|\varphi|^2)$ — פולינומי. ■

הערה על דיוק החסם: בסיכום נכתב שאורך $\hat{\varphi}$ אינו עולה על $2|\varphi|$. ספירה מדויקת של מופעי ליטרלים נותנת $3L$ ולא $2L$ (הקלט L ועוד 2 לכל אחת מעד L איטרציות). ההבדל אינו משנה דבר — שני החסמים לינאריים ולכן זמן הריצה $O(|\varphi|^2)$ בעינו. הערה נוספת ברמת הביטים: הרדוקציה מוסיפה עד L משתנים חדשים, וקידוד אינדקס של משתנה חדש עשוי לדרוש $O(\log L)$ ביטים, כך שאורך הפלט בביטים הוא $O(|\varphi| \log |\varphi|)$. עדיין פולינומי, וזמן הריצה עדיין פולינומי — אך כדאי לדעת שהחסם הלינארי הוא בספירת סמלים, לא בהכרח בספירת ביטים.

מסקנה: $3\mathrm{SAT}$ היא NP-שלמה

$3\mathrm{SAT} \in \mathrm{NP}$ — מסקנת משפט 4.

$3\mathrm{SAT}$ NP-קשה — לפי משפט קוק–לוין SAT NP-קשה, לפי משפט 6 מתקיים $\mathrm{SAT} \le_p 3\mathrm{SAT}$, ולפי מסקנה 3 של משפט 2 (טרנזיטיביות) מתקבל שכל $A \in \mathrm{NP}$ מקיימת $A \le_p \mathrm{SAT} \le_p 3\mathrm{SAT}$.

לכן $3\mathrm{SAT}$ NP-שלמה. ■

למה בכלל טורחים? אחרי משפט קוק–לוין כבר יש לנו בעיה NP-שלמה, אז מדוע להוסיף עוד אחת? כי 3SAT היא **נקודת מוצא נוחה בהרבה לרדוקציות עתידיות**: קלט של 3SAT הוא אוסף פסוקיות שכל אחת מהן מכילה לכל היותר 3 ליטרלים, מבנה נוקשה שקל להעתיק לגרף, לקבוצות או לאילוצים גיאומטריים. בשיעורים הבאים כמעט כל רדוקציה תתחיל מ-3SAT ולא מ-SAT. בהקלטה של שיעור 9 המרצה מציין שזו בדיוק הדרך של Karp: "הוא עשה את הרדוקציה מ-SAT ל-3SAT שהראינו, את הרדוקציה מ-SAT ל-IS, ואז מ-IS ל-CLIQUE" [01:20:52, תמלול 15].

משפט 7 (השלמה): הווריאנט "בדיוק 3 ליטרלים"
טענה. נסמן ב-$3\mathrm{SAT}^{=}$ את הבעיה שבה כל פסוקית מכילה **בדיוק** 3 ליטרלים. אז $3\mathrm{SAT} \leq_p 3\mathrm{SAT}^{=}$, ולכן גם $3\mathrm{SAT}^{=}$ NP-שלמה.

> **הערה:** הטענה הזו אינה בסיכום ואינה בהקלטה. היא נכללת כאן כי ההגדרה השנייה נפוצה בספרות, וכי היא משלימה את ניתוח המקרים לפסוקיות באורך 1 ו-2 — מקרים שההגדרה של הקורס פשוט אינה זקוקה לטיפול בהם.

הוכחה. בהינתן נוסחת 3CNF φ, נטפל בכל פסוקית לפי אורכה, עם משתנים חדשים y, y' **לכל פסוקית בנפרד**:
אורך 3: משאירים כמו שהיא.
אורך 2, $C = \ell_1 \vee \ell_2$: מחליפים ב-$(\ell_1 \vee \ell_2 \vee y) \wedge (\ell_1 \vee \ell_2 \vee \bar{y})$. נכונות: אם $v(\ell_1) = 1$ או $v(\ell_2) = 1$ — שתי הפסוקיות מסופקות בכל ערך של y. אם שניהם 0 — אחת משתי הפסוקיות נכשלת, כי אחד מ-$y, \bar{y}$ מקבל 0. כלומר הצמד מסופק אם ורק אם C מסופקת, בכל השמה ל-y.
אורך 1, $C = \ell_1$: מחליפים ב- $(\ell_1 \vee y \vee y') \wedge (\ell_1 \vee y \vee \bar{y}') \wedge (\ell_1 \vee \bar{y} \vee y') \wedge (\ell_1 \vee \bar{y} \vee \bar{y}')$. נכונות: אם $v(\ell_1) = 1$ הכול מסופק. אם $v(\ell_1) = 0$, אז לכל בחירה של (y, y') אחת מארבע הפסוקיות מכילה את שני הליטרלים המשלימים ומקבלת 0.
בשני המקרים המשתנים החדשים אינם מופיעים בשום מקום אחר, ולכן אפשר לצמצם/להרחיב השמות בדיוק כמו במשפט 5. גודל הפלט לכל היותר פי 4 מגודל הקלט, וזמן החישוב לינארי. ■

דוגמאות ותרגילים מהשיעור
דוגמה 1: מסלול מלא של נוסחה דרך הרדוקציה, בשני הכיוונים
ניקח את הדוגמה מעמוד 4 בסיכום: $\varphi = (x_1 \vee \bar{x}_2) \wedge (x_1 \vee x_3 \vee x_4 \vee \bar{x}_5 \vee \bar{x}_6)$.
איטרציה 1. הפסוקית הראשונה באורך > 3 היא $C = x_1 \vee x_3 \vee x_4 \vee \bar{x}_5 \vee \bar{x}_6$, כלומר $k = 5$, $\ell_1 = x_1$, $\ell_2 = x_3$. עם משתנה חדש z_1: $C' = x_1 \vee x_3 \vee z_1, \qquad C'' = x_4 \vee \bar{x}_5 \vee \bar{x}_6 \vee \bar{z}_1$. $\bar{z}_1 \quad (k - 1 = 4 \text{ literals})$, $\varphi_1 = (x_1 \vee \bar{x}_2) \wedge (x_1 \vee x_3 \vee z_1) \wedge (x_4 \vee \bar{x}_5 \vee \bar{x}_6 \vee \bar{z}_1)$.
איטרציה 2. הפסוקית הארוכה היחידה היא $x_4 \vee \bar{x}_5 \vee \bar{x}_6 \vee \bar{z}_1$ ($k = 4$), עם $\ell_1 = x_4,\ \ell_2 = \bar{x}_5$. עם משתנה חדש z_2: $\varphi_2 = (x_1 \vee \bar{x}_2) \wedge (x_1 \vee x_3 \vee z_1) \wedge (x_4 \vee \bar{x}_5 \vee z_2) \wedge (\bar{x}_6 \vee \bar{z}_1 \vee \bar{z}_2)$. כל הפסוקיות באורך ≤ 3 — זהו הפלט. שימו לב לאימות המספרים: $L = 2 + 5 = 7$ מופעי ליטרלים בקלט, שתי איטרציות (כי $5 - 3 = 2$), ובפלט $7 + 2 \cdot 2 = 11 = 3 + 3 + 3 + 2$ מופעים. בדיוק כמו שניתוח הזמן חזה.
מסלול קדימה (φ ספיקה $\Rightarrow \varphi_2$ ספיקה). ניקח $v:\ x_1 = 1,\ x_2 = 1,\ x_3 = 0,\ x_4 = 0,\ x_5 = 1,\ x_6 = 1$. v מספקת את φ: הפסוקית הראשונה בזכות x_1, השנייה בזכות x_1.
באיטרציה 1: $v(\ell_1) = v(x_1) = 1$ — זהו **מקרה B.2**, ולכן $\hat{v}(z_1) = 0$. בדיקה: $(x_1 \vee x_3 \vee \bar{z}_1) = 1$ בזכות x_1; $(x_4 \vee \bar{x}_5 \vee \bar{x}_6 \vee \bar{z}_1) = 1$ בזכות z_1.
באיטרציה 2, ביחס לנוסחה φ_1 ולהשמה שהתקבלה: $\ell_1 = x_4 = 0$ ו-$\ell_2 = \bar{x}_5 = 0$ — זהו **מקרה B.1**, ולכן $z_2 = 1$. בדיקה: $(x_4 \vee \bar{x}_5 \vee z_2) = 1$ בזכות z_2; $(\bar{x}_6 \vee \bar{z}_1 \vee \bar{z}_2) = 0 \vee 1 \vee 0 = 1$ בזכות $\bar{z}_1$.

ההשמה הסופית $\hat{v}: x_1{=}1, x_2{=}1, x_3{=}0, x_4{=}0, x_5{=}1, x_6{=}1, z_1{=}0, z_2{=}1$ מספקת את כל ארבע הפסוקיות של φ_2.

מסלול אחורה (φ_2 ספיקה $\Rightarrow$ φ ספיקה). ניקח הפעם השמה "עוינת" ל-φ_2 שמנסה להישען על משתני העזר: $u:\ x_1=0,\ x_2=0,\ x_3=0,\ x_4=0,\ x_5=0,\ x_6=0,\ z_1=1,\ z_2=0$. בדיקה: $(x_1\vee\bar{x}_2)=1$; $(x_1\vee x_3\vee z_1)=1$ בזכות z_1; $(x_4\vee\bar{x}_5\vee z_2)=1$ בזכות $\bar{x}_5$; $(\bar{x}_6\vee\bar{z}_1\vee\bar{z}_2)=1$ בזכות $\bar{x}_6$. אכן u מספקת את φ_2.

נצמצם: $v=u|_{x_1,\ldots,x_6}$, כלומר כל ה-x-ים אפס. האם v מספקת את φ? $(x_1\vee\bar{x}_2)=0\vee 1=1$; $(x_1\vee x_3\vee x_4\vee\bar{x}_5\vee\bar{x}_6)=0\vee 0\vee 0\vee 1\vee 1=1$. כן.

וזה בדיוק הטיעון של מקרה B.3 בפעולה: $u(z_1)=1$ אילץ את $\bar{z}_1$ להיות 0, כך שהפסוקית $(x_4\vee\bar{x}_5\vee\bar{x}_6\vee\bar{z}_1)$ נאלצה להיות מסופקת על ידי ליטרל **מקורי** — ואכן $\bar{x}_5=1$. משתנה העזר "העביר את החוב הלאה" ולא הצליח לפרוע אותו בעצמו.

דוגמה 2: $C'\wedge C''$ אינה שקולה ל-C

יהי $C=a\vee b\vee c\vee d$, ונפצל: $C'=a\vee b\vee z$, $C''=c\vee d\vee\bar{z}$.

קחו $a=1$ ו-$b=c=d=0$. אז C מסופקת. אבל אם בנוסף $z=1$: $C'=1$ ואילו $C''=0\vee 0=0$ — הצמד אינו מסופק.

קחו $a=b=c=d=0$. אז C אינה מסופקת, ואכן בשתי הבחירות של z הצמד נכשל: $z=1$ מפיל את C'', $z=0$ מפיל את C'.

המסקנה: לא לכל z מתקיים $C'\wedge C''$ כאשר C מתקיימת — אלא **קיים** z כזה. כל הוכחה שכותבת "$C\equiv C'\wedge C''$" שגויה; הניסוח הנכון הוא שקילות ספיקות, ולכן ההוכחה חייבת לעבור דרך בניית ההשמה בכל כיוון בנפרד.

תרגיל 1: מה נשבר אם משתמשים באותו z פעמיים?

התרגיל. נניח שבמקום להקצות משתנה חדש בכל איטרציה, האלגוריתם משתמש שוב ושוב באותו z. תנו דוגמה נגדית.

פתרון. יהי $\varphi=(a\vee b\vee c\vee d)\wedge(e\vee f\vee g\vee h)$. עם אותו z בשני הפיצולים מקבלים $\hat{\varphi}=(a\vee b\vee z)\wedge(c\vee d\vee\bar{z})\wedge(e\vee f\vee z)\wedge(g\vee h\vee\bar{z})$. קחו את ההשמה $a=1,\ g=1$ וכל השאר 0. אז φ מסופקת (הפסוקית הראשונה בזכות a, השנייה בזכות g). אבל ב-$\hat{\varphi}$:

אם $z=0$: הפסוקית $(e\vee f\vee z)=0$.

אם $z=1$: הפסוקית $(c\vee d\vee\bar{z})=0$.

יתרה מזאת, קל לבדוק ש-$\hat{\varphi}$ **אינה ספיקה כלל** תחת ההשמה הזו לשאר המשתנים, בעוד φ ספיקה — כלומר הרדוקציה השבורה מייצרת "לא" עבור קלט שהתשובה עליו "כן". הסיבה: משתנה עזר יחיד נדרש להעיד בו-זמנית "בפסוקית הראשונה הסתדרנו מוקדם" ו"בפסוקית השנייה הסתדרנו מאוחר", ואלה דרישות סותרות.

תרגיל 2: מה נשבר אם z אינו חדש?

התרגיל. מדוע דורשים ש-z לא יופיע ב-φ?

פתרון. נניח שהאלגוריתם "חוסך" ובוחר $z:=a$ שכבר מופיע בנוסחה. קחו $\varphi=(a\vee b\vee c\vee d)\wedge(\bar{a})\wedge(\bar{b})\wedge(c)$. ספיקה: $a=0,\ b=0,\ c=1$, ו-d כרצוננו — הפסוקית הארוכה מסופקת בזכות c. אבל הפיצול עם $z=a$ ו-$\ell_1=a,\ \ell_2=b$ נותן $C'=a\vee b\vee a\equiv a\vee b$,

ולכן $\hat{\varphi} = (a \vee b) \wedge (c \vee d \vee \bar{a}) \wedge (\bar{a}) \wedge (\bar{b}) \wedge (c)$, שאינה ספיקה: $(\bar{a}) \wedge (\bar{b})$ מכריחות $a = b = 0$ וסותרות את $(a \vee b)$.

הכשל המדויק בהוכחה: בשלב שבו כתבנו "z אינו מופיע ב-D, ולכן $\hat{v}$ ו-v מסכימות על משתני D" — אם z ישן, ההנחה הזו קורסת, ושינוי ערכו כדי לספק את C' יכול להפיל פסוקית אחרת.

תרגיל 3: כוח הביטוי של נוסחאות CNF (עמודים 7–8 בסיכום)

החלק הזה נראה כמו סטייה מהנושא, אבל הוא בדיוק ההכנה למשפט קוק–לוין: שם נצטרך לקודד ריצה של מכונת טיורינג כנוסחת CNF, וכל הטריקים כאן יחזרו. המרצה בשיעור 9 חוזר לזה שוב ושוב: "תזכרו שיהיה לכם בראש כל הזמן את בעיית 8 מלכות" [00:09:27, תמלול 15], ו"בעיית המלכות זה היה כמו משפט קוק בקטן" [00:20:03].

(א) בחירת קבוצה לא ריקה. $x_1 \vee x_2 \vee \cdots \vee x_{10}$ מבטאת בחירה של תת-קבוצה לא ריקה מתוך $\{1, \dots, 10\}$: מזהים תת-קבוצה A עם ההשמה $x_i = 1 \iff i \in A$. השמה מספקת את הנוסחה אם ורק אם היא נותנת ערך 1 לפחות למשתנה אחד, כלומר $A \neq \emptyset$.

(ב) לא ריקה וגם לא מלאה. $(x_1 \vee x_2 \vee \cdots \vee x_{10}) \wedge (\bar{x}_1 \vee \bar{x}_2 \vee \cdots \vee \bar{x}_{10})$ הפסוקית השנייה דורשת שלפחות משתנה אחד יקבל 0, כלומר $A \neq \{1, \dots, 10\}$. בסך הכול ההשמות המספקות הן בדיוק אלה המתאימות ל-$\emptyset \subsetneq A \subsetneq \{1, 2, \dots, 10\}$.

(ג) בדיוק אחד. $(x_1 \vee x_2 \vee x_3) \wedge (\bar{x}_1 \vee \bar{x}_2) \wedge (\bar{x}_1 \vee \bar{x}_3) \wedge (\bar{x}_2 \vee \bar{x}_3)$ הפסוקית הראשונה אומרת "לפחות אחד". כל פסוקית $(\bar{x}_i \vee \bar{x}_j)$ שקולה ל-$\neg(x_i \wedge x_j)$, כלומר "לא שניהם" — ויחד הן אומרות "לכל היותר אחד". לכן השמה מספקת את הנוסחה אם ורק אם היא נותנת 1 לבדיוק אחד מ-x_1, x_2, x_3. **זהו הגאדג'ט המרכזי בכל השיעור הבא** — "בתא הזה של הטבלה כתוב בדיוק סמל אחד".

(ד) 8 מלכות. לכל $1 \le i, j \le 8$ נגדיר משתנה בוליאני $x_{i,j}$, שהמשמעות המיועדת לו היא "יש מלכה במשבצת (i, j)".

בדיוק מלכה אחת בכל שורה: $B = \bigwedge_{i=1}^{8} \left[\left(\bigvee_{j=1}^{8} x_{i,j} \right) \wedge \bigwedge_{j \neq k} (\bar{x}_{i,j} \vee \bar{x}_{i,k}) \right]$

בדיוק מלכה אחת בכל עמודה: $C = \bigwedge_{j=1}^{8} \left[\left(\bigvee_{i=1}^{8} x_{i,j} \right) \wedge \bigwedge_{i \neq k} (\bar{x}_{i,j} \vee \bar{x}_{k,j}) \right]$ *לכל היותר מלכה אחת בכל אלכסון:* $D = \bigwedge_{\substack{(i,j) \neq (i',j') \\ |i-i'| = |j-j'|}} (\bar{x}_{i,j} \vee \bar{x}_{i',j'})$ והנוסחה כולה: $\varphi = B \wedge C \wedge D$. זו נוסחת CNF (חיתוך של נוסחאות CNF הוא CNF), והשמה מספקת אותה אם ורק אם היא מתארת מיקום חוקי של 8 מלכות על הלוח.

מה הפואנטה? לא פתרנו את בעיית 8 המלכות — **קידדנו** אותה. בהינתן פותר ל-SAT היינו מקבלים גם פותר ל-8 מלכות; וברמה הכללית, הבעיה של n מלכות מצטמצמת ל-SAT בזמן פולינומי, כי מספר המשתנים הוא n^2 ומספר הפסוקיות $O(n^4)$, וכולן ניתנות לכתיבה ישירה מ-n. אגב, כל הפסוקיות ב-B, C, D שאינן ה"או" הגדול הן באורך 2 — כלומר הנוסחה כמעט 3CNF ממילא; רק ה"או" על שורה שלמה (8 ליטרלים) דורש את הפיצול של משפט 6.

תרגיל 4: כמה גדל הפלט על פסוקית באורך 10?

התרגיל. נתונה פסוקית יחידה $C = \ell_1 \vee \cdots \vee \ell_{10}$. כמה איטרציות יבצע האלגוריתם, כמה משתנים חדשים יוסיף, ומה תהיה הנוסחה?

פתרון. מספר האיטרציות הוא $10 - 3 = 7$, וכך גם מספר משתני העזר $z_1, \dots, z_7$. נעקוב:

איטרציה 1: $(\ell_1 \vee \ell_2 \vee z_1) \wedge (\ell_3 \vee \cdots \vee \ell_{10} \vee \bar{z}_1)$ — הפסוקית השנייה באורך 9.
איטרציה 2 מפצלת אותה לפי שני הליטרלים הראשונים שבה, ℓ_3, ℓ_4: $(\ell_3 \vee \ell_4 \vee z_2) \wedge (\ell_5 \vee \cdots \vee \ell_{10} \vee \bar{z}_1 \vee \bar{z}_2)$ — הזנב באורך 8.
כל איטרציה נוספת מוציאה עוד שני ליטרלים מקוריים לפסוקית באורך 3, ומוסיפה עוד $\bar{z}$ לזנב. בסוף מתקבלות 8 פסוקיות ובהן $10 + 2 \cdot 7 = 24$ מופעי ליטרלים — בדיוק כמו שהניתוח חוזה ($L + 2\cdot$ מספר האיטרציות). שימו לב לאופי המבנה: הליטרלים המקוריים יוצאים שניים-שניים, ושרשרת ה-$\bar{z}$ מצטברת בפסוקית הזנב עד שגם היא מתקצרת. זו התנהגות האלגוריתם של הסיכום; בנייה חלופית מקובלת בספרות שומרת משתנה עזר אחד בלבד בכל פסוקית ומייצרת $k - 2$ פסוקיות באורך בדיוק 3.

הערות מהשיעור

> **קראו את זה קודם:** לשיעור הזה **אין הקלטה בקורפוס**, ולכן אין בו הערות מההרצאה שלו עצמו. ההערות שלהלן נלקחו מהקלטות השיעורים הסמוכים (9 ו-16 באפריל) ומובאות כאן משום שהן חלות ישירות על החומר של שיעור זה — לא משום שנאמרו בו. הציטוט המדויק והמספור של ההערה מציינים את הקובץ שממנו נלקחה.

מספר ההשמות הוא 2^n לפי מספר *המשתנים*, לא לפי מספר הליטרלים [00:19:28, תמלול 14]. סטודנט ענה "שתיים בחזקת כמות הליטרלים" והמרצה תיקן: ברגע שנתת ערך ל-x_1, קבעת גם את $\bar{x}_1$. טעות קטנה אבל היא משנה את החסם.
רדוקציה אינה פתרון [01:11:50, 01:13:27, תמלול 14]. סטודנט הציע "לנסות לפתור את זה באמצעות CLIQUE", והמרצה עצר: "אני לא מנסה לפתור — כל הרדוקציה זה רק ההמרה מפה לפה". זה תקף במלואו כאן: אלגוריתם 1 לא בודק ספיקות של שום דבר, הוא רק **כותב מחדש** את הנוסחה.
שני שלבים נפרדים בבניית רדוקציה [01:25:21]–[01:26:25, תמלול 14]. "כשאני מגדיר את המכונה אני לא יודע אם הקלט שייך לקבוצה. אם הייתי רוצה לדעת את זה, הייתי צריך מספר צעדים אקספוננציאלי. רק בשלב ההוכחה אני מניח שהקלט שייך ומראה שהפלט שייך." בשיעור הזה זה בולט: אלגוריתם 1 רץ בלי לדעת דבר על ספיקות, ורק משפט 5 מניח ספיקות ובונה השמה.
תמיד לכתוב את שתי הגרירות בנפרד, גם כשהן נראות סימטריות [01:22:33], [01:27:34, תמלול 14]. בשיעור הזה הן **אינן** סימטריות: בכיוון "$\varphi \Rightarrow \hat{\varphi}$" אנחנו בוחרים את הערך של z, ובכיוון ההפוך הוא נתון לנו ואנחנו מסיקים ממנו. זה בדיוק המקום שבו סטודנטים מוותרים על החצי הקשה.
על התקינות של הקלט [00:17:52, תמלול 14]. המרצה בחר במפורש לא לעסוק בקידוד: "ההנחה היא שהקלט מתקבל בצורה תקינה; אפשר לבדוק תקינות ולדחות". במבחן זו הערת שוליים לגיטימית, אבל ברדוקציה חייבים להגדיר גם מה עושים על קלט פסול — אחרת הפונקציה אינה מוגדרת על כל Σ^*.
מדוע 3SAT ולא SAT בהמשך [01:20:52, תמלול 15]. המרצה מספר על המאמר של Karp עם 21 בעיות NP-שלמות, ובראשן השרשרת $\mathrm{SAT} \to \mathrm{3SAT} \to \mathrm{IS} \to \mathrm{CLIQUE}$. הרדוקציה של השיעור הזה היא החוליה הראשונה בשרשרת ההיסטורית הזו.

הפער המרכזי, לפני כל השאר: לשיעור הזה אין הקלטה. נבדק כל קורפוס ההקלטות של הקורס, ולא נמצא בו ולו קטע אחד שבו נלמדת הבנייה $\mathrm{SAT} \le_p \mathrm{3SAT}$. תמלול 14 מסתיים בחומר של שיעור 7 (CLIQUE, IS), תמלול 15 הוא כבר שיעור קוק–לוין ומזכיר את הרדוקציה רק בדיעבד, ותמלול 16 ממשיך לכיסוי קודקודים ולצביעה. הסימנים מצביעים על כך שהחומר **ניתן ללימוד עצמי / כשיעורי בית**, וזה מתיישב עם כך שגיא סופר כתב עליו סיכום בן 8 עמודים.
המשמעות המעשית לקורא: כל מה שבקובץ הזה נשען על הסיכום הכתוב ועל השלמה מתמטית סטנדרטית שלי — ולא על הרצאה. הסיכום עצמו קריא לחלוטין ושלם מתמטית, ולכן `confidence: medium` ולא `low`; אך אין מקור שני להצלבה, ו-`coverage` של שני התמלולים סומנה `none`.

מה מהסיכום ומה השלמה שלי. מהסיכום: כל ההגדרות (עמוד 4), אלגוריתם 1 על ארבעת שלביו והדוגמה שלו (עמוד 4), ניסוח משפט 5 והוכחתו על ארבעת המקרים (עמודים 5–6), אלגוריתם הלולאה וניתוח הזמן (עמוד 7), דוגמאות כוח הביטוי ובעיית 8 המלכות (עמודים 7–8), וכן משפטים 1–3 (עמודים 1–3). השלמה שלי, מסומנת בגוף הקובץ בהערות: פירוט מקרה B.2, טיעון העצירה של הלולאה, האינדוקציה על שרשרת האיטרציות, ספירת מופעי הליטרלים המדויקת, תנאי הרעננות בכל איטרציה, הטיפול בקלט לא תקין, הניסוחים "מדוע לא בנייה נאיבית", דוגמה 2, תרגילים 1–2, ומשפט 7.
מקור: הסיכום, עמוד 5. **הפער:** בכיוון "φ ספיקה $\Rightarrow \hat{\varphi}$ ספיקה", המקרה $v(\ell_1) = 1$ או $v(\ell_2) = 1$ נכתב במילים "באופן דומה". **ההכרעה:** נכתב כאן במלואו (מקרה B.2), כולל הנימוק לכל אחת משלוש קבוצות הפסוקיות.
מקור: הסיכום, עמוד 7. **הפער:** נכתב שאורך הפלט אינו עולה על $2|\varphi|$. ספירה מדויקת של מופעי ליטרלים נותנת $3|\varphi|$ (הקלט, ועוד 2 לכל אחת מעד $|\varphi|$ איטרציות). **ההכרעה:** נכתב החסם המדויק $3L$, עם ציון שהאסימפטוטיקה $O(|\varphi|^2)$ אינה משתנה; נוספה הערה שברמת הביטים יש עוד גורם $\log$ בשל אינדקסי המשתנים החדשים.
מקור: הסיכום, עמוד 8. **הפער:** הנוסחה C (אילוץ העמודות בבעיית 8 המלכות) כתובה כמעט זהה ל-B (אילוץ השורות) — נראה שהאינדקסים i ו-j לא הוחלפו. **ההכרעה:** נכתבה כאן הגרסה המתוקנת שבה C סורקת עמודות; זו הכוונה הברורה מההקשר ("לבסוף נגדיר D עבור האלכסונים").
מקור: הסיכום, עמודים 5–6. **הפער:** מספור המקרים אינו עקבי — בכיוון הראשון מופיעים "מקרה 1"/"מקרה 1.1"/"מקרה 1.2" ובכיוון השני שוב "מקרה 1"/"מקרה 2" למשמעות אחרת לגמרי (הערך של $\hat{v}(z)$). **ההכרעה:** מוספרו כאן מחדש כ-B.1–B.4 עם תיאור מפורש של מה מפרידים בכל מקרה.
מקור: הסיכום, עמודים 1–3. **הפער:** שליש מהעמודים מוקדשים לחומר שהוא ברובו חזרה — $\mathrm{NP} \subseteq \mathrm{PSPACE}$, סגירות P תחת רדוקציות, והגדרות NP-קשה/NP-שלמה — שחלקו שייך תוכנית ללימוד לשיעורים 6–7. **ההכרעה:** נכלל כאן במלואו כי הוא מופיע ב-PDF של שיעור זה ומשמש ישירות במסקנה על 3SAT; ייתכן שיש חפיפה עם קובצי שיעורים 6–7 ועל הרכז לבדוק זאת.

מקור: הסיכום, עמוד 4. **הפער:** ההצדקה לרדוקציה $3\mathrm{SAT} \le_p \mathrm{SAT}$ כתובה בקיצור רב ("הרדוקציה מחזירה את אותה נוסחה"), ולא נאמר מה עושים עם קלט שאינו 3CNF. **ההכרעה:** נכתבה הצדקה מלאה, כולל הטיפול בקלט לא תקין.

מקור: האלגוריתם בסיכום. **הפער:** הסיכום אינו מציין במפורש שיש להקצות משתנה עזר **חדש בכל איטרציה** של הלולאה (הוא דורש רק ש-z יהיה חדש עבור הפעלה בודדת). **ההכרעה:** התנאי נוסח במפורש בהוכחת משפט 6, והכרחיותו הודגמה בתרגיל 1.

מקור: כל המקורות. **הפער:** לא נדונו פסוקיות באורך 1 ו-2 (הן חוקיות לפי הגדרת הקורס), ולא הווריאנט "בדיוק 3 ליטרלים". **ההכרעה:** נוסף משפט 7 כהשלמה, עם סימון מפורש שהוא אינו מהמקורות.

סיכום ונקודות למבחן

מה חייבים לזכור בעל פה.

הבנייה: פסוקית $C = \ell_1 \vee \cdots \vee \ell_k$ עם $k > 3$ מוחלפת ב- $(\ell_1 \vee \ell_2 \vee z) \wedge (\ell_3 \vee \cdots \vee \ell_k \vee \bar{z})$, כאשר z חדש; חוזרים עד שכל הפסוקיות באורך ≤ 3.

החשבון: מספר האיטרציות $\sum_{|C|>3}(|C|-3) = O(|\varphi|)$; כל איטרציה מוסיפה 2 מופעי ליטרלים ומשתנה אחד; אורך הפלט $O(|\varphi|)$; זמן ריצה $O(|\varphi|^2)$.

המסקנה: $3\mathrm{SAT} \in \mathrm{NP}$ (רדוקציית זהות ל-SAT) + $\mathrm{SAT} \le_p 3\mathrm{SAT}$ + קוק–לוין $\Rightarrow$ **3SAT NP-שלמה**.

$\mathrm{NP} \subseteq \mathrm{PSPACE}$; P (וכן $\mathrm{NP}, \mathrm{PSPACE}, \mathrm{EXP}$) סגורות תחת $\le_p$; אם A NP-שלמה אז $A \in \mathrm{P} \iff \mathrm{P} = \mathrm{NP}$.

המלכודות הסטנדרטיות.

לכתוב "$C \equiv C' \wedge C''$". לא נכון. השקילות היא בספיקות בלבד, ורק אחרי כימות קיומי על z. ראו דוגמה 2.

לוותר על הכיוון ההפוך. רוב הנקודות בשאלת רדוקציה יושבות בכיוון "הפלט ספיק $\Rightarrow$ הקלט ספיק", כי שם צריך להראות שמשתני העזר לא מרמים. הטיעון הוא תמיד: $\hat{v}(z)$ הוא 0 או 1; כל אחד מהם "מנטרל" את משתנה העזר באחת משתי הפסוקיות ומאלץ ליטרל מקורי לספק אותה.

לשכוח את הרעננות. משתנה עזר חדש לכל פיצול. תרגיל 1 מראה נוסחה ספיקה שהופכת לבלתי-ספיקה אם חוסכים משתנה.

להפוך את כיוון ה-$\le_p$. $\mathrm{SAT} \le_p 3\mathrm{SAT}$ מוכיח ש-3SAT קשה, לא ש-SAT קלה. הכיוון ההפוך ($3\mathrm{SAT} \le_p \mathrm{SAT}$) הוא הטריוויאלי ומוכיח רק ש-3SAT ב-NP.

לשכוח לחסום את אורך הפלט. בכל ניתוח סיבוכיות של רדוקציה או הרכבת רדוקציות צריך $|f(x)| \le P(|x|) + |x|$; בלעדיו ההרכבה של הפולינומים אינה מוצדקת.

להתעלם מקלט לא תקין. הרדוקציה היא פונקציה על כל Σ^*; יש להגדיר פלט קבוע ובלתי-ספיק לקלט פסול.

צ'ק-ליסט — אחרי השיעור אני יודע:

- [ ] להגדיר CNF, 3CNF, השמה, ספיקות, SAT, 3SAT, NP-קשה, NP-שלמה.
- [ ] לתאר את אלגוריתם הפיצול ולהריץ אותו על נוסחה קונקרטית עד לפלט 3CNF.

- [ ] להוכיח את שני כיווני הנכונות של צעד הפיצול, בפירוט מקרים מלא.
- [ ] לנתח את זמן הריצה ואת גודל הפלט של הרדוקציה ולהסביר מדוע הוא פולינומי.
- [ ] להסביר מדוע נדרש משתנה **חדש** ולתת דוגמה נגדית לגרסה שחוסכת.
- [ ] להוכיח $\mathrm{NP} \subseteq \mathrm{PSPACE}$ וסגירות תחת $\leq_p$, ולנסח את משמעות NP-שלמות.
- [ ] לקודד אילוצים פשוטים ("לפחות אחד", "לכל היותר אחד", "בדיוק אחד") כנוסחת CNF — הכנה ישירה למשפט קוק–לוין.

שאלות שנשארו פתוחות

לא קיימת בקורפוס הקלטה של השיעור הזה: נבדקו כל 30 הקבצים, ואף אחד מהם אינו מכיל את הבנייה SAT ≤p 3SAT; ככל הנראה החומר ניתן ללימוד עצמי.

כל ליבת השיעור — הבנייה, ההוכחה הדו-כיוונית וניתוח הגודל — נשענת על הסיכום הכתוב בלבד, ללא מקור שני להצלבה.

עמוד 8 בסיכום: הנוסחה C (אילוץ העמודות בבעיית 8 המלכות) נכתבה כמעט זהה ל-B; כאן נכתבה הגרסה המתוקנת שבה תפקידי i ו-j מוחלפים.

עמוד 7 בסיכום: החסם |φ̂| ≤ 2|φ| — ספירת מופעי ליטרלים מדויקת נותנת 3|φ|; האסימפטוטיקה זהה ולכן $O(|\varphi|^2)$ נשמר.

עמודים 5–6 בסיכום: המקרה השני בכיוון 'φ ספיקה ⟸ φ̂ ספיקה' נכתב כ'באופן דומה'; הפירוט כאן הוא השלמה שלי.

בסיכום 3CNF מוגדרת כ'לכל היותר 3 ליטרלים בכל פסוקית'; הווריאנט 'בדיוק 3' טופל כאן בנפרד ואינו מופיע במקור.

9 משפט קוק–לוין

השיעור מוכיח את משפט קוק–לוין: SAT היא NP-שלמה, על ידי קידוד טבלת החישוב של מוודא פולינומי כלשהו כנוסחת CNF שבה כל בדיקה היא מקומית — חלון בגודל 2×3.

ביטחון: high

בקצרה

השיעור מוכיח את **משפט קוק–לוין**: SAT היא NP-complete. זו הבעיה ה-NP-שלמה הראשונה, וממנה נגזרות כל האחרות ברדוקציות.

מה שצריך להראות הוא: **לכל** שפה $A \in \mathrm{NP}$ קיימת רדוקציית זמן פולינומי $A \le_p \mathrm{SAT}$. שימו לב לסדר הכמתים — לא "יש רדוקציה אחת שטובה לכל השפות", אלא לכל שפה רדוקציה משלה.

הקושי: על A לא ידוע דבר מלבד היותה ב-NP. כל מה שיש ביד הוא מכונה מוודאת M, פולינומים p, q, והקלט x עצמו. את העד w **אין** ביד — ובדיוק את אי-הידיעה הזאת אנחנו הופכים לחופש של ההשמה.

הרעיון: לקודד את **טבלת החישוב** (tableau) של M על (x, w) — כל שורה היא קונפיגורציה שלמה, שורה לכל צעד זמן — במשתנים בוליאניים $x_{i,j,s}$, ולבנות נוסחת CNF שנוסחה $\varphi = \varphi_{table} \wedge \varphi_{start} \wedge \varphi_{accept} \wedge \varphi_{move}$ שספיקה אם ורק אם קיים w שעליו M מקבלת.

ליבת ההוכחה: קידוד נאיבי של "שורה $i+1$ נובעת משורה i" דורש מספר **מעריכי** של גרירות (מילויים אפשריים לשורה, $|L|^{2r(n)+1}$). המוצא הוא **לוקליות** החישוב במכונת טיורינג: בין שתי שורות עוקבות משתנים לכל היותר שלושה תאים סמוכים, ולכן די לבדוק שכל **חלון 2×3** בטבלה חוקי — בדיקה מקומית שכופה נכונות גלובלית.

חשבון הגודל: $O(r(|x|)^2)$ משתנים ו-$O(r(|x|)^2)$ פסוקיות עד לקבועים התלויים רק ב-M, כאשר $r(n) = p(n + q(n))$ — כלומר פולינומי ב-$|x|$, ולכן הרדוקציה רצה בזמן פולינומי.

שני הרעיונות שכדאי לקחת מהשיעור, גם מעבר למבחן [01:14:55]: מידול בעיה כנוסחת CNF, והחלפת גרירה גלובלית בבדיקה מקומית בגודל קבוע.

רקע ותלויות

הקובץ הזה נשען על ארבעה דברים שכבר נלמדו; כדי לא לשלוח אתכם אחורה, כולם מנוסחים כאן במלואם.

1. מודל המכונה (ראו שיעור 4). מכונת טיורינג דטרמיניסטית היא $M = (Q, q_{start}, F, \Sigma, \Gamma, \delta)$ כאשר Q קבוצת המצבים, $q_{start} \in Q$ מצב ההתחלה, $F \subseteq Q$ המצבים המקבלים (נסמן ב-q_{accept} את המצב המקבל, וניתן להניח שהוא יחיד), Σ אלפבית הקלט, $\Gamma \supseteq \Sigma \cup \{B\}$ אלפבית הסרט הכולל את הסימן הריק B, ו-$\delta : Q \times \Gamma \to Q \times \Gamma \times \{L, R\}$ פונקציית המעברים. נסמן ב-$\mathrm{time}_M(a)$ את מספר הצעדים של M על הקלט a, וב-$\mathrm{space}_M(a)$ את מספר התאים בהם ביקרה.

הערה: גם הסיכום וגם ההרצה אינם רושמים את החמישייה/השישייה במפורש בשיעור הזה. רשמנו אותה כאן עם q_{start} בפנים, כי q_{start} מופיע בנוסחה φ_{start} ואי אפשר בלעדיו.

2. ההגדרה של NP דרך מוודא (ראו שיעור 6). $A \in \mathrm{NP}$ אם ורק אם קיימת מכונת טיורינג דטרמיניסטית M וקיימים פולינומים p, q כך ש:
לכל קלט a מתקיים $\mathrm{time}_M(a) \leq p(|a|)$;
לכל x: $x \in A \iff \exists w \in \{0,1\}^{q(|x|)}$ כך ש-M מקבלת את (x, w).
זו בדיוק נקודת הפתיחה של ההוכחה. המרצה מדגיש [00:04:15] שאפשר היה לעבוד גם עם ההגדרה דרך מכונה **אי-דטרמיניסטית**, וההוכחה דומה מאוד; בחרנו בדטרמיניסטית כי "אני יודע בכל צעד מה קורה בצעד הבא", וזה בדיוק מה שמאפשר את טיעון הדומינו בכיוון השני של ההוכחה.

3. רדוקציית זמן פולינומי, NP-קושי ו-NP-שלמות (ראו שיעור 7). $A \leq_p B$ פירושו: קיימת פונקציה f הניתנת לחישוב בזמן פולינומי כך שלכל x מתקיים $x \in A \iff f(x) \in B$. **כיוון החץ:** $A \leq_p B$ אומר ש-B **קשה לפחות כמו** A — כלומר B הוא הבעיה הקשה. בהקלטה, כמו בכל דיבור חופשי, הכיוון מתהפך לפעמים; החץ הוא הקובע.
B היא **NP-hard** אם לכל $A \in \mathrm{NP}$ מתקיים $A \leq_p B$. B היא **NP-complete** אם בנוסף $B \in \mathrm{NP}$.

4. SAT ונוסחאות CNF (ראו שיעור 7). SAT היא שפת נוסחאות הפסוקים הספיקות; אנחנו נבנה כאן נוסחת CNF, כלומר קוניונקציה של פסוקיות (דיסיונקציות של ליטרלים). הראנו כבר ש-$\mathrm{SAT} \in \mathrm{NP}$: העד הוא ההשמה עצמה, אורכה לינארי בגודל הנוסחה, ובדיקת ההשמה היא לינארית.

5. בעיית שמונה המלכות (ראו שיעור 7). המרצה חוזר אליה שוב ושוב [00:09:27], [00:20:03] וקורא לה "משפט קוק–לוין בקטן": לקחנו לוח שחמט, הגדרנו משתנה בוליאני לכל משבצת ("יש מלכה / אין מלכה"), וכתבנו שלוש תת-נוסחאות — לשורות, לעמודות ולאלכסונים — וחיברנו ב-$\wedge$. כאן נעשה בדיוק את אותו הדבר, רק עם עוד אינדקסים ועם ארבע תת-נוסחאות במקום שלוש. שווה לרענן אותה לפני שקוראים הלאה.

נקודת מפתח מתודית מההרצה [00:05:19]–[00:06:52]. לפני שבונים משהו, כדאי לשאול שאלה **תחבירית**: מי המשתנים שיש לי ביד? הכלל ש"קיים מביא לי משתנים, ולכל מוחק אותם בסוף הסקופ" (כמו פתיחת בלוק בקוד) נותן: יש לי את M, את p, את q — ובזמן ריצת הרדוקציה גם את x, כי הרדוקציה מקבלת את x כקלט. **אין** לי את w, כי הוא נמצא בתוך "לכל x" שנסגר. כל הבנייה שלהלן מקפידה על הכלל הזה, ואפשר לבדוק אותה בכל שלב בשאלה "האם השתמשתי כרגע רק במה שיש לי ביד?".

הגדרות

הגדרה 1: קידוד קונפיגורציה כשורה אחת

ניסוח. תהי M מכונת טיורינג בקונפיגורציה שבה תוכן הסרט הוא $\gamma_1\gamma_2\cdots\gamma_m$, המצב הוא q והראש מצביע על התא k. נקודד את הקונפיגורציה כמחרוזת אחת מעל האלפבית $\Gamma \cup Q$:
$\gamma_1 \cdots \gamma_{k-1}\, q\, \gamma_k\, \gamma_{k+1} \cdots \gamma_m$ כלומר: **סימן המצב נדחף לתוך המחרוזת מיד לפני התא שהראש קורא.**

אינטואיציה. בשיעורים על חישוביות ציירנו את הסרט, סימנו את מיקום הראש במשולש קטן, ורשמנו את המצב **מחוץ** לסרט [00:10:29]. עכשיו אנחנו רוצים הכול על מחרוזת אחת, כי מחרוזת אחת אפשר לשים בשורה של טבלה. אז במקום המשולש והמצב שבחוץ, אנחנו "מסכמים" ששם המצב שנכתב בתוך המחרוזת מסמן גם את המצב וגם את מיקום הראש: הראש עומד על התו שמימין לו. שימו לב שהקידוד מאריך את המחרוזת בתא אחד ביחס לסרט — זהו ה-$+1$ שיופיע ברוחב הטבלה.

דוגמה (מהלוח, עמוד 1 בסיכום). סרט $B\ B\ 0\ 1\ 0\ B\ B$, הראש על ה-1, המצב q_1. הקידוד: $B\ B\ 0\ q_1\ 1\ 0\ B\ B$ נניח $\delta(q_1,1)=(q_3,0,R)$: המכונה כותבת 0 במקום ה-1 וזזה ימינה. הקונפיגורציה הבאה מקודדת כ- $B\ B\ 0\ 0\ q_3\ 0\ B\ B$ כלומר שני התאים ששינו את תוכנם הם התא של המצב והתא שמימינו — הם התחלפו: $(q_1,1)\rightsquigarrow(0,q_3)$.

דוגמה נגדית (מה זה לא). המחרוזת $B\ B\ q_1\ 0\ q_3\ B$ **אינה** קידוד של קונפיגורציה: מופיעים בה שני סימני מצב, ולקונפיגורציה יש מצב אחד ומיקום ראש אחד. גם המחרוזת $B\ B\ 0\ 1\ B$ (בלי אף סימן מצב) אינה קידוד חוקי. שתי הפסילות האלה הן בדיוק מה ש-φ_{table} ו-φ_{start} יצטרכו לדאוג לו.

הגדרה 2: טבלת החישוב (tableau)

ניסוח. בהינתן M וקלט a, טבלת החישוב היא מטריצה שבה השורה ה-i היא הקידוד (לפי הגדרה 1) של הקונפיגורציה של M על a אחרי $i-1$ צעדים. שורה 1 היא הקונפיגורציה ההתחלתית.

אינטואיציה. זה בדיוק מה שכתבתם במחברת כשלמדתם מכונות טיורינג: ציירתם את הסרט, הזזתם את הראש, מחקתם, כתבתם — ושרטטתם את הסרט מחדש [00:09:57]. הטבלה היא פשוט כל השרטוטים האלה זה מתחת לזה. היא מכילה את **כל** האינפורמציה על הריצה: תוכן הסרט, מיקום הראש והמצב בכל רגע [00:08:56] — ולכן אפשר לבחון בעזרתה אם הריצה היא ריצה חוקית ומקבלת. חשוב: אלה **לא** כל הקונפיגורציות האפשריות, אלא רק אלה שהריצה באמת עברה דרכן [00:10:29].

המידות. נניח $A\in\mathrm{NP}$ עם M,p,q כלעיל, ויהי x קלט באורך $n=|x|$. הקלט של M הוא (x,w) שאורכו $n+q(n)$, ולכן מספר הצעדים חסום ב-$p(n+q(n))$. נסמן $r(n)=p\big(n+q(n)\big)$ ואז:

מספר השורות בטבלה הוא $r(n)$ — שורה לכל צעד זמן [00:13:43].

מספר העמודות הוא $2r(n)+1$. למה פעמיים? [00:15:18]–[00:15:49] הזמן חוסם את המקום, ולכן הראש לא מתרחק יותר מ-$r(n)$ תאים מנקודת ההתחלה — אבל **אינני יודע מראש לאיזה כיוון הוא ילך**, ולכן אני שומר $r(n)$ תאים שמאלה ו-$r(n)$ ימינה. ה-$+1$ הוא התא שבו נכתב סימן המצב [00:17:59].

מסקנה: הראש מתחיל בעמודה $r(n)+1$, מבצע לכל היותר $r(n)-1$ צעדים, ולכן **סימן המצב תמיד נמצא בעמודה k עם $2\le k\le 2r(n)$** — לעולם לא בעמודות הקצה. זו עובדה שנשתמש בה בהוכחת הלמה המרכזית.

הערה חשובה — הטבלה דמיונית. המרצה חוזר על כך חמש פעמים לפחות [00:16:25], [00:18:31], [00:32:31]: הרדוקציה **לא** בונה את הטבלה ולא ממלאת אותה, כי כדי למלא אותה היה צריך את w ואת w אין לנו. הטבלה היא אובייקט שאנחנו חושבים עליו כדי לכתוב את הנוסחה; הרדוקציה כותבת רק נוסחה.

הגדרה 3: האלפבית L והמשתנים $x_{i,j,s}$
ניסוח. נסמן $L = \Gamma_M \cup \{0,1\} \cup Q_M$ — קבוצת כל הסימנים שיכולים להופיע בתא של הטבלה [00:21:07]. (הסימנים $0, 1$ מופיעים במפורש כי הם התווים של העד w; אם $\{0,1\} \subseteq \Gamma_M$ האיחוד מיותר, ואינו מזיק.) שימו לב ש-$|L|$ תלוי **רק ב-**M ולא ב-x.
יהי $x = a_1 a_2 \cdots a_n$. לכל $1 \leq i \leq r(n)$ — אינדקס השורה, כלומר צעד הזמן — ולכל $1 \leq j \leq 2r(n)+1$ — אינדקס העמודה, כלומר התא — ולכל $s \in L$, נגדיר **משתנה בוליאני יחיד** $x_{i,j,s}$.
אינטואיציה — וזו הנקודה שבה נופלים. תחבירית, $x_{i,j,s}$ הוא פשוט משתנה. אין לו "משמעות"; שלושת האינדקסים הם רק שם, בדיוק כמו שאפשר לכתוב סכום עם שלושה אינדקסים [00:23:17]. סמנטית, כשתגיע השמה v, נחשוב על $v(x_{i,j,s}) = 1$ כאילו היא אומרת: **"בתא (i,j) של הטבלה כתוב הסימן s"** [00:24:19]. שאלת סטודנט בהרצה [00:23:47] — "מה זה s?" — קיבלה תשובה בשני שלבים, ושווה לזכור את שניהם: פורמלית אין מה להסביר, זה אינדקס רץ על L; אינטואיטיבית זה הסימן שנטען שכתוב בתא.
מה עוד לא נאמר. כרגע ההשמה יכולה לתת 1 גם ל-$x_{i,j,s}$ וגם ל-$x_{i,j,t}$ עם $s \neq t$ — כלומר "בתא כתובים שני סימנים" [00:24:52]. שום דבר עדיין לא אוסר את זה. בדיוק בשביל זה קיימת φ_{table}.
דוגמה. בטבלה של הדוגמה מסעיף "דוגמאות ותרגילים" למטה, בתא $(1,4)$ כתוב q_{start}; כלומר בהשמה המתאימה $v(x_{1,4,q_{start}}) = 1$ ו-$v(x_{1,4,s}) = 0$ לכל $s \neq q_{start}$.
הגדרה 4: חלון 2×3 וחלון חוקי
ניסוח. חלון בטבלה הוא תת-מטריצה של שתי שורות סמוכות ושלוש עמודות סמוכות. **מאנדקסים חלון לפי התא השמאלי-עליון שלו** [01:05:18]: החלון (i,j) מורכב מהתאים (i,j) $(i,j+1)$ $(i,j+2)$ $(i+1,j)$ $(i+1,j+1)$ $(i+1,j+2)$ ותכולתו היא שישייה $(a_1,a_2,a_3,a_4,a_5,a_6) \in L^6$ לפי הסדר

a_1	a_2	a_3
a_4	a_5	a_6

שישייה נקראת **חוקית** אם קיימת ריצה כלשהי של M שבתיאור הטבלאי שלה מופיע חלון כזה [00:57:01]. שקול ומעשי יותר: השישייה חוקית אם ורק אם היא נובעת מ-δ — כלומר קיימות קונפיגורציה C ועוקבתה $C' = \delta(C)$ ומיקום עמודה שבו החלון של שתי השורות המקודדות הוא בדיוק השישייה — **או** שהיא העתקה של שורה שמכילה מצב סופי [01:03:44]. נסמן את קבוצת השישיות החוקיות $\mathrm{Legal}(M) \subseteq L^6$.
אינטואיציה. "חלון חוקי" הוא בדיקת שפיות מקומית: האם מה שרואים דרך חור המנעול הזה יכול היה לקרות במכונה M? התשובה תלויה **רק ב-**δ, כלומר רק ב-M, ולא ב-x, ולא ב-n [01:06:22]. לכן אפשר לחשב את $\mathrm{Legal}(M)$ פעם אחת, עוד לפני שראינו את הקלט, על ידי מעבר על כל $|L|^6$ השישיות.
כמה שישיות ישנן? $|L|^6$ — לא $\binom{|L|}{6}$. הסטודנט בהרצה ניחש "L מעל 6" ותוקן [00:58:38]: השישיות **אינן חייבות** להיות מורכבות מסימנים שונים, ולכן זהו $|L| \cdot |L| \cdots |L|$ שש פעמים. חשוב לא להתבלבל בבסיס ובמעריך.

כלל הריפוד (התוספת "העתקה של מצב סופי"). חסם הזמן p הוא חסם **מלמעלה**; אף אחד לא הבטיח שהמכונה תרוץ בדיוק $r(n)$ צעדים [01:03:12]. אם המכונה עצרה במצב מקבל אחרי $t < r(n)$ צעדים, אין לנו שורות להמשיך איתן. הפתרון: מכריזים שהעתקה מדויקת של שורה שמכילה q_{accept} היא מעבר חוקי, וממלאים את שאר הטבלה באותה שורה שוב ושוב. המרצה מלווה את זה בבדיחה על ההוכחה של איש מדעי המחשב ש"כל האי-זוגיים ראשוניים": 3 ראשוני, 5 ראשוני, 7 ראשוני, 7 ראשוני, 7 ראשוני… [01:04:15]. זה בדיוק מה שקורה כאן, וכאן זה חוקי.

> **הערה:** בהרצה נאמר כלל הריפוד רק עבור q_{accept}. אם המכונה עוצרת במצב דוחה לפני הזמן, אין שישייה חוקית שממשיכה את השורה ולכן φ_{move} לא תסופק — וזה בסדר גמור, כי במקרה כזה אנחנו ממילא רוצים ש-φ תהיה לא-ספיקה. אפשר גם להרחיב את כלל הריפוד לכל מצב עוצר; אז φ_{move} תסופק אבל φ_{accept} לא, והמסקנה זהה.

דוגמה נגדית לחוקיות. אם M אף פעם לא זזה שמאלה, אז החלון $\begin{array}{|c|c|c|}\hline 0 & q_1 & 1 \\ \hline q_3 & 0 & 1 \\ \hline \end{array}$ אינו חוקי: סימן המצב בשורה התחתונה נמצא שמאלה מהמקום שבו היה, כלומר הראש זז שמאלה [01:02:11].

משפטים והוכחות

משפט 1: משפט קוק–לוין

SAT היא NP-complete. כלומר: (א) $\mathrm{SAT} \in \mathrm{NP}$, ו-(ב) לכל $A \in \mathrm{NP}$ מתקיים $A \leq_p \mathrm{SAT}$.

סדר הכמתים — אזהרה מפורשת מההרצה [00:01:08]. הטענה היא "**לכל** שפה ב-NP **קיימת** רדוקציה ל-SAT", ולא "קיימת רדוקציה שמתאימה לכל השפות". לכל שפה תהיה רדוקציה משלה, שנבנית מהמוודא הספציפי שלה. זה מקור נפוץ מאוד לשגיאה בניסוח.

חלק (א): $\mathrm{SAT} \in \mathrm{NP}$

בהינתן נוסחה ψ מעל m משתנים, העד הוא ההשמה המספקת $v \in \{0,1\}^m$. אורכה $m \leq |\psi|$, כלומר פולינומי (אפילו לינארי) בגודל הקלט; ובדיקה שההשמה מספקת נעשית במעבר אחד על הנוסחה, בזמן $O(|\psi|)$. לכן $\mathrm{SAT} \in \mathrm{NP}$. זה הוכח כבר בשיעור 7 והובא כאן כדי לסגור את הטענה; הסיכום עוצר בסוף עמוד 3 על "SAT היא NP-קשה" ואינו חוזר על החלק הזה.

חלק (ב): הבנייה

תהי $A \in \mathrm{NP}$. לפי ההגדרה יש בידינו M, p ו-q המקיימים את שני התנאים מסעיף "רקע ותלויות". נסמן $n = |x|$, $L = \Gamma_M \cup \{0,1\} \cup Q_M$, $r(n) = p(n + q(n))$, ונשתמש במשתנים $x_{i,j,s}$ של הגדרה 3. נבנה $\varphi = \varphi_{table} \wedge \varphi_{start} \wedge \varphi_{accept} \wedge \varphi_{move}$

הרעיון המנחה, שכדאי להחזיק בראש לכל אורך הבנייה [00:07:56]: "$x \in A$**" פירושו "**קיים** w", ו"φ ספיקה" פירושו "**קיימת** השמה". אנחנו רוצים לגרור את הכמת הקיומי הזה מצד אחד לצד השני. כל ארבע התת-נוסחאות נועדו לוודא שהחופש היחיד שנשאר להשמה הוא בדיוק החופש בבחירת w.

φ_{table} — בכל תא בדיוק סימן אחד

$$\varphi_{table} = \bigwedge_{\substack{1 \le i \le r(n) \\ 1 \le j \le 2r(n)+1}} \left(\left(\bigvee_{s \in L} x_{i,j,s} \right) \wedge \left(\bigwedge_{\substack{s,t \in L \\ s \neq t}} \left(\overline{x_{i,j,s}} \vee \overline{x_{i,j,t}} \right) \right) \right)$$

מה זה אוכף ולמה. הקוניונקציה החיצונית רצה על כל תא בטבלה. עבור תא נתון: הפסוקית הראשונה, $\bigvee_{s\in L} x_{i,j,s}$, אומרת ש**לפחות אחד** מהסימנים מקבל אמת בתא הזה. היא לבדה לא מספיקה — היא לא אוסרת שניים [00:29:23]. לכן באה הקבוצה השנייה של פסוקיות: לכל זוג סימנים שונים $s \neq t$, הפסוקית $\overline{x_{i,j,s}} \vee \overline{x_{i,j,t}}$ אומרת שלא ייתכן ששניהם אמת — כלומר **לכל היותר אחד**. יחד: בדיוק אחד. זו בדיוק אותה תבנית "בחר בדיוק אחד מבין k" שראינו בבעיית המלכות [00:29:55].
למה בכלל צריך את זה? שאלת סטודנטית בהרצה [00:34:09]: למה אסור שיהיו שניים? כי אני רוצה **טבלה** שמתארת סרט של מכונה, ובכל תא בסרט של מכונת טיורינג רשום בדיוק תו אחד, ובכל קונפיגורציה יש בדיוק מצב אחד. בלי האילוץ הזה, "הטבלה" שההשמה מתארת אינה טבלה בכלל.
טענה 1.1. לכל השמה v המספקת את φ_{table}, ולכל i, j, קיים $s \in L$ **יחיד** כך ש-$v(x_{i,j,s}) = 1$.
ולהפך: לכל מילוי של הטבלה בסימנים מ-L קיימת השמה המספקת את φ_{table} ומתאימה לו.
הוכחה. כיוון ראשון: φ_{table} היא קוניונקציה, ולכן השמה מספקת מספקת כל אחד מהאיברים; נקבע i, j. האיבר המתאים הוא עצמו קוניונקציה של שני חלקים. מהחלק הראשון, $\bigvee_s x_{i,j,s} = 1$, נובע שקיים s עם $v(x_{i,j,s}) = 1$. מהחלק השני, לכל $s \neq t$ מתקיים $\overline{x_{i,j,s}} \vee \overline{x_{i,j,t}} = 1$, כלומר לא ייתכן ש-$v(x_{i,j,s}) = v(x_{i,j,t}) = 1$. ביחד: קיים ואין שניים, כלומר קיים יחיד [00:33:04]–[00:33:35].
כיוון שני: בהינתן מילוי $T : \{1..r(n)\} \times \{1..2r(n)+1\} \to L$, נגדיר $v(x_{i,j,s}) = 1$ אם ורק אם $T(i,j) = s$. כל פסוקית מהצורה $\bigvee_s x_{i,j,s}$ מסופקת (על ידי $s = T(i,j)$), וכל פסוקית $\overline{x_{i,j,s}} \vee \overline{x_{i,j,t}}$ מסופקת כי לכל היותר אחד מבין s, t שווה ל-$T(i,j)$. $\square$

> **הערה:** בהרצה הכיוון השני נאמר במשפט אחד — "ודרך אגב גם הפוך" [00:34:09] — ומיד אחריו הובהר למה הוא חשוב: "להפך חשוב בגלל הכיוון השני של הרדוקציה" [00:35:46]. בלי הכיוון השני אי אפשר להסיק מ"$x \in A$" ש-φ ספיקה, כי צריך להמיר טבלה אמיתית להשמה. הפירוט לעיל הוא מה שההערה הזאת מייצגת.

חשוב מה φ_{table} לא אומרת [00:32:01]: היא מבטיחה טבלה — אבל טבלה של ג'יברish. שום דבר בה לא קושר את הטבלה למכונה M או לקלט x. את זה עושות שלוש הנוסחאות הבאות.
φ_{start} — השורה הראשונה היא הקונפיגורציה ההתחלתית
יהי $x = a_1 \cdots a_n$. אז $\varphi_{start} = \underbrace{x_{1,1,B} \wedge x_{1,2,B} \wedge \cdots \wedge x_{1,r(n),B}}_{\text{blanks}} \wedge x_{1,r(n)+1,q_{start}} \wedge \underbrace{x_{1,r(n)+2,a_1} \wedge \cdots \wedge x_{1,r(n)+n+1,a_n}}_{x} \wedge \underbrace{\big(x_{1,r(n)+n+2,0} \vee x_{1,r(n)+n+2,1}\big) \wedge \cdots \wedge \big(x_{1,r(n)+n+1+q(n),0} \vee x_{1,r(n)+n+1+q(n),1}\big)}_{w} \wedge \underbrace{x_{1,r(n)+n+2+q(n),B} \wedge \cdots \wedge x_{1,2r(n)+1,B}}_{\text{blanks}}$
מה זה אוכף ולמה. בשורה 1 אני יודע **כל** תו — חוץ מ-w [00:36:22]:
העמודות $1..r(n)$: תאים ריקים. אלה ה-$r(n)$ תאים שמשמאל לראש, השמורים למקרה שהראש ילך שמאלה [00:37:56].
עמודה $r(n)+1$: q_{start} — כאן מתחיל הראש.

עמודות $r(n)+2$ עד $r(n)+n+1$: הקלט x, תו אחר תו.
עמודות $r(n)+n+2$ עד $r(n)+n+1+q(n)$: העד w. כאן **איני יודע** מה כתוב, אבל אני כן יודע שני דברים: את **האורך** ואת זה שכל תא הוא 0 או 1 [00:39:31]. לכן במקום ליטרל יחיד יש פה פסוקית $(\cdot \vee \cdot)$.
שאר העמודות עד $2r(n)+1$: תאים ריקים.
זו הנקודה שבה נכנס החופש. כל שאר הקוניונקציות הן ליטרלים יחידים ולכן כופות ערך; רק בתאי w יש בחירה. לכן להשמה המספקת את φ_{start} יש בדיוק $q(n)$ ביטי חופש, והם מתאימים אחד לאחד לתווי w [00:43:23]. המרצה מדגיש: "זה החופש שאני רוצה, כי אני רוצה לקשר בין 'קיים w' ל'קיימת השמה'".
מה נדרש כדי לבנות אותה? [00:42:18] את x עצמו (בשביל $a_1..a_n$), את n, ואת הפולינומים r ו-q. הכול ביד. שימו לב לניואנס שהמרצה מדגיש כבדיקת שפיות: ב-φ_{table} השתמשנו רק ב-$n=|x|$ ולא ב-x עצמו; כאן אנחנו באמת צריכים את x עצמו.
שאלה מהכיתה [01:03:12] סביב אילוץ המצב: למה φ_{start} לא צריכה לומר גם "אין מצב אחר בשורה הראשונה"? כי φ_{table} כבר אומרת שבכל תא כתוב בדיוק סימן אחד, וכל עמודה בשורה 1 קיבלה כאן ערך מפורש. עקרון העבודה הוא: כל תת-נוסחה עומדת בפני עצמה ודורשת רק את מה שהיא צריכה; העיקר שהן לא סותרות זו את זו [00:45:01].
φ_{accept} — איפשהו בטבלה יש מצב מקבל

$$\varphi_{accept}=\bigvee_{\substack{1\le i\le r(n)\\ 1\le j\le 2r(n)+1}} x_{i,j,q_{accept}}$$

מה זה אוכף ולמה. זו פסוקית אחת ארוכה: קיים תא בטבלה שכתוב בו q_{accept}. זה הכול [00:44:30].
שתי הערות דקות.
אין צורך לדרוש יחידות — "בתא שכתוב בו q_{accept} לא כתוב שום דבר אחר" מובטח כבר על ידי φ_{table} [00:45:31].
מותר שיופיעו כמה תאים עם q_{accept}, ואף שכיח שכן: בגלל כלל הריפוד, ברגע שהגענו למצב מקבל אנחנו מעתיקים את השורה עד סוף הטבלה, ולכן q_{accept} יופיע בכל שורה משם והלאה. יחידות נדרשת ברמת התא, לא ברמת הטבלה.
φ_{move} — הלב של ההוכחה
קודם: למה הקידוד הנאיבי נכשל. [00:48:06]–[00:50:11] אינטואיטיבית אני רוצה לומר: "אם השורה הראשונה מולאה כך — אז השורה השנייה מולאה כך". גרירות אינן מפחידות אותנו, כי $\alpha \to \beta$ שקול ל-$\overline{\alpha} \vee \beta$ ולכן ניתן להמרה ל-CNF. הבעיה היא **הכמות**: כמה מילויים אפשריים יש לשורה אחת? לכל תא יש $|L|$ אפשרויות ויש $2r(n)+1$ תאים, כלומר $|L|^{2r(n)+1}$ מילויים. (הסטודנט שניחש "גודל שורה עצרת" תוקן: זו חזקה, לא עצרת [00:49:08].) אני לא יודע מראש איזו שורה תתקבל — כי אני לא יודע מה w — ולכן אצטרך גרירה לכל מילוי אפשרי: **מספר מעריכי** של תת-נוסחאות. הנוסחה שלי חייבת להיות פולינומית ב-n. אז זה נופל.
המוצא: לוקליות. [00:50:11]–[00:51:15] "היופי של ההוכחה, והיופי של המודל הזה" — החישוב במכונת טיורינג הוא **מקומי מאוד**. במעבר משורה לשורה הבאה, רוב מוחלט של התאים **לא משתנים**; המקומות היחידים שיכולים להשתנות הם התא של סימן המצב ותא אחד ימינה או שמאלה

ממנו. לכן אין צורך לגרור שורה שלמה על שורה שלמה — מספיק לעבור על **חלונות** 2×3 ולוודא שכולם חוקיים. זו בדיוק הסיבה שבגללה צריך מודל חישוב "פרימיטיבי אבל מדויק" כמו מכונת טיורינג [00:46:33].

הנוסחה. $\varphi_{move} = \bigwedge_{1 \le i \le r(n)-1} \bigwedge_{1 \le j \le 2r(n)-1} \Big[\bigwedge_{(a_1,\ldots,a_6) \notin \mathrm{Legal}(M)} \Big(\overline{x_{i,j,a_1}} \vee \overline{x_{i,j+1,a_2}} \vee \overline{x_{i,j+2,a_3}} \vee \overline{x_{i+1,j,a_4}} \vee \overline{x_{i+1,j+1,a_5}} \vee \overline{x_{i+1,j+2,a_6}} \Big) \Big]$

התחומים. [01:05:18]–[01:05:51] — זו הייתה שאלת סטודנטית והתשובה שווה זכירה. החלון מאונדקס לפי התא השמאלי-עליון שלו. התא השמאלי-עליון יכול להגיע לכל היותר עד **השורה שלפני האחרונה**, כי לחלון יש שתי שורות — ומכאן $i \le r(n) - 1$. הוא יכול להגיע לכל היותר עד **שתיים לפני העמודה האחרונה**, כי לחלון יש שלוש עמודות ומספר העמודות הוא $2r(n) + 1$ — ומכאן $j \le (2r(n)+1) - 2 = 2r(n) - 1$.

הצורה: מ-DNF ל-CNF. כפי שנכתבה, כל תת-נוסחה של חלון היא **דיסיונקציה של קוניונקציות**, כלומר DNF ולא CNF. יש לזה תיקון סטנדרטי ופשוט שכדאי להכיר, והוא גם מקצר את הנוסחה: **במקום למנות את השישיות החוקיות, אוסרים את הלא-חוקיות.** בהינתן φ_{table} (שמבטיחה סימן יחיד בכל תא), החלון (i,j) חוקי אם ורק אף שישייה לא-חוקית אינה מופיעה בו, ולכן אפשר לכתוב במקום זאת $\varphi'_{move} = \bigwedge_{\substack{1 \le i \le r(n)-1 \\ 1 \le j \le 2r(n)-1}} \bigwedge_{(a_1,\ldots,a_6) \notin \mathrm{Legal}(M)} \Big(\overline{x_{i,j,a_1}} \vee \overline{x_{i,j+1,a_2}} \vee \overline{x_{i,j+2,a_3}} \vee \overline{x_{i+1,j,a_4}} \vee \overline{x_{i+1,j+1,a_5}} \vee \overline{x_{i+1,j+2,a_6}} \Big)$ זו כבר CNF ישירה: לכל חלון לכל היותר $|L|^6$ פסוקיות, כל אחת בת 6 ליטרלים.

> **הערה:** בהרצה נאמר רק שהמרת גרירות ל-CNF "לא מפחידה" [00:48:37], והסיכום משאיר את φ_{move} בצורת DNF-לכל-חלון. הפירוט כאן הוא מה שההערה הזאת מייצגת. שתי הצורות שקולות מעל השמות המספקות את φ_{table}, ושתיהן פולינומיות; הצורה השנייה נוחה יותר כי היא CNF כפי שנדרש להגדרת SAT ולרדוקציה ל-$3\mathrm{SAT}$ בהמשך.

טענה 1.2 (למת הלוקליות) — למה בדיקה מקומית מספיקה

זו הטענה שבלעדיה ההוכחה חסרה, והמקום שבו סיכומים נוטים לדחוס הכי חזק.

ניסוח. תהי T טבלה (מילוי של L בכל תא), ונניח:

השורה הראשונה של T היא קידוד חוקי של הקונפיגורציה ההתחלתית של M על (x, w) עבור w כלשהו, כלומר סימן מצב יחיד בעמודה $r(n)+1$;

כל חלון 2×3 ב-T חוקי.

אז לכל i: השורה i היא קידוד חוקי של קונפיגורציה, והשורה $i+1$ היא הקידוד של **הקונפיגורציה העוקבת** לה (או העתקה שלה, אם היא מכילה מצב סופי).

הוכחה, באינדוקציה על i. בסיס: תנאי 1 נותן שהשורה הראשונה היא קידוד קונפיגורציה, עם סימן מצב יחיד בעמודה $k_1 = r(n)+1$.

צעד: נניח שהשורה i היא קידוד של קונפיגורציה C, שבה סימן המצב יושב בעמודה k. כפי שהראינו בהגדרה 2, $2 \le k \le 2r(n)$ — הראש לעולם אינו על עמודת קצה. נראה שהשורה $i+1$ נקבעת במלואה, והיא הקידוד של $\delta(C)$.

(א) תאים רחוקים מהראש נשמרים. יהי j עם $|j-k|\geq 2$. נתבונן בחלון $(i, j-1)$, שעמודותיו $j-1, j, j+1$. אף אחת מהן אינה k (כי $j-1=k$ היה מחייב $j=k+1$, ו-$j+1=k$ היה מחייב $j=k-1$; שניהם נשללו). לכן שורתו העליונה של החלון **אינה מכילה סימן מצב**. כל שישייה חוקית שהשורה העליונה שלה נטולת מצב מקיימת $a_5=a_2$, כלומר התא האמצעי אינו משתנה: הרי בשישייה חוקית נלקחת מעבר אמיתי של M; המעבר משנה רק את התא שתחת הראש ואת סימן המצב, שנשאר במרחק ≥ 1 מ-k, ולכן תא בעמודה j עם $|j-k|\geq 2$ אינו יכול לא לשנות את תוכנו ולא לקבל סימן מצב חדש (הראש בזמן $i+1$ נמצא בעמודה $k\pm 1$, שמרחקה מ-j הוא לפחות 1). מסקנה: $T(i+1,j)=T(i,j)$ — בדיוק כמו בקונפיגורציה העוקבת.

(ב) תאים ליד הראש נקבעים על ידי δ. נתבונן בחלון $(i, k-1)$ — הוא קיים בזכות $2\leq k\leq 2r(n)$. שורתו העליונה היא $(T(i,k-1),\ q,\ T(i,k+1))$, כלומר סימן המצב יושב **במרכז**. כיוון ש-M דטרמיניסטית, $\delta(q, T(i,k+1))$ קובע באופן יחיד מה תהיה שורת החלון התחתונה:

אם $\delta(q,\gamma)=(q',\gamma',R)$: $(T(i,k-1),\ q,\ \gamma)\ \rightsquigarrow\ (T(i,k-1),\ \gamma',\ q')$;

אם $\delta(q,\gamma)=(q',\gamma',L)$: $(c,\ q,\ \gamma)\ \rightsquigarrow\ (q',\ c,\ \gamma')$.

בשני המקרים כל שלושת התאים $k-1, k, k+1$ בשורה $i+1$ נקבעים במלואם, ובדיוק כמו בקונפיגורציה העוקבת. (המקרה של מצב סופי מטופל בכלל הריפוד: השורה מועתקת.)

(א) ו-(ב) יחד מכסים את כל העמודות, ולכן השורה $i+1$ שווה בדיוק לקידוד של $\delta(C)$ — ובפרט היא בעצמה קידוד חוקי של קונפיגורציה, מה שמאפשר את המשך האינדוקציה. $\square$

> **הערה:** הטיעון הזה נאמר בהרצה כאינטואיציה — "רוב התאים לא השתנו, המקום היחיד שהשתנה הוא ליד הראש" [00:50:42] — ובאמצעות דוגמאות על הלוח. הפירוט הפורמלי, כולל ההבחנה שהראש לעולם אינו על עמודת קצה (ולכן החלון $(i,k-1)$ תמיד קיים), הוא מה שההערה מייצגת.

למה דווקא 6 תאים? [00:58:07], [01:01:21] — תיאורטית אפשר היה חלון גדול יותר; אנחנו רוצים כמה שפחות, כי מספר הפסוקיות לחלון הוא $|L|$ בחזקת גודל החלון. פחות מ-3×2 **לא** יספיק: בצעד יחיד יכולים להשתנות עד שלושה תאים סמוכים (במעבר שמאלה: $k-1, k, k+1$), ולכן חלון 2×2 עלול לפספס שינוי. שש הוא בדיוק המינימום שמכסה את כל השינויים האפשריים.

חשבון הגודל — למה הרדוקציה פולינומית

זהו החלק שהופך את הבנייה לרדוקציה. נסמן $r=r(n)=p(n+q(n))$ — פולינום ב-n, כי הרכבה של פולינומים היא פולינום.

רכיב	ספירה	סדר גודל
משתנים	$r\cdot(2r+1)\cdot\lvert L\rvert$	$O(\lvert L\rvert\cdot r^2)$
φ_{table}	לכל תא: פסוקית אחת באורך $\lvert L\rvert$, ועוד $\binom{\lvert L\rvert}{2}$ פסוקיות באורך 2	$O(\lvert L\rvert^2\cdot r^2)$
φ_{start}	$2r+1$ קוניונקטים, כל אחד באורך ≤ 2	$O(r)$

רכיב	ספירה	סדר גודל
φ_{accept}	פסוקית אחת באורך $r \cdot (2r+1)$	$O(r^2)$
φ'_{move}	$(r-1)(2r-1)$ חלונות, לכל חלון $\leq \lvert L\rvert^6$ פסוקיות באורך 6	$O(\lvert L\rvert^6 \cdot r^2)$

המפתח: $\lvert L\rvert$ תלוי **רק ב-**M ולא ב-x ולא ב-n. לכן $\lvert L\rvert^6$ הוא גורם קבוע מבחינת גודל הקלט — הגם שהמרצה מסתייג מהמילה "קבוע" ומעדיף "לא תלוי ב-n" [01:07:23]. סך הכול $\lvert\varphi\rvert = O\big(r(\lvert x\rvert)^2\big)$. $n = \lvert x\rvert$ פולינומי ב-$O\big(r(n)^2\big) = O\big(p(n+q(n))^2\big)$, בדיוק כפי שנרשם בסיכום: **וגם זמן הבנייה פולינומי, לא רק הגודל.** [00:26:30] המכונה M_{CL} המבצעת את הרדוקציה מקבלת x ו:

מחשבת $n = \lvert x\rvert$ ואת $r(n) = p(n+q(n))$ — חישוב אריתמטי על פולינומים ידועים;

מחשבת פעם אחת את הטבלה של $\mathrm{Legal}(M)$ על ידי מעבר על כל $\lvert L\rvert^6$ השישיות ובדיקת כל אחת מול δ — עבודה שלא תלויה כלל ב-x [01:06:52];

פולטת את הפסוקיות של $\varphi_{table}, \varphi_{start}, \varphi_{accept}, \varphi'_{move}$ בלולאות על i, j;

מחזירה $\varphi = \varphi_{table} \wedge \varphi_{start} \wedge \varphi_{accept} \wedge \varphi_{move}$.

כל פסוקית נכתבת בזמן קבוע, ומספר הפסוקיות פולינומי, ולכן M_{CL} רצה בזמן פולינומי ב-$\lvert x\rvert$.

חזרה על מה שהמכונה כן ולא עושה [00:46:02]: M_{CL} **לא** מחפשת השמה, **לא** מנחשת את w, **לא** מריצה את M. היא רק כותבת נוסחה. כל הסמנטיקה — הטבלה, ההשמה, ה"מלכה נמצאת/לא נמצאת" — היא בראש שלנו בזמן שאנחנו מוכיחים נכונות.

כיוון 1: $x \in A \implies \varphi$ ספיקה

נניח $x \in A$. לפי הגדרת NP קיים $w \in \{0,1\}^{q(\lvert x\rvert)}$ כך ש-M מקבלת את (x, w), ומספר הצעדים חסום ב-$r(n)$.

נבנה טבלה T: השורה ה-i היא הקידוד של הקונפיגורציה של M על (x,w) אחרי $i-1$ צעדים, ואם הריצה עצרה במצב מקבל אחרי $t < r(n)$ צעדים — כל השורות שמעבר לכך הן העתק של השורה שבה הופיע q_{accept} (כלל הריפוד).

לפי טענה 1.1 (הכיוון השני) יש השמה v המתאימה למילוי הזה: $v(x_{i,j,s}) = 1 \iff T(i,j) = s$. נבדוק שהיא מספקת את כל ארבעת החלקים:

φ_{table}: מיידי מהבנייה של v — בכל תא בדיוק סימן אחד.

φ_{start}: השורה הראשונה של T היא הקונפיגורציה ההתחלתית: $r(n)$ תאים ריקים, q_{start}, אחריו x תו-תו, אחריו w תו-תו, אחריו תאים ריקים. הליטרלים היחידים מסופקים; ובכל אחת מהפסוקיות $\big(x_{1,j,0} \vee x_{1,j,1}\big)$ עבור $r(n)+n+2 \le j \le r(n)+n+1+q(n)$, בדיוק אחד משני הליטרלים מקבל אמת — זה שמתאים ל-$w_{j-(r(n)+n+1)}$ [01:10:46]–[01:11:48].

φ_{accept}: הריצה מקבלת, ולכן קיימת שורה שבה מופיע q_{accept}; התא הזה נותן ליטרל אמיתי בדיסיונקציה.

φ_{move}: כל חלון בטבלה נלקח משתי שורות עוקבות של ריצה אמיתית של M (או מזוג שורות זהות אחרי הקבלה), ולכן השישייה שבו חוקית לפי ההגדרה. לכן בכל חלון קיים איבר אחד בדיסיונקציה שמסופק.

לכן $\varphi \models v$, כלומר $\varphi \in \mathrm{SAT}$. $\square$

כיוון 2: $x \in A \implies$ ספיקה φ

נניח שקיימת השמה מספקת v עבור φ. נשחזר ממנה את w ואת הריצה.

שלב 1 — הטבלה מוגדרת היטב. v מספקת את φ_{table}, ולכן לפי טענה 1.1 לכל (i,j) יש סימן יחיד s עם $v(x_{i,j,s}) = 1$. נגדיר $T(i,j) = s$. קיבלנו טבלה.

שלב 2 — קריאת w. v מספקת את φ_{start}, ולכן השורה הראשונה של T היא: תאים ריקים, q_{start}, הקלט x, אחר כך $q(n)$ תאים שכל אחד מהם 0 או 1, ואז תאים ריקים. נגדיר $w_\ell =$ $w \in \{0,1\}^{q(|x|)}$ זהו $T\big(1,\ r(n)+n+1+\ell\big), \qquad \ell = 1, \ldots, q(n)$, מוגדר היטב [01:17:02]–[01:18:09]. זה בדיוק מה שמסתתר מאחורי המשפט "נתבונן ב-w לפי ערכי האמת למשתנים המתאימים" בעמוד 3 בסיכום.

שלב 3 — הטבלה מתארת את הריצה על (x,w). v מספקת את φ_{move}, ולכן כל חלון 2×3 ב-T חוקי. יחד עם העובדה ששורה 1 היא הקונפיגורציה ההתחלתית על (x,w), למת הלוקליות (טענה 1.2) נותנת באינדוקציה: לכל i, השורה $i+1$ היא הקונפיגורציה העוקבת לשורה i. כלומר T היא **בדיוק** טבלת החישוב של M על (x,w).

זהו טיעון הדומינו של ההרצה [01:16:30]: ברגע שקבעתי את w, הדטרמיניזם של M קובע את כל שאר הטבלה. "זה כמו אבן ראשונה של דומינו שמפילה את כל השאר." שימו לב שכאן נכנס לשימוש הדטרמיניזם — זו הסיבה שנוח לעבוד עם ההגדרה דרך מוודא דטרמיניסטי.

שלב 4 — הריצה מקבלת. v מספקת את φ_{accept}, ולכן קיים תא ב-T שבו כתוב q_{accept}. לפי שלב 3, T מתארת את הריצה האמיתית של M על (x,w), ולכן הריצה הזאת מגיעה למצב q_{accept} — כלומר M מקבלת את (x,w).

לכן קיים $w \in \{0,1\}^{q(|x|)}$ שעליו M מקבלת את (x,w), ומהגדרת NP נובע $x \in A$. $\square$

סיכום ההוכחה

$x \in A \iff \varphi = M_{CL}(x) \in \mathrm{SAT}$ רצה בזמן פולינומי ומקיימת M_{CL}, כלומר $A \le_p \mathrm{SAT}$.

זה נכון לכל $A \in \mathrm{NP}$, ולכן SAT היא NP-hard; יחד עם חלק (א), SAT היא NP-complete. $\blacksquare$

> **הערה על off-by-one:** מספר השורות שנקבע בסיכום הוא $r(n)$, אבל $r(n)$ שורות מתארות רק $r(n)-1$ **צעדים**, בעוד חסם הזמן מתיר $r(n)$ צעדים. התיקון הקל: לקחת $r(n)+1$ שורות (או להבחין ש-p תמיד ניתן להגדלה בקבוע). שום דבר בהוכחה לא משתנה — כל התחומים והחסמים נשארים באותו סדר גודל.

משפט 2 (מסקנה): $\mathrm{CNF\text{-}SAT}$ היא NP-complete, ובעקבותיה $\mathrm{3SAT}$

הנוסחה שבנינו (בצורת φ'_{move}) היא כבר CNF, ולכן ההוכחה מראה יותר: $\mathrm{CNF\text{-}SAT}$ **היא NP-hard**. מכאן, בעזרת הרדוקציה $\mathrm{SAT} \le_p \mathrm{3SAT}$ שראינו בשיעור 7 (פיצול פסוקיות ארוכות באמצעות משתנים חדשים), מקבלים ש-$\mathrm{3SAT}$ היא NP-complete.

זו נקודת המוצא לכל התחום: המרצה מציין [01:20:20] שאחרי המאמר של קוק ולוין בא **ריצ'רד קארפ** עם 21 בעיות אלגוריתמיות שהראה שכולן NP-שלמות — למשל $\mathrm{SAT} \le_p \mathrm{3SAT} \le_p \mathrm{IS} \le_p \mathrm{CLIQUE}$ — והיום ידועות אלפים.

דוגמאות ותרגילים מהשיעור

דוגמה 1: הקידוד של צעד יחיד (מהלוח, עמוד 1 בסיכום)

מכונה בקונפיגורציה: סרט $B\,B\,0\,1\,0\,B\,B$, ראש על ה-1, מצב q_1, ו-$\delta(q_1,1)=(q_3,0,R)$.

שורה i	B	B	0	q_1	1	0	$B\,B$
שורה $i+1$	B	B	0	q_3	0	0	$B\,B$

שאלת סטודנט בהרצה [00:12:07]: "אפשר להסביר את המעבר הזה?" התשובה: בשרטוט הרגיל הראש עמד על ה-1, כתב 0 וזז ימינה. בקידוד, המצב נרשם תמיד תא אחד לפני מה שהראש קורא — ולכן q_1 שישב לפני ה-1 מתחלף: התא שלו מקבל את הסימן שנכתב (0), והתא שמימינו מקבל את q_3, כי עכשיו הראש קורא את התא שאחריו.

דוגמה 2: הרדוקציה מקצה לקצה על אינסטנס קונקרטי

נקבע שפה, מוודא, וקלט — ונעקוב אחרי הרדוקציה בשני הכיוונים.

השפה. $A=\{x\in\{0,1\}^* : x \text{ contains at least one } 1\}$. זו כמובן שפה ב-P, אבל היא מוגדרת כאן דרך מוודא כדי שהבנייה תהיה מוחשית.

המוודא. $q(n)=n$; העד $w\in\{0,1\}^n$ אמור להצביע על מיקום של 1 בקלט. M מקבלת קלט (x,w) הכתוב על הסרט כ-x ואחריו w. עבור $n=1$ מספיק: $\Sigma=\{0,1\},\quad \Gamma=\{0,1,B\},\quad Q=\{q_{start},q_1,q_{accept},q_{reject}\}$ $\delta(q_{start},1)=(q_1,1,R),\quad \delta(q_{start},0)=(q_{reject},0,R),\quad \delta(q_1,1)=(q_{accept},1,R),\quad \delta(q_1,0)=(q_{reject},0,R)$ כלומר: קרא את x_1; אם הוא 0 — דחה; אם הוא 1 — עבור ל-q_1 ובדוק ש-$w_1=1$ (כלומר שהעד באמת מצביע על המיקום הזה).

הפרמטרים. $n=|x|=1$, $q(1)=1$, אורך הקלט של M הוא $n+q(n)=2$. ניקח $p(m)=m+1$, ואז $r(1)=p(1+1)=3$ מספר שורות, מספר עמודות $=2\cdot 3+1=7$, $L=\{0,1,B,q_{start},q_1,q_{accept},q_{reject}\}$ כך ש-$|L|=7$.

הנוסחה שהרדוקציה פולטת עבור $x=1$. מספר המשתנים: $3\cdot 7\cdot 7=147$. ו-$\varphi_{start}=$ $x_{1,1,B}\wedge x_{1,2,B}\wedge x_{1,3,B}\wedge x_{1,4,q_{start}}\wedge x_{1,5,1}\wedge\big(x_{1,6,0}\vee x_{1,6,1}\big)\wedge x_{1,7,B}$ (שלושה תאים ריקים בעמודות $1..r(1)=3$; q_{start} בעמודה $r(1)+1=4$; הקלט $a_1=1$ בעמודה $2=5$; העד בעמודה $r(1)+n+2=6$; תא ריק בעמודה $2r(1)+1=7$.) **שימו לב:** רק בעמודה 6 יש חופש — בדיוק ביט אחד, בדיוק אורך w.

$\varphi_{accept}=\bigvee_{1\le i\le 3,\ 1\le j\le 7} x_{i,j,q_{accept}}$ כלומר פסוקית אחת בת 21 ליטרלים.

φ_{move} רצה על $i\in\{1,2\}$ ו-$j\in\{1,\dots,5\}$, כלומר 10 חלונות.

כיוון $\Rightarrow$: מ-$x\in A$ להשמה. $x=1$ שייך ל-A, והעד הוא $w=1$. הטבלה:

$i\backslash j$	**1**	**2**	**3**	**4**	**5**	**6**	**7**
1	B	B	B	q_{start}	1	1	B
2	B	B	B	1	q_1	1	B

$i\backslash j$	1	2	3	4	5	6	7
3	B	B	B	1	1	q_{accept}	B

שורה 2 מתקבלת מ-$\delta(q_{start},1)=(q_1,1,R)$: העמודות $4,5$ עוברות מ-$(q_{start},1)$ ל-$(1,q_1)$.
שורה 3 מתקבלת מ-$\delta(q_1,1)=(q_{accept},1,R)$: העמודות $5,6$ עוברות מ-$(q_1,1)$ ל-$(1,q_{accept})$.
ההשמה v מוגדרת לפי הטבלה, והיא מספקת את כל ארבעת החלקים: φ_{table} (סימן יחיד בכל תא), φ_{start} (השורה הראשונה, ובעמודה 6 הליטרל $x_{1,6,1}$ אמיתי), φ_{accept} ($x_{3,6,q_{accept}}$ אמיתי), φ_{move} (כל חלון נלקח משתי שורות עוקבות של ריצה אמיתית).

כיוון $\Leftarrow$: מהשמה ל-w ולשייכות. נניח שקיבלנו השמה מספקת v. מ-φ_{table} נגזרת טבלה; מ-φ_{start} אנו יודעים שהשורה הראשונה היא $B\ B\ B\ q_{start}\ 1\ ?\ B$, ובעמודה 6 בדיוק אחד מבין $x_{1,6,0}, x_{1,6,1}$ אמיתי. נקרא משם את w_1. אילו היה $w_1=0$: לפי φ_{move} ולמת הלוקליות הטבלה חייבת להיות שורה 2: $B\ B\ B\ 1\ q_1\ 0\ B$, ושורה 3: $B\ B\ B\ 1\ 0\ q_{reject}\ B$. ואז אין בטבלה אף תא עם q_{accept} — סתירה ל-φ_{accept}. לכן בהכרח $w_1=1$, ואז הטבלה היא זו שלמעלה ו-M אכן מקבלת את $(1,1)$, כלומר $x=1\in A$.

האינסטנס השלילי. עבור $x=0$: φ_{start} כופה $x_{1,5,0}$; לפי $\delta(q_{start},0)=(q_{reject},0,R)$ שורה 2 היא $B\ B\ B\ 0\ q_{reject}\ w_1\ B$; מ-$q_{reject}$ אין מעבר, ואין כלל ריפוד עבורו, ולכן אין השמה שמספקת את φ_{move} — φ אינה ספיקה. (ואם מרחיבים את כלל הריפוד לכל מצב עוצר, אז שורה 3 מעתיקה את שורה 2 ו-φ_{accept} היא זו שנכשלת. בשני המקרים $\varphi\notin\mathrm{SAT}$, בהתאם ל-$0\notin A$.)

דוגמה 3: אילו חלונות חוקיים ואילו לא (בעקבות הלוח)

עם המכונה של דוגמה 2 — שאף פעם אינה זזה שמאלה:

(א) חוקי — מעבר אמיתי:

B	q_{start}	1
B	1	q_1

זהו בדיוק החלון $(1,3)$ בטבלה של דוגמה 2: $\delta(q_{start},1)=(q_1,1,R)$.

(ב) חוקי — שורה עליונה נטולת מצב:

B	B	B
B	B	B

הראש רחוק, שום דבר לא משתנה. זה מה שהופך את רוב הטבלה ל"שקטה", וזו הלוקליות בפעולה.

(ג) לא חוקי — הראש צץ יש מאין [01:03:12]:

B	B	B
B	q_1	B

שאלה מנחה מההרצה: מאיפה הראש הזה היה יכול להגיע? רק מהתא משמאל או מהתא מימין — אבל בשורה העליונה של החלון אין סימן מצב באף אחד מהם, ומחוץ לחלון הוא רחוק מדי מכדי להגיע בצעד אחד. לכן אין ריצה שמייצרת חלון כזה.

(ד) לא חוקי — תזוזה שמאלה במכונה שאינה זזה שמאלה [01:02:11]:

1	q_1	1
q_{accept}	1	1

כאן סימן המצב עבר שמאלה, כלומר הראש זז שמאלה. ב-δ שלנו כל המעברים הם R, ולכן השישייה אינה ב-$\mathrm{Legal}(M)$. שימו לב לניסוח המדויק שהמרצה תיקן בהרצה: הנימוק אינו "לא הגיע מימין" אלא "הראש הזה **לעולם אינו זז שמאלה** במכונה הזאת".

(ה) לא חוקי — שינוי בלי ראש: $\begin{array}{|c|c|c|}\hline 0 & 1 & 0 \\ \hline 0 & 0 & 0 \\ \hline \end{array}$ בשורה העליונה אין סימן מצב, ולמרות זאת התא האמצעי שינה את תוכנו. מכונת טיורינג כותבת רק תחת הראש.

תרגיל 1 (מההרצה [00:13:43], [00:15:18]): כמה שורות וכמה עמודות?

שאלה. למה מספר השורות הוא $2p(|x|+q(|x|))+1$ ומספר העמודות הוא $p(|x|+q(|x|))$?

פתרון. מספר השורות = מספר הקונפיגורציות בריצה = מספר צעדי הזמן, החסום ב-p של אורך הקלט, כלומר $p(|x|+q(|x|))=r(n)$. מספר העמודות: זמן חוסם מקום — בכל צעד הראש זז תא אחד לכל היותר, ולכן מנקודת ההתחלה הוא לא יתרחק ביותר מ-$r(n)$. אבל **איננו יודעים מראש לאיזה כיוון** ילך, ולכן שומרים $r(n)$ תאים לכל צד: $2r(n)$. ה-$+1$ הוא התא שבו נרשם סימן המצב לפי הקידוד של הגדרה 1. סה"כ $2r(n)+1$.

תרגיל 2 (מההרצה [00:49:08]): כמה מילויים אפשריים לשורה?

שאלה. אם רציתי לכתוב "אם השורה הראשונה מולאה כך אז השורה השנייה כך", כמה גרירות אצטרך?

פתרון. לכל אחד מ-$2r(n)+1$ התאים יש $|L|$ אפשרויות, ולכן מספר המילויים הוא $|L|^{2r(n)+1}$ — מעריכי ב-n. (לא עצרת! זו חזקה: בחירה בלתי-תלויה בכל תא.) נוסחה בגודל כזה לא ניתנת לכתיבה בזמן פולינומי, ולכן הגישה הזאת נכשלת, ולכן צריך את החלונות.

תרגיל 3 (מההרצה [00:58:38]): כמה שישיות לחלון?

שאלה. על כמה איברים רצה הדיסיונקציה בתוך חלון בודד?

פתרון. $|L|^6$, לא $\binom{|L|}{6}$: התאים בחלון **אינם** חייבים להכיל סימנים שונים (וכפי שראינו, לרוב חמישה מתוך שישה זהים בזוגות). זהו $|L|\cdot|L|\cdot|L|\cdot|L|\cdot|L|\cdot|L|$. הגודל הזה תלוי רק ב-$M$.

תרגיל 4 (מההרצה [01:04:47]): מאיפה ה--1 וה--1 בתחומי φ_{move}?

שאלה. למה $1\le i\le r(n)-1$ ו-$1\le j\le 2r(n)-1$, ולא עד הסוף?

פתרון. חלון מאונדקס לפי התא השמאלי-עליון. לחלון שתי שורות, ולכן התא השמאלי-עליון יכול להיות לכל היותר בשורה $r(n)-1$ — משורה $r(n)$ אין שורה שמתחתיה. לחלון שלוש עמודות, ולכן התא השמאלי-עליון יכול להיות לכל היותר בעמודה $(2r(n)+1)-2=2r(n)-1$.

הערות מהשיעור

[00:01:08] סדר הכמתים. "להיזהר, כי הרבה פעמים אנשים אומרים 'יש רדוקציה מכל שפה ב-NP ל-SAT' — זה לא אותו דבר. 'יש רדוקציה לכל שפה' משמעו רדוקציה אחת שטובה לכולן, וזה לא המצב." הכיוון הנכון: **לכל** $A\in\mathrm{NP}$ **קיימת** רדוקציה, התלויה ב-A.

[00:02:41] דטרמיניסטי או אי-דטרמיניסטי. אפשר להוכיח את קוק–לוין משתי ההגדרות של NP. נבחרה הדטרמיניסטית כי היא מאפשרת לומר "אני יודע בכל צעד מה קורה בצעד הבא" — וזה בדיוק מה שנחוץ בכיוון $\Leftarrow$.

[00:05:19]–[00:06:52] "מי יש לי בידך?" — טכניקה, לא רק אנקדוטה. קיים מביא משתנים, לכל סוגר סקופ ומוחק אותם. יש: M,p,q ובזמן ריצה גם x. אין: w. המרצה חוזר לזה בכל תת-נוסחה כבדיקת שפיות — למשל [00:42:18]: "φ_{table} צריכה רק את n; φ_{start} צריכה את x עצמו".

[00:09:27], [00:20:03] בעיית שמונה המלכות היא "קוק–לוין בקטן". אותה טכניקה בדיוק: משתנה בוליאני לכל משבצת, תת-נוסחה לכל אילוץ, ו-$\wedge$ ביניהן. אם הקידוד כאן נראה לכם מסובך — חזרו לשם.

[00:23:47]–[00:24:52] קפיצה מכוונת בין תחביר לסמנטיקה. "כשאני מסביר את ההוכחה אני כל הזמן קופץ בין התחביר של הנוסחה למה שאני רוצה שהוא יגיד" [00:43:23]. זה מקור בלבול נפוץ: הרדוקציה בונה תחביר בלבד; המשמעות ("בתא כתוב s") קיימת רק בהוכחת הנכונות.

[00:32:31] מה φ_{table} לא מבטיחה. "היא תבנה לך טבלה — יכולה להיות טבלה של ג'יבריש, שלא קשורה למכונה בכלל." הקשר למכונה נוצר רק ב-φ_{start} וב-φ_{move}.

[00:35:46] למה צריך את הכיוון ההפוך בטענה 1.1. "להפך חשוב בגלל הכיוון השני של הרדוקציה." בלי המרה של טבלה להשמה, אי אפשר להוכיח $x \in A \Rightarrow \varphi \in \mathrm{SAT}$.

[00:45:01]–[00:45:31] כל תת-נוסחה עומדת בפני עצמה. אין צורך ש-φ_{accept} תדרוש יחידות — φ_{table} כבר עשתה זאת. עיקרון העבודה: כל נוסחה דורשת רק את שלה, ובלבד שאין סתירה ביניהן.

[00:46:33] "השפיץ של המשפט". "עד לפה זה כמעט אותו דבר כמו בעיית המלכות, רק יותר אינדקסים. הגדולה של קוק–לוין — ואולי הסיבה שאנחנו צריכים את המודל הפרימיטיבי-אבל-מדויק הזה של מכונות טיורינג — היא הנוסחה האחרונה."

[01:03:44]–[01:04:47] בדיחת "כל האי-זוגיים ראשוניים". 3, 5, 7, 7, 7, 7… — כך נראה כלל הריפוד. חסם הזמן הוא מלמעלה, ולכן צריך משהו למלא בו את שאר הטבלה.

[01:06:22]–[01:07:23] מה תלוי במה. קבוצת השישיות החוקיות תלויה **רק ב-**δ, כלומר רק ב-M; גודל הטבלה תלוי מאוד ב-x. המרצה מסרב לקרוא ל-$\lfloor L \rfloor^6$ "קבוע": "אין קבוע, יש תלוי בזה או לא תלוי בזה".

[01:16:30] מטאפורת הדומינו. "ברגע שכתבתי את w — זו כמו אבן ראשונה של דומינו שמפילה את כל השאר." זו התמצית של כיוון $\Leftarrow$.

[01:19:42] "קחו שבועיים". "זו לא הוכחה שאפשר לראות פעם אחת אונליין; היא דורשת עיכול." אם משהו כאן לא התיישב מהקריאה הראשונה — זה צפוי.

[01:14:25], [01:21:25] על המבחן. המרצה מסרב לענות על "מה מהחומר יהיה במבחן" ומבקש להסתכל על היופי של הרעיון. מה שכן נאמר על התרגיל: יהיו בו הרבה רדוקציות זמן פולינומי, ותהיה שאלה של "משחק עם ההגדרות" — שינוי קטן בהגדרה ובחינת מה משתנה — שהמרצה מדגיש כחשובה במיוחד, בלי קשר למבחן.

[01:20:20] הקשר היסטורי. המאמר של קוק ולוין היה "יריית הפתיחה"; אחריו בא ריצ'רד קארפ עם 21 בעיות NP-שלמות, וביניהן הרדוקציות $\mathrm{SAT} \to \mathrm{3SAT} \to \mathrm{IS} \to \mathrm{CLIQUE}$ שראינו/נראה בקורס.

[01:22:29] מה הלאה. אחרי שיודעים שבעיה היא NP-קשה — מה בכל זאת אפשר לעשות? זה מוביל לקירובים ולאלגוריתמים הסתברותיים בשיעורים הבאים: "אני מוכן לוותר על דברים בשביל שהאלגוריתם ירוץ בזמן סביר".

פערים בין הסיכום להקלטה

מקור: עמוד 1 בסיכום. **הפער:** תנאי המוודא נכתב $w \in \{0,1\}^{q(|w|)}$. **ההכרעה:** זו טעות — האורך של העד נקבע לפי אורך **הקלט**, כלומר $w \in \{0,1\}^{q(|x|)}$. ההקלטה [00:03:45] וכל שאר הסיכום (עמודים 2–3) משתמשים ב-$q(|x|)$. תוקן בגוף הקובץ.

מקור: עמוד 2 בסיכום, φ_{start}. **הפער:** טווח תאי ה-w נכתב כמסתיים ב-$r(n)+q(n)$, והריפוד בבלנקים מתחיל ב-$r(n)+q(n)+1$. זה מתעלם מ-$n+1$ התאים של q_{start} ושל x שלפניהם. **ההכרעה:** הטווח הנכון הוא $r(n)+n+1+q(n) \le j \le r(n)+n+2$, ובלנקים מ-$r(n)+n+2+q(n)$ עד $2r(n)+1$. זה עקבי עם התחלת ה-w שנכתבה נכון באותה שורה ($r(n)+(n+2)$), עם הטווח הנכון שמופיע בהמשך עמוד 2, ועם ההקלטה [00:40:02]. תוקן.

מקור: עמוד 2 בסיכום, φ_{move}. **הפער:** הנוסחה נכתבת כדיסיונקציה של קוניונקציות לכל חלון (DNF), בעוד שההרצה [00:27:13] מדגישה שכל אחת מארבע התת-נוסחאות היא CNF. **ההכרעה:** שתי הצורות נכונות ושקולות (מעל השמות שמספקות את φ_{table}); הוצגה גם הצורה השקולה φ'_{move} שאוסרת את השישיות הלא-חוקיות ושהיא CNF ישירה עם $\le |L|^6$ פסוקיות בנות 6 ליטרלים לכל חלון. אין סתירה — רק דחיסה בסיכום.

מקור: שני המקורות. **הפער:** מספר השורות נקבע $r(n)$, אך $r(n)$ שורות מתארות $r(n)-1$ צעדים בלבד, בעוד חסם הזמן מתיר $r(n)$ צעדים. **ההכרעה:** off-by-one שפיר. תוקן בהערה בגוף הקובץ (לוקחים $r(n)+1$ שורות, או מגדילים את p בקבוע); אף חסם או תחום אחר אינו משתנה בסדר גודלו.

מקור: שני המקורות. **הפער:** אף אחד מהם אינו רושם את שישיית המכונה במפורש, אף שהבנייה משתמשת ב-q_{start}, q_{accept}, Γ_M, Q_M ו-δ. **ההכרעה:** נרשמה במפורש בסעיף הרקע כ-$M = (Q, q_{start}, F, \Sigma, \Gamma, \delta)$, לפי מוסכמת הסימון של הקורס.

מקור: ההקלטה [00:55:48]–[01:03:12]. **הפער:** המרצה שרטט על הלוח מכונה קונקרטית ("היא סופרת / בודקת…") וארבעה-חמישה חלונות, ודן בחוקיותם — אך תוכן השרטוטים אינו ניתן לשחזור מהאודיו. **ההכרעה:** נבנתה מכונה מפורשת (דוגמה 2) ואיתה חמישה חלונות (דוגמה 3) שמשמרים בדיוק את נימוקי החוקיות שנשמעו: "מאיפה הראש הגיע", "המכונה הזאת לעולם לא זזה שמאלה", ו"שינוי בלי ראש".

מקור: ההקלטה. **הפער:** ההסבר על **למה** הקידוד הנאיבי (גרירה שורה-על-שורה) נכשל, וחישוב $|L|^{2r(n)+1}$ המילויים — נמצאים רק בהקלטה [00:48:06]–[00:50:11] ואינם מופיעים כלל בסיכום. **ההכרעה:** נכללו במלואם; זה החומר שמסביר למה הבנייה נראית כפי שהיא נראית.

מקור: ההקלטה. **הפער:** ההערות המתודיות ("קיים מביא משתנים, לכל מוחק אותם"), ההשוואה החוזרת לבעיית שמונה המלכות, ומטאפורת הדומינו — כולן בהקלטה בלבד. **ההכרעה:** נכללו בסעיף "הערות מהשיעור".

מקור: עמוד 3 בסיכום. **הפער:** הסיכום מסיים ב"לכן SAT היא NP-קשה" ואינו חוזר על $\mathrm{SAT} \in \mathrm{NP}$, בעוד שכותרת המשפט בעמוד 1 היא "SAT היא NP-שלמה". **ההכרעה:** הובא חלק (א) המלא של המשפט (העד הוא ההשמה), בהסתמך על שיעור 7.

מקור: ההקלטה, [00:00:00]–[00:05:00]. **הפער:** הדקות הראשונות הן חזרה על רדוקציות זמן פולינומי, NP-קושי ו-NP-שלמות משיעור 7, ולא חומר של שיעור זה. **ההכרעה:** שולבו בסעיף "רקע ותלויות" בלבד.

מקור: שני המקורות. **הפער:** המשתנים מסומנים $x_{i,j,s}$ בעוד ש-x מסמן גם את הקלט. **ההכרעה:** נשמר הסימון של הסיכום כפי שהוא (הוא גם הסימון שנאמר בהרצה), עם הבהרה מפורשת בהגדרה 3 שהאינדקסים הם רק שם ואין קשר בין השניים.

מקור: ההקלטה [01:03:44]. **הפער:** כלל הריפוד נאמר רק עבור q_{accept}; מקרה של עצירה במצב דוחה לפני תום $r(n)$ הצעדים אינו נדון. **ההכרעה:** נוסחה הערה מפורשת — במקרה כזה φ_{move} אינה ספיקה, וזה תקין כי ממילא רצינו $\varphi \notin \mathrm{SAT}$; לחלופין אפשר להרחיב את הריפוד לכל מצב עוצר ואז φ_{accept} היא שנכשלת. שתי הדרכים נכונות.

סיכום ונקודות למבחן

מה לזכור בעל פה

המשפט: SAT היא NP-complete. הניסוח המדויק: לכל $A \in \mathrm{NP}$ מתקיים $A \le_p \mathrm{SAT}$, ובנוסף $\mathrm{SAT} \in \mathrm{NP}$.

הפרמטרים: $r(n) = p(n + q(n))$; טבלה עם $r(n)$ שורות ו-$2r(n) + 1$ עמודות; אלפבית $L = \Gamma_M \cup \{0,1\} \cup Q_M$; משתנים $x_{i,j,s}$ שמשמעותם "בתא (i,j) כתוב s".

ארבעת החלקים ומה כל אחד עושה: φ_{table} — בכל תא בדיוק סימן אחד. φ_{start} — השורה הראשונה היא הקונפיגורציה ההתחלתית על (x, w), כשהחופש היחיד הוא $q(n)$ תאי w. φ_{accept} — איפשהו בטבלה q_{accept}. φ_{move} — כל חלון 2×3 חוקי.

הגודל: $O(r(|x|)^2)$ עד לגורמים התלויים רק ב-M (בפרט $|L|^6$) — ומכאן שהרדוקציה פולינומית.

המלכודות הסטנדרטיות

הפיכת כיוון הרדוקציה. $A \le_p B$ אומר ש-B קשה לפחות כמו A. כאן: $A \le_p \mathrm{SAT}$, כלומר SAT היא הקשה.

הפיכת סדר הכמתים. "לכל שפה יש רדוקציה" $\neq$ "יש רדוקציה לכל שפה".

בלבול בין שורות לעמודות. שורות $= r(n)$ (זמן), עמודות $= 2r(n) + 1$ (מקום). ה-2 נובע מאי-ידיעת כיוון התנועה; ה-$+1$ מהתא של סימן המצב.

במקום $|L|^6$. $\binom{|L|}{6}$ תאי החלון אינם חייבים להיות שונים.

לשכוח את הכיוון ההפוך בטענה על φ_{table}. צריך גם "מכל טבלה להשמה", אחרת כיוון $\Rightarrow$ של הרדוקציה נשבר.

לחשוב שהרדוקציה מריצה את M או מנחשת את w. היא רק כותבת נוסחה. אין לה w ואין לה השמה.

לשכוח את הריפוד. חסם הזמן הוא מלמעלה; בלי כלל ההעתקה של שורה מקבלת, טבלה של ריצה קצרה אינה מוגדרת עד הסוף.

לטעון שחלון 2×2 מספיק. מעבר שמאלה משנה שלושה תאים סמוכים.

צ'ק-ליסט: מה צריך לדעת לעשות אחרי השיעור

- [ ] לנסח את משפט קוק–לוין עם סדר הכמתים הנכון, ולהסביר למה הוא נותן את הבעיה ה-NP-שלמה הראשונה.
- [ ] לקודד קונפיגורציה נתונה של מכונת טיורינג כשורה, ולחשב את השורה הבאה בהינתן δ.
- [ ] לכתוב את ארבע התת-נוסחאות מהזיכרון, עם התחומים הנכונים של i ו-j בכל אחת מהן — כולל להסביר את ה-$1-$ וה-$1-$ ב-φ_{move}.
- [ ] להכריע אם שישייה נתונה היא חלון חוקי עבור מכונה נתונה, ולנמק ("מאיפה הראש הגיע", "האם δ מאפשרת", "האם השתנה תא בלי ראש").
- [ ] להסביר למה הקידוד הנאיבי של גרירה בין שורות נכשל, ולחשב $|L|^{2r(n)+1}$.
- [ ] לבצע חשבון גודל מלא של φ ולהסביר למה הוא פולינומי ב-$|x|$ ולא ב-$|L|$.
- [ ] להוכיח את שני כיווני הנכונות, כולל שחזור w מהשמה מספקת וטיעון הדומינו הדטרמיניסטי.
- [ ] להסביר איפה בדיוק נכנס בהוכחה כל אחד מהתנאים: זמן פולינומי, אורך העד, ודטרמיניזם.

הסיכום הכתוב שעליו מבוסס קובץ זה נכתב על ידי גיא סופר.

שאלות שנשארו פתוחות

בעמוד 2 בסיכום טווח תאי ה-w ב-φ_{start} נכתב עד $r(n)+q(n)$; זו החסרה של $n+1$ והוא תוקן לפי הטווח הנכון שמופיע בהמשך אותו עמוד.

המכונה הקונקרטית והחלונות שהמרצה שרטט על הלוח בין [00:55:48] ל-[01:03:12] אינם ניתנים לשחזור מהאודיו; נבנתה מכונה מפורשת מקבילה שמשמרת בדיוק את נימוקי החוקיות שנאמרו.

מספר השורות בסיכום הוא $r(n)$, ולכן מתוארים $r(n)-1$ צעדים בלבד; ההצמדה המדויקת דורשת $r(n)+1$ שורות. זהו off-by-one שאינו משנה דבר בהוכחה והוא סומן בגוף הקובץ.

הסיכום מסיים ב־SAT היא NP-קשה בלבד; ההשלמה ל-NP-שלמה נשענת על $\mathrm{SAT}\in\mathrm{NP}$ שהוכח בשיעור 7 והובאה כאן שוב.

10 כיסוי בקודקודים, MAXCUT וצביעת גרפים

מרחיבים את אוסף הבעיות ה-NP-קשות בעזרת שלוש רדוקציות: 3NAE ≤p MAXCUT, VC ≤p IS ו-3COL ≤p 3NAE, מוכיחים ש-2COL ∈ P, ולומדים איך נראית הוכחת נכונות מלאה של רדוקציה בשני הכיוונים.

ביטחון: medium

בקצרה

מרחיבים את "אוצר" הבעיות ה-NP-קשות: בשיעור שעבר היו לנו SAT, $\mathrm{3SAT}$, IS ו-CLIQUE; כאן מצטרפות VC, MAXCUT, $\mathrm{3COL}$ ו-kCOL.

הבחנה מרכזית: $U \subseteq V$ היא כיסוי בקודקודים של G אם ורק אם $V \setminus U$ היא קבוצה בלתי תלויה. מההבחנה הזו נובעת רדוקציה כמעט־זהותית $\mathrm{IS} \le_p \mathrm{VC}$ שמשנה רק את המספר: $\langle G, k\rangle \mapsto \langle G, |V| - k\rangle$.

מגדירים סיפוק **במובן** (Not All Equal) **NAE** ואת הבעיה $k\mathrm{NAE}$, ומקבלים (דרך רדוקציות שניתנו כתרגיל בית) ש-$\mathrm{3NAE}$ היא NP-קשה. משם ממשיכים.

$\mathrm{3NAE} \le_p \mathrm{MAXCUT}$: קודקוד לכל ליטרל, קשת "כחולה" בין ליטרל לשלילתו, משולש "אדום" לכל פסוקית, ויעד $n + 2m$. הקסם הוא שמשולש תורם לחתך *בדיוק* 2 או *בדיוק* 0 קשתות, ולכן חסם עליון על הקשתות האדומות כופה שכל הקשתות הכחולות בחתך.

$\mathrm{3NAE} \le_p \mathrm{3COL}$: קודקוד לכל ליטרל, קודקוד מיוחד N המחובר לכולם, ומשולש לכל פסוקית שקודקודיו מחוברים לליטרלים המתאימים. הצבע של N "שורף" צבע אחד ומשאיר שני צבעים שמתפקדים כאמת/שקר.

$\mathrm{3COL} \le_p \mathrm{4COL}$ אינה מוכחת כאן אלא ב**שיעור 11** (משפט 2 שם, לפי עמודים 2–3 בסיכום ההוא); בקובץ הזה נשארת הפניה בלבד. מהמפגש ההוא נשמרה כאן רק הטעות העקרונית שהמרצה הקדיש לה זמן רב: **רדוקציה אינה רואה את הצביעה**.

לצד הקשיות: $\mathrm{2COL} \in \mathrm{P}$ (שקול לדו-צדדיות), וכן — אם k הוא חלק מה-DNA של הבעיה ולא חלק מהקלט, בעיות מסוימות קורסות ל-P (למשל IS עם k קבוע).

כל רדוקציה כאן מוכחת **בשני הכיוונים** ובניתוח זמן ריצה מפורש. זהו הפורמט המדויק שנדרש במבחן.

רקע ותלויות

מה חייבים לדעת לפני השיעור.

מ**שיעור 6** נדרשת ההגדרה של רדוקציית זמן פולינומי. נזכיר אותה במלואה, כי כל השיעור נשען עליה: לשפות $A, B \subseteq \Sigma^*$ נאמר ש-$A \le_p B$ אם קיימת פונקציה $f : \Sigma^* \to \Sigma^*$ הניתנת לחישוב בזמן פולינומי (כלומר קיימת מכונת טיורינג $M = (Q, q_{start}, F, \Sigma, \Gamma, \delta)$ המחשבת אותה, כך ש-$\mathrm{time}_M(x) \le p(|x|)$ עבור פולינום p), המקיימת $\forall x \in \Sigma^* : \quad x \in A \iff f(x) \in B$.

הערה על כיוון: $A \le_p B$ נקרא "A ניתנת לרדוקציה ל-B", ומשמעותו ש-B **היא הבעיה הקשה לפחות כמו** A. כלומר החץ מצביע מהבעיה הידועה-כקשה אל הבעיה שאנחנו רוצים להוכיח שהיא קשה. בהקלטות אוטומטיות הכיוון הזה מתהפך כל הזמן; בכל רדוקציה בקובץ הזה נאמר את הכיוון גם במילים.

משיעור 7 נדרשים: ההגדרה $\mathrm{IS} = \{\langle G, k\rangle \mid G$ גרף, $k \in \mathbb{N}$, וקיימת ב-G קבוצה בלתי תלויה בגודל לפחות $k\}$, כאשר $U \subseteq V$ נקראת **בלתי תלויה** אם לכל $x, y \in U$ מתקיים $xy \notin E$; וכן הרדוקציה $\mathrm{IS} \le_p \mathrm{CLIQUE}$ (מעבר לגרף המשלים).

משיעור 8–9 נדרש משפט קוק–לוין: SAT היא NP-קשה, ובעקבותיו שרשרת התזכורת שנפתח בה השיעור (עמוד 1 בסיכום):

$$\mathrm{SAT}\text{ is NP-hard} \implies \mathrm{SAT} \le_p \mathrm{3SAT} \implies \mathrm{3SAT} \le_p \mathrm{IS} \implies \mathrm{IS} \le_p \mathrm{CLIQUE}.$$

הראשונה נראתה בכיתה, השנייה ניתנה כתרגיל בית (המרצה נתן את הרדוקציה ודרש רק את הוכחת הנכונות), השלישית הוכחה בשיעור. בסיכום נרשמה השורה השלישית כ-$\mathrm{SAT} \le_p \mathrm{IS}$; שתי הגרסאות נכונות, שכן $\le_p$ טרנזיטיבית.

התזכורת הטכנית שנשתמש בה שוב ושוב: אם A היא NP-קשה ו-$A \le_p B$ אז B היא NP-קשה. ההוכחה היא בדיוק טרנזיטיביות: לכל $C \in \mathrm{NP}$ מתקיים $C \le_p A \le_p B$, והרכבה של שתי פונקציות פולינומיות היא פולינומית (הפלט של הראשונה חסום פולינומית באורך הקלט, ולכן זמן הריצה של השנייה עליו הוא פולינום בפולינום).

מוטיבציה שהמרצה נתן ל[00:02:08]: המטרה בשבוע הקרוב אינה טכניקה חדשה אלא *הרחבת המאגר*. ככל שהמאגר גדול יותר, כך כשנרצה להוכיח שבעיה חדשה היא NP-קשה נוכל לבחור ממנו בעיה **דומה** לה ולעשות רדוקציה קצרה, במקום לחזור כל פעם ל-$3\mathrm{SAT}$. שתי רדוקציות בשיעור עוברות "בין עולמות" (מנוסחאות בוליאניות לגרפים) ואחת נשארת באותו עולם (גרפים→גרפים).

הגדרות

הגדרה 1: כיסוי בקודקודים (Vertex Cover)

יהי $G = (V, E)$ גרף לא מכוון. קבוצה $U \subseteq V$ תיקרא **כיסוי בקודקודים** (vertex cover) אם

$$\forall e \in E: \quad e \cap U \neq \emptyset.$$

ההגדרה מנצלת את העובדה שקשת בגרף לא מכוון היא *קבוצה* של שני קודקודים — זוג לא סדור, כלומר $e = \{x, y\}$ — ולכן החיתוך $e \cap U$ הוא ביטוי חוקי. במילים: כל קשת מכילה לפחות קודקוד אחד מהכיסוי.

השפה המתאימה:

$$\mathrm{VC} = \left\{ \langle G, k\rangle \;\middle|\; \begin{array}{l} G = (V,E)\ \text{graph},\ k \in \mathbb{N}, \\ \exists U \subseteq V\ \text{a vertex cover of}\ G,\ |U| \le k \end{array} \right\}$$

צורת כתיבה נוספת (עמוד 1 בסיכום, ואסייד ארוך ב-[00:04:50]–[00:11:13]). אפשר להגדיר את אותה בעיה בדיוק כך:

קלט: גרף $G = (V, E)$ ומספר טבעי $k \in \mathbb{N}$. **שאלה:** האם קיים כיסוי בקודקודים $U \subseteq V$ בגודל לכל היותר k?

אין שום הבדל בין שתי הצורות — כל האינפורמציה נמצאת בשתיהן. הצורה השנייה נותנת יותר חופש במבנה (אין צורך לדחוס הכול לתוך תיאור של קבוצת קידודים), ולכן היא נוחה יותר לבעיות הכרעה קומבינטוריות. הצורה הראשונה נאמנה יותר להגדרה של "שפה" כפי שהוגדרה בחישוביות. במבחן שתיהן מקובלות; העיקר שיהיה ברור מה הקלט ומה השאלה.

אינטואיציה ומוטיבציה ([00:09:34]). דמיינו מפת כבישים: הקודקודים הם צמתים והקשתות הן כבישים. אנחנו רוצים למקם מצלמות בצמתים כך שכל כביש ייצפה על ידי לפחות מצלמה אחת, ובמספר מצלמות מינימלי. זה בדיוק כיסוי בקודקודים. השם המלא הוא למעשה "כיסוי הקשתות בקודקודים", ו-"כיסוי בקודקודים" הוא קיצור.

דוגמה (עמוד 1 בסיכום). יהי G הגרף על $V = \{a, b, u_1, u_2, c\}$ עם $E =$ $\{au_1,\ bu_2,\ u_1u_2,\ u_1c,\ u_2c\}$. אז $U = \{u_1, u_2\}$ היא כיסוי בקודקודים: $au_1 \ni u_1$, $bu_2 \ni u_2$, $u_1u_2 \ni u_1$, $u_1c \ni u_1$, $u_2c \ni u_2$. כלומר $\langle G, 2\rangle \in \mathrm{VC}$.

אי-דוגמה. $U' = \{u_1\}$ אינה כיסוי: הקשת bu_2 מקיימת $bu_2 \cap U' = \emptyset$. ואכן $\langle G, 1\rangle \notin \mathrm{VC}$, כי au_1 ו-bu_2 הן קשתות זרות ולכן דרושים לפחות שני קודקודים.

הגדרה 2: סיפוק במובן NAE, והבעיה $k\mathrm{NAE}$

תהי φ נוסחה בצורת CNF ותהי V הצבה לקבוצת המשתנים של φ (הצבה = פונקציה מהמשתנים ל-$\{0, 1\}$).

תזכורת (אינה חלק מההגדרה החדשה). V **מספקת** את φ אם ורק אם לכל פסוקית C ב-φ קיים ליטרל ב-C ש-V נותנת לו את הערך 1.

ההגדרה החדשה. נאמר ש-V **מספקת את** φ **במובן Not All Equal**, ונסמן זאת בקיצור NAE, אם לכל פסוקית C ב-φ קיים ליטרל ב-C ש-V נותנת לו 1 **וגם** קיים ליטרל ב-C ש-V נותנת לו 0.

הבעיה:

$k\mathrm{NAE}$ — **קלט:** נוסחה φ מצורת $k\mathrm{CNF}$ (כלומר CNF שבכל פסוקית שלה יש k ליטרלים). **שאלה:** האם קיימת הצבה V למשתני φ המספקת את φ במובן NAE?

אינטואיציה. סיפוק רגיל אומר "בכל פסוקית יש לפחות אמת אחת". סיפוק במובן NAE אומר "בכל פסוקית יש גם אמת וגם שקר" — כלומר הפסוקית אינה מונוכרומטית מבחינת ערכי האמת. שימו לב היטב ([00:35:48], והמרצה חזר על זה שלוש פעמים): **התכונה הזו היא תכונה של הזוג (נוסחה, הצבה)**, לא של הנוסחה לבדה. כשאומרים "φ מסופקת במובן NAE" מתכוונים "קיימת הצבה שמספקת אותה במובן NAE".

אי-דוגמה מבנית ([00:36:21], שאלת סטודנט). אם ב-φ יש פסוקית עם ליטרל יחיד, אז **אף** הצבה אינה מספקת את φ במובן NAE, כי לא ייתכן שאותו ליטרל יקבל גם 1 וגם 0. זה לא סותר את ההגדרה — פשוט הנוסחה אינה ב-NAE.

דוגמה (עמוד 3 בסיכום). תהי $\varphi = (x_1 \vee x_2 \vee x_3) \wedge (\overline{x_1} \vee x_2)$.

ההצבה V הנותנת לכל משתנה את הערך 1 **מספקת** את φ אך **אינה** מספקת אותה במובן NAE: בפסוקית הראשונה כל שלושת הליטרלים מקבלים 1.

ההצבה $V(x_1)=0,\ V(x_2)=V(x_3)=1$ מספקת את φ אך שוב לא במובן NAE: הפסוקית הראשונה מקבלת $(0,1,1)$ — מצוין — אבל השנייה מקבלת $(\overline{x_1}=1,\ x_2=1)$, כלומר שני ליטרלים בערך 1.

ההצבה $V(x_1)=0,\ V(x_2)=0,\ V(x_3)=1$ **כן** מספקת את φ במובן NAE: הפסוקית הראשונה מקבלת $(0,0,1)$, השנייה מקבלת $(1,0)$. בשתיהן יש גם 1 וגם 0.

הגדרה 3: חתך מושרה ובעיית MAXCUT

יהי $G=(V,E)$ **מולטיגרף** — גרף לא מכוון שבו מותרות קשתות מקבילות (יותר מקשת אחת בין אותו זוג קודקודים), ובאופן עקרוני גם לולאות. (גרף פשוט הוא גרף שבו בין כל שני קודקודים יש לכל היותר קשת אחת; כל גרף פשוט הוא בפרט מולטיגרף.)

תהי $U\subseteq V$. **החתך המושרה ב-G על ידי** U הוא קבוצת הקשתות

$$\mathrm{cut}_G(U)=\{\,e\in E\ \mid\ |e\cap U|=1\,\},$$

כלומר כל הקשתות שיש להן **בדיוק** קצה אחד ב-U. מקובל לומר ש-U ו-$V\setminus U$ הם שני **צדדי** החתך, ושהקשתות בחתך **חוצות** אותו.

הבעיה:

> **MAXCUT — קלט:** מולטיגרף $G=(V,E)$ ומספר $k\in\mathbb{N}$. **שאלה:** האם קיימת $U\subseteq V$ כך שהחתך המושרה על ידיה מכיל **לפחות** k קשתות?

למה דווקא "לפחות" ([00:51:48], [00:55:09]). בכיסוי בקודקודים ובקבוצה בלתי תלויה יכולנו להחליף "לכל היותר"/"לפחות" ב-"בדיוק", כי מה שסופרים הוא בדיוק מה שבוחרים — קודקודים. כאן **בוחרים קודקודים אבל סופרים קשתות**, ואין שליטה עדינה: הזזה של קודקוד יחיד מדרגה גבוהה יכולה לשנות את גודל החתך דרמטית. ייתכן אפילו גרף שבו כל חתך הוא בגודל זוגי, ואז לא נוכל להגיע ל-k אי-זוגי בדיוק גם אם קיים חתך גדול יותר. לכן ה-"לפחות" כאן **קריטי** ואי אפשר להחליפו.

דוגמה (עמוד 4 בסיכום, [00:47:35]–[00:49:39]). יהי G על $V=\{a,b,c,d,e,f\}$ עם

$$E=\{\,ab,\ af,\ ac,\ bc,\ bd,\ cd,\ ce,\ de,\ ef\,\},$$

ותהי $U=\{b,c,f\}$. אז

$$\mathrm{cut}_G(U)=\{\,ab,\ af,\ ac,\ bd,\ cd,\ ce,\ ef\,\},\qquad |\mathrm{cut}_G(U)|=7.$$

שתי הקשתות שאינן בחתך ממחישות את שני אופני הכישלון: bc אינה בחתך כי **שני** קצותיה ב-U, ו-de אינה בחתך כי **אף אחד** מקצותיה אינו ב-U.

הגדרה 4: צביעה חוקית ובעיות kCOL

יהי $G=(V,E)$ גרף ויהי $k\in\mathbb{N}$. **צביעה של G ב-k צבעים** היא פונקציה $f:V\longrightarrow[k]=\{1,2,\dots,k\}$. הצביעה תיקרא **חוקית** אם לכל קשת $uv\in E$ מתקיים $f(u)\neq f(v)$.

במילים אחרות: אין בגרף קשת **מונוכרומטית** (קשת ששני קצותיה צבועים באותו צבע).

הבעיה:

> **kCOL — קלט:** גרף $G=(V,E)$. **שאלה:** האם קיימת צביעה חוקית של G ב-k צבעים?

נקודה עדינה מאוד ([01:38:26], שאלת סטודנטית). שימו לב ש-k **אינו חלק מהקלט** — הוא חלק מה-DNA של הבעיה. יש בעיה בשם $2\mathrm{COL}$, בעיה אחרת בשם $3\mathrm{COL}$, בעיה שלישית בשם $4\mathrm{COL}$ וכן הלאה; לכל k קבוע זו בעיה נפרדת. זה שונה מהותית מ-IS, CLIQUE ו-VC, שבהן k הוא חלק מהקלט.

מה ההבדל עושה ([01:40:00]–[01:42:12]). נגדיר IS_k = הבעיה שבה הקלט הוא גרף בלבד והשאלה היא האם יש בו קבוצה בלתי תלויה בגודל k, כאשר k קבוע. אז $\mathrm{IS}_k \in \mathrm{P}$: מספר תת-הקבוצות בגודל k הוא $\binom{|V|}{k} \leq |V|^k$, ולכל אחת מהן בדיקת אי-תלות עולה זמן פולינומי; מכיוון ש-k קבוע, $|V|^k$ הוא פולינום בגודל הקלט. אותה בעיה עצמה, כאשר k הוא חלק מהקלט, היא NP-שלמה. ההבדל אינו קוסמטי: $|V|^k$ עם k מהקלט הוא **אקספוננציאלי** בגודל הקלט.

דוגמה. משולש K_3 אינו 2-צביע (שלושה קודקודים המחוברים הדדית), אך הוא 3-צביע. K_4 אינו 3-צביע אך הוא 4-צביע.

אי-דוגמה לתפיסה שגויה ([00:15:50] בהקלטה 17). צביעה ב-k צבעים אינה חייבת להיות **על**: אין בהגדרה שום דרישה להשתמש בכל k הצבעים. לכן גרף 3-צביע הוא בפרט 4-צביע — פשוט לא נשתמש בצבע הרביעי.

משפטים והוכחות

משפט 1 (ההבחנה המרכזית): U כיסוי בקודקודים $\iff$ $V \setminus U$ בלתי תלויה

טענה. יהי $G = (V, E)$ גרף ותהי $U \subseteq V$. אז U היא כיסוי בקודקודים של G אם ורק אם $V \setminus U$ היא קבוצה בלתי תלויה ב-G.

הוכחה.

כיוון $\Longleftarrow$: נניח ש-$V \setminus U$ בלתי תלויה; נראה ש-U היא כיסוי בקודקודים.

צריך להראות: לכל $xy \in E$ מתקיים $x \in U$ או $y \in U$.

נניח בשלילה ש-$xy \in E$. מכיוון ש-U כיסוי בקודקודים, לקשת xy יש קצה ב-U, כלומר $x \in U$ או $y \in U$. אבל שנינו הנחנו $x, y \in V \setminus U$, כלומר $x \notin U$ וגם $y \notin U$ — סתירה. לכן $xy \notin E$, ומכיוון ש-x, y היו שרירותיים, $V \setminus U$ בלתי תלויה. $\square$ (כיוון ראשון)

כיוון $\Longrightarrow$: נניח ש-$V \setminus U$ בלתי תלויה; נראה ש-U כיסוי בקודקודים.

צריך להראות: לכל קשת יש קצה ב-U. תהי $e = xy \in E$ קשת. מכיוון ש-$V \setminus U$ בלתי תלויה, לא ייתכן ש-x, y **שניהם** ב-$V \setminus U$ (אחרת הייתה ביניהם קשת בסתירה לאי-תלות). לכן $x \notin V \setminus U$ או $y \notin V \setminus U$, כלומר $x \in U$ או $y \in U$, כלומר $e \cap U \neq \emptyset$. מכיוון ש-e הייתה שרירותית, U היא כיסוי בקודקודים. $\blacksquare$

הערה מתודית מהשיעור ([00:14:59]–[00:19:48]): המרצה עצר את הכיתה פעמיים על **מבנה** ההוכחה ולא על התוכן. (א) בכיוון הראשון סטודנט הציע מיד "נניח בשלילה". המרצה: אל תרוצו להוכחה בשלילה כשזה לא המבנה הנכון. המבנה הנכון מתחיל מ-"יהיו $x, y \in V \setminus U$", ורק אחרי שניסחנו *מה בדיוק צריך להוכיח* מגיעה השלילה, ורק על הצעד הנקודתי. "לדעת לנסח מה אנחנו רוצים להוכיח זה לפעמים 90% מהפתרון". (ב) בכיוון השני: כשההנחה שלנו היא טענת "לכל" (אי-תלות של $V \setminus U$) אין מה "לצטט" אותה — פשוט מפעילים אותה על העצם הקונקרטי שבידינו. כשההנחה היא טענת "קיים", כן כדאי לפתוח אותה ולתת שם למשתנה שהיא מספקת, כי נשתמש בו בהמשך.

משפט 2: $\mathrm{IS} \leq_p \mathrm{VC}$, ולכן VC היא NP-שלמה

הכיוון במילים: אנחנו מבצעים רדוקציה **מ**-IS (הבעיה שכבר ידוע שהיא NP-קשה) **אל** VC (הבעיה שאנחנו רוצים להוכיח שהיא קשה). התוצאה היא ש-VC קשה לפחות כמו IS.

הרדוקציה (עמוד 2 בסיכום). נתבונן באלגוריתם הבא:

קלט: גרף $G = (V, E)$ ומספר $k \in \mathbb{N}$.
החזר את $\langle G,\ |V| - k \rangle$.

זהו. אותו גרף בדיוק, רק המספר משתנה.

ניתוח זמן ריצה. האלגוריתם מעתיק את הקלט ומבצע חיסור יחיד. במודל RAM זה אפילו זמן קבוע; במכונת טיורינג יש לבצע חיסור בינארי על מספר שאורכו לכל היותר אורך הקלט, כלומר זמן פולינומי (למעשה $O(|\langle G, k\rangle|^2)$ בגישה נאיבית). בכל מקרה — **פולינומי בגודל הקלט**, וזה כל מה שנדרש; אין צורך להתחייב ליותר.

נכונות. יהיו $G = (V, E)$ גרף ו-$k \in \mathbb{N}$.

כיוון $\Longrightarrow$: נניח $\langle G, k\rangle \in \mathrm{IS}$.
אז קיימת $U \subseteq V$ בלתי תלויה ב-G עם $|U| = k$. לפי **משפט 1**, $V \setminus U$ היא כיסוי בקודקודים של G, וגודלה $|V| - |U| = |V| - k$. לכן $|V \setminus U| = |V| - k$ כיסוי בקודקודים בגודל $|V| - k$, ומכאן $\langle G, |V| - k\rangle \in \mathrm{VC}$.

כיוון $\Longleftarrow$: נניח $\langle G, |V| - k\rangle \in \mathrm{VC}$.
אז קיים כיסוי בקודקודים $U \subseteq V$ של G עם $|U| = |V| - k$. לפי **משפט 1**, $V \setminus U$ היא קבוצה בלתי תלויה ב-G, וגודלה $|V \setminus U| = |V| - (|V| - k) = k$. לכן $\langle G, k\rangle \in \mathrm{IS}$.

קיבלנו שלכל קלט $\langle G, k\rangle$ מתקיים $\langle G, k\rangle \in \mathrm{IS} \iff \langle G, |V| - k\rangle \in \mathrm{VC}$, והאלגוריתם רץ בזמן פולינומי; לכן זו רדוקציית זמן פולינומי מ-IS ל-VC, ומכאן ש-VC היא NP-קשה. ■

נקודה טכנית שהמרצה הוסיף באדום ([00:30:14]–[00:31:46], שאלת סטודנטית). בהוכחה השתמשנו בגודל **בדיוק** k ובגודל **בדיוק** $|V| - k$, בעוד שההגדרות מדברות על "לפחות k" ב-IS ועל "לכל היותר k" ב-VC. זה חוקי, וזו למעשה טענת עזר שכדאי לזכור:

ב-VC: אם יש כיסוי בגודל $k \leq$ (ו-$k \leq |V|$), אפשר תמיד **להוסיף** קודקודים שרירותיים עד לגודל k בדיוק — הוספת קודקוד לכיסוי לעולם אינה מקלקלת את היותו כיסוי. לכן "קיים כיסוי בגודל לכל היותר k" $\iff$ "קיים כיסוי בגודל בדיוק k".

ב-IS: אם יש קבוצה בלתי תלויה בגודל $\geq k$, אפשר תמיד **להוציא** קודקודים עד לגודל k בדיוק — תת-קבוצה של קבוצה בלתי תלויה היא בלתי תלויה. לכן "קיימת קבוצה בלתי תלויה בגודל לפחות k" $\iff$ "בגודל בדיוק k".

שימו לב שהכיווניות הפוכה בין שתי הבעיות, וזה בדיוק המקום שבו זה מסוכן. בכל בעיה חדשה יש לשאול מחדש האם "לכל היותר"/"לפחות"/"בדיוק" שקולים.

$\mathrm{VC} \in \mathrm{NP}$ **([00:31:46]).** בהינתן $\langle G, k \rangle$ והעד $U \subseteq V$ (שאורכו לכל היותר $|V|$, כלומר פולינומי בגודל הקלט), המאמת בודק ש-$|U| \leq k$ ועובר על כל קשת $e \in E$ ומוודא ש-$e \cap U \neq \emptyset$. זמן: $O(|E| \cdot |U|)$, פולינומי. לכן $\mathrm{VC} \in \mathrm{NP}$, ויחד עם ה-NP-קשיות: VC **היא NP-שלמה.**

> **שאלת סטודנט ([00:21:22]):** "למה לא לקחת פשוט את הזהות כרדוקציה?" התשובה כללה שני חלקים. ראשית, הכיוון: אנחנו לא רוצים רדוקציה *מ-*VC, אלא *אל* VC — כי המטרה היא להוכיח ש-VC קשה. שנית, הזהות "כמעט" עובדת: הגרף אכן נשאר אותו גרף, אבל **המספר חייב להשתנות**, בדיוק בגלל הקשר בין גודל קבוצה לגודל המשלים שלה.

משפט 3: $\mathrm{3NAE}$ ו-$\mathrm{4NAE}$ הן NP-קשות

טענה (עמוד 3 בסיכום, נמסרה כתרגיל בית, [00:43:55]). מתקיימות שתי הרדוקציות $3\mathrm{SAT} \leq_p 4\mathrm{NAE}$, $\quad 4\mathrm{NAE} \leq_p 3\mathrm{NAE}$.

מסקנה. מכיוון ש-$3\mathrm{SAT}$ היא NP-קשה, הרדוקציה הראשונה נותנת ש-$4\mathrm{NAE}$ היא NP-קשה; והרכבה של השתיים (טרנזיטיביות של $\leq_p$) נותנת $3\mathrm{SAT} \leq_p 3\mathrm{NAE}$, ולכן גם $3\mathrm{NAE}$ **היא NP-קשה**.

> **הערה:** בהרצאה זה נאמר בקיצור — שתי הרדוקציות עצמן נמסרו כתרגיל בית והמרצה דילג עליהן. הפירוט שנדרש כאן הוא רק חשבון הטרנזיטיביות, שאותו נכתוב במלואו: אם f מחשבת את $3\mathrm{SAT} \leq_p 4\mathrm{NAE}$ בזמן $p(n)$ ו-g מחשבת את $4\mathrm{NAE} \leq_p 3\mathrm{NAE}$ בזמן $q(n)$, אז $|f(x)| \leq p(|x|)$ (כי בזמן $p(|x|)$ אי אפשר לכתוב יותר מ-$p(|x|)$ תווים), ולכן חישוב $g(f(x))$ עולה $p(|x|) + q(p(|x|))$ — הרכבה של פולינומים, כלומר פולינום. וכן $x \in 3\mathrm{SAT} \iff f(x) \in 4\mathrm{NAE} \iff g(f(x)) \in 3\mathrm{NAE}$.

מכאן ואילך נשתמש ב-$3\mathrm{NAE}$ כ"נקודת המוצא הקשה" לשתי הרדוקציות הבאות.

הנחת נורמליזציה שנשתמש בה ([00:54:03]). נניח שבכל פסוקית של נוסחת $3\mathrm{CNF}$ יש **בדיוק** שלושה ליטרלים (שונים). זו הנחה סטנדרטית שהצדקתה פורסמה לכיתה בשקף נפרד: תמיד אפשר לשכפל ליטרל או להוסיף משתנה עזר כדי להגיע לבדיוק שלושה.

משפט 4: $3\mathrm{NAE} \leq_p \mathrm{MAXCUT}$, ולכן MAXCUT היא NP-קשה

הכיוון במילים: רדוקציה **מ-**$3\mathrm{NAE}$ (עולם הנוסחאות הבוליאניות) **אל** MAXCUT (עולם הגרפים). קלט הרדוקציה הוא נוסחה; הפלט הוא זוג $\langle$מולטיגרף, מספר$\rangle$.

הרדוקציה (עמוד 4 בסיכום). נתבונן באלגוריתם הבא:

קלט: נוסחה φ מצורת $3\mathrm{CNF}$.
נסמן את משתני φ ב-$x_1, \ldots, x_n$ ואת מספר הפסוקיות ב-m.
נבנה מולטיגרף $G = (V, E)$ באופן הבא:
2.1 לכל $1 \le i \le n$ נגדיר קודקוד עבור x_i וקודקוד עבור $\overline{x_i}$. (סה"כ $2n$ קודקודים — קודקוד לכל ליטרל.)
2.2 לכל $1 \le i \le n$ נוסיף קשת בין x_i ל-$\overline{x_i}$. נקרא לקשתות אלה **קשתות כחולות**.
2.3 לכל פסוקית C נוסיף קשת בין כל שני ליטרלים שלה (משולש). נקרא לקשתות אלה **קשתות אדומות**.
החזר את $\langle G,\ n + 2m \rangle$.

הצבעים אינם חלק מהמתמטיקה — הם מכשיר תיאורי, כדי שיהיה נוח לדבר על "קשתות מסוג ראשון" ו-"קשתות מסוג שני" בתוך ההוכחה ([00:58:27], שאלת סטודנט).

למה מולטיגרף ([00:58:58], [01:02:15]). אם שתי פסוקיות שונות מכילות את אותו זוג ליטרלים, נקבל שתי קשתות אדומות מקבילות; ואם פסוקית מכילה גם x_i וגם $\overline{x_i}$, נקבל קשת אדומה מקבילה לקשת הכחולה. אלה קשתות **שונות** של המולטיגרף, וזה בדיוק מה שמאפשר לספור כל פסוקית בנפרד.

ניתוח זמן ריצה ([01:05:23]–[01:08:05], עמוד 5 בסיכום). נסמן ב-$|\varphi|$ את אורך הקלט.
שלב 1 (סימון משתנים וספירת פסוקיות): מעבר יחיד על הנוסחה, $O(|\varphi|)$.
שלב 2.1 (יצירת קודקודים): מספר המשתנים הוא לכל היותר $|\varphi|$, ולכן $O(|\varphi|)$.
שלב 2.2 (קשתות כחולות): n קשתות, $n \le |\varphi|$, כלומר $O(|\varphi|)$.
שלב 2.3 (קשתות אדומות): כאן היחיד שדורש נימוק. מכיוון שהנוסחה היא $3\mathrm{CNF}$, כל פסוקית תורמת **בדיוק שלוש** קשתות (משולש על שלושה ליטרלים). לכן סך הקשתות האדומות הוא $3m \le 3|\varphi|$, כלומר $O(|\varphi|)$. **שימו לב שזה אינו ריבועי** — לו הפסוקיות היו באורך שרירותי, מספר הקשתות למשולש היה ריבועי באורך הפסוקית.
שלב 3 (חישוב $n + 2m$ וכתיבת הפלט): $O(|\varphi|)$.
סך הכול האלגוריתם רץ בזמן **ליניארי** באורך הקלט, ובפרט פולינומי. ✓

נכונות. תהי φ נוסחה מצורת $3\mathrm{CNF}$, נסמן את משתניה $x_1, \ldots, x_n$ ואת מספר פסוקיותיה m, ויהי G הגרף שהאלגוריתם בונה.

כיוון $\Longrightarrow$: נניח $\varphi \in 3\mathrm{NAE}$.
אז קיימת הצבה V המספקת את φ במובן NAE. נגדיר $U = \{\, \ell \mid \ell \text{ a literal vertex},\ V(\ell) = 1 \,\}$, כלומר U היא קבוצת קודקודי הליטרלים שההצבה נותנת להם 1. נראה שהחתך המושרה על ידי U מכיל לפחות $n + 2m$ קשתות.
הקשתות הכחולות. לכל $1 \le i \le n$, בדיוק אחד מבין $x_i, \overline{x_i}$ מקבל את הערך 1 (כי $V(\overline{x_i}) = 1 - V(x_i)$). לכן בדיוק אחד מהם ב-$U$, ולכן הקשת הכחולה $x_i\overline{x_i}$ מקיימת $|e \cap U| = 1$ — היא בחתך. סך הכול **כל** n **הקשתות הכחולות בחתך**.

הקשתות האדומות. תהי C פסוקית, ויהיו ℓ_1, ℓ_2, ℓ_3 ליטרליה. מכיוון ש-V מספקת את C במובן NAE, קיים j עם $V(\ell_j) = 1$ ולכן $\ell_j \in U$, וקיים j' עם $V(\ell_{j'}) = 0$ ולכן $\ell_{j'} \notin U$. שלושת הליטרלים יוצרים משולש, וכעת נספור: שני הקודקודים $\ell_j, \ell_{j'}$ נמצאים בצדדים שונים, ולכן הקשת ביניהם חוצה. נותר הקודקוד השלישי — לא משנה באיזה צד הוא נמצא, מבין שתי הקשתות הנותרות **בדיוק אחת** חוצה (זו המחברת אותו לקודקוד שבצד השני). לכן מבין שלוש הקשתות של המשולש **בדיוק שתיים** בחתך.

בסך הכול, מכיוון שהקשתות האדומות של פסוקיות שונות הן קשתות שונות במולטיגרף, אפשר לסכום בנפרד: $\langle G, n+2m\rangle \in \text{לכן } |\mathrm{cut}_G(U)| = \underbrace{n}_{\text{blue}} + \underbrace{2m}_{\text{red}} = n+2m \geq n+2m.$ MAXCUT.

כיוון $\Longleftarrow$: נניח $\langle G, n+2m\rangle \in \mathrm{MAXCUT}$.

אז קיימת $U \subseteq V$ כך שבחתך המושרה על ידיה יש **לפחות** $n+2m$ קשתות. אנחנו רוצים לבנות ממנה הצבה שמספקת את φ במובן NAE.

צעד 1 — חסם עליון על הקשתות האדומות. כאן דרוש טיעון "הפוך" מכל השאר: עד כה עבדנו עם "לפחות", וכעת נזדקק ל-"לכל היותר". תהי C פסוקית כלשהי, והמשולש המתאים לה. לא משנה מהי U: או ששלושת קודקודי המשולש באותו צד (אז 0 קשתות חוצות), או שהם מתחלקים 2–1 (אז בדיוק 2 חוצות). בשני המקרים $\#\{\text{red edges of } C \text{ in the cut}\} \leq 2$. לכן בכל חתך שהוא, סך הקשתות האדומות בחתך הוא לכל היותר $2m$.

צעד 2 — כפיית הקשתות הכחולות. בחתך שלנו יש לפחות $n+2m$ קשתות, ומהן לכל היותר $2m$ אדומות; לכן יש בו **לפחות** n קשתות כחולות. אבל בגרף יש בסך הכול בדיוק n קשתות כחולות. לכן בחתך יש **בדיוק** n קשתות כחולות — כולן. מכאן שלכל $1 \leq i \leq n$ הקשת $x_i\overline{x_i}$ בחתך, כלומר **בדיוק אחד** מבין $x_i, \overline{x_i}$ שייך ל-U.

צעד 3 — הגדרת ההצבה. נגדיר הצבה V על ידי $V(\ell) = 1 \iff \ell \in U$ מצעד 2 נובע שההגדרה **עקבית ומוגדרת היטב**: מכל זוג $\{x_i, \overline{x_i}\}$ בדיוק אחד ב-U, ולכן בדיוק אחד מקבל 1 והשני 0, כנדרש מהצבה. $\text{for every literal vertex } \ell.$

צעד 4 — כל פסוקית מסופקת במובן NAE. בחתך יש בדיוק n קשתות כחולות, ולכן מתוך לפחות $n+2m$ קשתות, לפחות $2m$ הן אדומות. מצד שני כל פסוקית תורמת לכל היותר 2. אילו פסוקית אחת הייתה תורמת פחות מ-2, סך התרומות האדומות היה קטן מ-$2m$ — סתירה. לכן **כל פסוקית תורמת בדיוק שתי קשתות** לחתך.

תהי C פסוקית. אילו כל שלושת קודקודי המשולש שלה היו באותו צד, היא הייתה תורמת 0 קשתות. לכן היא מתחלקת: קיים ליטרל $\ell \in C$ עם $\ell \in U$, ולכן $V(\ell) = 1$, וקיים ליטרל $\ell' \in C$ עם $\ell' \notin U$, ולכן $V(\ell') = 0$. זו בדיוק ההגדרה של סיפוק C במובן NAE.

מכיוון ש-C הייתה שרירותית, V מספקת את φ במובן NAE, ולכן $\varphi \in \mathrm{3NAE}$. ■

מסקנה. $\mathrm{3NAE} \leq_p \mathrm{MAXCUT}$ ולכן MAXCUT היא NP-קשה. היא גם ב-NP (העד הוא U; המאמת עובר על כל הקשתות וסופר כמה מהן מקיימות $|e \cap U| = 1$ — זמן פולינומי), ולכן **NP-שלמה**.

למה דווקא 3 ([01:20:43]–[01:22:19], שאלת סטודנט "האם זה עובד לכל $k\mathrm{CNF}$?"): הקסם כאן הוא שמשולש תורם לחתך *בדיוק* 2 או *בדיוק* 0 — אין אפשרויות אחרות. בפסוקית בגודל 4 או 5 הקודקודים ה"חופשיים" יכולים להתחלק במספר דרכים ומספר הקשתות החוצות אינו נקבע חד-משמעית; החסם העליון בצעד 1 היה נעשה רופף והכפייה בצעד 2 הייתה נשברת. המרצה אמר שהוא לא בדק אם אפשר להציל את זה, אבל שהמספר 3 "משחק מאוד חזק לטובתי" כי מספר האפשרויות זעיר.

הערה על אסימטריה של רדוקציות ([01:24:24]): בכיוון $\Longleftarrow$ סטודנטים נטו לחשוב שצריך "ללכת אחורה ברדוקציה" ולבנות נוסחה מגרף. **לא.** הרדוקציה אינה סימטרית: התחלנו מנוסחה φ שקיבלנו "מהשמיים", ממנה בנה האלגוריתם את G, וכעת **שניהם בידינו**. בפרט אנחנו יודעים בדיוק איך G נראה, כי אנחנו בנינו אותו. אין שום שלב שבו אמרנו "יהי G גרף".

משפט 5: $2\mathrm{COL} \in \mathrm{P}$

טענה. הבעיה $2\mathrm{COL}$ — האם גרף נתון ניתן לצביעה חוקית בשני צבעים — היא ב-P.

הוכחה. נטען ש-G הוא 2-צביע אם ורק אם G הוא **דו-צדדי**.

$(\Rightarrow)$ תהי $f : V \to \{1, 2\}$ צביעה חוקית. נגדיר $A = f^{-1}(1)$ ו-$B = f^{-1}(2)$. אלה שתי קבוצות זרות שאיחודן V, ולכל קשת $uv \in E$ מתקיים $f(u) \neq f(v)$, כלומר קצה אחד ב-A והשני ב-B. לכן אין קשת בתוך A ואין קשת בתוך B — זו בדיוק חלוקה דו-צדדית.

$(\Leftarrow)$ אם $V = A \dot\cup B$ חלוקה דו-צדדית, נגדיר $f(v) = 1$ עבור $v \in A$ ו-$f(v) = 2$ עבור $v \in B$; כל קשת עוברת בין הצדדים ולכן קצותיה בצבעים שונים.

מקורס האלגוריתמים ידוע שבדיקת דו-צדדיות היא בזמן פולינומי (ואף ליניארי): גרף הוא דו-צדדי אם ורק אם אין בו מעגל באורך אי-זוגי, ואלגוריתם BFS שצובע שכבות לסירוגין מגלה מעגל אי-זוגי או מפיק חלוקה דו-צדדית. לכן $2\mathrm{COL} \in \mathrm{P}$. ■

הערה מהשיעור ([01:43:26]–[01:46:33]): הסטודנטית שענתה "דו-צדדי" עשתה זאת מיידית והמרצה התלהב, אבל הוסיף במפורש: "מי שלא ראה את זה — לא להרגיש לא בנוח; אני הייתי מאלה שאף פעם לא קלטו את זה בזמן השיעור". לשלוט בחומר אין פירושו לשלוף אותו בשנייה.

משפט 6: $3\mathrm{NAE} \leq_p 3\mathrm{COL}$, ולכן $3\mathrm{COL}$ היא NP-שלמה

הכיוון במילים: רדוקציה **מ**-$3\mathrm{NAE}$ **אל** $3\mathrm{COL}$. הקלט הוא נוסחה $3\mathrm{CNF}$; הפלט הוא **גרף בלבד** — אין מספר, כי $k = 3$ הוא חלק מה-DNA של הבעיה.

הרדוקציה (עמוד 7 בסיכום, [01:47:38]–[01:51:01]).

קלט: נוסחה φ מצורת $3\mathrm{CNF}$, עם משתנים $x_1, \ldots, x_n$ ו-m פסוקיות.
נבנה גרף $G = (V, E)$ כך:
1.1 קודקודים: לכל $1 \le i \le n$ קודקוד עבור x_i וקודקוד עבור $\overline{x_i}$ (קודקודי ליטרלים); קודקוד מיוחד נוסף N; ולכל פסוקית C_j שלושה קודקודים נוספים, אחד לכל ליטרל שלה (קודקודי פסוקית). סה"כ $2n + 1 + 3m$ קודקודים.
1.2 קשתות: נחבר את N לכל קודקודי הליטרלים (**קשתות שחורות**, $2n$ קשתות); נחבר כל ליטרל לשלילתו (**קשתות כחולות**, n קשתות); ולכל פסוקית נחבר את שלושת קודקודי הפסוקית זה לזה (משולש) וכן כל קודקוד פסוקית לקודקוד הליטרל המתאים לו (**קשתות אדומות**, $3 + 3 = 6$ קשתות לפסוקית).
החזר את G.

שימו לב להבחנה שבלבלה את הכיתה ([01:55:50], [02:07:26]): לכל פסוקית יש **שלושה קודקודים משלה**, שהם עצמים נפרדים מקודקודי הליטרלים. קודקוד פסוקית "מתאים" לליטרל רק במובן שקיימת ביניהם קשת אדומה.

האינטואיציה מאחורי הבנייה ([01:53:40]–[01:54:41]). נניח שיש צביעה חוקית ב-3 צבעים. בלי הגבלת הכלליות $f(N) = 1$ (אפשר תמיד להחליף שמות צבעים). מכיוון ש-N מחובר לכל קודקודי הליטרלים, כל קודקוד ליטרל צבוע ב-2 או ב-3; ומכיוון ש-x_i מחובר ל-$\overline{x_i}$, מכל זוג כזה **בדיוק אחד** צבוע ב-2 ובדיוק אחד ב-3. כלומר הצבעים $\{2, 3\}$ מתפקדים בדיוק כמו $\{\mathrm{true}, \mathrm{false}\}$, והקודקוד N "שורף" עבורנו את הצבע הראשון. זה בדיוק ההפרדה שהייתה לנו ברדוקציה הקודמת. המשולשים של הפסוקיות הם המנגנון שאוכף את תנאי ה-NAE.

ניתוח זמן ריצה ([01:56:51]–[01:57:54]).
קודקודים: $2n$ קודקודי ליטרלים $+ 3m + 1$ קודקודי פסוקיות. מכיוון ש-$n, m \le |\varphi|$, זה $O(|\varphi|)$.
קשתות שחורות: $2n = O(|\varphi|)$.
קשתות כחולות: $n = O(|\varphi|)$.
קשתות אדומות: **בדיוק שש** לכל פסוקית (שלוש במשולש ושלוש לליטרלים), כלומר $6m = O(|\varphi|)$.
סך הכול $|V| + |E| = O(|\varphi|)$ והאלגוריתם רץ בזמן ליניארי בגודל הקלט, ובפרט פולינומי. ✓

נכונות. תהי φ נוסחה מצורת $3\mathrm{CNF}$ ויהי G הגרף שהאלגוריתם בונה.

כיוון $\Longrightarrow$: נניח $\varphi \in 3\mathrm{NAE}$.
אז קיימת הצבה V המספקת את φ במובן NAE. נבנה צביעה $f : V(G) \to \{1, 2, 3\}$:
$f(N) = 1$.
לכל $1 \le i \le n$: אם $V(x_i) = 1$ אז $f(x_i) = 2$ ו-$f(\overline{x_i}) = 3$; אחרת $f(x_i) = 3$ ו-$f(\overline{x_i}) = 2$.
.
תהי C פסוקית עם ליטרלים ℓ_1, ℓ_2, ℓ_3 וקודקודי פסוקית c_1, c_2, c_3 (כאשר c_t מחובר ל-ℓ_t). מכיוון ש-V מספקת את C במובן NAE, קיים t עם $V(\ell_t) = 1$ וקיים t' עם $V(\ell_{t'}) = 0$; נבחר **אחד** מכל סוג. נצבע:
$f(c_t) = 3$ (הקודקוד המתאים לליטרל שקיבל 1),
$f(c_{t'}) = 2$ (הקודקוד המתאים לליטרל שקיבל 0),

$f(c_{t''}) = 1$ עבור הקודקוד השלישי.

הערה חשובה על שלב 2 ([02:02:33], שאלת סטודנט): אי אפשר לצבוע "את כל ה-x_i ב-2 ואת כל ה-$\overline{x_i}$ ב-3". הצביעה **חייבת** להיות תלויה בהצבה, כי אחרת שני ליטרלים שההצבה נתנה להם ערכים שונים היו מקבלים אותו צבע והקשר בין צבע לערך אמת היה נשבר. נשים לב שההגדרה בשלב 2 שקולה לכלל האחיד:

$$f(\ell) = 2 \iff V(\ell)=1, \qquad f(\ell) = 3 \iff V(\ell)=0 \qquad \text{for every literal } \ell . \tag{$\ast$}$$

(אכן: אם $V(x_i) = 1$ אז $f(x_i) = 2$ ו-$V(\overline{x_i}) = 0$ עם $f(\overline{x_i}) = 3$; ואם $V(x_i) = 0$ אז $f(x_i) = 3$ ו-$V(\overline{x_i}) = 1$ עם $f(\overline{x_i}) = 2$.)

כעת נוודא שאף קשת אינה מונוכרומטית, קבוצה אחרי קבוצה:

קשתות שחורות (N–ליטרל): $f(N) = 1$ ולכל ליטרל $f(\ell) \in \{2, 3\}$, ולכן $f(N) \neq f(\ell)$. ✓

קשתות כחולות (x_i–$\overline{x_i}$): לפי הבנייה בשלב 2, אחד מהם צבוע 2 והשני 3. ✓

קשתות המשולש של פסוקית (c_t–$c_{t'}$ וכו'): לפי שלב 3 שלושת הקודקודים קיבלו $1, 2, 3$ — שלושה צבעים שונים. ✓

קשתות אדומות בין קודקוד פסוקית לליטרל שלו:

c_t (הליטרל שקיבל 1): $f(c_t) = 3$, ולפי $(\ast)$ $f(\ell_t) = 2$. שונים. ✓

$c_{t'}$ (הליטרל שקיבל 0): $f(c_{t'}) = 2$, ולפי $(\ast)$ $f(\ell_{t'}) = 3$. שונים. ✓

$c_{t''}$: $f(c_{t''}) = 1$, ואילו $f(\ell_{t''}) \in \{2, 3\}$. שונים. ✓ (הצבע 1 תמיד פנוי לקודקוד פסוקית, כי הצבע 1 ניתן רק ל-N, ו-N אינו מחובר לקודקודי פסוקיות.)

לכן f היא צביעה חוקית של G בשלושה צבעים, ומכאן $G \in \mathrm{3COL}$.

שימו לב גם ש**כל משולש פסוקית נצבע בנפרד לחלוטין**, בלי להתחשב בפסוקיות אחרות ([02:07:58]) — בדיוק כמו שברדוקציה ל-MAXCUT כל פסוקית תרמה קשתות משלה.

כיוון $\Longleftarrow$: נניח $G \in \mathrm{3COL}$.

> **הערה:** את הכיוון הזה המרצה השאיר כתרגיל בית ורק שרטט אותו בדקה האחרונה של ההקלטה ([02:11:40]). להלן ההשלמה המלאה, לפי הסקיצה שלו.

תהי f צביעה חוקית של G בשלושה צבעים. מכיוון שהחלפת שמות הצבעים (פרמוטציה על $\{1, 2, 3\}$) שומרת על חוקיות הצביעה, נוכל להניח בלי הגבלת הכלליות ש-$f(N) = 1$.

צעד 1. כל קודקוד ליטרל ℓ מחובר ל-N בקשת שחורה, ולכן $f(\ell) \neq 1$, כלומר $f(\ell) \in \{2, 3\}$.

צעד 2. לכל $1 \le i \le n$ הקשת הכחולה $x_i\overline{x_i}$ מחייבת $f(x_i) \neq f(\overline{x_i})$. יחד עם צעד 1: **בדיוק אחד** מבין $x_i, \overline{x_i}$ צבוע ב-2 והשני ב-3.

צעד 3 (הגדרת ההצבה). נגדיר הצבה V על ידי $f(x_i) = 2 \iff V(x_i) = 1$. מצעד 2 נובע שאז $f(\overline{x_i}) = 3$, ולכן שוב מתקיים הכלל האחיד $(\ast)$: לכל ליטרל ℓ, $V(\ell) = 1$ ו-$V(\ell) = 0 \iff f(\ell) = 3$. ההגדרה עקבית ומוגדרת היטב לכל משתנה.

צעד 4 (כל פסוקית מסופקת במובן NAE). תהי C פסוקית עם ליטרלים ℓ_1, ℓ_2, ℓ_3 וקודקודי פסוקית c_1, c_2, c_3. שלושת הקודקודים c_1, c_2, c_3 יוצרים משולש, ולכן בצביעה חוקית הם נושאים שלושה **צבעים שונים**, כלומר $\{f(c_1), f(c_2), f(c_3)\} = \{1, 2, 3\}$. בפרט:

קיים t עם $f(c_t)=2$. הקשת האדומה $c_t\ell_t$ מחייבת $f(\ell_t)\neq 2$, ומצעד 1 נובע $f(\ell_t)=3$, ולכן לפי $(*)$ מתקיים $V(\ell_t)=0$.
קיים s עם $f(c_s)=3$. הקשת האדומה $c_s\ell_s$ מחייבת $f(\ell_s)\neq 3$, ולכן $f(\ell_s)=2$, ולכן $V(\ell_s)=1$.
(ו-$t\neq s$ כי הצבעים שונים, ולכן $\ell_t\neq\ell_s$ הם שני ליטרלים שונים של C — כאן נכנסת ההנחה שבכל פסוקית שלושה ליטרלים שונים.)
קיבלנו שב-C יש ליטרל שההצבה נותנת לו 1 וליטרל שההצבה נותנת לו 0 — כלומר V מספקת את C במובן NAE. מכיוון ש-C שרירותית, V מספקת את φ במובן NAE, ולכן $\varphi\in 3\mathrm{NAE}$. ■

מסקנה. $3\mathrm{NAE}\le_p 3\mathrm{COL}$, ולכן $3\mathrm{COL}$ היא NP-קשה. היא גם ב-NP (העד הוא הצביעה f, שאורכה $O(|V|\log 3)$; המאמת עובר על כל הקשתות ובודק אי-מונוכרומטיות), ולכן **NP-שלמה**.

הרחבה (מוכחת בשיעור 11): $3\mathrm{COL}\le_p 4\mathrm{COL}$
לשלמות התמונה: גם $4\mathrm{COL}$, ובאופן כללי $k\mathrm{COL}$ לכל $k\ge 3$ קבוע, היא NP-שלמה, ברדוקציה **מ-$3\mathrm{COL}$ אל $4\mathrm{COL}$** — רדוקציה "בתוך אותו עולם", גרף לגרף. רעיון הבנייה בשורה אחת: מוסיפים לגרף קודקוד חדש אחד ומחברים אותו בקשת לכל קודקודי V, וכך הקודקוד החדש "שורף" את הצבע הרביעי ומשאיר לכל קודקוד מקורי בדיוק שלושה צבעים; ובכלליות מוסיפים $k-3$ קודקודים חדשים, מחברים אותם זה לזה (קליק) וכן לכל קודקודי V.
הרדוקציה הזו אינה נמצאת בשמונת עמודי הסיכום של השיעור הזה אלא בעמודים 2–3 של סיכום **שיעור 11**, ושם היא נכתבת במלואה: הבנייה, שני כיווני הנכונות, ניתוח זמן הריצה, ההוכחה ש-$4\mathrm{COL}\in\mathrm{NP}$, מעקב מלא אחרי C_5, המופע השלילי $K_4\mapsto K_5$, ושלושת הניסיונות שנשברו בדרך (הזהות, קודקוד מבודד, ו"נצבע אותו בצבע רביעי"). **ראו שיעור 11, משפט 2.** כאן נשארת רק המסקנה שנשתמש בה: $k\mathrm{COL}$ היא NP-שלמה לכל $k\ge 3$ קבוע, בעוד ש-$2\mathrm{COL}\in\mathrm{P}$ (משפט 5).

דוגמאות ותרגילים מהשיעור
דוגמה 1: כיסוי בקודקודים והמעבר לקבוצה בלתי תלויה
יהי G הגרף מהגדרה 1: $V=\{a,b,u_1,u_2,c\}$, $E=\{au_1,bu_2,u_1u_2,u_1c,u_2c\}$, $|V|=5$.
$U=\{u_1,u_2\}$ היא כיסוי בקודקודים, ולכן $\langle G,2\rangle\in\mathrm{VC}$.
לפי משפט 1, $V\setminus U=\{a,b,c\}$ חייבת להיות בלתי תלויה. נבדוק: $ab\notin E$, $ac\notin E$, $bc\notin E$. ✓ ואכן $\langle G,3\rangle\in\mathrm{IS}$.
מסלול הרדוקציה של משפט 2 קדימה: הקלט $\langle G,3\rangle$ לבעיית IS מתורגם ל- $\langle G,5-3\rangle=\langle G,2\rangle$ לבעיית VC. שתי הבעיות עונות "כן". ✓
מסלול הרדוקציה אחורה (אי-דוגמה): האם $\langle G,4\rangle\in\mathrm{IS}$? הרדוקציה מתרגמת אותו ל- $\langle G,5-4\rangle=\langle G,1\rangle$. אין ב-$G$ כיסוי בגודל 1, כי au_1 ו-bu_2 הן קשתות זרות ואף קודקוד יחיד לא נוגע בשתיהן. לכן $\langle G,1\rangle\notin\mathrm{VC}$, ולכן — לפי הרדוקציה — גם $\langle G,4\rangle\notin\mathrm{IS}$. אכן: קבוצה בלתי תלויה בגודל 4 הייתה משאירה משלים בגודל 1 שהוא כיסוי, וראינו שאין כזה. ✓

דוגמה 2: חתך מושרה

בגרף מהגדרה 3, עם $U = \{b, c, f\}$, קיבלנו חתך בגודל 7. שתי דרכי הציור שקולות: אפשר לצייר את הגרף כרגיל ולעגל את U, ואפשר לצייר שני "עמודים" — $\{b, c, f\}$ מצד אחד ו-$\{a, d, e\}$ מהצד השני — ולראות אילו קשתות עוברות ביניהם. שבע הקשתות $ab, af, ac, bd, cd, ce, ef$ עוברות; bc ו-de אינן.

דוגמה 3: הרצת הרדוקציה $3\mathrm{NAE} \le_p \mathrm{MAXCUT}$ מקצה לקצה (עמודים 4–5 בסיכום)

תהי $\varphi = (\overline{x_1} \vee x_2 \vee \overline{x_3}) \wedge (x_1 \vee x_2 \vee x_3) \wedge (\overline{x_1} \vee x_2 \vee x_3)$. כאן $n = 3$ ו-$m = 3$, ולכן הפלט הוא $\langle G, n + 2m \rangle = \langle G, 3 + 6 \rangle = \langle G, 9 \rangle$.

הגרף G. שישה קודקודים: $x_1, \overline{x_1}, x_2, \overline{x_2}, x_3, \overline{x_3}$.

קשתות כחולות (3): $x_1\overline{x_1}$, $x_2\overline{x_2}$, $x_3\overline{x_3}$.

קשתות אדומות של $C_1 = (\overline{x_1}, x_2, \overline{x_3})$: $\overline{x_1}x_2$, $x_2\overline{x_3}$, $\overline{x_1}\,\overline{x_3}$.

קשתות אדומות של $C_2 = (x_1, x_2, x_3)$: x_1x_2, x_2x_3, x_1x_3.

קשתות אדומות של $C_3 = (\overline{x_1}, x_2, x_3)$: $\overline{x_1}x_2$, x_2x_3, $\overline{x_1}x_3$.

סה"כ $12 = 9 + 3$ קשתות. שימו לב לשני זוגות **קשתות מקבילות**: $\overline{x_1}x_2$ מופיעה גם מ-C_1 וגם מ-C_3, וכן x_2x_3 מופיעה גם מ-C_2 וגם מ-C_3. זו בדיוק הסיבה שהבעיה הוגדרה על מולטיגרפים.

כיוון $\Longrightarrow$ בפועל. ניקח את ההצבה $V(x_1) = 0,\ V(x_2) = 0,\ V(x_3) = 1$. נבדוק שהיא מספקת במובן NAE:

C_1: $(\overline{x_1}, x_2, \overline{x_3}) \mapsto (1, 0, 0)$ — יש 1 ויש 0. ✓

C_2: $(x_1, x_2, x_3) \mapsto (0, 0, 1)$. ✓

C_3: $(\overline{x_1}, x_2, x_3) \mapsto (1, 0, 1)$. ✓

לכן $U = \{\overline{x_1}, \overline{x_2}, x_3\}$. נספור את החתך:

כחולות: כל שלוש חוצות (מכל זוג בדיוק אחד ב-U). $\to 3$

C_1: $\overline{x_1} \in U$, $x_2 \notin U$, $\overline{x_3} \notin U$. הקשת $\overline{x_1}x_2$ חוצה, $\overline{x_1}\,\overline{x_3}$ חוצה, $x_2\overline{x_3}$ לא (שניהם בחוץ). $\to 2$

C_2: $x_1 \notin U$, $x_2 \notin U$, $x_3 \in U$. x_2x_3 חוצה, x_1x_3 חוצה, x_1x_2 לא. $\to 2$

C_3: $\overline{x_1} \in U$, $x_2 \notin U$, $x_3 \in U$. $\overline{x_1}x_2$ חוצה, x_2x_3 חוצה, $\overline{x_1}x_3$ לא (שניהם ב-U). $\to 2$

סך הכול $3 + 2 + 2 + 2 = 9 \ge 9$. ✓ ואכן $\langle G, 9 \rangle \in \mathrm{MAXCUT}$.

כיוון $\Longleftarrow$ בפועל, ומה קורה כשההצבה גרועה. ניקח קבוצה אחרת: $U' = \{x_1, \overline{x_2}, x_3\}$, שהיא "לגיטימית" במובן שמכל זוג בדיוק אחד בה, ולכן מגדירה את ההצבה $V'(x_1) = 1, V'(x_2) = 0, V'(x_3) = 1$. נספור:

כחולות: 3.

C_1: $\overline{x_1} \notin U'$, $x_2 \notin U'$, $\overline{x_3} \notin U'$ — כל שלושת הקודקודים באותו צד! $\to 0$

C_2: $x_1 \in U'$, $x_2 \notin$, $x_3 \in$. $\to 2$

C_3: $\overline{x_1} \notin$, $x_2 \notin$, $x_3 \in$. $\to 2$

סה"כ $3 + 0 + 2 + 2 = 7 < 9$. ובאמת V' **אינה** מספקת את φ במובן NAE: $C_1 \mapsto (0, 0, 0)$. זו בדיוק הדינמיקה שהוכחנו — פסוקית שאינה מסופקת במובן NAE "מפסידה" שתי קשתות, והחתך צונח מתחת ל-$n + 2m$.

דוגמה 4: הרצת הרדוקציה $3\mathrm{NAE} \le_p 3\mathrm{COL}$ מקצה לקצה (עמוד 8 בסיכום)

תהי $\varphi = (\overline{x_1} \vee x_2 \vee \overline{x_3}) \wedge (x_1 \vee x_2 \vee x_3) \wedge (\overline{x_1} \vee \overline{x_2} \vee \overline{x_3})$.

הגרף. $2 \cdot 3 + 1 + 3 \cdot 3 = 16$ קודקודים: $x_1, \overline{x_1}, x_2, \overline{x_2}, x_3, \overline{x_3}$, הקודקוד N, ושלושה קודקודים לכל אחת מ-C_1, C_2, C_3. הקשתות: 6 שחורות (מ-N לכל ליטרל), 3 כחולות, ו-6 אדומות לכל פסוקית, כלומר 18; סה"כ 27 קשתות.

הצביעה. ניקח שוב $V(x_1) = 0,\ V(x_2) = 0,\ V(x_3) = 1$. נבדוק NAE: $C_1 \mapsto (1,0,0)$ ✓; $C_2 \mapsto (0,0,1)$ ✓; $C_3 = (\overline{x_1}, \overline{x_2}, \overline{x_3}) \mapsto (1,1,0)$ ✓.

לפי הבנייה:

1. $f(N) = 1$.
2. $V(x_1) = 0 \Rightarrow f(x_1) = 3,\ f(\overline{x_1}) = 2$.
3. $V(x_2) = 0 \Rightarrow f(x_2) = 3,\ f(\overline{x_2}) = 2$.
4. $V(x_3) = 1 \Rightarrow f(x_3) = 2,\ f(\overline{x_3}) = 3$.

קודקודי הפסוקיות (נסמן את קודקוד הפסוקית המתאים לליטרל ℓ ב-$c[\ell]$):

C_1: ליטרל שקיבל 1 הוא $\overline{x_1} \Rightarrow f(c[\overline{x_1}]) = 3$. ליטרל שקיבל 0 — נבחר $x_2 \Rightarrow f(c[x_2]) = 2$. השלישי $\overline{x_3} \Rightarrow f(c[\overline{x_3}]) = 1$. בדיקה: $2 = f(\overline{x_1}) \neq 3$ ✓; $3 = f(x_2) \neq 2$ ✓; $1 \neq f(\overline{x_3}) = 3$ ✓; המשולש $\{3,2,1\}$ ✓.

C_2: הליטרל שקיבל 1 הוא $x_3 \Rightarrow$ צבע 3; ליטרל שקיבל 0 — נבחר $x_1 \Rightarrow$ צבע 2; השלישי $x_2 \Rightarrow$ צבע 1. בדיקה: $2 = f(x_3) \neq 3$ ✓; $3 = f(x_1) \neq 2$ ✓; $1 \neq f(x_2) = 3$ ✓.

C_3: הליטרל שקיבל 1 — נבחר $\overline{x_1} \Rightarrow$ צבע 3; הליטרל שקיבל 0 הוא $\overline{x_3} \Rightarrow$ צבע 2; השלישי $\overline{x_2} \Rightarrow$ צבע 1. בדיקה: $2 = f(\overline{x_1}) \neq 3$ ✓; $3 = f(\overline{x_3}) \neq 2$ ✓; $2 = f(\overline{x_2}) \neq 1$ ✓.

כל הקשתות השחורות בסדר (1 מול $\{2,3\}$), כל הכחולות בסדר (2 מול 3). קיבלנו צביעה חוקית ב-3 צבעים.

הכיוון ההפוך על אותה דוגמה. נניח שקיבלנו צביעה חוקית f ל-G ובה, אחרי החלפת שמות צבעים, $f(N) = 1$. נניח למשל שקראנו מהצביעה $f(x_1) = 3, f(\overline{x_1}) = 2, f(x_2) = 3, f(\overline{x_2}) = 2, f(x_3) = 2, f(\overline{x_3}) = 3$. אז ההצבה המשוחזרת היא $V(x_i) = 1 \iff f(x_i) = 2$, כלומר $V(x_1) = 0, V(x_2) = 0, V(x_3) = 1$ — בדיוק ההצבה שהתחלנו ממנה.

עבור C_3: משולש הפסוקית נצבע בשלושה צבעים שונים; הקודקוד שצבוע 2 מחובר לליטרל שצבעו חייב להיות 3, כלומר לליטרל שערכו 0 — במקרה שלנו $\overline{x_3}$; הקודקוד שצבוע 3 מחובר לליטרל שצבעו 2, כלומר לליטרל שערכו 1 — למשל $\overline{x_1}$. קיבלנו ליטרל אמיתי וליטרל שקרי ב-C_3, כנדרש.

תרגיל מהשיעור 1: מדוע $\mathrm{VC} \in \mathrm{NP}$

שאלה ([00:31:46]). הוכיחו ש-$\mathrm{VC} \in \mathrm{NP}$. **פתרון.** ניתן עד $U \subseteq V$ המקודד ברשימה שאורכה $|U| \le k$; (ב) לכל $e \in E$ ש-$e \cap U \neq \emptyset$ — פולינומי בגודל הקלט. המאמת בודק (א) ש-$U \subseteq V$ ו-$O(|V| \log |V|)$. שני השלבים בזמן פולינומי. אם $\langle G, k \rangle \in \mathrm{VC}$ קיים עד כזה שיתקבל, ואם לא — שום עד לא יתקבל, כי בדיקת (ב) עוברת רק על כיסויים אמיתיים.

תרגיל מהשיעור 2: האם MAXCUT על גרפים פשוטים קשה גם היא?
שאלה ([00:52:52]). הגדרנו את MAXCUT על מולטיגרפים. הוכיחו שהגרסה על גרפים פשוטים שקולה. **פתרון (הכיוון הקל, שנמסר לבית).** כל גרף פשוט הוא בפרט מולטיגרף, ולכן הגרסה למולטיגרפים "מכילה" את הגרסה הפשוטה, ומכאן שהיא לא קלה יותר. לכיוון השני יש להחליף כל צרור של t קשתות מקבילות בין u, v במבנה שקול על גרף פשוט — למשל, לשכפל את הקודקודים; זהו התרגיל שנמסר לבית.
תרגיל מהשיעור 3: מה קורה כש-k הוא חלק מהבעיה ולא מהקלט
שאלה ([01:39:29], שאלת סטודנטית). נגדיר IS_k: הקלט הוא גרף בלבד, השאלה היא האם יש בו קבוצה בלתי תלויה בגודל k, כאשר k קבוע. מה אפשר לומר על הבעיה? **פתרון מלא.** $\mathrm{IS}_k \in \mathrm{P}$. אלגוריתם: עבור על כל תת-הקבוצות של V בגודל k ובדוק לכל אחת אם היא בלתי תלויה. מספרן הוא $\binom{|V|}{k} = \frac{|V|(|V|-1)\cdots(|V|-k+1)}{k!} \le |V|^k$, ולכל אחת הבדיקה עולה $O(k^2)$ (מעבר על כל זוג בקבוצה). מכיוון ש-k **קבוע** ואינו חלק מהקלט, $|V|^k \cdot k^2$ הוא פולינום בגודל הקלט. שימו לב היטב: אותו חישוב עצמו, כאשר k מגיע מהקלט, אינו פולינומי — כי אז $|V|^k$ הוא אקספוננציאלי באורך הייצוג של k.

הערות מהשיעור
[00:04:50]–[00:11:13] — שתי צורות הכתיבה של בעיית הכרעה. אפשר לכתוב בעיה כשפה (קבוצת קידודים) ואפשר לכתוב אותה כזוג "קלט/שאלה". אין הבדל באינפורמציה; לצורה השנייה יש יותר חופש מבני והיא נוחה במיוחד לבעיות קומבינטוריות, בניגוד לבעיות חישוביות שבהן הצורה הראשונה טבעית יותר. המרצה גם חידד לפי שאלת סטודנט שקשת בגרף לא מכוון היא **זוג לא סדור**, כלומר קבוצה, ולכן הכתיב $e \cap U \neq \emptyset$ הוא חוקי.
[00:09:34] — מוטיבציה אמיתית. מיקום מצלמות על כל כביש במפת כבישים. "המון בעיות עולם אמיתי מתורגמות לבעיות בגרפים; ראיתם את זה בקורס אלגוריתמים".
[00:14:59] — אל תרוצו לשלילה. "אל תרוצו להוכחה בשלילה כשזה לא המבנה הנכון... אני יכול להבריג בורג פיליפס עם מברג שטוח או עם סכין, אבל אני לא רוצה לעשות את זה".
[00:15:29] — "לדעת לנסח מה אנחנו רוצים להוכיח זה לפעמים 90% מהפתרון". אם יודעים לנסח, ההוכחה "כותבת את עצמה".
[00:18:12] — מתי מצטטים טענה. טענת "קיים" — פותחים ונותנים שם למשתנה, כי נשתמש בו. טענת "לכל" — לא מצטטים, פשוט מפעילים על העצם הקונקרטי.
[00:30:14]–[00:31:46] — "לכל היותר" מול "לפחות" מול "בדיוק". ב-VC אפשר להוסיף קודקודים ולכן "לכל היותר k" $\equiv$ "בדיוק k"; ב-IS אפשר להוריד קודקודים ולכן "לפחות k" $\equiv$ "בדיוק k". **הכיווניות הפוכה בין הבעיות**, וזו טעות נפוצה.
[00:36:21] — שאלת סטודנט: פסוקית באורך 1 לעולם אינה מסופקת במובן NAE.
[00:51:48], [00:55:09] — למה ב-MAXCUT ה-"לפחות" קריטי. בוחרים קודקודים אבל סופרים קשתות; אין שליטה עדינה על מספר הקשתות. הזזת קודקוד מדרגה גבוהה משנה את החתך דרמטית, וייתכן גרף שבו כל החתכים בגודל זוגי.

[01:04:19] — "אתם בתנאי חממה". בתרגילי הבית או שנותנים לכם את הרדוקציה ומבקשים להוכיח (או להפריך!) שהיא רדוקציה, או שמבקשים רדוקציה דומה מאוד למשהו שכבר ראיתם. בניית רדוקציה אמיתית מאפס עשויה לקחת שבוע-שבועיים, ולא תידרשו לכך.

[01:15:39] — השם MAXCUT מטעה. בעיית ההכרעה **אינה** שואלת אם החתך מקסימלי, אלא אם קיים חתך בגודל **לפחות** k.

[01:20:43]–[01:22:19] — שאלת סטודנט: האם הרדוקציה ל-MAXCUT עובדת גם ל-$k\mathrm{CNF}$ כללי? התשובה הכנה של המרצה: "צריך לחשוב על זה, לא חשבתי על זה" — אבל מבנה המשולש נוח במיוחד כי מספר האפשרויות זעיר, ובפסוקיות ארוכות יותר החסמים נעשים רופפים.

[01:24:24] — הרדוקציה אינה סימטרית. בכיוון ההפוך של ההוכחה אין "ללכת אחורה"; הנוסחה בידינו מלכתחילה והגרף נבנה ממנה, ולכן אנחנו יודעים בדיוק את מבנהו.

[01:32:15] — "המשחקים האלה של לכל היותר / לכל הפחות, קדימה ואחורה, הם חשובים מאוד". בכל רדוקציה יהיה כיוון אחד פחות ישיר מהשני.

[01:38:26]–[01:42:12] — שאלת סטודנטית (נועה): איפה ה-k ב-kCOL? התשובה: הוא חלק מה-DNA של הבעיה, לא תלוי בקלט. המרצה קרא לזה "שאלה פנטסטית", ומכאן הגיע הדיון על $\mathrm{IS}_k \in \mathrm{P}$.

[01:56:51] — ניתוח זמן הריצה הוא החלק הקל. "כל הרדוקציות האלה — זמן הריצה זה הדבר הכי פשוט". יש להתעכב עליו רק כשיש נקודה לא ברורה, למשל מספר הקשתות למשולש.

[02:02:33] — שאלת סטודנט על הצביעה: למה לא לצבוע את כל ה-x_i ב-2 ואת כל השלילות ב-3? כי אז הקשר בין צבע לערך אמת נשבר, וליטרלים עם ערכים שונים היו מקבלים אותו צבע.

[00:19:33]–[00:23:45] (הקלטה 17) — "החטא הכבד". סטודנט הציע רדוקציה מ-$3\mathrm{COL}$ ל-$4\mathrm{COL}$ בניסוח "נוסיף קודקוד ונצבע אותו בצבע חדש". המרצה עצר את השיעור לחמש דקות: **רדוקציה אינה באה לפתור את הבעיה, ואין לה גישה לצביעה.** האלגוריתם מקבל גרף בלבד; הוא לא מחפש צביעה, לא מקבל אותה, לא יודע עליה דבר. הערבוב בין תיאור האלגוריתם לבין הוכחת הנכונות (שבה כן יש לנו צביעה ביד) הוא הטעות. ההשוואה שנתן: זה כמו לומר ברדוקציה מ-HALT ש-"אם המכונה עוצרת נחזיר כך" — אי אפשר לבדוק את זה. הוא הוסיף מפורשות שאין בכך נזיפה: "אי אפשר ללמוד ללכת בלי ליפול; זה safe space". **הרדוקציה שעליה נסוב הדיון, $3\mathrm{COL} \le_p 4\mathrm{COL}$, מוכחת במלואה ב-שיעור 11 (משפט 2 שם); כאן נשמר האסייד המתודי בלבד, מפני שהוא נכון לכל רדוקציה בקורס.**

[00:16:53] (הקלטה 17) — כלל אצבע: אם כיוון אחד של רדוקציה יוצא קל בצורה חשודה, בדקו את הכיוון השני בידיים על דוגמה. שם K_4 הפילה מיד את רדוקציית הזהות מ-$3\mathrm{COL}$ ל-$4\mathrm{COL}$ (ראו שיעור 11).

[00:00:00]–[00:12:25] (הקלטה 17) — אסייד שנפתח בו המפגש השני. אם $A \in \mathrm{P}$ ו-B אינה טריוויאלית (כלומר $B \neq \emptyset$ ו-$B \neq \Sigma^*$), אז $A \le_p B$. הבנייה: בוחרים $b_1 \in B$ ו-$b_0 \notin B$, ומגדירים מכונה שמריצה על x את המכריע הפולינומי M_A ומדפיסה b_1 אם קיבל ו-b_0 אחרת. הנקודה העדינה: b_0, b_1 עשויים להיות ארוכים מאוד, אבל אורכם **אינו תלוי בקלט** (הם נקבעו לפני שראינו את x, והמכונה "מחזיקה אותם בבטן"), ולכן כתיבתם היא זמן קבוע כפונקציה של $|x|$.

המשמעות: רדוקציות זמן פולינומי הן כלי **גס מדי** מכדי להבדיל בין בעיות בתוך P — מבחינתן כל

הבעיות ב-P שקולות. זה מעיד על הכלי, לא על P (בתוך P בהחלט יש היררכיית קושי, לפי משפטי ההיררכיה). הטענה עצמה נכתבת במלואה ב-שיעור 11 (משפט 1 שם, עמוד 1 בסיכום ההוא); כאן היא מובאת כהערה בלבד.

פערים בין הסיכום להקלטה

מקור: עמוד 1 בסיכום. **הפער:** שרשרת התזכורת נקראת "$\mathrm{SAT} \le_p \mathrm{IS}$ — נראה בבית", בעוד שבהקלטה ([00:01:06]) המרצה מתאר את הרדוקציה שנמסרה לבית כרדוקציה מ-$3\mathrm{SAT}$ ל-IS. **ההכרעה:** שתי הטענות נכונות (לפי טרנזיטיביות של $\le_p$ ובגלל $\mathrm{SAT} \le_p 3\mathrm{SAT}$); בגוף הקובץ נרשמה השרשרת עם $3\mathrm{SAT} \le_p \mathrm{IS}$ וצוין שהסיכום כותב SAT.

מקור: עמוד 4 בסיכום, רשימת קשתות החתך בדוגמה. **הפער:** הכתב מאפשר לקרוא גם bc וגם bd. **ההכרעה:** ההקלטה ([00:48:37]–[00:49:09]) מכריעה חד-משמעית — bc **אינה** בחתך (שני קצותיה ב-U) ו-bd **כן**. נרשם bd.

מקור: עמוד 8 בסיכום. **הפער:** הסיכום מסתיים בסוף כיוון $\Longrightarrow$ של $3\mathrm{NAE} \le_p 3\mathrm{COL}$; כיוון $\Longleftarrow$ אינו מופיע כלל. בהקלטה ([02:09:01], [02:11:40]) המרצה אמר שהכיוון השני נשאר לבית והספיק רק לשרטט אותו בשתי משפטים לפני סוף ההקלטה. **ההכרעה:** הכיוון הושלם כאן במלואו לפי הסקיצה (WLOG על $f(N) = 1$; משולש הפסוקית מקבל שלושה צבעים שונים; הקודקוד שצבעו 2 כופה ליטרל בערך 0 והקודקוד שצבעו 3 כופה ליטרל בערך 1), וסומן כהשלמה.

מקור: סיכום השיעור מול הקלטה 17. **הפער:** הרדוקציה $3\mathrm{COL} \le_p 4\mathrm{COL}$ (הקלטה 17, [00:13:09]–[00:38:29]) אינה מופיעה באף אחד משמונת עמודי הסיכום של השיעור הזה. **ההכרעה:** הפער נסגר — הרדוקציה נמצאת ב**עמודים 2–3 של סיכום שיעור 11** (תחת הכותרת הירוקה "4COL הוא NP שלם", עם הבנייה הממוסגרת של $\hat{G}$ ו-$\hat{v}$ ושני הכיוונים). היא שייכת אפוא לשיעור 11 ונכתבת שם במלואה; בקובץ הזה נשארת רק הפניה קצרה בסוף סעיף המשפטים, בלי בנייה ובלי הוכחה, וכן דוגמת ההרצה שלה הוסרה מכאן.

מקור: מקורות הקובץ. **הפער:** הקלטה 17 סומנה בעבר `coverage: partial` בטענה שחלק ממנה שייך לשיעור הזה. זה שגוי: כל תוכנה — הטענה על רדוקציות משפות ב-P ([00:00:00]–[00:12:25]), $3\mathrm{COL} \le_p 4\mathrm{COL}$ ([00:13:09]–[00:38:29]) ו-SUBSET SUM ([00:38:29] ואילך) — הוא חומר של שיעור 11. **ההכרעה:** סומנה `coverage: none`, והשיעור הזה נשען כעת על הקלטה 16 בלבד. ממנה נלקחו רק אסידים פדגוגיים: "החטא הכבד" ([00:19:33]–[00:23:45]), כלל האצבע על בדיקת הכיוון השני ([00:16:53]), האסייד על גסות $\le_p$ ([00:00:00]–[00:12:25]) והאי-דוגמה בהגדרה 4 בדבר צביעה שאינה על ([00:15:50]) — כולם מסומנים במפורש כ"הקלטה 17".

מקור: רמת הביטחון. **הפער:** לאחר הוצאת הקלטה 17 נותרו שני מקומות שאינם נשענים על שני מקורות מסכימים: כיוון $\Longleftarrow$ של משפט 6, שאינו בסיכום כלל והושלם כאן מסקיצה בת שתי שורות בהקלטה 16 ([02:11:40]); וארבע ההערות שנלקחו מהקלטה 17, שאינה מקור של השיעור הזה. **ההכרעה:** גוף השיעור (הגדרות 1–4, משפטים 1–6, דוגמאות 1–4) מכוסה במלואו גם בסיכום וגם בהקלטה 16 ולכן הוא איתן; אך משום שני החריגים הללו הורד `confidence` מ-`high` ל-`medium`.

מקור: ההקלטה מול הסיכום. **הפער:** הדיון על $\mathrm{IS}_k \in \mathrm{P}$ ועל k כחלק מה-DNA של הבעיה ([01:38:26]–[01:42:12]) אינו בסיכום. **ההכרעה:** נכלל, כי הוא מבהיר את ההגדרה של kCOL שכן מופיעה בסיכום (עמוד 7).

מקור: ההקלטה, [01:03:18]. **הפער:** בהקלטה נשמע המספר "28" כתשובה ליעד של הדוגמה. **ההכרעה:** זו טעות של סטודנט שהמרצה תיקן מיד; היעד הנכון הוא $n + 2m = 3 + 6 = 9$, כפי שרשום בסיכום (עמוד 4: "$(G, 9)$").

מקור: ההקלטה, [00:07:24]. **הפער:** תמלול משובש בהגדרת VC ("אפשר בגודל K ואפשר בגודל K"). **ההכרעה:** לפי ההקשר והסיכום, הכוונה היא "אפשר לכתוב 'בגודל לכל היותר k' ואפשר 'בגודל בדיוק k' — זה לא משנה", וההצדקה ניתנה מאוחר יותר ב-[00:30:45]. נרשמה הגרסה "לכל היותר k" כפי שבסיכום.

מקור: סימון. **הפער:** הסיכום כותב את בעיות הצביעה כ-"$2\mathrm{Col}k$", "$3\mathrm{Col}$", "Coloring". **ההכרעה:** בגוף הקובץ נעשה שימוש בכתיב הזקוף האחיד $\mathrm{kCOL}, \mathrm{3COL}, \mathrm{2COL}$ לשם עקביות עם שאר הקורפוס; המשמעות זהה.

סיכום ונקודות למבחן

מה חייבים לזכור בעל פה

ההבחנה: U כיסוי בקודקודים $\iff$ $V \setminus U$ בלתי תלויה. מכאן $\mathrm{IS} \leq_p \mathrm{VC}$ על ידי $\langle G, k \rangle \mapsto \langle G, |V| - k \rangle$ (ובאותו אופן גם הכיוון ההפוך $\mathrm{VC} \leq_p \mathrm{IS}$).

סיפוק במובן NAE: בכל פסוקית יש ליטרל בערך 1 **וגם** ליטרל בערך 0. $\mathrm{3NAE}$ ו-$\mathrm{4NAE}$ הן NP-קשות (דרך $\mathrm{3SAT} \leq_p \mathrm{4NAE} \leq_p \mathrm{3NAE}$).

$\mathrm{3NAE} \leq_p \mathrm{MAXCUT}$: קודקוד לכל ליטרל; קשת כחולה $x_i\overline{x_i}$; משולש אדום לכל פסוקית; יעד $n + 2m$.

$\mathrm{3NAE} \leq_p \mathrm{3COL}$: קודקוד לכל ליטרל; קודקוד מיוחד N המחובר לכולם; משולש לכל פסוקית שקודקודיו מחוברים לליטרלים המתאימים. $f(N) = 1$, וצבעים $2, 3$ מייצגים אמת/שקר.

$\mathrm{2COL} \in \mathrm{P}$ (שקילות לדו-צדדיות).

שלוש הבעיות $\mathrm{VC}, \mathrm{MAXCUT}, \mathrm{3COL}$ הן **NP-שלמות** (קשיות + שייכות ל-NP עם עד קצר) — אלה תוצאות השיעור הזה.

לא מהשיעור הזה, אבל שייך לאותה משפחה: $\mathrm{3COL} \leq_p \mathrm{4COL}$ (קודקוד חדש אחד המחובר לכל הגרף; בכלליות $k - 3$ קודקודים חדשים המחוברים זה לזה ולכל V), ומכאן ש-kCOL היא NP-שלמה לכל $k \geq 3$ קבוע. **הרדוקציה והוכחתה בשיעור 11, משפט 2** — למדו אותה משם.

מלכודות סטנדרטיות

כיוון הרדוקציה. $A \leq_p B$ פירושו B קשה לפחות כמו A. כדי להוכיח שבעיה חדשה קשה, מבצעים רדוקציה **אליה**, לא ממנה.

"לפחות" מול "לכל היותר". ב-MAXCUT אי אפשר להחליף "לפחות" ב-"בדיוק"; ב-$\mathrm{IS/VC}$ כן, אבל בכיוונים הפוכים. אל תעתיקו את ההצדקה מבעיה לבעיה בלי לבדוק.

רדוקציה אינה פותרת. האלגוריתם אינו רשאי להתייחס לפתרון (הצבה, צביעה, קבוצה) — רק הוכחת הנכונות רשאית. ערבוב בין השניים הוא הטעות שהמרצה הדגיש הכי חזק בשיעור.

k בקלט מול k בבעיה. kCOL אינה מקבלת k בקלט; IS כן. שינוי הסטטוס הזה יכול להעביר בעיה מ-NP-שלמה ל-P.

החסם הדו-כיווני. בכיוון ההפוך של $3\mathrm{NAE} \leq_p \mathrm{MAXCUT}$ חייבים חסם **עליון** ($2 \leq$ אדומות לפסוקית) כדי לכפות חסם **תחתון** על הכחולות. ניסיון להוכיח את הכיוון הזה בעזרת "לפחות" בלבד ייתקע.

מולטיגרף. בלי קשתות מקבילות הספירה "כל פסוקית תורמת בדיוק 2" קורסת כשאותו זוג ליטרלים מופיע בשתי פסוקיות.

הצביעה תלויה בהצבה. אין לצבוע את כל המשתנים החיוביים באותו צבע.

צ'ק-ליסט: אחרי השיעור הזה אני יודע ל...

- [ ] לכתוב בעיית הכרעה בשתי הצורות (שפה / קלט-שאלה) ולהסביר למה הן שקולות.
- [ ] להוכיח את ההבחנה כיסוי $\leftrightarrow$ בלתי תלויה בשני הכיוונים, במבנה נכון ובלי שלילה מיותרת.
- [ ] לבנות רדוקציה מלאה: אלגוריתם, ניתוח זמן ריצה מנומק, והוכחת $x \in A \iff f(x) \in B$ בשני הכיוונים.
- [ ] לתאר את גרף ה-MAXCUT ואת גרף ה-$3\mathrm{COL}$ בעל פה מתוך נוסחת $3\mathrm{CNF}$, כולל היעד $n + 2m$.
- [ ] להריץ מופע קונקרטי דרך כל רדוקציה בשני הכיוונים ולספור קשתות/צבעים בפועל.
- [ ] להסביר למה $2\mathrm{COL} \in \mathrm{P}$ (ולדעת שהקשיות של kCOL לכל $k \geq 3$ מוכחת בשיעור 11).
- [ ] לזהות "רדוקציה" פסולה שמסתכלת על הפתרון, ולהפריך רדוקציה מוצעת בעזרת דוגמה נגדית קטנה (כמו K_4).

הסיכום הכתוב שעליו מבוסס קובץ זה הוא של גיא סופר.

שאלות שנשארו פתוחות

עמוד 1 בסיכום: שורת התזכורת נקראת SAT ≤p IS, בעוד שבהקלטה הרדוקציה שניתנה בבית תוארה כרדוקציה מ-3SAT; שתי הטענות נכונות ובגוף הקובץ נרשמו שתיהן.

עמוד 8 בסיכום: הפסוקית השלישית בדוגמת הצביעה נקראה כ-(¬x₃ ∨ ¬x₂ ∨ x₁), בעוד שבדוגמת MAXCUT בעמוד 4 הפסוקית השלישית היא (¬x₃ ∨ x₂ ∨ x₁); ייתכן שמדובר בשתי דוגמאות שונות בכוונה.

עמוד 8 בסיכום מסתיים אחרי כיוון ⇐ בלבד של 3COL ≤p 3NAE; הכיוון השני הושלם כאן לפי הסקיצה שבהקלטה ב-[02:11:40].

עמוד 4 בסיכום: ברשימת קשתות החתך בדוגמה קשה להכריע בין bd ל-bc; ההקלטה [00:48:37] מכריעה שהקשת היא bd ושהקשת bc אינה בחתך.

11 בעיית SUBSET SUM ושלמותה ב-NP

בשיעור מוכיחים ש-SUBSET SUM היא NP-complete באמצעות רדוקציה מ-VC הבונה מספרים ספרה-ספרה כך שלא נוצרות נשאות, ומבחינים בין ערך המספרים לבין אורך הייצוג שלהם — ההבחנה שמסבירה מדוע אלגוריתם התכנון הדינמי מסדר $O(n\cdot S)$ אינו אלגוריתם פולינומי.

ביטחון: high

בקצרה

מוכיחים שהבעיה $\mathrm{SUBSET\text{-}SUM}$ — בהינתן מספרים טבעיים $a_1,\dots,a_n$ ומספר יעד S, האם קיימת תת-קבוצת אינדקסים שסכום איבריה בדיוק S — היא NP-complete.

החלק הקל: שייכות ל-NP, באמצעות certificate שהוא קבוצת האינדקסים עצמה.

החלק המהותי: רדוקציה $\mathrm{VC} \le_p \mathrm{SUBSET\text{-}SUM}$, שבה כל קודקוד וכל קשת מקבלים מספר שנבנה **ספרה-ספרה**: עמודה אחת לכל קשת, ועוד עמודה מובילה שסופרת קודקודים.

לב ההוכחה הוא טיעון **אי-נשאות**: בכל עמודת קשת סכום הספרות של *כל* המספרים הוא לכל היותר 3, ולכן חיבור ארוך בבסיס 10 אף פעם אינו נושא, וניתן להסיק מן הסכום מסקנה נפרדת על כל עמודה בנפרד. בלי הטיעון הזה כל ההוכחה קורסת.

בנוסף מוכיחים בשיעור שתי תוצאות "מסביב": כל שפה ב-P ניתנת לרדוקציה לכל שפה לא-טריוויאלית (ולכן $\le_p$ הוא כלי גס מדי מכדי להבחין בין בעיות בתוך P), ו-$4\mathrm{COL}$ היא NP-complete באמצעות רדוקציה מ-$3\mathrm{COL}$.

מבחינים בין **ערך** המספרים לבין **אורך הייצוג** שלהם: אלגוריתם התכנון הדינמי מקורס האלגוריתמים רץ בזמן $O(n\cdot S)$, וזה **אינו** זמן פולינומי בגודל הקלט. זו הסיבה ש-$\mathrm{SUBSET\text{-}SUM}$ היא NP-hard "חלשה" בלבד.

מי שקורא רק את הסעיף הזה צריך לדעת: הרדוקציה עצמה קצרה, אבל היא נשענת על שתי נקודות עדינות (אי-נשאות, ו"בדיוק K" מול "לכל היותר K") שנבחנות בדיוק בגללן.

רקע ותלויות

השיעור מניח את הדברים הבאים.

מחלקות ו-verifiers (שיעורים 7–8). P היא מחלקת השפות הניתנות להכרעה בזמן פולינומי במכונת טיורינג דטרמיניסטית; NP היא מחלקת השפות שעבורן קיים verifier פולינומי, כלומר קיימים פולינום p ומכונה V הרצה בזמן פולינומי כך ש-$x \in L$ אם ורק אם קיים c באורך $|c| \le p(|x|)$ שעבורו $V(x,c)$ מקבלת. באופן שקול, NP היא מחלקת השפות הנכרעות בזמן פולינומי במכונה אי-דטרמיניסטית.

רדוקציות (שיעורים 8–9). $A \le_p B$ פירושו: קיימת פונקציה f הניתנת לחישוב בזמן פולינומי כך שלכל x מתקיים $x \in A \iff f(x) \in B$. **שימו לב לכיוון:** $A \le_p B$ אומר ש-B היא הבעיה *הקשה* יותר — אפשר לפתור את A אם יודעים לפתור את B. בהקלטה, כמו בכל דיבור חופשי, הכיוון

מתהפך לעיתים קרובות; תמיד תרגמו חזרה לניסוח הפורמלי. שפה B היא NP-hard אם לכל $A \in \mathrm{NP}$ מתקיים $A \le_p B$, והיא NP-complete אם בנוסף $B \in \mathrm{NP}$. הכלי המרכזי: אם C היא NP-hard ו-$C \le_p B$, אז גם B היא NP-hard, מפני שהיחס $\le_p$ טרנזיטיבי.

התוצאות שנשתמש בהן בפועל. משפט קוק–לוין (שיעור 9) נותן לנו את SAT כבעיה ה-NP-complete הראשונה, ומשיעור 10 יש בידינו ש-$\mathrm{3SAT}$, $\mathrm{3COL}$ ו-VC הן NP-complete. בשיעור הזה נשתמש ישירות רק בשתי עובדות: $\mathrm{3COL}$ היא NP-hard, ו-VC היא NP-hard.

נזכיר במלואן את שתי ההגדרות מהשיעור הקודם, כדי שלא תצטרכו לקפוץ:

VC (Vertex Cover): הקלט הוא זוג (G, K) כאשר $G = (V, E)$ גרף לא מכוון ו-$K \in \mathbb{N}$. **כיסוי בקודקודים** הוא קבוצה $U \subseteq V$ כך שלכל קשת $e \in E$ יש **לפחות** קצה אחד ב-U (בהקלטה [00:53:37] סטודנט הציע "בדיוק אחד" והמרצה תיקן במפורש ל"לפחות אחד"; שימו לב שלפי זה V עצמה היא תמיד כיסוי). מתקיים $(G, K) \in \mathrm{VC}$ אם ורק אם קיים כיסוי בקודקודים U עם $|U| \le K$.

kCOL: הקלט הוא גרף $G = (V, E)$, והשאלה היא האם קיימת פונקציה $f : V \to \{1, \dots, k\}$ כך שאף קשת אינה מונוכרומטית, כלומר לכל $xy \in E$ מתקיים $f(x) \neq f(y)$. k הוא חלק *משם הבעיה*, לא מהקלט. הפונקציה **אינה** חייבת להיות על: מותר שצבע לא ינוצל כלל ([00:15:50]).

הגדרות

הגדרה 1: שפה טריוויאלית

תהי Σ אלפבית. שפה $B \subseteq \Sigma^*$ נקראת **טריוויאלית** אם $B = \emptyset$ או $B = \Sigma^*$. אחרת היא **אינה טריוויאלית**, כלומר קיימים $b_1 \in B$ וגם $b_0 \notin B$.

אינטואיציה. שפה טריוויאלית היא שפה שהתשובה עליה קבועה מראש ואינה תלויה בקלט: אפשר להכריע אותה בזמן קבוע ובמקום קבוע, בלי אפילו לקרוא את הקלט. לכן היא "קלה מדי" מכל בחינה, ובפרט אי אפשר לבצע אליה רדוקציה משפה כלשהי שאינה טריוויאלית — אין לאן לשלוח את שני סוגי הקלטים.

דוגמה. SAT אינה טריוויאלית: הנוסחה $x \vee \neg x$ ספיקה, והנוסחה $x \wedge \neg x$ אינה. *אי-דוגמה.* השפה $\{x : |x| \ge 0\} = \Sigma^*$ טריוויאלית.

הגדרה 2: הבעיה SUBSET SUM

הקלט הוא סדרה של n מספרים טבעיים $a_1, a_2, \dots, a_n$ ומספר טבעי נוסף S, כולם נתונים בבסיס 10. השאלה:

$$(a_1, \dots, a_n, S) \in \text{SUBSET-SUM} \iff \exists\, I \subseteq \{1, \dots, n\} \ \text{s.t.} \ \sum_{i \in I} a_i = S.$$

אינטואיציה. מבקשים לבחור חלק מן המספרים כך שיפגעו בדיוק ביעד. שימו לב שמדובר ב**סדרה** ולא בקבוצה: מותר שיופיעו חזרות, ולכן תת-הקבוצה היא של **אינדקסים** ולא של ערכים ([00:03:08] בהקלטה של שיעור 12, לגבי הבעיה האחות PARTITION — אותה הערה בדיוק).

דוגמה. $(3, 7, 11, 2 \ ; \ S = 13) \in \text{SUBSET-SUM}$ שכן $11 + 2 = 13$. *אי-דוגמה.* $(4, 6, 10 \ ; \ S = 13) \notin \text{SUBSET-SUM}$: כל המספרים זוגיים ולכן כל סכום חלקי זוגי.

הערת בסיס. בסיס 10 נבחר לנוחות בלבד — הוא מאפשר לכתוב על הלוח "חיבור ארוך" ולראות את העמודות ([00:56:15]). כל בסיס $b \geq 2$ נותן את אותה בעיה בדיוק, מפני שההמרה בין בסיס 2 לבסיס 10 משנה את אורך הייצוג בגורם קבוע $\log_2 10$. **הבסיס האונרי הוא היוצא מן הכלל היחיד** — ראו הגדרה 3.

הגדרה 3: ערך מספר מול אורך הייצוג שלו

עבור $a \in \mathbb{N}$, **הערך** הוא a עצמו, ואילו **אורך הייצוג** בבסיס $b \geq 2$ הוא $\lceil \log_b(a+1) \rceil$ ספרות.

הקשר ביניהם מעריכי: כדי לייצג את n נחוצים $\Theta(\log n)$ ביטים.

אינטואיציה. אלגוריתם נקרא פולינומי אם זמן ריצתו פולינומי ב**אורך הקלט**, לא בערכיו. כשהקלט הוא גרף גדול ומספר קטן, ההבחנה אינה מזיקה: בבעיות כמו CLIQUE ו-IS מקבלים (G, K), ו-$K \leq |V|$, כך שהגרף "בולע" את המספר ותרומתו לאורך הקלט זניחה ([00:48:18]). כשהקלט מורכב **כולו** ממספרים, כמו כאן, ההבחנה קריטית.

אי-דוגמה מאירה. אלגוריתם בדיקת ראשוניות הנאיבי עובר על כל המספרים עד $\sqrt{n}$ ובודק חלוקה. מספר האיטרציות $\sqrt{n}$ נראה פולינומי, אך אורך הקלט הוא $\Theta(\log n)$, ולכן $\sqrt{n} = 2^{\frac{1}{2}\log n}$ הוא **מעריכי** באורך הקלט ([00:49:19]).

המקרה האונרי. אם מייצגים מספר בבסיס 1 (אונרי), אורך הייצוג שווה לערך. אז — ורק אז — אלגוריתם שזמנו פולינומי בערך הופך לאלגוריתם פולינומי ([00:50:25]).

משפטים והוכחות

משפט 1: כל שפה ב-P ניתנת לרדוקציה לכל שפה לא-טריוויאלית

תהיינה $A, B \subseteq \Sigma^*$ שפות. אם $A \in P$ ו-B אינה טריוויאלית, אז $A \leq_p B$.

תזכורת מחישוביות ([00:00:32]). ראינו שם את הטענה המקבילה: אם $A \in R$ (כריעה) ו-B אינה טריוויאלית, אז $A \leq_m B$. ההוכחה כאן היא *אותה הוכחה בדיוק*; ההבדל היחיד הוא שכאן מתחייבים גם על זמן הריצה של הרדוקציה.

הוכחה. מכיוון ש-$A \in P$, קיימת מכונה M_A המכריעה את A בזמן פולינומי. מכיוון ש-B אינה טריוויאלית, קיים $b_1 \in B$ וקיים $b_0 \notin B$. **שני המחרוזות האלה קבועות ונבחרות לפני שהמכונה רואה קלט כלשהו.**

נגדיר מכונה M באופן הבא. על קלט x:

הרץ את M_A על x.

אם M_A קיבלה את x — החזר b_1. אחרת — החזר b_0.

נכונות. יהי $x \in \Sigma^*$.

נניח $x \in A$. אז M_A מקבלת את x, ולכן $M(x) = b_1 \in B$.

נניח $x \notin A$. אז M_A דוחה את x, ולכן $M(x) = b_0 \notin B$.

בשני המקרים $M(x) \in B \iff x \in A$, כנדרש.

זמן ריצה. שלב 1 דורש זמן פולינומי ב-$|x|$, לפי הגדרת M_A. שלב 2 הוא כתיבת אחת משתי מחרוזות **קבועות**. כאן ישנה נקודה עדינה שסטודנטית העלתה בהקלטה ([00:09:43]): "אבל b_0, b_1 עלולים להיות ארוכים מאוד!" — נכון, אבל אורכם אינו תלוי ב-x. המכונה M מחזיקה אותם "בבטן" כחלק

מתיאורה, היא לא מקבלת אותם מבחוץ, והם נקבעו לפני שהוגדר x. לכן, **כפונקציה של** $|x|$, שלב 2 לוקח זמן קבוע. סך הכול M רצה בזמן פולינומי בגודל הקלט, ולכן $A \leq_p B$. ■

המשמעות ([00:02:37]–[00:04:12]). הטענה אומרת ש-P היא המחלקה הקלה ביותר ביחס לרדוקציות זמן פולינומי: כל שפה לא-טריוויאלית "קשה לפחות כמו" *כל* שפה ב-P. אבל אנחנו יודעים שגם בתוך P יש דרגות קושי — למשל, ממשפט ההיררכיה לזמן (מן הפרק הראשון של הקורס) יש שפה הניתנת להכרעה בזמן n^3 ולא בזמן ליניארי. המסקנה: **רדוקציות זמן פולינומי הן כלי גס מדי מכדי להבחין בין בעיות בתוך** P — מבחינתן כל הבעיות ב-P הן אותו דבר. זהו הכלי המתאים להוכחת קושי, לא לדירוג עדין.

> **הערה:** בהרצאה זה נאמר בקיצור; הפירוט כאן. השימוש הישיר בטענה (בשיעורי הבית, [00:12:25]) הוא להראות שמחלקה כמו $\mathrm{DTime}(n^{10})$ **אינה סגורה** לרדוקציות זמן פולינומי. הנימוק: קחו $B \in \mathrm{DTime}(n^{10})$ לא-טריוויאלית כלשהי (למשל $B = \{x : x$ מתחיל ב-$\{0$, שהיא אפילו ליניארית). לפי משפט ההיררכיה לזמן קיימת $A \in \mathrm{DTime}(n^{11}) \setminus \mathrm{DTime}(n^{10})$, ובפרט $A \in P$. לפי משפט 1, $A \leq_p B$. אילו $\mathrm{DTime}(n^{10})$ הייתה סגורה כלפי מטה ל-$\leq_p$, היה נובע $A \in \mathrm{DTime}(n^{10})$ — סתירה.

משפט 2: $4\mathrm{COL}$ היא NP-complete

שייכות ל-NP. ה-certificate הוא הצביעה עצמה, $g : V \to \{1,2,3,4\}$, שאורכה $2|V|$ ביטים — פולינומי בגודל הקלט. ה-verifier עובר על כל הקשתות ובודק לכל $xy \in E$ ש-$g(x) \neq g(y)$; זמן $O(|E|)$. הבדיקה מקבלת אם ורק אם קיימת צביעה חוקית, כנדרש.

NP-hardness: $3\mathrm{COL} \leq_p 4\mathrm{COL}$.

האלגוריתם. על קלט $G = (V, E)$:

בנה גרף $\hat{G}$ על ידי הוספת קודקוד חדש $\hat{v}$ לגרף, וחיבורו בקשת לכל הקודקודים ב-V.

החזר את $\hat{G}$.

זמן ריצה. הבנייה מוסיפה קודקוד אחד ו-$|V|$ קשתות, ולכן היא לינארית בגודל הקלט; בפרט פולינומית. הפלט קטן מפי שניים מן הקלט ועוד קבוע, כך שגודלו פולינומי בגודל הקלט ([00:26:10]).

נכונות. יהי $G = (V, E)$ גרף. נסמן ב-$\hat{G} = (\hat{V}, \hat{E})$ את הגרף המוחזר על ידי האלגוריתם בהרצתו על G, וב-$\hat{v}$ את הקודקוד הנוסף.

כיוון ראשון: $G \in 3\mathrm{COL} \Rightarrow \hat{G} \in 4\mathrm{COL}$. קיימת צביעה חוקית $f : V \to \{1,2,3\}$, כלומר אין ב-G קשת מונוכרומטית. נגדיר $g : \hat{V} \to \{1,2,3,4\}$ על ידי

$$g(v) = \begin{cases} f(v) & v \in V \\ 4 & \text{otherwise} \end{cases}$$

תהא $e = xy \in \hat{E}$.

אם $e \in E$, אז $g(x) = f(x)$ ו-$g(y) = f(y)$, ומכיוון ש-f צביעה חוקית של G נובע $g(x) \neq g(y)$.

אחרת e היא קשת חדשה, ולכן $x = \hat{v}$ או $y = \hat{v}$. הקודקוד $\hat{v}$ צבוע ב-4 והשני צבוע בצבע מתוך $\{1,2,3\}$, ולכן שוב $g(x) \neq g(y)$.

כך או כך $g(x) \neq g(y)$, ולכן g היא צביעה חוקית של $\hat{G}$ ב-4 צבעים, כלומר $\hat{G} \in 4\mathrm{COL}$.

כיוון שני: $\hat{G} \in 4\mathrm{COL} \Rightarrow G \in 3\mathrm{COL}$. קיימת צביעה חוקית $g : \hat{V} \to \{1,2,3,4\}$ של $\hat{G}$. ללא הגבלת הכלליות $g(\hat{v}) = 4$ — הצבעים סימטריים לחלוטין, ואם קיבל צבע אחר נחליף את שמות שני הצבעים. נגדיר $f : V \to \{1,2,3,4\}$ על ידי $f(v) = g(v)$ לכל $v \in V$, ונראה שהטווח בפועל הוא $\{1,2,3\}$: יהי $x \in V$. מכיוון שחיברנו את $\hat{v}$ ל**כל** קודקודי V, מתקיים $x\hat{v} \in \hat{E}$, ולכן $g(x) \neq g(\hat{v}) = 4$. לכן לכל $x \in V$ מתקיים $f(x) \in \{1,2,3\}$.
כעת תהא $xy \in E$ קשת. לא הסרנו קשתות, ולכן גם $xy \in \hat{E}$, ומכיוון ש-g חוקית ב-$\hat{G}$ נקבל $f(x) = g(x) \neq g(y) = f(y)$. לכן f היא צביעה חוקית של G ב-3 צבעים, כלומר $G \in 3\mathrm{COL}$. ■

למה הבנייה נראית כך — שני ניסיונות שנשברו.

ניסיון ראשון: הזהות ([00:16:53]–[00:18:30]). סטודנט הציע להחזיר את G עצמו: הרי אם G הוא 3-צביע אז בפרט הוא 4-צביע. הכיוון הראשון עובד — וזו בדיוק הסיבה לחשוד. הכיוון השני קורס: הקליק K_4 הוא 4-צביע (כל קודקוד בצבע משלו) ובוודאות אינו 3-צביע, שכן בקליק בגודל n כל שני קודקודים מחוברים ולכן דרושים n צבעים. אז $K_4 \in 4\mathrm{COL}$ אבל $K_4 \notin 3\mathrm{COL}$, והזהות אינה רדוקציה.

ניסיון שני: להוסיף קודקוד בלי לחבר אותו ([00:31:29]–[00:34:41]). סטודנטית שאלה למה בכלל צריך את הקשתות החדשות. גם כאן הכיוון הראשון עובר בלי שינוי. הכיוון השני נשבר בדיוק בשורה אחת: הצעד שאומר "לכל $x \in V$ מתקיים $g(x) \neq 4$" נשען כולו על קיום הקשת $x\hat{v}$. בלי הקשתות אין שום מניעה שקודקוד ב-V ייצבע ב-4, והצמצום של g ל-V לא יהיה צביעה בשלושה צבעים.

> **הערה:** בהרצאה נאמר על כך רק ש"ההוכחה נשברת"; שימו לב שזה **אינו** מוכיח שהבנייה החלופית אינה רדוקציה — היא באמת אינה, אבל כדי לטעון זאת דרושה דוגמה נגדית, ולא רק כישלון של הוכחה מסוימת. דוגמה נגדית: $G = K_4$ ללא הקשתות החדשות נותן גרף שהוא K_4 בתוספת קודקוד מבודד; הגרף הזה 4-צביע, ואילו K_4 אינו 3-צביע.

ניסיון שלישי — ולמעשה הטעות החמורה מכולן ([00:21:39]–[00:23:45]). סטודנט ניסח את אותה בנייה נכונה במילים "נוסיף קודקוד חדש **ונצבע אותו** בצבע רביעי", והמרצה עצר את השיעור וכינה זאת "חטא כבד". שימו לב היכן בדיוק נמצאת הטעות: הבנייה זהה, אבל הניסוח מייחס לאלגוריתם גישה לצביעה. **לאלגוריתם הרדוקציה אין ולא יכולה להיות גישה לפתרון.** הוא מקבל גרף ומחזיר גרף; הוא אינו מחפש צביעה, אינו מקבל אחת ואינו יודע אם קיימת. הצביעות f ו-g מופיעות אך ורק ב**הוכחת הנכונות**, ששם — ורק שם — מותר להניח "קיימת צביעה חוקית". זו הסיבה שבניסוח שלמעלה שלב 1 של האלגוריתם מדבר רק על קודקודים וקשתות, ואילו הפונקציה g מוגדרת רק בתוך כיוון ההוכחה. המרצה השווה זאת לרדוקציה מ-HALT: אסור לכתוב "אם המכונה עוצרת אז נחזיר כך", מפני שאי אפשר לבדוק זאת. אותו עיקרון בדיוק חוזר במשפט 4 להלן — הרדוקציה מ-VC ל-$\mathrm{SUBSET\text{-}SUM}$ בונה מספרים מהגרף ומ-K בלבד, ואינה מחפשת כיסוי.

משפט 3: $\mathrm{SUBSET\text{-}SUM} \in \mathrm{NP}$

הוכחה. ה-certificate הוא קבוצת האינדקסים $I \subseteq \{1,\dots,n\}$, שאפשר לקודד ב-$n$ ביטים — פולינומי בגודל הקלט. ה-verifier מקבל $(a_1,\dots,a_n,S)$ ואת I, מסכם $\sum_{i\in I} a_i$ ומשווה ל-S. אם כל מספר תופס לכל היותר ℓ ספרות, חיבור של עד n מספרים כאלה דורש $O(n\ell)$ פעולות,

וההשוואה $O(\ell)$ — כלומר זמן פולינומי באורך הקלט. ה-verifier מקבל עבור $certificate$ כלשהו אם ורק אם קיימת I עם הסכום הנכון, כלומר אם ורק אם הקלט בשפה. באופן שקול: בוחרים את I **באופן אי-דטרמיניסטי** ומסכמים. ■

> **הערה:** המרצה הדגיש שוב ושוב שלא אומרים "מגרילים" אלא "בוחרים באופן אי-דטרמיניסטי" — הגרלה שייכת לאלגוריתמים אקראיים, ואי-דטרמיניזם הוא דבר אחר לגמרי (ההערה נאמרה במפורש בשיעור העוקב, [00:03:40] בתמליל 18, לגבי אותו טיעון בדיוק).

משפט 4 (לב השיעור): $\mathrm{VC} \le_p \text{SUBSET-SUM}$, ולכן SUBSET-SUM היא NP-complete
הרעיון. נבנה מספרים שאפשר לחשוב עליהם כשורות בטבלה: עמודה מיוחדת אחת בשם d, ועוד עמודה אחת לכל קשת. שורת קודקוד "מדווחת" באילו קשתות הוא נוגע; שורת קשת היא וקטור יחידה. סכום היעד דורש בדיוק 2 בכל עמודת קשת ובדיוק K בעמודה d. הקסם הוא שהדרישה "בדיוק 2" ניתנת לסיפוק אם ורק אם לפחות אחד משני קצות הקשת נבחר.
האלגוריתם. על קלט $G=(V,E)$ ו-$K \in \mathbb{N}$, נסמן $m = |E|$ ו-$E = \{e_1, \dots, e_m\}$.
אם $K > |V|$, החלף את K ב-$|V|$. (הצדקה למטה.)
לכל קודקוד $v \in V$ נייצר מספר a_v בן $m+1$ ספרות, שבו הספרה השמאלית ביותר היא 1, ולכל $1 \le j \le m$ הספרה ה-$(j+1)$ משמאל היא 1 אם $v \in e_j$ ו-0 אחרת.
לכל קשת $e \in E$ נייצר מספר a_e בן $m+1$ ספרות, שבו הספרה השמאלית ביותר היא 0, ולכל $1 \le j \le m$ הספרה ה-$(j+1)$ משמאל היא 1 אם ורק אם $e = e_j$, ואחרת 0.
נגדיר מספר יעד S בן $\lceil \log_{10}(K+1) \rceil + m$ ספרות: $\lceil \log_{10}(K+1) \rceil$ הספרות השמאליות ביותר מייצגות את K, וכל יתר הספרות שוות 2.
החזר את רשימת המספרים $\{a_v\}_{v \in V} \cup \{a_e\}_{e \in E}$ ואת S.
באלגברה, במקום בציור, אלה בדיוק המספרים

$$a_v \;=\; 10^{m} \;+\; \sum_{j=1}^{m} [\, v \in e_j \,] \cdot 10^{m-j}, \qquad a_{e_i} \;=\; 10^{m-i}, \qquad S \;=\; K \cdot 10^{m} \;+\; \sum_{j=1}^{m} 2 \cdot 10^{m-j}.$$

על צעד 0 והביטוי "בדיוק K". ההגדרה של VC מדברת על כיסוי בגודל **לכל היותר** K, ואילו הבנייה כופה בעמודה d סכום של **בדיוק** K. הפער אינו מזיק, משתי סיבות: (א) הוספת קודקודים לכיסוי משאירה אותו כיסוי, ולכן אם קיים כיסוי בגודל $\le K$ ו-$K \le |V|$, אפשר להשלים אותו לכיסוי בגודל בדיוק K; (ב) אם $K > |V|$ אז $(G,K) \in \mathrm{VC}$ תמיד (הקבוצה V עצמה מכסה), ולכן ההחלפה $K \leftarrow |V|$ אינה משנה את התשובה, שכן $(G,K) \in \mathrm{VC} \iff (G, \min(K,|V|)) \in \mathrm{VC}$. צעד 0 מבוצע בזמן $O(\log K + \log |V|)$.

> **הערה:** בהרצאה ובסיכום עוברים ישר ל"קיים U כיסוי עם $|U| = K$" ([01:13:18]) בלי לומר מדוע מותר; הפירוט כאן.

למה 4.1 (אי-נשאות) — הצעד שבלעדיו כלום לא עובד
תהי I תת-קבוצה כלשהי של המספרים שנבנו. נסמן $U = I \cap \{a_v\}_{v \in V}$ (ונזהה אותה עם קבוצת קודקודים), ולכל $1 \le j \le m$ נסמן

$$c_j \;=\; \big|\{ v \in U : v \in e_j \}\big| \;+\; [\, a_{e_j} \in I \,].$$

אזי:

$0 \le c_j \le 3$ לכל j;

$\sum_{x \in I} x \;=\; |U| \cdot 10^m \;+\; \sum_{j=1}^{m} c_j \cdot 10^{\,m-j}$, וזהו בדיוק הייצוג העשרוני של הסכום בספרות $c_1, \ldots, c_m$ — כלומר **החיבור הארוך אינו נושא באף עמודת קשת**;

$$\sum_{j=1}^{m} c_j \cdot 10^{\,m-j} < 10^m.$$

הוכחה. (1) לקשת e_j יש **בדיוק שני** קצוות. לכן לכל היותר שני מספרי קודקוד נושאים 1 בעמודה j, ובנוסף בדיוק מספר קשת אחד — a_{e_j} — נושא שם 1. סך כל האחדות בעמודה j על פני **כל** המספרים שנבנו הוא לכל היותר $2 + 1 = 3$, ובפרט זה חסם על c_j.

(2) הזהות עצמה נובעת מפתיחת הסכום לפי ההצגה האלגברית שלמעלה וקיבוץ לפי חזקות 10. הטענה שזהו הייצוג העשרוני נובעת מ-(1): כל מקדם c_j מקיים $0 \le c_j \le 3 \le 9$, ולכן הוא **ספרה חוקית** בבסיס 10 ואין העברה לעמודה שמשמאלה. זו כל המשמעות של "אין נשאות": בסיס 10 נבחר גדול דיו מכדי שסכום עמודה כלשהי יגלוש. (למעשה כל בסיס ≥ 4 היה מספיק; בסיס 10 נבחר מטעמי נוחות כתיבה בלבד.)

(3) $\displaystyle\sum_{j=1}^{m} c_j 10^{m-j} \le \sum_{j=1}^{m} 3 \cdot 10^{m-j} = 3 \cdot \frac{10^m - 1}{9} = \frac{10^m - 1}{3} < 10^m.$ ■

למה זה קריטי. בלי (1) לא היינו רשאים "לקרוא ספרה-ספרה". אילו סכום עמודה כלשהי היה מגיע ל-10 או יותר, הוא היה מעביר 1 שמאלה, וסכום כולל שנראה נכון היה יכול להתקבל מצירוף עמודות שגוי לגמרי — למשל 10 אחדות בעמודה אחת היו "מתחזות" לספרה 1 בעמודה שכנה. הטיעון כולו נשען על כך שאין שום קשר בין העמודות, ולכן **שוויון הסכומים גורר שוויון בכל ספרה בנפרד**. זה מנוסח כמסקנה הבאה.

מסקנה 4.2 (קריטריון הספרות)

בסימוני למה 4.1, מתקיים $\sum_{x \in I} x = S$ אם ורק אם $|U| = K$ וגם $c_j = 2$ לכל $1 \le j \le m$.

הוכחה. ($\Leftarrow$) הצבה ישירה בזהות של למה 4.1(2).

($\Rightarrow$) נסמן $L = \sum_j c_j 10^{m-j}$ ו-$L' = \sum_j 2 \cdot 10^{m-j}$. לפי למה 4.1(3) מתקיים $0 \le L < 10^m$, ובאותו חשבון גם $0 \le L' < 10^m$. מן ההנחה, $|U| \cdot 10^m + L \;=\; K \cdot 10^m + L' \quad\Longrightarrow\quad \big(|U| - K\big) \cdot 10^m \;=\; L' - L.$ אגף ימין מקיים $|L' - L| < 10^m$, ואגף שמאל הוא כפולה שלמה של 10^m; לכן שני האגפים אפס. מכאן $|U| = K$ וגם $L = L'$. שני הסכומים כתובים במקדמים שכולם בין 0 ל-9 (למה 4.1(1), ו-$9 \le 2$), ולכן מיחידות ההצגה בבסיס 10 נובע $c_j = 2$ לכל j. ■

שימו לב היכן נכנס כאן הצורך לכתוב את K כ**בלוק** של ספרות ולא כספרה בודדת: מספר הקודקודים הנבחרים $|U|$ עשוי להיות 10 או יותר, ואז "הספרה" השמאלית איננה ספרה. הטיעון לעיל אינו מניח דבר על $|U|$ — הוא רק מנצל את העובדה שכל מה שמתחת ל-10^m אינו מגיע ל-10^m.

הוכחת המשפט

זמן ריצה. האלגוריתם עובר לולאה אחת על הקודקודים ולולאה אחת על הקשתות, וכותב לכל אחד מהם מספר בן $m+1$ ספרות; בנוסף הוא כותב את S. סך גודל הפלט הוא $O\big((|V|+m)\cdot(m+\log K)\big)$ ספרות — פולינומי בגודל הקלט. בדיקת "האם $v \in e_j$" היא $O(1)$ בייצוג רשימות שכנויות, ולכן זמן החישוב פרופורציוני לגודל הפלט. המרצה ציין שהאלגוריתם רץ למעשה בזמן ליניארי בגודל הפלט ([01:11:00]).

> **הערה חשובה שנאמרה רק ברמז:** ה**ערך** של כל מספר שנבנה הוא בסדר גודל 10^m — מעריכי בגודל הקלט! זו אינה בעיה, מפני שהרדוקציה נדרשת לרוץ בזמן פולינומי, ו**כתיבת** מספר כזה עולה רק $m+1$ ספרות. זו בדיוק ההבחנה של הגדרה 3, מן הצד השני שלה: הרדוקציה חוקית רק מפני שמותר לה לייצר מספרים בעלי ערך אדיר באורך ייצוג צנוע.

נכונות, כיוון ראשון: הפלט ב-SUBSET-SUM. $(G,K)\in \text{VC} \Rightarrow$
נניח $(G,K)\in \text{VC}$ (לאחר צעד 0 מתקיים $K \le |V|$). לפי הדיון על צעד 0 קיים כיסוי בקודקודים $U \subseteq V$ עם $|U| = K$ **בדיוק**. נסמן $I_1 = \{a_u \mid u \in U\}$.
נסכום את המספרים ב-I_1. בעמודה d כל אחד מהם תורם 1, ובחרנו בדיוק K קודקודים, ולכן התרומה שם היא K — בדיוק כמו ב-S.
כעת יהי $1 \le j \le m$. מכיוון ש-U כיסוי, **לפחות** אחד מקצות e_j שייך ל-U; ומכיוון של-e_j יש רק שני קצוות, **לכל היותר** שניים שייכים. לכן סכום הספרות בעמודה j הוא 1 או 2.
נגדיר I_2 כך: לכל j שעבורו סכום העמודה יצא 1, נוסיף ל-I_2 את המספר a_{e_j} המתאים לאותה קשת. המספר a_{e_j} מוסיף 1 בדיוק לעמודה j ואפס לכל עמודה אחרת (כולל עמודת d), ולכן הוא "מתקן" מ-1 ל-2 בלי לגעת בשום מקום אחר. שימו לב שהוא **אינו** יכול לתקן מ-0 ל-2 — וזה מדויק: המצב 0 לא ייתכן כאן דווקא מפני ש-U כיסוי ([01:18:47]).
נקבל $c_j = 2$ לכל j ו-$|U| = K$, ולפי מסקנה 4.2 סכום המספרים ב-$I_1 \cup I_2$ הוא בדיוק S.
נכונות, כיוון שני: הפלט ב-SUBSET-SUM. $\Rightarrow (G,K)\in \text{VC}$

> **הערה:** כיוון זה אינו כתוב בסיכום, ובהרצאה הוא נאמר בעל פה בלבד ([01:29:33]) עם המשפט "אתם רוצים באמת להרגיש שאתם מבינים את זה — תכתבו את זה". הנה הכתיבה.

נניח שקיימת תת-קבוצה I של המספרים שנבנו שסכומה בדיוק S. נסמן, כמו בלמה 4.1, $U = I \cap \{a_v\}_{v\in V}$ (מזוהה עם קבוצת קודקודים). לפי מסקנה 4.2 מתקיים

$$|U| = K, \qquad c_j = \big|\{v \in U : v \in e_j\}\big| + [\,a_{e_j} \in I\,] = 2 \quad \text{for every } 1 \le j \le m.$$

יהי $1 \le j \le m$. המחובר $[\,a_{e_j} \in I\,]$ הוא לכל היותר 1, שכן יש **מספר אחד בלבד** המתאים לקשת e_j ולכן אפשר לבחור אותו לכל היותר פעם אחת. לכן

$$\big|\{v \in U : v \in e_j\}\big| \;=\; 2 - [\,a_{e_j} \in I\,] \;\ge\; 1.$$

כלומר לכל קשת e_j יש לפחות קצה אחד ב-U, ולכן U הוא כיסוי בקודקודים של G. גודלו $|U| = K \le K$, ולכן $(G,K)\in \text{VC}$. ■

מסקנה. VC היא NP-hard (שיעור 10), ולפי הטרנזיטיביות של $\le_p$ נובע ש-SUBSET-SUM היא NP-hard. יחד עם משפט 3 מתקבל ש-SUBSET-SUM היא NP-complete.

משפט 5: אלגוריתם התכנון הדינמי אינו אלגוריתם פולינומי

בקורס האלגוריתמים ראינו אלגוריתם תכנון דינמי המכריע את SUBSET-SUM בזמן $O(n \cdot S)$ (טבלה בגודל $n \times S$). **האלגוריתם הזה אינו פולינומי בגודל הקלט.**

הוכחה. נתבונן במשפחת קלטים שבה המספרים גדולים משמעותית מכמותם: לכל $1 \le i \le n$ מתקיים $2^n \le a_i \le 2^{2n}$, וכן $2^n \le S \le 2^{2n}$.

גודל הקלט. יש $n+1$ מספרים, וכל אחד מהם דורש לכל היותר $2n$ ביטים. לכן אורך הקלט הוא לכל היותר $(n+1) \cdot 2n = O(n^2)$ ביטים.

זמן הריצה. $n \cdot S \ge n \cdot 2^n$, שכן $S \ge 2^n$.

ההשוואה. נסמן ב-N את אורך הקלט; אז $N = \Theta(n^2)$, כלומר $n = \Theta(\sqrt{N})$, וזמן הריצה הוא לפחות $2^{\Omega(\sqrt{N})}$. הפונקציה $2^{\sqrt{N}}$ גדולה אסימפטוטית מכל פולינום ב-N, ולכן זמן הריצה אינו פולינומי בגודל הקלט. ■

מה זה בדיוק ([00:46:11], [00:47:13]). הביטוי $2^{\sqrt{N}}$ הוא לא בדיוק "מעריכי" — זה מעריכי בשורש של גודל הקלט — אבל הוא בוודאות אינו פולינומי. המרצה הקפיד על הניסוח הזה. אלגוריתם כזה נקרא **pseudo-polynomial**: פולינומי בערך המספרים ולא באורך ייצוגם.

המסקנה על הבעיה. מכאן ש-SUBSET-SUM היא NP-hard **חלשה** (weakly NP-hard): אם היו מייצגים את המספרים בבסיס אונרי, אורך הייצוג היה שווה לערך, אלגוריתם ה-$O(n \cdot S)$ היה נעשה פולינומי, והבעיה הייתה נופלת ל-P. שימו לב שזה אינו סותר את משפט 4: הרדוקציה שם מייצרת מספרים שערכם כ-10^m, וכתיבתם בבסיס אונרי הייתה דורשת מקום מעריכי — כלומר הרדוקציה **אינה** רדוקציה ל-SUBSET-SUM האונרית.

דוגמאות ותרגילים מהשיעור

דוגמה 1: מעקב מלא אחרי הרדוקציה $\text{VC} \le_p \text{SUBSET-SUM}$

זהו בדיוק המופע שהמרצה הריץ על הלוח והופיע בעמוד 5 בסיכום.

הגרף. $V = \{1,2,3,4,5\}$, ריבוע $1-2-3-4-1$ ובתוכו קודקוד 5 המחובר ל-2 ול-4.

הקשתות ממוספרות:

$$e_1 = \{1,2\},\quad e_2 = \{2,3\},\quad e_3 = \{3,4\},\quad e_4 = \{1,4\},\quad e_5 = \{2,5\},\quad e_6 = \{4,5\},\qquad K = 3.$$

כאן $n = |V| = 5$, $m = |E| = 6$, וכל מספר הוא בן 7 ספרות.

המספרים שהאלגוריתם מייצר.

	d	e_1	e_2	e_3	e_4	e_5	e_6
a_1	1	1	0	0	1	0	0
a_2	1	1	1	0	0	1	0
a_3	1	0	1	1	0	0	0
a_4	1	0	0	1	1	0	1

	d	e_1	e_2	e_3	e_4	e_5	e_6
a_5	1	0	0	0	0	1	1
a_{e_1}	0	1	0	0	0	0	0
a_{e_2}	0	0	1	0	0	0	0
a_{e_3}	0	0	0	1	0	0	0
a_{e_4}	0	0	0	0	1	0	0
a_{e_5}	0	0	0	0	0	1	0
a_{e_6}	0	0	0	0	0	0	1
S	**3**	2	2	2	2	2	2

בקריאה כמספרים: $a_3 = 1011000$, $a_{e_5} = 0000010$, $S = 3222222$. שורות הקשתות הן בדיוק מטריצת היחידה ([01:24:48])‏, ושורת קודקוד היא שורת מטריצת השכנויות קודקוד–קשת עם 1 מוביל.

כיוון ראשון (מכיסוי לסכום). ניקח את הכיסוי $U = \{2, 4, 5\}$, שגודלו $|U| = 3 = K$. ואכן הוא כיסוי: e_1 מכוסה על ידי 2, e_2 על ידי 2, e_3 על ידי 4, e_4 על ידי 4, e_5 על ידי 2 ו-5, ו-e_6 על ידי 4 ו-5.

$$I_1 = \{a_2, a_4, a_5\}, \qquad a_2 + a_4 + a_5 \;=\; 3111122.$$

בדיקה עמודה-עמודה: d: $3 = 1 + 1 + 1$. e_1: $1 = 0 + 0 + 1$. e_2: $1 = 0 + 0 + 1$. e_3: $0 + 1 = 1$. e_4: $1 = 0 + 1 + 0$. e_5: $2 = 1 + 0 + 1$. e_6: $2 = 1 + 1 + 0$. אף עמודה לא עברה את 2 — כמובטח בלמה 4.1.

העמודות e_1, e_2, e_3, e_4 יצאו 1, ולכן

$$I_2 = \{a_{e_1}, a_{e_2}, a_{e_3}, a_{e_4}\},$$

ובחיבור:

$$3111122 + 0100000 + 0010000 + 0001000 + 0000100 \;=\; 3222222 \;=\; S. \qquad \checkmark$$

כיוון שני (מסכום לכיסוי). נניח שמישהו נותן לנו את הקבוצה $\{a_2, a_4, a_5, a_{e_1}, a_{e_2}, a_{e_3}, a_{e_4}\}$ ואומר שסכומה S. לפי מסקנה 4.2 אנחנו קוראים מן הסכום: הבלוק השמאלי הוא 3, ולכן נבחרו בדיוק 3 מספרי קודקוד — הקודקודים $\{2, 4, 5\}$. בכל עמודת קשת הסכום הוא 2; למשל בעמודה e_3 תרם a_4 אחת ו-a_{e_3} אחת. מכיוון ש-a_{e_3} יכול לתרום לכל היותר 1, בהכרח לפחות אחד מקצות e_3 נמצא בקבוצה — וזה 4. חוזרים על אותו שיקול לכל אחת משש העמודות ומקבלים ש-$\{2, 4, 5\}$ מכסה את כל הקשתות, כלומר כיסוי בקודקודים בגודל $\le K$. $\checkmark$

מה היה קורה בלי אי-נשאות? נניח לרגע שהיינו עובדים בבסיס 2 **ובעמודה של e_5 היו שלושה מספרים עם** 1. אז $1 + 1 + 1 = 3$ היה נכתב כ-11_2, כלומר נשא 1 לעמודה של e_4, וסכום סופי "נכון" היה יכול להתקבל מקבוצה שאינה כיסוי כלל. זו בדיוק הסיבה שאנחנו סופרים כמה אחדות יכולות להצטבר בעמודה (לכל היותר 3) ובוחרים בסיס גדול מזה.

דוגמה 2: הדוגמה עם 7 קשתות שנמחקה על הלוח

בעמוד 4 בסיכום מופיע אותו גרף עם 7 קשתות, ו-$a_3 = 10110001$, $S = 32222222$. בהקלטה ([01:22:44], [01:23:15]) המרצה אומר "מחקתי קשת אחת כדי שזה ייכנס לי ללוח" — כלומר עמוד 4 מתעד את המצב לפני המחיקה ועמוד 5 את המצב הסופי. שתי הגרסאות תקינות; הדוגמה המלאה והמאומתת היא זו שבדוגמה 1.

דוגמה 3: מעקב מלא אחרי הרדוקציה $3\mathrm{COL} \le_p 4\mathrm{COL}$

מופע חיובי. ניקח $G = C_5$, המעגל באורך 5: $V = \{1,2,3,4,5\}$ והקשתות $12, 23, 34, 45, 51$.

הבנייה. האלגוריתם מוסיף קודקוד $\hat{v}$ ומחבר אותו לכל חמשת הקודקודים. הגרף המתקבל $\hat{G}$ הוא הגלגל בעל 6 קודקודים ו-$10 = 5 + 5$ קשתות.

מ-$3\mathrm{COL}$ ל-$4\mathrm{COL}$. מעגל אי-זוגי אינו 2-צביע אבל כן 3-צביע; ניקח $f(1) = 1,\ f(2) = 2,\ f(3) = 1,\ f(4) = 2,\ f(5) = 3.$

בדיקה: $1 : 2 \neq 1$, $2 : 3 \neq 1$, $3 : 4 \neq 2$, $4 : 5 \neq 3$, $5 : 1 \neq 1$ — צביעה חוקית. לפי הבנייה שבמשפט 2 נגדיר g שמסכימה עם f על V ומקצה $g(\hat{v}) = 4$. חמש הקשתות הישנות בסדר כי f חוקית; חמש הקשתות החדשות בסדר כי $\hat{v}$ לבדו נושא את הצבע 4. לכן $\hat{G} \in 4\mathrm{COL}$. ✓

מ-$4\mathrm{COL}$ ל-$3\mathrm{COL}$. נניח שקיבלנו את הצביעה החוקית $g(1) = 2,\ g(2) = 3,\ g(3) = 2,\ g(4) = 3,\ g(5) = 4,\ g(\hat{v}) = 1.$

כאן $g(\hat{v}) \neq 4$, ולכן נפעיל את שלב "ללא הגבלת הכלליות": נחליף בין שמות הצבעים 1 ו-4 ונקבל $g'(\hat{v}) = 4$, $g'(5) = 1$, ושאר הערכים ללא שינוי. החלפת שמות צבעים שומרת על חוקיות, שכן היא פרמוטציה חח"ע של הטווח. כעת $f = g'|_V$ נותנת

$$f(1) = 2,\ f(2) = 3,\ f(3) = 2,\ f(4) = 3,\ f(5) = 1,$$

וכל הערכים אכן ב-$\{1,2,3\}$ — **בדיוק** מפני שכל קודקוד ב-V שכן של $\hat{v}$ ולכן אסור לו לקבל 4. הצביעה חוקית על כל חמש הקשתות של C_5, ולכן $G \in 3\mathrm{COL}$. ✓

מופע שלילי. ניקח $G = K_4$. אז $\hat{G} = K_5$. אכן $K_4 \notin 3\mathrm{COL}$ (בקליק בגודל n דרושים n צבעים) וגם $K_5 \notin 4\mathrm{COL}$ מאותו נימוק — הרדוקציה שולחת "לא" ל"לא", כנדרש. ✓

אותו מופע שובר את הבנייה השגויה. אילו לא היינו מחברים את $\hat{v}$ בקשתות, היינו מקבלים על הקלט K_4 את הגרף "K_4 ועוד קודקוד מבודד", שהוא 4-צביע. אז מופע ה"לא" היה נשלח למופע "כן" — דוגמה נגדית מפורשת לכך שהבנייה החלופית אינה רדוקציה.

תרגיל 1 (נפתר בכיתה): מדוע הזהות אינה רדוקציה מ-$3\mathrm{COL}$ ל-$4\mathrm{COL}$?

פתרון. צריך למצוא גרף שהוא 4-צביע ואינו 3-צביע. הקליק K_4 הוא כזה: הוא 4-צביע כי אפשר לתת לכל קודקוד צבע משלו, והוא אינו 3-צביע כי בקליק כל שני קודקודים מחוברים ולכן דרושים לפחות 4 צבעים. לכן $\mathrm{id}(K_4) = K_4 \in 4\mathrm{COL}$ אך $K_4 \notin 3\mathrm{COL}$, בסתירה לתנאי הרדוקציה.

תרגיל 2 (נפתר בכיתה): האם היה אפשר לעשות רדוקציה מ-IS או מ-CLIQUE במקום מ-VC?

פתרון ([00:54:41]). כן. יש רדוקציה מיידית $\mathrm{IS} \le_p \mathrm{VC}$: הקבוצה U היא כיסוי בקודקודים אם ורק אם $V \setminus U$ היא קבוצה בלתי תלויה, ולכן מספיק להעביר $(G, K) \mapsto (G, |V| - K)$. אפשר לשלב אותה בחזית הרדוקציה שלנו ולקבל $\mathrm{IS} \le_p \mathrm{SUBSET\text{-}SUM}$ ישירות. מ-CLIQUE עוברים

תחילה לגרף המשלים ואז ל-$|V| - K$. המרצה הדגיש שהבחירה ב-VC שרירותית לחלוטין ונובעת מכך שזו הרדוקציה הקלאסית בספרות ([00:55:43]) — לא מפני שהאחרות שגויות, אלא מפני שהן מוסיפות רעש להוכחה.

תרגיל 3 (שיעורי בית): $\mathrm{DTime}(n^{10})$ אינה סגורה לרדוקציות זמן פולינומי

פתרון. ראו ההערה בסוף משפט 1: בוחרים $B \in \mathrm{DTime}(n^{10})$ לא-טריוויאלית, לוקחים ממשפט ההיררכיה $A \in P \setminus \mathrm{DTime}(n^{10})$, ומקבלים ממשפט 1 ש-$A \le_p B$ בעוד $A \notin \mathrm{DTime}(n^{10})$.

תרגיל 4: מה גודל טבלת התכנון הדינמי?

פתרון ([01:05:32] בתמליל 18). סטודנט הציע לפתור בעיה קרובה בעזרת טבלה בגודל K. שאלת הבדיקה שהמרצה החזיר: כמה ביטים דרושים כדי לתאר את K? התשובה $\log K$, ולכן טבלה בגודל K היא **מעריכית** באורך הייצוג של K. זו בדיוק הבדיקה שיש להריץ בכל פעם שמופיע בקלט מספר, והיא זהה בתוכנה למשפט 5.

הערות מהשיעור

כל התזמונים מתייחסים לתמליל $Qf E6eBttdJg$ אלא אם צוין אחרת.

[00:21:39]–[00:23:45] — הטעות שהמרצה כינה "חטא כבד". סטודנט הציע כרדוקציה: "נוסיף קודקוד חדש ונצבע אותו בצבע רביעי". הבנייה עצמה נכונה, אבל **הניסוח** שגוי מיסודו: לאלגוריתם הרדוקציה אין שום גישה לצביעה. הוא מקבל גרף ומחזיר גרף, הוא לא מחפש צביעה, לא מקבל אותה ולא מעניין אותו אם קיימת. הצביעה מופיעה **רק בהוכחה** שהאלגוריתם הוא רדוקציה. המרצה השווה זאת לרדוקציה מ-HALT שבה אסור לומר "אם המכונה עוצרת אז נחזיר כך" — אי אפשר לבדוק זאת. עקרון הברזל: **רדוקציה אינה באה להכריע את הבעיה**, אלא רק להעביר תכונה הלאה מבלי לדעת כלל אם היא מתקיימת. זו בדיוק הנקודה שסטודנטים מפילים עליה במבחן.

[00:16:53] — איך בודקים ניסיון רדוקציה. "אם הכיוון הראשון קל מדי — תחשדו." זו הוריסטיקה טובה: כאשר כיוון אחד יוצא בשורה, בדרך כלל השני נשבר.

[00:15:50]–[00:16:21] — הפונקציה בצביעה אינה חייבת להיות על. צביעה ב-3 צבעים היא גם צביעה ב-4 צבעים שבה הצבע הרביעי לא נוצל. ואפילו אם רוצים "בדיוק 4", אפשר לצבוע קודקוד אחד מחדש בצבע הרביעי בלי ליצור קשת מונוכרומטית (בגרף עם לפחות ארבעה קודקודים). ב-MAXCUT, לעומת זאת, "לפחות" כן שינה — לא תמיד אפשר לעבור בין "בדיוק" ל"לכל היותר".

[00:09:43] — שאלת סטודנטית ששווה זהב. "אבל b_1 עלול להיות מחרוזת ארוכה מאוד, אז איך שלב 2 לוקח זמן קבוע?" התשובה: b_0, b_1 נקבעו **לפני** שראינו את הקלט; הם חלק מתיאור המכונה, לא חלק מהקלט. זמן ריצה נמדד תמיד כפונקציה של גודל הקלט, ולכן כתיבתם היא $O(1)$ ב-$|x|$. עצה תחבירית שהמרצה נתן: כתבו את המשתנים בסדר הופעתם — b_0, b_1 קודמים ל-x, ולכן אינם יכולים לתלות בו.

[00:52:32] — קיצורים. המרצה סירב במפורש לקצר את $\mathrm{SUBSET\text{-}SUM}$ לראשי תיבות. שווה לאמץ בכתיבה שלכם: ראשי תיבות מקומיים הם מקור נפוץ לבלבול בבדיקה.

[01:19:56]–[01:21:36] — "אל תשאלו איך הייתם חושבים על זה". אחרי שהוצגה הרדוקציה, סטודנטית שאלה איך בכלל חושבים על בנייה כזאת. תשובת המרצה: זו אינה השאלה הנכונה בשלב הזה. השאלה הנכונה היא "האם הבנתי **למה** זה נכון". על הבנייה הזו ישבו אנשים חודשים; הציפייה

מכם היא לדעת אותה, להבין למה היא עובדת ולעבוד איתה — לא להמציא אותה מאפס. לעומת זאת, על רדוקציה כמו $3\mathrm{COL} \leq_p 4\mathrm{COL}$ **כן** מצפים מכם להגיע לבד ([01:21:03]).

[01:29:33] — הכיוון השני נשאר כתרגיל. המרצה הציג את הכיוון $\Leftarrow$ בעל פה בלבד ואמר "אם אתם רוצים באמת להרגיש שאתם מבינים את זה — תכתבו את זה". הוא כתוב במלואו במשפט 4 לעיל.

[00:44:01] — המשפט שכדאי לזכור בעל פה. "כשעובדים עם מספרים, הערך של המספר והקידוד של המספר זה לא אותו דבר."

[00:38:29], [00:40:49] — היסטוריית האלגוריתמים לבעיה. ראיתם את הבעיה במבוא (פתרון רקורסיבי: לכל איבר מחליטים בפנים/בחוץ, עץ רקורסיה בגודל 2^n) ובאלגוריתמים (תכנון דינמי, טבלה בגודל $n \times S$). האלגוריתם הנאיבי ביותר הוא מעבר על כל 2^n תת-הקבוצות.

פערים בין הסיכום להקלטה

מקור: תמליל $QfE6eBttdJg$, [00:00:00]. **הפער:** הכתוביות אומרות "נניח כי A ב-P וכי B טריוויאלית", בלי השלילה. **ההכרעה:** זו נפילת שלילה אופיינית לתמלול אוטומטי. הסיכום (עמוד 1) והתזכורת מחישוביות ב-[00:00:32] אומרים שניהם "B **אינה** טריוויאלית", וזה גם המצב המתמטי הנכון — עבור B טריוויאלית הטענה שקרית. תוקן בגוף הקובץ.

מקור: עמוד 5 בסיכום. **הפער:** הסיכום מוכיח רק את הכיוון $(G, K) \in \mathrm{VC} \Rightarrow$ פלט ב-$\mathrm{SUBSET\text{-}SUM}$; הכיוון ההפוך חסר לגמרי, ובהקלטה הוא נאמר בעל פה בלבד ([01:29:33]). **ההכרעה:** הכיוון השני נכתב כאן במלואו לפי הסקיצה שנאמרה, כולל הנימוק שמספר קשת יכול לתרום לכל היותר 1 ולכן בהכרח לפחות קצה אחד נבחר.

מקור: הסיכום וההקלטה כאחד. **הפער:** טיעון אי-הנשאות אינו מנוסח בשום מקום כטענה; שניהם רק מציינים שסכום עמודת קשת הוא בין 1 ל-2 בכיסוי מסוים. **ההכרעה:** נוסח כאן כלמה 4.1 עם הוכחה מלאה (חסם 3 על סכום עמודה, ולכן ספרה חוקית בבסיס 10; כל בסיס ≥ 4 מספיק), ומסקנה 4.2 שמצדיקה את הקריאה ספרה-ספרה.

מקור: הסיכום (עמוד 5) וההקלטה ([01:13:18]). **הפער:** שניהם עוברים מ-"$(G, K) \in \mathrm{VC}$" ישירות ל-"קיים כיסוי U עם $|U| = K$", בעוד ההגדרה של VC היא "לכל היותר K". **ההכרעה:** אין כאן שגיאה מהותית, אבל יש חוסר. נוסף צעד 0 לאלגוריתם ($K \leftarrow \min(K, |V|)$) והצדקה שהשלמת כיסוי לגודל בדיוק K אפשרית.

מקור: הסיכום (עמוד 4) וההקלטה ([01:07:50]). **הפער:** נכתב ש-S הוא בן $|E| + \log_{10} K$ ספרות. **ההכרעה:** מספר הספרות המדויק הוא $|E| + \lceil \log_{10}(K+1) \rceil$; זהו עיגול מקובל ולא שגיאה, אך נכתב כאן במדויק. נשמר הדגש של ההקלטה ([00:59:38]) שהבלוק השמאלי **אינו ספרה בודדת**.

מקור: עמוד 4 בסיכום מול עמוד 5. **הפער:** הדוגמה בעמוד 4 היא על גרף בעל 7 קשתות ($a_3 = 10110001$, $S = 32222222$) ואילו עמוד 5 מציג גרף בעל 6 קשתות. **ההכרעה:** אין כאן סתירה — בהקלטה ([01:22:44]) המרצה אומר שמחק קשת אחת כדי שהטבלה תיכנס ללוח. הדוגמה המפורטת בקובץ היא של עמוד 5, שנבדקה עמודה-עמודה.

מקור: עמוד 4 בסיכום. **הפער:** שורת הקלט של הבעיה כתובה "k מספרים $a_1, \ldots, a_n$", עם אי-התאמה בין k ל-n. **ההכרעה:** הקלט הוא n מספרים; זו כנראה פליטת קולמוס, ובכל יתר הסיכום ובהקלטה ([00:39:09]) מופיע n. תוקן.

מקור: ההקלטה בלבד. **הפער:** כל הדיון בהבחנה בין ערך לאורך ייצוג ([00:40:49]–[00:51:30]) — האלגוריתם הנאיבי על 2^n תת-קבוצות, בדיקת ראשוניות נאיבית, המקרה האונרי, ואי-תלות הבסיס — מופיע בסיכום רק כשתי שורות כחולות. **ההכרעה:** שוחזר במלואו ונוסח כמשפט 5 ובהגדרה 3.

מקור: ההקלטה בלבד. **הפער:** שני "הניסיונות שנשברו" ברדוקציה $3\mathrm{COL} \le_p 4\mathrm{COL}$ (הזהות; הוספת קודקוד בלי קשתות) והדיון על מה מותר לרדוקציה לדעת ([00:16:53], [00:21:39], [00:31:29]) אינם בסיכום כלל. **ההכרעה:** נכללו במלואם, כולל דוגמאות נגדיות מפורשות שההרצאה לא נתנה; זהו החומר החשוב ביותר בהקלטה שאינו בסיכום.

מקור: חלוקת החומר בין קבצי השיעורים. **הפער:** הרדוקציה $3\mathrm{COL} \le_p 4\mathrm{COL}$ נמצאת בעמודים 2–3 של סיכום שיעור 11 (הקובץ הזה) ולא בסיכומי שיעור 10, אף שבמקור נכתבה גם שם. **ההכרעה:** לפי הסיכום הכתוב היא שייכת לשיעור 11 ונכתבת כאן במלואה (משפט 2, דוגמה 3, תרגיל 1); על הקובץ של שיעור 10 להפנות לכאן.

מקור: הקצאת התמלילים במשימה. **הפער:** תמליל 18 ($fnWzohq8Tdo$) הוגדר כתמליל הראשי לשיעור זה, אך תוכנו הוא שיעור 12 (PARTITION, BIN PACKING, מעגלים המילטוניים, TSP), והוא נפתח במילים "בשיעור האחרון ראינו את SUBSET SUM". **ההכרעה:** תמליל 17 ($QfE6eBttdJg$) הוא התמליל הראשי בפועל — חמשת עמודי הסיכום מופיעים בו לפי הסדר. סומן בהתאם בשדה `sources`.

סיכום ונקודות למבחן

מה לזכור בעל פה.

$\mathrm{SUBSET\text{-}SUM}$: בהינתן $a_1, \ldots, a_n, S$ בבסיס ≥ 2, האם קיימת $I \subseteq \{1, \ldots, n\}$ עם $\sum_{i \in I} a_i = S$. הבעיה NP-complete.

הרדוקציה: $\mathrm{VC} \le_p \mathrm{SUBSET\text{-}SUM}$. $m + 1$ עמודות: עמודה מובילה d + עמודה לכל קשת. a_v מתחיל ב-1 ומסמן את הקשתות הנוגעות ב-v; a_e מתחיל ב-0 והוא וקטור יחידה; $S = K \cdot 10^m + \sum_j 2 \cdot 10^{m-j}$.

הטיעון: בכל עמודת קשת מצטברות לכל היותר 3 אחדות $\Rightarrow$ אין נשאות $\Rightarrow$ שוויון סכומים = שוויון ספרה-ספרה $\Rightarrow$ "בדיוק 2 בכל עמודה" $\iff$ "לפחות קצה אחד נבחר", ו-"K בעמודה d" $\iff$ "נבחרו בדיוק K קודקודים".

DP בזמן $O(n \cdot S)$ הוא pseudo-polynomial ולא פולינומי. ערך מול אורך ייצוג: $\log$ ביטים לערך n.

$A \in P$ ו-B לא-טריוויאלית $\Rightarrow A \le_p B$; מכאן ש-$\le_p$ גס מדי מכדי להבחין בין בעיות בתוך P.

$4\mathrm{COL}$ היא NP-complete באמצעות הוספת קודקוד המחובר לכל השאר.

מלכודות סטנדרטיות.

לכתוב רדוקציה שמסתכלת על הפתרון. "אם הגרף 3-צביע נחזיר..." — אסור. האלגוריתם רואה רק את הקלט הגולמי. הצביעה/הכיסוי/ההשמה מופיעים אך ורק בהוכחת הנכונות.

לשכוח להוכיח את הכיוון השני. בדיוק הכיוון שהסיכום מדלג עליו הוא הכיוון שנשבר בבניות שגויות.
להניח אי-נשאות בלי לנמק. במבחן צריך לומר במפורש: בכל עמודה מצטברות לכל היותר 3 אחדות, ולכן בבסיס 10 אין נשאות, ולכן אפשר לקרוא ספרה-ספרה.
לבלבל בין "לכל היותר K" ל"בדיוק K" בהגדרת VC.
לקרוא ל-$O(n \cdot S)$ "פולינומי". זו המלכודת המרכזית של השיעור. תמיד שאלו: מה אורך הייצוג של המספר, לא מה ערכו.
להפוך את כיוון הרדוקציה. $A \le_p B$ פירושו ש-B קשה לפחות כמו A. כדי להוכיח ש-B קשה, מתחילים מבעיה קשה ידועה ו**אליה** לא עושים רדוקציה — עושים **ממנה**.
צ'ק-ליסט: אחרי השיעור אתם צריכים לדעת
לנסח את $\mathrm{SUBSET\text{-}SUM}$ פורמלית ולהוכיח שהיא ב-NP עם certificate מפורש.
לבנות את המספרים a_v, a_e, S עבור גרף קטן נתון, ולחשב את הסכום בשתי הבחירות.
לנמק במלואו מדוע אין נשאות ולמה בלעדיה הטיעון קורס.
להוכיח את שני כיווני הנכונות של הרדוקציה, ולנמק מדוע היא פולינומית — כולל למה מותר לה לייצר מספרים בעלי ערך מעריכי.
לחשב אורך קלט מול זמן ריצה במשפחת הקלטים $2^n \le a_i, S \le 2^{2n}$, ולהסביר מדוע $O(n \cdot S)$ אינו פולינומי.
לבנות את הרדוקציה $3\mathrm{COL} \le_p 4\mathrm{COL}$ מאפס, ולהסביר מדוע הזהות ומדוע קודקוד לא מחובר אינם עובדים.

שאלות שנשארו פתוחות

עמוד 4 בסיכום: כותרת המשנה הכחולה שמעל דוגמת הגדלים ($n \le a_i \le 2^{2n}$) אינה חד־משמעית; שוחזרה לפי ההקשר כ'הבחנה'.

עמוד 4 בסיכום: שורת הקלט כתובה 'k מספרים $a_1,\dots,a_n$'; מדובר כנראה בפליטת קולמוס והכוונה ל-n מספרים.

עמוד 5 בסיכום: הערה קצרה בכתב יד ליד חץ הסיכום בדוגמה שוחזרה כ'ונחבר אותם לסכום שקיבלנו'; הניסוח המדויק אינו ודאי.

בהקלטה [00:12:25] נאמר שבשיעורי הבית יש להוכיח שמחלקה מהצורה $\mathrm{DTime}(n^{10})$ אינה סגורה לרדוקציות זמן פולינומי; החזקה המדויקת שנאמרה אינה ברורה בכתוביות.

ה-slug 'subset-sum' מתאר בחסר את הקובץ: השיעור מכסה גם את הטענה על רדוקציות משפות ב-P (עמוד 1) וגם את 3COL ≤p 4COL (עמודים 2–3). ההיקף האמיתי נמצא ב-title_he. שם הקובץ לא שונה, כנדרש.

הרדוקציה 3COL ≤p 4COL מופיעה בעמודים 2–3 של סיכום שיעור 11 ולא בסיכומי שיעור 10; היא נכתבת כאן במלואה, ועל הקובץ של שיעור 10 להפנות לכאן במקום לשכפל אותה.

12 PARTITION ו-BIN PACKING, הבעיות ההמילטוניות ו-TSP

השיעור מרחיב את אוסף הבעיות ה-NP-hard בשתי בעיות מספרים — $PARTITION$ ו-$BIN\text{-}PACKING$ — בשרשרת הרדוקציות $SUBSET\text{-}SUM \le_p PARTITION \le_p BIN\text{-}PACKING$, שבה איבר ריפוד יחיד מחושב אלגברית כדי להמיר סכום יעד שרירותי לחלוקה שווה, וממשיך לארבע הבעיות ההמילטוניות ולרדוקציה $UHC \le_p TSP$.

ביטחון: high

בקצרה

מרחיבים את "שק" הבעיות ה-NP-hard בשתי בעיות שעוסקות במספרים ולכן הן "קרובות משפחה" של SUBSET-SUM: PARTITION (האם אפשר לפצל רב-קבוצה של מספרים לשני חלקים שווי-סכום) ו-BIN-PACKING (האם אפשר לארוז n פריטים ב-k תאים בעלי קיבולת 1).

לב השיעור הוא שרשרת הרדוקציות $\text{SUBSET-SUM} \le_p \text{PARTITION} \le_p \text{BIN-PACKING}$. שני הצעדים משתמשים באותו טריק: **מחשבים את הסכום הכולל ומכניסים אותו לתוך הקלט החדש** — פעם אחת כאיבר ריפוד נוסף, ופעם אחת כמכנה של נרמול.

הליבה החישובית של הצעד הראשון היא איבר ריפוד יחיד $a_{n+1} = 2S - \sum a_i$ (או $\sum a_i - 2S$), שערכו נגזר אלגברית מהדרישה "מה עוד חסר לצד השני כדי להגיע ל-S". הגזירה הזאת היא כל ההוכחה, ולכן היא נעשית כאן מלכתחילה ולא מוצגת כעובדה.

הרדוקציה השנייה מוכיחה יותר ממה שביקשנו: היא מראה ש-BIN-PACKING נשארת NP-hard גם כאשר מספר התאים קבוע מראש ושווה 2 — בניגוד ל-CLIQUE ול-IS, שבהן קיבוע k מפיל את הבעיה ל-P, ובדומה ל-3COL.

חוזרים לעולם הגרפים ומגדירים ארבע וריאציות המילטוניות (DHP, DHC, UHP, UHC). מציינים בלי הוכחה ש-$\text{3SAT} \le_p DHP$, ומראים שכל ארבעתן **שקולות פולינומית** — ולכן די בארבע רדוקציות ולא ב-12.

הרדוקציה האחרונה בקורס לזמן הקרוב היא $UHC \le_p TSP$: משלימים את הגרף לגרף מלא, נותנים משקל 1 לקשתות המקוריות ו-2 לחדשות, ושואלים על מעגל במשקל $\le |V|$. הבחירה ב-$\{1, 2\}$ ולא ב-$\{0, 1\}$ אינה מקרית והמרצה הסביר למה.

לאורך כל השיעור חוזרת ההבחנה שהתחילה בשיעור 11 — **ערך מספר מול אורך הייצוג שלו**. זו הסיבה ש"טבלת תכנון דינמי בגודל k" אינה אלגוריתם פולינומי, וזו הסיבה שהבעיות האלה קשות למרות שהן נראות כמו חשבון פשוט.

רקע ותלויות

השיעור הזה הוא הרביעי ברצף של "אוסף בעיות NP-hard", והוא מניח שלושה דברים משיעורים קודמים.

1. רדוקציית זמן פולינומי וכיוון החץ (שיעורים 7–9). נזכיר את ההגדרה במלואה. שפה A ניתנת לרדוקציה בזמן פולינומי לשפה B, ומסמנים $A \leq_p B$, אם קיימת פונקציה f הניתנת לחישוב בזמן פולינומי כך שלכל x
$$x \in A \iff f(x) \in B.$$
כיוון החץ: הסימון $A \leq_p B$ אומר ש-B היא **הבעיה הקשה יותר** — אם היינו יודעים לפתור את B בזמן פולינומי היינו יודעים לפתור גם את A. בכל הרדוקציות בקובץ הזה נאמר את הכיוון גם במילים, כי בדיבור חופשי מחליפים אותו כל הזמן. שתי תכונות שבהן נשתמש: $\leq_p$ טרנזיטיבי, ואם A היא NP-hard ו-$A \leq_p B$ אז גם B היא NP-hard.

2. $\mathrm{SUBSET\text{-}SUM}$ ושלמותה ב-NP (שיעור 11). נשתמש בתוצאה במלואה, ולכן נחזור עליה:
$$(a_1, \ldots, a_n, S) \in \mathrm{SUBSET\text{-}SUM} \iff \exists\, I \subseteq \{1, \ldots, n\} \text{ s.t. } \sum_{i \in I} a_i = S.$$
המספרים $a_1, \ldots, a_n, S$ הם מספרים טבעיים הנתונים בייצוג מיקומי (המרצה אומר "בבסיס 10"), והוכח בשיעור 11 ש-$\mathrm{VC} \leq_p \mathrm{SUBSET\text{-}SUM}$ ולכן $\mathrm{SUBSET\text{-}SUM}$ היא NP-complete.

3. ההבחנה בין ערך לבין אורך ייצוג (שיעור 11). מספר a הכתוב בבסיס 10 תופס $\Theta(\log a)$ תווים. לכן אלגוריתם שרץ בזמן $O(n \cdot S)$ הוא פולינומי ב**ערך** S אך **מעריכי באורך הייצוג** של S, ואינו אלגוריתם פולינומי. ההבחנה הזאת חוזרת כאן פעמיים: פעם בדיון של המרצה על טבלת תכנון דינמי בגודל k ([01:05:32]), ופעם בשאלה מה בכלל מותר לוריפייר לעשות.

4. תפקיד ה-k בקלט (שיעור 10). בשיעור 10 ראינו ש-$3\mathrm{COL}$ נשארת NP-hard גם כאשר מספר הצבעים קבוע ואינו חלק מהקלט, בעוד שב-CLIQUE ו-IS קיבוע k מראש מעביר את הבעיה ל-P (אפשר לעבור על כל $\binom{n}{k} = O(n^k)$ תת-הקבוצות). ההבחנה הזאת תחזור כאן במלוא עוצמתה כשנשאל מה קורה ל-$\mathrm{BIN\text{-}PACKING}$ עם $k = 2$ קבוע.

הגדרות

הגדרה 1: הבעיה $\mathrm{PARTITION}$

קלט: n מספרים טבעיים $a_1, \ldots, a_n$, בייצוג מיקומי (בסיס 10).

שאלה: האם קיימת קבוצת אינדקסים $I \subseteq \{1, 2, \ldots, n\}$ כך ש
$$\sum_{i \in I} a_i \;=\; \sum_{i \notin I} a_i \;?$$
ניסוח שקול, שהוא זה שבו נשתמש בפועל: האם קיימת $I \subseteq \{1, \ldots, n\}$ כך ש
$$\sum_{i \in I} a_i \;=\; \tfrac{1}{2} \sum_{i=1}^{n} a_i \;?$$
השקילות מיידית: אם נסמן $T = \sum_{i=1}^{n} a_i$ אז $\sum_{i \notin I} a_i = T - \sum_{i \in I} a_i$, והשוויון בין שני הצדדים שקול ל-$\sum_{i \in I} a_i = T/2$.

אינטואיציה. השאלה היא פשוט "האם אפשר לחלק את ערימת המספרים לשתי ערימות באותו משקל". זו בעיית ההוגנות הפשוטה ביותר שאפשר לנסח: שני שותפים, אוסף חפצים במשקלים ידועים, האם יש חלוקה שווה בדיוק.

למה קבוצת אינדקסים ולא תת-קבוצה של המספרים ([00:03:08]). המרצה הדגיש את הנקודה הזאת במפורש ואמר במכוון "עֲנִיָּה של מספרים" ולא "**קבוצה** של מספרים": איש לא הבטיח שהמספרים שונים זה מזה, ובקלט יכולות להיות חזרות. אילו היינו מדברים על תת-קבוצה של

המספרים עצמם, הקלט $(5,5)$ היה מתמוטט לקבוצה $\{5\}$ ומאבד את המידע. לכן החלוקה נעשית תמיד על **מרחב האינדקסים** $\{1,\dots,n\}$: האינדקסים כולם שונים גם כשהמספרים אינם.

דוגמה. $(3,4,5,6) \in \text{PARTITION}$: $T = 18$, $T/2 = 9$, ו-$I = \{1,4\}$ נותנת $3+6 = 9$ והמשלים $4+5 = 9$.

אי-דוגמה מסוג ראשון (סכום אי-זוגי). $(1,2,4) \notin \text{PARTITION}$: $T = 7$ אי-זוגי, ולכן $T/2$ אינו שלם ואף סכום חלקי של שלמים לא יוכל להשתוות לו. זהו תנאי הכרחי שקל לבדוק ולכן הוא **אינו** מקל על הבעיה.

אי-דוגמה מסוג שני (איבר דומיננטי). $(1,1,10) \notin \text{PARTITION}$: $T = 12$, $T/2 = 6$, אבל $a_3 = 10 > 6$ — כל צד שמכיל את 10 עובר את החצי. הדוגמה הזאת אינה שולית: בדיוק המקרה הזה יהפוך למקרה הראשון בטיפול של הרדוקציה הבאה.

הגדרה 2: הבעיה BIN-PACKING (אריזה בתאים)

קלט: מספרים $a_1,\dots,a_n \in (0,1]$ ומספר טבעי $k \in \mathbb{N}$.

שאלה: האם ניתן לחלק את המספרים ל-k תאים כך שסכום המספרים בכל תא הוא לכל היותר 1?

ניסוח פורמלי (המידול המתמטי שנעשה בכיתה ב-[00:35:59]–[00:37:33]). בהגדרות הקודמות ה"קיים" היה בולט — קיימת קבוצת קודקודים, קיימת השמה, קיימת תת-קבוצת אינדקסים. כאן הוא מוסתר במילים "ניתן לחלק", וצריך לחלץ אותו. חלוקה של n פריטים ל-k תאים מיוצגת בנוחות המרבית כ**פונקציה** מהאינדקסים לתאים, ולכן:

$$(a_1,\dots,a_n,k) \in \text{BIN-PACKING} \iff \exists\, f : \{1,\dots,n\} \to \{1,\dots,k\} \;\text{ s.t. }\; \forall\, 1 \le \ell \le k : \; \textstyle\sum_{i\,:\,f(i)=\ell} a_i \le 1.$$

הביטוי $\{i : f(i) = \ell\}$ הוא בדיוק אוסף האינדקסים ש-f מכניסה לתא ה-ℓ, ולכן הסכום שמעליו הוא משקלו הכולל של התא ה-ℓ.

אינטואיציה. יש לי מכולות בקיבולת 1 ופריטים בגדלים שברִיים; האם k מכולות מספיקות. זו בעיה שממדלת מספר עצום של בעיות עולם אמיתי — הקצאת קבצים לדיסקים, משימות למעבדים, פרסומות לבלוקי שידור.

למה $a_i > 0$ ולא $a_i \ge 0$ ([00:33:41]). אפסים הם מיותרים: אפשר להוציא אותם מהקלט מבלי לשנות את התשובה, שהרי אפשר לדחוס את כולם לתא כלשהו בלי להעלות שום סכום. לכן ההגדרה מוציאה אותם מראש והקטע הוא חצי-פתוח $(0,1]$. הקצה הימני **סגור**: פריט בגודל 1 בדיוק הוא קלט חוקי (הוא ממלא תא שלם לבדו).

"לכל היותר k" מול "בדיוק k" ([00:34:11]). שאלה טובה שעלתה בכיתה. ההבדל אינו מהותי: אם הצלחנו לארוז ב-$j < k$ תאים, ויש לנו לפחות k פריטים, אפשר תמיד "לפתוח עוד תא" ולהעביר אליו פריט בודד — הוא בגודל ≤ 1 ולכן התא החדש חוקי. הניסוח עם הפונקציה f שלמעלה תופס ממילא את "לכל היותר", שכן f אינה נדרשת להיות על.

דוגמה. $\left(\tfrac{1}{3},\tfrac{1}{3},\tfrac{1}{3},\tfrac{1}{2},\tfrac{1}{2}\;;\;k=2\right) \in \text{BIN-PACKING}$: תא אחד מקבל את שלושת השלישים (סכום 1) והשני את שני החצאים (סכום 1).

אי-דוגמה. $\left(\tfrac{3}{4},\tfrac{3}{4},\tfrac{3}{4}\;;\;k=2\right) \notin \text{BIN-PACKING}$: לפי שובך היונים תא אחד יקבל לפחות שני פריטים, וסכומם $\tfrac{3}{2} > 1$. שימו לב לאי-דוגמה הזאת — היא בדיוק ה"קלט השלילי המומצא" שהרדוקציה במשפט 4 תשתמש בו.

הגדרה 3: ארבע הבעיות ההמילטוניות

נזכיר שני מושגים מקורס האלגוריתמים. **מסלול המילטוני** בגרף הוא מסלול העובר דרך כל קודקוד בגרף בדיוק פעם אחת. **מעגל המילטוני** הוא מעגל העובר דרך כל קודקוד בדיוק פעם אחת, פרט לקודקוד ההתחלה שהוא גם קודקוד הסיום וסוגר את המעגל. אפשר לשאול כל אחת מהשאלות בגרף מכוון ובגרף לא מכוון, ומכאן ארבע בעיות:

DHP. קלט: גרף מכוון $G = (V, E)$. שאלה: האם קיים ב-G מסלול המילטוני?

DHC. קלט: גרף מכוון $G = (V, E)$. שאלה: האם קיים ב-G מעגל המילטוני?

ובאופן מקביל UHP ו-UHC עבור גרפים **לא** מכוונים (ה-D הוא directed וה-U הוא undirected).

וריאציה עם קצוות נתונים ([01:10:55]). אפשר לנסח גם גרסה שבה הקלט כולל שני קודקודים s, t ושואלים אם קיים מסלול המילטוני **מ-s ל-t**. כל הגרסאות שקולות; לא נטפל בהן בנפרד.

דוגמה. הגרף המעגלי C_4 (קודקודים $1, 2, 3, 4$ וקשתות $12, 23, 34, 41$) שייך ל-UHC — הוא בעצמו מעגל המילטוני.

אי-דוגמה. המסלול P_4 (קשתות $12, 23, 34$) שייך ל-UHP אך **לא** ל-UHC: לקודקודים 1 ו-4 יש דרגה 1 כל אחד, ובמעגל כל קודקוד חייב דרגה לפחות 2.

הגדרה 4: הבעיה TSP (בעיית הסוכן הנוסע)

קלט: גרף מלא $G = (V, E)$, פונקציית משקלים על הקשתות $w : E \to [0, \infty)$, ומספר $K \in \mathbb{N}$.

שאלה: האם קיים ב-G מעגל המילטוני שמשקלו לכל היותר K? משקלו של מעגל הוא סכום משקלי קשתותיו.

למה הגרף מלא ולמה צריך את המשקל ([01:19:56]). אם לא היינו מוסיפים משקלים, השאלה הייתה טריוויאלית: בגרף מלא על יותר משלושה קודקודים **תמיד** קיים מעגל המילטוני, שכן כל הקשתות קיימות ואפשר לעבור על הקודקודים בכל סדר. הקושי כולו טמון במשקל: קל למצוא מעגל, קשה למצוא מעגל **זול**.

האינטואיציה שנתנה לבעיה את שמה ([01:21:07]). יש n ערים; סוכן נוסע יוצא מהמפעל, רוצה לעבור בכל אחת מהערים בדיוק פעם אחת ולחזור הביתה, במחיר נסיעה כולל של לכל היותר K.

דוגמה. $V = \{1, 2, 3, 4\}$, כל הקשתות במשקל 1, $K = 4$. המעגל $1 - 2 - 3 - 4 - 1$ הוא המילטוני ומשקלו $4 \le 4$, ולכן הקלט שייך ל-TSP.

אי-דוגמה. אותו גרף עם $K = 3$: כל מעגל המילטוני על 4 קודקודים מכיל בדיוק 4 קשתות, ולכן משקלו לפחות $4 > 3$.

הערה מקדימה על אופטימיזציה ([01:22:12]). TSP היא הגשר לנושא הבא בקורס: גרסת האופטימיזציה שלה אינה מקבלת K אלא מבקשת את המעגל הזול ביותר. ההגדרה שלמעלה היא גרסת ה**הכרעה**, וזו הגרסה היחידה שעליה NP-hardness מוגדרת פורמלית, מפני שהיא מוגדרת באמצעות רדוקציות בין **שפות**.

משפטים והוכחות

משפט 1: $\mathrm{PARTITION} \in \mathrm{NP}$

טענה. $\mathrm{PARTITION} \in \mathrm{NP}$.

הוכחה (שתי הדרכים שנאמרו בכיתה, [00:03:40]–[00:04:45]).

דרך א — מכונה אי-דטרמיניסטית. על קלט $(a_1, \ldots, a_n)$ המכונה **בוחרת באופן אי-דטרמיניסטי** תת-קבוצה $I \subseteq \{1, \ldots, n\}$ (כלומר, n צעדים אי-דטרמיניסטיים, בכל אחד "בפנים/בחוץ"), מחשבת את שני הסכומים ומקבלת אם ורק אם הם שווים. חישוב שני הסכומים הוא $O(n)$ חיבורים של מספרים באורך לכל היותר אורך הקלט, ולכן זמן פולינומי. לפי ההגדרה של NP כמחלקת השפות המוכרעות בזמן פולינומי אי-דטרמיניסטי, $\mathrm{PARTITION} \in \mathrm{NP}$.

דרך ב — verifier. ה-certificate הוא עצמה, מקודדת כמחרוזת n ביטים — אורך n, בוודאי פולינומי באורך הקלט. הוריפייר קורא את I, מחשב את שני הסכומים ומשווה. זמן פולינומי. ■

> **הערה:** המרצה עצר את השיעור על ניסוח ([00:03:40]): אין לומר "**מגרילים**" קבוצה, וגם לא "מנחשים". המילה הנכונה היא "**בוחרים באופן אי-דטרמיניסטי**". הגרלה שייכת לאלגוריתמים אקראיים, שבהם הבחירה נעשית לפי התפלגות ולאלגוריתם יש הסתברות טעות; אי-דטרמיניזם הוא דבר אחר לגמרי — הוא קבלה אם **קיים** ריצה מקבלת. הבלבול בין השניים הוא מקור טעויות קבוע במבחנים.

משפט 2 (לב השיעור): $\text{SUBSET-SUM} \le_p \mathrm{PARTITION}$, ולכן $\mathrm{PARTITION}$ היא NP-hard

כיוון הרדוקציה במילים. נראה שאם היה בידינו אלגוריתם פולינומי ל-$\mathrm{PARTITION}$, היינו יכולים לפתור בעזרתו את SUBSET-SUM בזמן פולינומי. כלומר $\mathrm{PARTITION}$ היא **הבעיה הקשה יותר** מבין השתיים, ומכיוון ש-SUBSET-SUM היא NP-hard (שיעור 11), גם $\mathrm{PARTITION}$ היא NP-hard.

למה דווקא מ-SUBSET-SUM ([00:05:16]–[00:05:47], [00:29:19]–[00:30:24])

בכיתה הוצע לעשות רדוקציה מ-SAT. המרצה קיבל שזה **אפשרי** — כל בעיה NP-complete ניתנת לרדוקציה לכל בעיה NP-complete אחרת — אבל דחה את זה כבחירה: "לקודד נוסחה בעזרת קבוצה של מספרים" זו עבודה מיותרת. העיקרון שהוא ניסח: מעבירים בין בעיות מ**אותו עולם**. כאן הקלט מספרים והפלט מספרים, ולכן אפשר לעבור מסכום בפלט לסכום בקלט ובחזרה בלי לתרגם עולמות. רדוקציות שעוברות בין עולמות (כמו $\mathrm{VC} \le_p \text{SUBSET-SUM}$ משיעור 11) הן היפות יותר — אבל כשבונים רדוקציה בפועל, מעדיפים את הבעיה הקרובה ביותר.

הגזירה: מהיכן בא איבר הריפוד

זהו החלק שאסור לדלג עליו. הרעיון: ב-SUBSET-SUM יש **סכום יעד חיצוני** S, וב-$\mathrm{PARTITION}$ אין — הסכום היעד מוכתב מבפנים והוא בהכרח חצי מהסכום הכולל. הרדוקציה חייבת "להטמיע את ה-S פנימה" ([00:06:51]).

נסמן $T = \sum_{i=1}^{n} a_i$. נניח לרגע — רק לצורך **החשיבה**, לא כחלק מהאלגוריתם — שקיימת I עם $\sum_{i \in I} a_i = S$, ונשאל מה חסר. הצד השני של החלוקה סוכם ל-$T - S$. אנחנו רוצים ששני הצדדים יסתכמו לאותו דבר, ולכן נוסיף איבר b לצד ה"קטן". במקרה $S > T/2$ הצד הקטן הוא המשלים, ולכן נדרוש:

$$\sum_{i \in I} a_i = S, \qquad \sum_{i \notin I} a_i + b = S.$$

מכאן

$$b \;=\; S - \textstyle\sum_{i\notin I} a_i \;=\; S - \Big(\underbrace{\sum_{i=1}^{n} a_i}_{=\,T} - \underbrace{\sum_{i\in I} a_i}_{=\,S}\Big) \;=\; S - T + S \;=\; 2S - T.$$

וכאן נמצא כל היופי ([00:12:16]–[00:13:20]). הביטוי האמצעי $S - \sum_{i\notin I} a_i$ הוא **בלתי ניתן לחישוב** על ידי הרדוקציה: הוא תלוי ב-I, ו-I הוא בדיוק האובייקט שאין לנו ושאותו אנחנו לא מחפשים. אבל הביטוי הסופי $2S - T$ תלוי אך ורק בקלט — S ניתן לנו, ו-T מחושב בזמן לינארי. שאלת הביניים "מה b?" עברה מ"תלוי בפתרון" ל"תלוי בקלט", ובזה הרדוקציה הפכה לחוקית.

באופן סימטרי, אם $S < T/2$ הצד הקטן הוא I עצמה, ואז נדרוש $\sum_{i\in I} a_i + b = \sum_{i\notin I} a_i$, כלומר $S + b = T - S$ ומכאן

$$b \;=\; T - 2S.$$

בשני המקרים $b > 0$ ממש, בדיוק בגלל תנאי המקרה. וכאשר $S = T/2$ אין מה לרפד.

> **הערה:** בהרצאה ההצדקה למה b חייב להיות חיובי לא נאמרה במפורש; היא נחוצה כדי שהפלט יהיה קלט חוקי של $\mathrm{PARTITION}$ מעל המספרים הטבעיים, והיא נובעת ישירות מתנאי המקרה: $S > T/2 \Rightarrow 2S - T > 0$, ו-$S < T/2 \Rightarrow T - 2S > 0$.

הרדוקציה

אלגוריתם R. על קלט $(a_1, \ldots, a_n, S)$ — מספרים טבעיים בבסיס 10:

חשב $T \leftarrow \sum_{i=1}^{n} a_i$.

אם $2S = T$ (כלומר $S = \frac{1}{2}T$): החזר $(a_1, \ldots, a_n)$ ללא שינוי.

אם $2S > T$ (כלומר $S > \frac{1}{2}T$): החזר $(a_1, \ldots, a_n,\ 2S - T)$.

אם $2S < T$ (כלומר $S < \frac{1}{2}T$): החזר $(a_1, \ldots, a_n,\ T - 2S)$.

> **הערה:** בסיכום ובהרצאה ההשוואה נכתבת כ-S מול $\frac{1}{2}\sum a_i$. כאן היא נכתבת כ-$2S$ מול T כדי להישאר בשלמים גם כאשר T אי-זוגי; זו אותה השוואה בדיוק. שימו לב שכאשר T אי-זוגי מקרה 2 פשוט אינו יכול להתרחש, ובכל אחד משני המקרים האחרים האיבר המוסף עדיין שלם.

הערה קריטית על מה שהרדוקציה עושה ואיננה עושה ([00:08:29], [00:21:06]–[00:22:11]). האלגוריתם **מחשב** את T ומשווה אותו ל-$2S$ — וזה בסדר גמור, זו פעולה חשבונית פשוטה. הוא **אינו** בודק אם קיימת תת-קבוצה שסכומה S, ואינו יכול. ההבחנה הזאת עלתה כשאלה מהכיתה: "אז החזרנו מספר שעוזר לנו לפתור?" והתשובה הייתה נחרצת — לא. האיבר a_{n+1} אינו מסייע במאום להכריע את השאלה; הוא מבטיח רק את המשפט "אם היה פתרון קודם, יש פתרון עכשיו, ולהפך". רדוקציה לעולם אינה באה להכריע את הבעיה.

עוד אי-הבנה שתוקנה בכיתה ([00:14:53]): הרדוקציה **אינה** מחזירה זוג מהצורה (מספרים, סכום יעד). הפלט הוא רשימה של $n+1$ מספרים בלבד, כי כזה בדיוק הוא קלט של $\mathrm{PARTITION}$. איש לא הבטיח ש-n יישאר קבוע.

ניתוח זמן ריצה

נסמן ב-m את אורך הייצוג הארוך ביותר מבין $a_1, \ldots, a_n, S$, ובגודל הקלט $|x| \geq n + m$.

שלב 1 מבצע $n-1$ חיבורים. הסכום החלקי אינו עולה על $n \cdot 10^m$ ולכן אורכו לכל היותר $m +$ $\lceil \log_{10} n \rceil + 1$. חיבור אחד עולה זמן לינארי באורכים, ולכן שלב 1 עולה $= O(n\,(m + \log n))$ $O(|x|^2)$.

שלב 2 הוא השוואה אחת ($2S$ הוא הזזה/הכפלה ב-2, זמן לינארי).

שלבים 3–4 הם חיסור אחד, זמן לינארי.

הכתיבה של הפלט: $n+1$ מספרים, כל אחד באורך $O(m + \log n)$.

סך הכול $O(|x|^2)$ — **פולינומי בגודל הקלט**. חשוב לשים לב שזמן הריצה נמדד באורך הייצוג ולא בערך המספרים: לו היינו צריכים לספור עד T הרדוקציה לא הייתה פולינומית.

אורך הפלט הוא $O(|x|)$; זה חשוב לטרנזיטיביות של $\leq_p$ (רדוקציה שמנפחת את הקלט מעריכית אינה שמישה בהרכבה).

נכונות, כיוון ראשון: $(a_1, \ldots, a_n, S) \in \text{SUBSET-SUM} \Rightarrow R(x) \in \text{PARTITION}$ יהיו $a_1, \ldots, a_n, S$ ונניח $(a_1, \ldots, a_n, S) \in \text{SUBSET-SUM}$. אז קיימת $I \subseteq \{1, \ldots, n\}$ כך ש-$\sum_{i \in I} a_i = S$. נפצל לשלושה מקרים.

מקרה 2 (זה שהוצג בהרצאה, [00:19:23]–[00:21:06]): $2S > T$. נסמן $a_{n+1} = 2S - T$. האלגוריתם מחזיר $(a_1, \ldots, a_{n+1})$. הסכום הכולל של הפלט הוא

$$\sum_{i=1}^{n+1} a_i \;=\; T + (2S - T) \;=\; 2S,$$

ולכן חצי הסכום הוא בדיוק S. עבור אותה I עצמה (שהיא תת-קבוצה של $\{1, \ldots, n\} \subseteq$ $\{1, \ldots, n+1\}$) מתקיים

$$\sum_{i \in I} a_i \;=\; S \;=\; \tfrac{1}{2} \sum_{i=1}^{n+1} a_i,$$

ולכן גם $\sum_{i \notin I} a_i = 2S - S = S$. מצאנו חלוקה שווה, ומכאן $(a_1, \ldots, a_{n+1}) \in$ PARTITION.

מקרה 1: $2S = T$. האלגוריתם מחזיר את הקלט כפי שהוא. חצי הסכום הוא $T/2 = S$, ואותה I מקיימת $\sum_{i \in I} a_i = S = \frac{1}{2}\sum_{i=1}^{n} a_i$. מכאן $(a_1, \ldots, a_n) \in \text{PARTITION}$.

מקרה 3: $2S < T$. נסמן $a_{n+1} = T - 2S > 0$. הסכום הכולל של הפלט הוא $T + (T - 2S) = 2(T - S)$, וחציו $T - S$. הפעם ניקח את **המשלים** $J = \{1, \ldots, n\} \setminus I$ כצד אחד:

$$\sum_{i \in J} a_i \;=\; T - S \;=\; \tfrac{1}{2} \sum_{i=1}^{n+1} a_i.$$

מכאן $(a_1, \ldots, a_{n+1}) \in \text{PARTITION}$.

> **הערה:** בהרצאה נאמר "מקרים 1 ו-3 לבית" ([00:28:47]); הם נכתבים כאן במלואם. שימו לב שמקרה 3 אינו העתקה מילולית של מקרה 2 — בו הצד ה"טוב" הוא המשלים של I ולא I עצמה, וזו בדיוק הנקודה שבה סטודנטים נופלים.

נכונות, כיוון שני: $R(x) \in \text{PARTITION} \Rightarrow (a_1, \ldots, a_n, S) \in \text{SUBSET-SUM}$

הערה מתודית שנאמרה בכיתה ובצדק ([00:24:27]–[00:25:28]). כשמוכיחים את הכיוון הזה, יש בידינו **שני** דברים בו-זמנית: הקלט המקורי $(a_1, \ldots, a_n, S)$, שממנו התחלנו, ו**גם** הפלט של האלגוריתם. אין צורך "לשחזר" את הקלט מן הפלט. בפרט יש לנו גישה חופשית ל-S ול-a_i בתוך ההוכחה, למרות שלאלגוריתם עצמו לא הייתה גישה לשום פתרון. זה מקור בלבול קבוע.

מקרה 2: $2S > T$. הפלט הוא $(a_1, \ldots, a_n, a_{n+1})$ עם $a_{n+1} = 2S - T$, וסכומו הכולל $2S$. נניח שהפלט שייך ל-$\mathrm{PARTITION}$. אז קיימת $J \subseteq \{1, \ldots, n+1\}$ כך ש
$$\sum_{i \in J} a_i \;=\; \sum_{i \notin J} a_i \;=\; \tfrac{1}{2} \cdot 2S \;=\; S.$$
עכשיו מגיע הצעד שהודגש בכיתה ([00:27:03]): איננו יכולים להחזיר את J כפתרון של SUBSET-SUM, כי ייתכן ש-$n+1 \in J$ ואז J אינה תת-קבוצה של $\{1, \ldots, n\}$. הפתרון: **בלי הגבלת הכלליות** $n+1 \notin J$, שכן אם $n+1 \in J$ נחליף את J במשלים שלה $\overline{J} = \{1, \ldots, n+1\} \setminus J$. זה חוקי בדיוק מפני ש-$\mathrm{PARTITION}$ סימטרית: שני הצדדים מסתכמים לאותו מספר S, ולכן המשלים הוא פתרון תקף באותה מידה, והאיבר $n+1$ נמצא באחד משני הצדדים בלבד.

לאחר ההחלפה, $J \subseteq \{1, \ldots, n\}$ ומתקיים $\sum_{i \in J} a_i = S$. לפי ההגדרה, $(a_1, \ldots, a_n, S) \in \text{SUBSET-SUM}$.

מקרה 1: $2S = T$. הפלט הוא הקלט עצמו וסכומו $T = 2S$. אם קיימת $J \subseteq \{1, \ldots, n\}$ עם $\sum_{i \in J} a_i = \frac{1}{2}T = S$, זו בדיוק עדות ל-$\text{SUBSET-SUM}$. (כאן לא צריך טיעון משלים, שכן לא נוסף איבר.)

מקרה 3: $2S < T$. הפלט הוא $(a_1, \ldots, a_n, T - 2S)$ וסכומו $2(T - S)$, כך שכל צד מסתכם ל-$T - S$. תהי J צד של חלוקה שווה; בלי הגבלת הכלליות $n+1 \notin J$ (אחרת נעבור למשלים, כמו קודם), ולכן $J \subseteq \{1, \ldots, n\}$ ומתקיים $\sum_{i \in J} a_i = T - S$. נגדיר $I = \{1, \ldots, n\} \setminus J$; אז
$$\sum_{i \in I} a_i \;=\; T - \sum_{i \in J} a_i \;=\; T - (T - S) \;=\; S,$$
ולכן $(a_1, \ldots, a_n, S) \in \text{SUBSET-SUM}$. $\blacksquare$

מסקנה. היא רדוקציה בזמן פולינומי מ-SUBSET-SUM ל-$\mathrm{PARTITION}$. מכיוון ש-SUBSET-SUM היא NP-hard (שיעור 11), גם $\mathrm{PARTITION}$ היא NP-hard, ויחד עם משפט 1 — $\mathrm{PARTITION}$ היא **NP-complete**.

משפט 3: $\text{BIN-PACKING} \in \mathrm{NP}$

טענה. $\text{BIN-PACKING} \in \mathrm{NP}$.

הוכחה. ה-certificate הוא הפונקציה f עצמה, מקודדת כרשימה של n ערכים $f(1), \ldots, f(n)$, כל אחד באורך $O(\log k)$ ביטים — סך הכול $O(n \log k)$, פולינומי באורך הקלט. הוריפייר סורק את הרשימה, צובר עבור כל תא את סכום הפריטים שהוקצו אליו, ומוודא שכל סכום הוא ≤ 1. לחלופין, מכונה אי-דטרמיניסטית בוחרת את f באופן אי-דטרמיניסטי ומוודאת. $\blacksquare$

> **הערה:** בהרצאה ([00:37:33]–[00:39:04]) הווידוא תואר כמעבר על $\ell = 1, \ldots, k$. זה מדויק רק אם k אינו גדול מדי — וזו בדיוק הנקודה שהמרצה עצמו הדגיש ב-[01:05:32]: k נכתב בייצוג מיקומי ולכן ערכו יכול להיות **מעריכי** באורך הקלט, ולולאה באורך k תהיה מעריכית. שני תיקונים אפשריים, ושניהם נכונים: (א) לסרוק רק את התאים שאליהם הוקצה לפחות פריט אחד — לכל היותר n תאים; (ב) להבחין שאפשר להניח בלי הגבלת הכלליות $k \leq n$, שכן אם $k \geq n$ ניתן להכניס כל פריט לתא נפרד וכל תא מסתכם ל-$a_i \leq 1$, ולכן הקלט הוא בהכרח כן-קלט. בשני התיקונים הווידוא הוא פולינומי, וכך גם הקידוד של ה-certificate.

משפט 4: $\text{PARTITION} \leq_p \text{BIN-PACKING}$, ולכן BIN-PACKING היא NP-hard
כיוון הרדוקציה במילים. אלגוריתם פולינומי ל-BIN-PACKING היה נותן לנו אלגוריתם פולינומי ל-PARTITION; BIN-PACKING היא הקשה מבין השתיים.
למה מ-PARTITION ולא מ-SUBSET-SUM ([00:39:47]–[00:41:21])
השאלה נשאלה בכיתה. התשובה: PARTITION **היא בדיוק "חלוקה לשני תאים"**. הבעיה הקטנה ביותר של אריזה בתאים היא $k = 2$, וב-PARTITION סכום היעד קבוע מראש לחצי — כלומר, ה-S כבר "נבלע" בתוך הבעיה. מ-SUBSET-SUM **אפשר** לעשות רדוקציה, אבל אז צריך לשלב את S בעצמנו, ו-k עלול לצאת תלוי בערכי המספרים; והרי מספר התאים מופיע בתיאור הפונקציה f, ולכן k גדול מדי היה מנפח את הפלט. המרצה הדגיש: בחירת בעיה אחרת אינה שגויה, היא פשוט פחות פשוטה.
הרעיון: נרמול לפי חצי הסכום ([00:43:26])
אנחנו מקבלים מספרים טבעיים שיכולים להיות עצומים, וצריכים להוציא מספרים ב-$(0, 1]$. הדבר המתבקש הוא לחלק בקבוע. באיזה קבוע? נסמן $T = \sum_{j=1}^{n} a_j$. אם נחלק ב-T נקבל סכום כולל 1 — אפשר לדחוס הכול לתא אחד, והבעיה נעשית טריוויאלית. אם נחלק ב-$T/2$ נקבל סכום כולל 2 בדיוק, וכעת אריזה ב-2 תאים בעלי קיבולת 1 אפשרית **אם ורק אם** מתחלקים בדיוק 1 ו-1 — לא נשאר שום מרווח. הצמידות המוחלטת הזאת היא מנוע הרדוקציה.
המכשול והטיפול בו ([00:44:31]–[00:46:45])
הנרמול $b_i = \dfrac{a_i}{T/2} = \dfrac{2a_i}{T}$ מייצר קלט חוקי רק אם $b_i \leq 1$ לכל i, כלומר רק אם $a_i \leq T/2$ לכל i. אם קיים i עם $a_i > T/2$, הנרמול נכשל — אבל במקרה הזה אנחנו יודעים **בוודאות** שהקלט אינו ב-PARTITION, שכן כל צד שמכיל את a_i עובר את החצי. זהו מקרה פרטי שקל לזהות בזמן פולינומי (השוואה אחת אחרי חישוב T), ולכן מותר לנו במקרה הזה להחזיר **קלט שלילי מומצא** כלשהו של BIN-PACKING. הקלט שנבחר הוא $\left(\frac{3}{4}, \frac{3}{4}, \frac{3}{4}, 2\right)$, שאינו ב-$\text{BIN-PACKING}$ מטעמי שובך יונים.
הרדוקציה
אלגוריתם R'. על קלט $(a_1, \ldots, a_n)$, מספרים טבעיים (בלי הגבלת הכלליות $a_i > 0$ לכל i; אפסים אפשר להשמיט מבלי לשנות את התשובה):
חשב $T \leftarrow \sum_{j=1}^{n} a_j$.
אם קיים $1 \leq i \leq n$ כך ש-$2a_i > T$: החזר $\left(\frac{3}{4}, \frac{3}{4}, \frac{3}{4}, 2\right)$.
אחרת, לכל $1 \leq i \leq n$ הגדר $b_i \leftarrow \dfrac{2a_i}{\sum_{j=1}^{n} a_j}$, והחזר $(b_1, \ldots, b_n, 2)$.

> **הערה:** התנאי בשלב 2 נכתב בסיכום (עמוד 2) עם $\geq$ ובהקלטה נאמר "גדול מ" ([00:44:31]). האי-שוויון החד הוא הנכון: אם $a_i = T/2$ בדיוק, אז $\{i\}$ מול המשלים היא חלוקה חוקית, הקלט **כן** ב-PARTITION, ואילו הפלט של שלב 2 אינו ב-BIN-PACKING — הרדוקציה הייתה נשברת. עם $<$ הכול תקין, ואף מתקיים $b_i \leq 1$ במקרה הגבול $a_i = T/2$ שנותן $b_i = 1$, שהוא ערך חוקי.

על הייצוג של הפלט. ה-b_i הם רציונליים ומיוצגים כזוג שלמים — מונה $2a_i$ ומכנה T. אורך כל אחד מהם $O(m + \log n)$ ולכן כל הפלט פולינומי באורך הקלט. שאלה שעלתה בכיתה ([01:07:39]) הייתה בדיוק על כך: אין דרישה שהקלט של BIN-PACKING יהיה שלם — ההגדרה מדברת על מספרים בקטע $(0, 1]$, וזה בדיוק הצורך שבגללו הגדרנו כך.

התכונה המרכזית של הפלט

בשלב 3 מתקיים

$$\sum_{i=1}^{n} b_i \;=\; \sum_{i=1}^{n} \frac{2a_i}{\sum_{j=1}^{n} a_j} \;=\; \frac{2}{\sum_{j=1}^{n} a_j} \sum_{i=1}^{n} a_i \;=\; \frac{2}{T} \cdot T \;=\; 2,$$

כאשר ההוצאה של $\frac{2}{T}$ מחוץ לסכום מותרת כי הוא **קבוע ואינו תלוי ב-**i. כמו כן $b_i > 0$ (כי $a_i > 0$) ו-$b_i \le 1$ (כי $2a_i \le T$ בשלב זה), ולכן $b_i \in (0, 1]$ והפלט הוא קלט חוקי.

ניתוח זמן ריצה

חישוב T הוא $O(n(m + \log n))$ כמו קודם. שלב 2 הוא n השוואות. שלב 3 הוא n פעולות של כתיבת זוג $(2a_i, T)$ — אין צורך בחילוק ממשי. סך הכול $O(|x|^2)$, פולינומי, ואורך הפלט $O(|x|)$.

נכונות, כיוון ראשון: $(a_1, \ldots, a_n) \in \text{PARTITION} \Rightarrow R'(x) \in \text{BIN-PACKING}$

נניח $(a_1, \ldots, a_n) \in \text{PARTITION}$: קיימת $I \subseteq \{1, \ldots, n\}$ עם $\sum_{i \in I} a_i \;=\; \sum_{i \notin I} a_i \;=\; \frac{1}{2}\sum_{j=1}^{n} a_j \;=\; \frac{T}{2}$.

קודם כול נראה שהאלגוריתם לא נכנס לשלב 2. לכל $1 \le i \le n$, האיבר a_i שייך לאחד משני הצדדים, וסכום הצד כולו הוא $T/2$; מכיוון שכל האיברים אי-שליליים, $a_i \le T/2$, כלומר $2a_i \le T$.

לכן התנאי בשלב 2 אינו מתקיים לאף i, והפלט הוא $(b_1, \ldots, b_n, 2)$.

עכשיו נבנה אריזה. נכניס לתא הראשון את כל האיברים שהאינדקס שלהם ב-I, ולתא השני את כל השאר. (מכיוון שיש רק שני תאים, אפשר לתאר חלוקה בעזרת תת-קבוצה של אינדקסים במקום בעזרת פונקציה f — הן מייצגות אותו דבר, [00:57:27].) אז

$$\sum_{i \in I} b_i \;=\; \sum_{i \in I} \frac{2a_i}{\sum_{j=1}^{n} a_j} \;=\; \frac{2}{T}\sum_{i \in I} a_i \;=\; \frac{2}{T} \cdot \frac{T}{2} \;=\; 1 \;\le\; 1,$$

ובאופן זהה $\sum_{i \notin I} b_i = 1 \le 1$. שני התאים חוקיים, ולכן $(b_1, \ldots, b_n, 2) \in \text{BIN-PACKING}$.

נכונות, כיוון שני: $R'(x) \in \text{BIN-PACKING} \Rightarrow (a_1, \ldots, a_n) \in \text{PARTITION}$

נניח שהפלט שייך ל-BIN-PACKING.

שלב א — זיהוי איזה ענף של האלגוריתם רץ ([01:00:12]–[01:01:17]). הפלט של שלב 2 הוא $\left(\frac{3}{4}, \frac{3}{4}, \frac{3}{4}, 2\right)$, והוא **אינו** ב-$\text{BIN-PACKING}$: יש שלושה פריטים ושני תאים, ולכן לפי שובך היונים תא אחד מקבל לפחות שניים מהם, וסכומם $\frac{3}{2} > 1$. מכיוון שהפלט **כן** ב-BIN-PACKING, האלגוריתם בהכרח לא עבר בשלב 2, ולכן הפלט הוא $(b_1, \ldots, b_n, 2)$ עם $b_i = \frac{2a_i}{T}$.

שלב ב — מסקנה על החלוקה. מכיוון ש-$k = 2$, קיימת $I \subseteq \{1, \ldots, n\}$ (התא הראשון) כך ש $\sum_{i \in I} b_i \le 1$

וגם

$$\sum_{i \notin I} b_i \le 1.$$

אבל ראינו ש-$\sum_{i=1}^{n} b_i = 2$ בדיוק. אילו אחד משני הסכומים היה קטן ממש מ-1, סכומם היה קטן ממש מ-2 — סתירה. לכן **שני** הסכומים שווים ל-1 בדיוק. זו הנקודה שבה "הצמידות" של הבנייה משתלמת.

שלב ג — חזרה לקלט. מהשוויון $\sum_{i\in I} b_i = 1$ נקבל
$1 = \sum_{i\in I} \frac{2a_i}{T} = \frac{2}{T}\sum_{i\in I} a_i \implies \sum_{i\in I} a_i = \frac{T}{2} = \frac{1}{2}\sum_{j=1}^{n} a_j.$
זו בדיוק ההגדרה של $\mathrm{PARTITION}$, ולכן $(a_1,\dots,a_n)\in \mathrm{PARTITION}$. ■

מסקנה. $\mathrm{PARTITION} \le_p \text{BIN-PACKING}$; לפי משפט 2 ולפי הטרנזיטיביות של $\le_p$ מתקבל $\mathrm{SUBSET\text{-}SUM} \le_p \text{BIN-PACKING}$, ולכן BIN-PACKING היא NP-hard. יחד עם משפט 3 — היא **NP-complete**.

משפט 5 (בונוס של אותה הוכחה): BIN-PACKING נשארת NP-hard גם כאשר $k = 2$ קבוע

טענה. תהי BIN-PACKING_2 הבעיה שקלטה $a_1,\dots,a_n \in (0,1]$ בלבד והשאלה היא אם ניתן לארוז אותם בשני תאים בעלי קיבולת 1. אז BIN-PACKING_2 היא NP-hard.

הוכחה. אותו אלגוריתם R' בדיוק, למעט שאינו מדפיס את ה-2 בסוף — כי 2 אינו חלק מהקלט של הבעיה החדשה. כל שלבי ההוכחה של משפט 4 עוברים מילה במילה, שכן בשום שלב לא השתמשנו ב-k אלא כמספר קבוע. ■

למה זה מעניין ([00:48:20]–[00:53:44]). הרדוקציה שבנינו שולחת את **כל** הקלטים לתת-קבוצה מאוד צרה של מרחב הקלטים של BIN-PACKING — רק כאלה שבהם $k = 2$. המרצה נתן את התמונה הכללית: אם A ניתנת לרדוקציה ל-B אבל הרדוקציה שולחת את כל הקלטים לתוך תת-בעיה $C \subseteq B$ (וכל אי-הקלטים לתוך $\overline{C}$), אז אותה רדוקציה עצמה מוכיחה גם ש-C קשה. זה בדיוק מה שהיה בחישוביות ברדוקציות מ-HALT ל-HALT_0 ול-$\mathrm{HALT}_\varepsilon$ — פונקציית המקבע שלחה את כל הקלטים לקבוצה זעירה ולכן סגרה כמה בעיות במחיר אחד.

ההשוואה שכדאי לזכור. קיבוע k מראש **לא תמיד** מוריד את הקושי:

בעיה	חלק מהקלט k	קבוע מראש k
CLIQUE, IS	NP-complete	ב-P (סריקת $O(n^k)$ תת-קבוצות)
kCOL	NP-complete	NP-hard כבר עבור $k = 3$
BIN-PACKING	NP-complete	NP-hard כבר עבור $k = 2$

משפט 6: מדוע "תכנון דינמי לפי מספר התאים" אינו אלגוריתם פולינומי

השאלה עלתה מהכיתה ([01:05:00]–[01:05:32]) והתשובה היא ההבחנה המרכזית של שני השיעורים האחרונים, ולכן היא נרשמת כאן כטענה.

טענה. אלגוריתם ל-BIN-PACKING שמחזיק טבלה שבה k תאים (או k שורות) אינו אלגוריתם פולינומי בגודל הקלט.

הוכחה. המספר k נתון בייצוג מיקומי ולכן אורך הייצוג שלו הוא $\Theta(\log k)$ תווים. אם $|x|$ הוא גודל הקלט אז $\log k \le |x|$, כלומר k יכול להיות עד $2^{\Theta(|x|)}$. טבלה בגודל k היא אפוא בגודל **מעריכי** ב-$|x|$, ובוודאי גם הזמן הדרוש כדי למלא אותה. ■

הערה: ההרחבה הבאה לא נאמרה בהרצאה במפורש, אך היא ההמשך הישיר של אותו טיעון ומופיעה בשיעור 11 עבור SUBSET-SUM. אותו הסבר עצמו מסביר מדוע אלגוריתם התכנון הדינמי הידוע ל-SUBSET-SUM, הרץ בזמן $O(n \cdot S)$, ואלגוריתם דומה ל-PARTITION הרץ בזמן $O(n \cdot T)$, אינם אלגוריתמים פולינומיים: הם פולינומיים ב**ערך** המספרים ומעריכיים ב**אורך הייצוג** שלהם. אלגוריתמים כאלה נקראים פסאודו-פולינומיים, והבעיות SUBSET-SUM, PARTITION ו-BIN-PACKING נקראות NP-hard **חלשות**: לו המספרים היו נתונים בייצוג אונרי, אורך הייצוג היה שווה לערך והבעיות היו נופלות ל-P. זו הסיבה שהמרצה טורח לומר בכל פעם "בבסיס 10" ([00:02:06], [00:41:54]) — זה אינו קישוט, זו ההנחה שכל הקושי תלוי בה.

משפט 7: ארבע הבעיות ההמילטוניות

טענה א (נאמרת בלי הוכחה). $3\text{SAT} \leq_p DHP$, ולכן DHP היא NP-hard.

הערה על הוויתור. המרצה הצהיר במפורש ([01:14:51]–[01:15:25]) שהרדוקציה הזאת "חמודה אבל מאוד מאוד טרחנית" ולכן מוותרים עליה בקורס: **את התוצאה צריך לדעת, את ההוכחה לא.**

טענה ב. בין כל שתיים מארבע הבעיות DHP, DHC, UHP, UHC קיימת רדוקציה בזמן פולינומי; כלומר כולן **שקולות פולינומית**, ולכן כולן NP-hard.

איך זה נעשה ביעילות ([01:16:34]–[01:18:11]). לכאורה צריך להראות רדוקציה בין כל זוג סדור, כלומר $4 \cdot 3 = 12$ רדוקציות. אבל $\leq_p$ טרנזיטיבי, ולכן די **במעגל** של ארבע רדוקציות:

$$DHP \leq_p DHC \leq_p UHC \leq_p UHP \leq_p DHP,$$

ומכל צומת אפשר להגיע לכל צומת אחר לאורך המעגל. עלינו מ-12 ל-4.

הערה: בהרצאה נאמר "אם אני אראה שמזה יש רדוקציה לזה ומזה לזה... זה מספיק בגלל הטרנזיטיביות" בלי לרשום את המעגל במפורש; הכתיבה המפורשת שלמעלה היא השלמה. הרדוקציות עצמן ניתנו כתרגילי בית ולכן אינן נכתבות כאן.

טענה ג. כל ארבע הבעיות שייכות ל-NP.

הוכחה ([01:12:33]). ה-certificate הוא סדר של הקודקודים (תמורה של V), באורך $O(|V| \log |V|)$. הוריפייר בודק שכל שתי קודקודים עוקבים בסדר מחוברים בקשת (ובגרף מכוון — בקשת בכיוון הנכון), ובמקרה של מעגל בודק גם את הקשת הסוגרת מהאחרון לראשון. זמן פולינומי. ■

אזהרה שעלתה בכיתה ([01:13:05]). סטודנט הזכיר שבקורס האלגוריתמים ראינו אלגוריתם פולינומי בעזרת **מיון טופולוגי**. זה נכון — אבל רק עבור גרף מכוון **חסר מעגלים** (DAG), שהוא מקרה מאוד מאוד ספציפי. אין בכך סתירה לקושי של הבעיה הכללית.

משפט 8: $UHC \leq_p TSP$, ולכן TSP היא NP-hard

כיוון הרדוקציה במילים. אלגוריתם פולינומי ל-TSP היה מכריע את UHC בזמן פולינומי; TSP היא הקשה יותר.

למה דווקא מ-UHC ([01:24:53]). אפשר היה לצאת גם ממסלול המילטוני — יש רדוקציות בין כל הגרסאות — אבל TSP שואלת על **מעגל** בגרף **לא מכוון**, ולכן UHC היא הבעיה הקרובה ביותר. שוב אותו עיקרון: להתחיל מהבעיה הקרובה ביותר.

הרדוקציה

אלגוריתם R''. על קלט $G = (V, E)$ — גרף פשוט לא מכוון:

יהי $\hat{G} = (V, \hat{E})$ הגרף המלא על קבוצת הקודקודים V.

הגדר $w : \hat{E} \to [0, \infty)$ על ידי $w(e) = \begin{cases} 1 & e \in E \\ 2 & e \notin E \end{cases}$

החזר $\Big(\hat{G},\ w,\ |V|\Big)$.

הערה על שלב 1 ([01:26:59], [01:32:50]). ברגע שקבענו את V, קיים **גרף מלא יחיד** על V; אין כאן שום בחירה. בפועל שלב 1 פירושו "לכתוב את כל הקשתות", כולל אלה שלא היו ב-G.

הניסיון הראשון וההחלטה לזנוח אותו ([01:27:31]–[01:29:06])

הבנייה הטבעית הראשונה שעלתה בכיתה הייתה: משקל 0 לקשתות המקוריות, משקל 1 לחדשות, ולהחזיר $K = 0$. **הבנייה הזאת נכונה לחלוטין** והיא עובדת. בכל זאת המרצה החליף אותה מדעת ל-$\{1, 2\}$ עם $K = |V|$, ונימק: בהמשך הקורס תוגדר תת-בעיה של TSP שנרצה שגם היא תישאר NP-hard, ולתת-הבעיה הזאת משקלי אפס אינם מתאימים. הרדוקציה עם $\{1, 2\}$ נופלת בתוך תת-הבעיה ולכן מוכיחה גם עליה קושי, בדיוק לפי העיקרון של משפט 5.

> **הערה:** בהרצאה לא נאמר במפורש מהי תת-הבעיה. ההשלמה הטבעית: משקלים בערכים $\{1, 2\}$ מקיימים את **אי-שוויון המשולש**, שכן לכל שלושה קודקודים u, x, v מתקיים $w(u, v) \le 2 = 1 + 1 \le w(u, x) + w(x, v)$. לכן אותה רדוקציה בדיוק מוכיחה ש-TSP נשארת NP-hard גם בגרסה המטרית, שבה מובטח שהמשקלים מקיימים את אי-שוויון המשולש — וזו הגרסה שעבורה קיים אלגוריתם קירוב. עם משקלי 0 ו-1 אי-שוויון המשולש נשבר ($1 \not\le 0 + 0$), ולכן הבנייה הראשונה לא הייתה נותנת את הבונוס.

ניתוח זמן ריצה ([01:29:40]–[01:33:53])

זהו ניתוח שדורש זהירות, והמרצה עמד עליו באריכות. העבודה שהאלגוריתם עושה היא מעבר על כל הקשתות של $\hat{E}$ וכתיבת משקל לכל אחת, כלומר $\Theta(|\hat{E}|)$. הפיתוי הוא לומר "זה לינארי" — **אבל לינארי במה?** זה לינארי בגודל הגרף ה**חדש**, ואת זמן הריצה חייבים לחסום בגודל ה**קלט**.

הבעיה: איננו יודעים כמה קשתות היו ב-G. תיאורטית ייתכן שהיו מעט מאוד, אפילו אפס. לכן אי אפשר לחסום את $|\hat{E}|$ באמצעות $|E|$. מה שכן ידוע בוודאות הוא

$$|\hat{E}| \;=\; \tbinom{|V|}{2} \;\le\; |V|^2,$$

ומספר הקודקודים אינו משתנה ברדוקציה וחסום בגודל הקלט. לכן זמן הריצה הוא $O(|V|^2) = O(|x|^2)$ — **ריבועי בגודל הקלט**, ובפרט פולינומי.

הערה: המרצה ציין ([01:33:22]) שמקובל לעצור בניסוח "ריבועי במספר הקודקודים", כי תמיד אפשר לתרגם זאת לגודל הקלט; אבל formally מה שמעניין הוא גודל הקלט, ובהוכחות הראשונות בקורס זה נכתב במפורש.

נכונות, כיוון ראשון: $G \in UHC \Rightarrow (\hat{G}, w, |V|) \in TSP$
נניח $G \in UHC$; אז קיים ב-G מעגל המילטוני C. מכיוון ש-$E \subseteq \hat{E}$, אותו C עצמו הוא מעגל בגרף $\hat{G}$, והוא המילטוני גם שם — קבוצת הקודקודים לא השתנתה, רק הוספנו קשתות ([01:40:12]).
מעגל המילטוני על $|V|$ קודקודים מכיל בדיוק $|V|$ קשתות, וכל אחת מהן היא קשת של E ולכן משקלה 1. לכן
$$w(C) \;=\; |V| \cdot 1 \;=\; |V| \;\le\; |V|,$$
ומכאן $(\hat{G}, w, |V|) \in TSP$.
נכונות, כיוון שני
בהרצאה ניתנו **שתי** גרסאות של הכיוון השני, במכוון ([01:39:09]) — כדי להראות שאין שום קדושה בשאלה אם מוכיחים "שייך $\Rightarrow$ שייך" או "לא שייך $\Rightarrow$ לא שייך". שתיהן נכתבות כאן.
גרסה א (בדרך השלילה, כפי שנעשתה קודם, [01:36:32]–[01:37:37]). נניח $G \notin UHC$, ויהי C מעגל המילטוני **כלשהו** ב-$\hat{G}$ (כזה קיים, שהרי $\hat{G}$ מלא). ל-C יש בדיוק $|V|$ קשתות ומשקל כל אחת לפחות 1. כמו כן, ב-C קיימת קשת שאינה ב-E — אחרת כל קשתותיו היו ב-E ו-C היה מעגל המילטוני ב-G, בסתירה להנחה. משקלה של אותה קשת הוא 2. לכן
$$w(C) \;\ge\; (|V| - 1) \cdot 1 + 2 \;=\; |V| + 1 \;>\; |V|.$$
זה נכון לכל מעגל המילטוני ב-$\hat{G}$, ולכן אין מעגל המילטוני במשקל $\le |V|$, כלומר $(\hat{G}, w, |V|) \notin TSP$.
גרסה ב (ישירה, ושתי שורות קצרה יותר, [01:38:07]). נניח $(\hat{G}, w, |V|) \in TSP$; אז קיים מעגל המילטוני C ב-$\hat{G}$ עם $w(C) \le |V|$. מכיוון שמשקל כל קשת ב-$\hat{G}$ הוא לפחות 1 ול-C יש בדיוק $|V|$ קשתות, מתקיים $w(C) \ge |V|$. משתי אי-השוויונות $w(C) = |V|$ בדיוק. כעת $w(C)$ הוא סכום של $|V|$ מחוברים שכל אחד מהם ≥ 1, וסכומם הוא בדיוק $|V|$; אילו מחובר אחד היה > 1 הסכום היה עולה על $|V|$. לכן משקל כל אחת מ-$|V|$ הקשתות הוא בדיוק 1, ולפי הגדרת w כל אחת מהן ב-E. לכן C הוא מעגל המילטוני ב-G, כלומר $G \in UHC$. ■
מסקנה. $UHC \le_p TSP$; מכיוון ש-UHC היא NP-hard (משפט 7), גם TSP היא NP-hard. יחד עם שייכותה ל-NP (certificate: תמורה של הקודקודים, ומחשבים את סכום המשקלים ומשווים ל-K, [01:23:46]) — TSP היא **NP-complete**.

דוגמאות ותרגילים מהשיעור
דוגמה 1: מעקב מלא אחרי $\text{SUBSET-SUM} \le_p \text{PARTITION}$, מקרה $S > T/2$
הקלט: $(a_1, a_2, a_3, a_4) = (3, 4, 5, 6)$, $S = 12$.
הרדוקציה. $T = 3 + 4 + 5 + 6 = 18$. בודקים: $2S = 24 > 18 = T$, ולכן מקרה 3 באלגוריתם — מוסיפים
$$a_5 \;=\; 2S - T \;=\; 24 - 18 \;=\; 6.$$

הפלט: $(3,4,5,6,6)$. סכום כולל 24, חצי סכום $S=12$.

מעקב קדימה. בקלט המקורי, $I=\{1,2,3\}$ נותנת $S=12$ — $3+4+5=12$ הקלט אכן ב-SUBSET-SUM. אותה I בדיוק בפלט: $\sum_{i\in I} a_i = 12$, והמשלים $\{4,5\}$ נותן $6+6=12$. חלוקה שווה — הפלט ב-PARTITION. ✔

מעקב אחורה. נניח שקיבלנו מ"פותר PARTITION" את החלוקה $J=\{4,5\}$ (שני השישים), $\sum_{i\in J} a_i = 12$. מכיוון ש-$5=n+1\in J$, עוברים למשלים: $\overline{J}=\{1,2,3\}$, שגם סכומו 12 ואינו מכיל את $n+1$. מכאן $I=\{1,2,3\}$ ו-$a_1+a_2+a_3=12=S$. ✔ שימו לב שבלי מעבר למשלים היינו נתקעים עם קבוצה שמכילה אינדקס שאינו קיים בקלט המקורי.

דוגמה 2: אותה רדוקציה, מקרה $S<T/2$ (המקרה שהושאר לבית)

הקלט: $(3,4,5,6)$, $S=5$. $T=18$, $2S=10<18$, ולכן מקרה 4:

$$a_5 \;=\; T-2S \;=\; 18-10 \;=\; 8.$$

הפלט: $(3,4,5,6,8)$. סכום כולל 26, חצי 13.

קדימה. $I=\{3\}$ נותנת $S=5=a_3$. הפעם הצד ה"טוב" הוא **המשלים** בתוך $\{1,\dots,n\}$: $J=\{1,2,4\}$ נותן $3+4+6=13$ — בדיוק חצי. ✔

אחורה. נניח שהתקבלה החלוקה $J'=\{3,5\}$: $5+8=13$. מכיוון ש-$5=n+1\in J'$, עוברים למשלים $\{1,2,4\}$ שסכומו 13. עכשיו $I=\{1,2,3,4\}\setminus\{1,2,4\}=\{3\}$, ואכן $a_3=5=S$. ✔

דוגמה 3: מקרה שלילי — הרדוקציה חייבת לשמור גם על "לא"

הקלט: $(3,4,5,6)$, $S=2$. אין תת-קבוצה שסכומה 2 (המספר הקטן ביותר הוא 3), ולכן הקלט **אינו** ב-SUBSET-SUM.

הרדוקציה. $2S=4<18$, ולכן $a_5=18-4=14$. **הפלט:** $(3,4,5,6,14)$, סכום 32, חצי 16.

בדיקה שאין חלוקה. נבדוק את כל האפשרויות לפי מיקום האיבר 14:

14 בצד אחד: צריך עוד 2 מתוך $\{3,4,5,6\}$ — בלתי אפשרי (המינימום הוא 3).

14 בצד השני: הצד הראשון צריך להסתכם ל-16 מתוך $\{3,4,5,6\}$ שסכומם הכולל 18; הסכומים האפשריים הם $3,4,5,6,7,8,9,10,11,12,13,14,15,18$ — הערך 16 אינו ביניהם (כדי לקבל 16 צריך להשמיט בדיוק 2).

אין חלוקה, ולכן הפלט אינו ב-PARTITION. ✔ הרדוקציה שמרה על ה"לא".

דוגמה 4: מעקב מלא אחרי $\text{PARTITION} \le_p \text{BIN-PACKING}$

הקלט: $(3,4,5,6)$. $T=18$, $T/2=9$.

בדיקת שלב 2. האיבר הגדול ביותר הוא 6, ו-$2\cdot 6 = 12 \le 18$; אין i עם $2a_i > T$, אז ממשיכים לשלב 3.

הנרמול. $b_i = \dfrac{2a_i}{18} = \dfrac{a_i}{9}$:

$$b_1=\tfrac{3}{9}=\tfrac{1}{3},\quad b_2=\tfrac{4}{9},\quad b_3=\tfrac{5}{9},\quad b_4=\tfrac{6}{9}=\tfrac{2}{3}.$$

הפלט: $\left(2\;;\;\tfrac{1}{3},\tfrac{4}{9},\tfrac{5}{9},\tfrac{2}{3}\right)$. בדיקת שפיות: $\frac{3+4+5+6}{9}=\frac{18}{9}=2$. ✔

קדימה. בקלט, $I=\{1,4\}$ נותנת $3+6=9=T/2$. באריזה: תא 1 מקבל את $\{b_1,b_4\}$ וסכומו $\frac{1}{3}+\frac{2}{3}=1\le 1$; תא 2 מקבל את $\{b_2,b_3\}$ וסכומו $\frac{4}{9}+\frac{5}{9}=1\le 1$. ✔

אחורה. נניח שפותר BIN-PACKING החזיר את האריזה תא $1=\{b_2,b_3\}$, תא $2=\{b_1,b_4\}$. אז $I=\{2,3\}$ ו-$\sum_{i\in I}b_i=1$, ולכן $\sum_{i\in I}a_i=\frac{18}{2}\cdot 1=9=T/2$ — ואכן $4+5=9$. ✔

דוגמה 5: מקרה 2 של הרדוקציה — האיבר הדומיננטי

הקלט: $(1,1,10)$. $T=12$. עבור $i=3$: $2a_3=20>12=T$, ולכן שלב 2 מופעל והפלט הוא $\left(\frac{3}{4},\frac{3}{4},\frac{3}{4},\ 2\right)$.

בדיקה משני הצדדים. הקלט אינו ב-PARTITION (כל צד שמכיל את 10 עובר את 6). הפלט אינו ב-BIN-PACKING (שני תאים, שלושה פריטים של $\frac{3}{4}$; תא כלשהו יקבל שניים וסכומם $>\frac{3}{2}>1$). ✔ שני הצדדים "לא" — הרדוקציה תקינה.

דוגמה 6: השרשרת המלאה $\text{SUBSET-SUM}\to\text{PARTITION}\to\text{BIN-PACKING}$

קלט מקורי: $(1,2,3)$ עם $S=4$.

צעד א. $T=6$, $2S=8>6$, ולכן מוסיפים $a_4=8-6=2$. מתקבל מופע PARTITION: $(1,2,3,2)$, סכום 8, חצי 4.

צעד ב. עכשיו $T'=8$; האיבר הגדול ביותר הוא 3 ו-$3\cdot 2=6\le 8$, אז שלב 3: $b_i=\frac{2a_i}{8}=\frac{a_i}{4}$, כלומר

$$\left(\tfrac{1}{4},\ \tfrac{1}{2},\ \tfrac{3}{4},\ \tfrac{1}{2}\ ;\ k=2\right)$$

סכום כולל $2=\frac{1+2+3+2}{4}$.

פתרון בקצה השרשרת. תא $\{\frac{1}{4},\frac{3}{4}\}=1$ סכומו 1; תא $\{\frac{1}{2},\frac{1}{2}\}=2$ סכומו 1. ✔

חזרה עד ההתחלה. תא 1 מתאים ל-$I=\{1,3\}$. במופע ה-PARTITION: $a_1+a_3=1+3=4=S$, שהוא בדיוק חצי מ-8. ✔ האיבר החדש a_4 נמצא בתא 2, כלומר $n+1=4\notin I$, ולכן אין צורך לעבור למשלים. במופע ה-SUBSET-SUM המקורי: $a_1+a_3=1+3=4=S$. ✔

דוגמה 7: מעקב אחרי $UHC\le_p TSP$ — מופע חיובי

הקלט: G עם $V=\{1,2,3,4\}$ ו-$E=\{12,23,34,41\}$ (מעגל C_4).

הרדוקציה. $\hat{G}=K_4$; הקשתות שנוספו הן 13 ו-24. המשקלים:

$$w(12)=w(23)=w(34)=w(41)=1,\qquad w(13)=w(24)=2.$$

הפלט הוא $(\hat{G},w,4)$ שכן $|V|=4$.

קדימה. המעגל $1-4-3-2-1$ הוא המילטוני ב-G, וב-$\hat{G}$ משקלו $1+1+1+1=4\le 4$. ✔

אחורה. נניח שפותר TSP החזיר "כן" עם מעגל C במשקל ≤ 4. ל-C יש 4 קשתות, כל אחת במשקל ≥ 1, ולכן $w(C)\ge 4$; מכאן $w(C)=4$ וכל קשת שוקלת בדיוק 1, כלומר כולן ב-E. אכן C הוא מעגל המילטוני ב-G. ✔

דוגמה 8: מעגל אחרי $UHC\le_p TSP$ — מופע שלילי

הקלט: G עם $V=\{1,2,3,4\}$ ו-$E=\{12,23,34\}$ (מסלול). לקודקודים 1 ו-4 דרגה 1, ולכן $G\notin UHC$.

הרדוקציה. $\hat{G}=K_4$, $w(12)=w(23)=w(34)=1$ ו-$w(13)=w(14)=w(24)=2$, ו-$K=4$.

בדיקת כל המעגלים ההמילטוניים של K_4 (יש שלושה, עד כדי כיוון ונקודת התחלה):

מעגל	קשתות	משקל
$1-2-3-4-1$	$12, 23, 34, 41$	$1+1+1+2=5$
$1-2-4-3-1$	$12, 24, 43, 31$	$1+2+1+2=6$
$1-3-2-4-1$	$13, 32, 24, 41$	$2+1+2+2=7$

כל המשקלים גדולים מ-4, ולכן $(\hat{G}, w, 4) \notin TSP$. ✔ שימו לב שהמעגל הזול ביותר משתמש בקשת אחת בדיוק שאינה ב-E, ולכן משקלו $|V| + 1 = 5$ — בדיוק החסם מגרסה א של ההוכחה.

תרגיל 1 (מהכיתה, [01:03:23]): אלגוריתם חמדני ל-BIN-PACKING

השאלה. למה לא למיין את הפריטים מהגדול לקטן, ולנסות להכניס כל פריט לתא הראשון שבו הוא נכנס?

הפתרון. האלגוריתם שתואר קרוב ל-**First-Fit Decreasing**: ממיינים בסדר יורד, ומכניסים כל פריט לתא הראשון שבו הוא נכנס. הוא אינו מכריע את הבעיה. הנה דוגמה נגדית מלאה עם $k = 2$.

הפריטים:

$$\frac{5}{10},\ \frac{4}{10},\ \frac{4}{10},\ \frac{3}{10},\ \frac{2}{10},\ \frac{2}{10}$$

סכום כולל $\frac{20}{10} = 2$.

קיימת אריזה בשני תאים: $\left\{ \frac{2}{10}, \frac{3}{10}, \frac{5}{10} \right\}$ סכומו 1, ו-$\left\{ \frac{2}{10}, \frac{4}{10}, \frac{4}{10} \right\}$ סכומו 1.

מה עושה החמדן. תא 1 מקבל $\frac{5}{10}$, ואז $\frac{4}{10}$ ומגיע ל-$\frac{9}{10}$. הפריט $\frac{4}{10}$ הבא אינו נכנס ($\frac{13}{10} > 1$), ולכן נפתח תא 2 עם $\frac{4}{10}$. הפריט $\frac{3}{10}$ אינו נכנס לתא 1 ($\frac{12}{10}$) ונכנס לתא 2 שמגיע ל-$\frac{7}{10}$. הפריט $\frac{2}{10}$ אינו נכנס לתא 1 ($\frac{11}{10}$) ונכנס לתא 2 שמגיע ל-$\frac{9}{10}$. הפריט האחרון $\frac{2}{10}$ אינו נכנס לאף אחד משני התאים — נדרש תא שלישי. החמדן החזיר "לא" על מופע שהתשובה הנכונה עליו היא "כן".

הנקודה העקרונית שהמרצה ניסח ([01:05:00]) חשובה מכל דוגמה נגדית ספציפית: החלטה מקומית על פריט אחד אינה יכולה להיות מודעת לשאריות שהיא מייצרת בהמשך, ולכן שום וריאציה חמדנית לא תעבוד. אילו היה קיים אלגוריתם חמדני נכון ופולינומי, היה נובע $P = \text{NP}$.

המשך ([01:08:11]). המרצה הוסיף שהאלגוריתם שהוצע "כמעט טוב" — והוא כמעט בדיוק אלגוריתם קירוב שיילמד בשיעור הבא. הרעיון: מוותרים על דיוק בתמורה לזמן פולינומי.

תרגיל 2 (מהכיתה, [01:05:00]): למה תכנון דינמי עם k תאים אינו עובד?

הפתרון. ראו משפט 6: כדי לתאר את k נדרשים $\log k$ ביטים, ולכן טבלה בגודל k היא מעריכית בגודל הקלט. זו אותה תבנית טיעון בדיוק שהופיעה בשיעור 11 עבור אלגוריתם ה-$O(n \cdot S)$ ל-SUBSET-SUM: המרחק בין **ערך** לבין **אורך ייצוג** הוא מעריכי.

תרגיל 3 (מהכיתה, [01:07:08]): "מצאתי קלט שאינו ב-PARTITION אבל כן עובר"

השאלה. סטודנט הציע את $(3, 3, 2)$: סכומו 8, התנאי הראשון של הרדוקציה עובר (אף איבר אינו גדול מ-4), אבל אי אפשר לחלק שווה — הצדדים היחידים האפשריים הם $\{3, 3\}$ מול $\{2\}$ או $\{3, 2\}$ מול $\{3\}$.

הפתרון. אין כאן סתירה. הרדוקציה מייצרת $b_i = \frac{2a_i}{8} = \frac{a_i}{4}$, כלומר $\left(\frac{3}{4}, \frac{3}{4}, \frac{1}{2}\ ;\ 2\right)$, שסכומם 2. האם זה ב-BIN-PACKING? חלוקה לשני תאים דורשת סכום 1 בכל תא בדיוק, והסכומים החלקיים האפשריים הם $\frac{3}{4}, \frac{1}{2}, \frac{3}{2}, \frac{5}{4}$ — הערך 1 אינו ביניהם. לכן הפלט **אינו** ב-BIN-PACKING,

בדיוק כמו שצריך. ✔ הטעות בהצעה הייתה בהנחה ש"התנאי הראשון עובר" משמעו "הפלט חיובי"; התנאי הראשון הוא רק מסנן לקלטים לא-חוקיים, לא הכרעה.

הערה נלווית ([01:07:39]). באותה שיחה עלתה שאלה חשובה: איך יכולים להיות בקלט של BIN-PACKING מספרים כמו $\frac{3}{4}$ אם המספרים "טבעיים"? התשובה: הם אינם. **הגדרנו** את קלט BIN-PACKING כמספרים בקטע החצי-פתוח $(0, 1]$, לא כשלמים. השלמים הם בקלט של PARTITION, וכל תפקידו של הנרמול הוא לגשר בין השניים.

תרגיל 4 (מהכיתה, [01:16:34]): כמה רדוקציות נדרשות לארבע הבעיות ההמילטוניות? **הפתרון.** נאיבית: 12 (בין כל זוג סדור). למעשה: 4, כמעגל $DHP \leq_p DHC \leq_p UHC \leq_p UHP \leq_p DHP$, מפני ש-$\leq_p$ טרנזיטיבי. שימו לב שהתשובה הזאת נכונה רק כדי להוכיח שכולן **NP-hard**; אם רוצים גם NP-completeness צריך בנוסף להוכיח שכל אחת מהן ב-NP, וזה עוד ארבע הוכחות קצרות (משפט 7, טענה ג).

הערות מהשיעור

[00:00:32] — מפת הדרכים. המרצה פתח בהצהרה על מבנה השיעור: שתי בעיות "קרובות משפחה" של SUBSET-SUM (PARTITION) ו-BIN-PACKING), חזרה לגרפים עם ארבע הווריאציות ההמילטוניות, ו-TSP לסיום. זה בדיוק סדר הסיכום.

[00:03:40] — "מגרילים" אסור. ראו ההערה במשפט 1. המרצה הסביר שהוא מעדיף "בוחרים באופן אי-דטרמיניסטי" גם על פני "מנחשים", כי סטודנטים לוקחים את "מנחשים" ועושים איתו עוד צעד אל "מגרילים", ואז מערבבים אי-דטרמיניזם עם אקראיות. שתי המחלקות המתקבלות שונות לגמרי.

[00:03:08] — למה "עֲנִיָּה" ולא "קבוצה". הקלט של PARTITION עלול להכיל חזרות, ולכן החלוקה היא של אינדקסים ולא של ערכים. אותה הערה תקפה ל-SUBSET-SUM ול-BIN-PACKING.

[00:08:29] ו-[00:10:39] — "בואו נניח רגע שיש". המרצה כתב את הנחות העבודה של הגזירה **באדום** והדגיש פעמיים שזה **אינו חלק מהאלגוריתם** אלא רק "איך אני חושב עליו". זו הבחנה שמפילה תשובות במבחן: מותר להניח קיום פתרון בתוך הוכחת הנכונות, אסור להניח אותו בתוך האלגוריתם.

[00:13:52] — למה בכלל לפצל למקרים לפי S? שאלה טובה מהכיתה: הרי הפיצול לא מכריע כלום. התשובה: הוא לא מכריע, אבל הוא נותן **מידע על הכיוון** — ברגע ש-$S > T/2$ אני יודע שאת הצד השני צריך להגדיל, ואז אני יודע מה לחפש. הפיצול הוא עזר לחשיבה, לא שלב בפתרון.

[00:21:39], [00:41:54], [00:42:24] — הרדוקציה אינה מכריעה. המשפט חזר שלוש פעמים בשלושה הקשרים שונים, פעם על a_{n+1}, פעם על BIN-PACKING ופעם בהתייחסות ל-kCOL משיעור 10 ("אני לא מחפש צביעה"). המרצה עצמו סימן את זה כ"מאוד מאוד מאוד חשוב".

[00:24:27] — שני האובייקטים ביד. בכיוון השני של הוכחת נכונות יש בידינו גם את הקלט המקורי וגם את הפלט. אין צורך לשחזר את הקלט. המרצה ציין שזה "תמיד נורא מבלבל סטודנטים".

[00:29:19] — עולם מול עולם. הרדוקציה הנוחה היא מבעיה קרובה. "אם לא חוצים אותי עם הגב לקיר, הבחירה הראשונה שלי לא תהיה SAT." רדוקציות שעוברות בין עולמות יפות יותר, אבל כשבונים — לוקחים את הקרובה.

[00:33:41] — למה מוציאים אפסים. פריט בגודל 0 אינו משפיע על שום דבר וניתן להעיף אותו מהקלט. ההגדרה בוחרת בקטע $[0, 1)$ כדי לא לגרור מקרי קצה.

[00:34:11] — "לכל היותר" מול "בדיוק". בתאים, בניגוד ל-MAXCUT למשל, אפשר תמיד לפתוח עוד תא או לסגור תא, ולכן ההבדל אינו מהותי.

[00:35:59] — מידול. "היכולת לקחת תיאור מילולי ולהפוך אותו למידול מתמטי מאוד חשובה." המרצה הוביל את הכיתה משאלה מילולית ("ניתן לחלק") לניסוח עם $\exists f$, כולל הבחירה שהתחום יהיה $\{1, \ldots, n\}$ ולא הקלט עצמו.

[00:48:20]–[00:53:44] — רדוקציה לתת-בעיה. הדיון הארוך והמעניין ביותר בשיעור. ראו משפט 5 והטבלה שם. ההשוואה שהמרצה חזר אליה: בחישוביות, פונקציית המקבע נתנה במחיר אחד רדוקציות מ-HALT להמון בעיות, בדיוק מפני ששלחה את כל הקלטים לקבוצה קטנה בפנים.

[01:05:32] — הערה שתחזור במבחן. "כמה ביטים אני צריך בשביל לתאר את k? — $\log k$. וגודל הטבלה הוא k. אז גודל הטבלה מעריכי בגודל הקלט." זו התשובה הסטנדרטית לשאלה "למה תכנון דינמי לא פותר את זה".

[01:06:05] — על שאלות. "אלה שאלות מצוינות. אם תשבו עליהן ותלושו אותן, אתם יכולים לענות עליהן בעצמכם." המרצה הדגיש שהוא רוצה שהסטודנטים יפתחו תחושת מסוגלות, לא שיפסיקו לשאול.

[01:14:51] — מה כן ומה לא במבחן. את הרדוקציה $3\mathrm{SAT} \leq_p DHP$ **לא** מוכיחים בקורס ("חמודה אבל מאוד טרחנית"). **את התוצאה צריך לדעת, את ההוכחה לא.**

[01:19:56] — למה בגרף מלא אין שאלה בלי משקלים. בגרף מלא על יותר משלושה קודקודים תמיד קיים מעגל המילטוני. כל הקושי ב-TSP מגיע מהמשקל.

[01:24:19] — "הרדוקציה האחרונה לזמן הקרוב". המרצה סימן במפורש שזו הרדוקציה האחרונה בפרק ה-NP-completeness, ואמר "תתענגו עליה".

[01:28:34]–[01:29:06] — למה $\{1, 2\}$ ולא $\{0, 1\}$. הבנייה עם משקלים 0 ו-1 ו-$K = 0$ נכונה לגמרי, והמרצה החליף אותה במכוון: "בהמשך נצטרך תת-בעיה שאני עדיין רוצה שהיא תהיה NP-קשה, וזו רדוקציה לאותה תת-בעיה. תזכרו את הרדוקציה הזאת ותזכרו ששיניתי מ-0 ל-2." ראו ההערה במשפט 8 על אי-שוויון המשולש.

[01:29:40]–[01:33:53] — חסימת זמן הריצה בגודל הקלט. הדיון הארוך על "לינארי במה". הכלל: אין להסתפק בחסם במונחי הגרף החדש; יש לתרגם לגודל הקלט. מקובל לעצור ב"ריבועי במספר הקודקודים", אבל צריך לדעת למה זה חוקי.

[01:34:56] — שם ארוך. כשסטודנט התלונן על השם UHC, המרצה ענה "מה אפשר לעשות, אנחנו נהנים, אז למה לקצר". בפועל הסיכום כן משתמש בקיצורים; חשוב רק להגדיר אותם.

[01:38:38]–[01:39:41] — לכתוב את שני הכיוונים. המרצה הוכיח את הכיוון השני **פעמיים** — פעם בשלילה ופעם ישירות — כדי להראות שאין כלל מיסטי שמחייב צורה מסוימת. הוא הוסיף המלצה מעשית: לפעמים אין מנוס מלכתוב את שתי הגרסאות ולבחור את היפה; "אל תנסו לנהל את

הזמן שלכם בקפידה יתרה — צריך להשקיע."

[01:40:43] — סיכום החלק השני של הקורס. בזה נסגר הפרק על NP-completeness. הפרק השלישי, "התמודדות עם NP-קושי", מתחיל מיד אחרי כן ועוסק בבעיות אופטימיזציה, אלגוריתמי קירוב ואלגוריתמים אקראיים — ראו שיעור 13.

פערים בין הסיכום להקלטה

מקור: עמוד 1 בסיכום, מקרה 3 של רדוקציית $\mathrm{PARTITION}$. **הפער:** האיבר המוחזר נקרא בכתב כ-$\sum_{i=1}^{n} a_i$, בעוד שבהקלטה ([00:15:28]) נאמר במפורש "הסכום הכולל **פחות** $2S$". **ההכרעה:** נכתב $T - 2S$, שהוא הנכון מתמטית — עם T לבדו הסכום הכולל היה $2T$, החצי T, ולא היה שום קשר ל-S. ייתכן שמדובר בקריאה חלקית שלי ולא בהשמטה בסיכום; נרשם ב- `open_questions` .

מקור: עמוד 2 בסיכום, תנאי 1 של רדוקציית $\mathrm{BIN\text{-}PACKING}$. **הפער:** התנאי נקרא כ- $a_i \geq \frac{1}{2}\sum a_j$ (אי-שוויון חלש), ובהקלטה ([00:44:31]) נאמר "a_i **גדול מ**הסכום חלקי 2". **ההכרעה:** נכתב אי-שוויון **חד** $2a_i > T$. עם אי-שוויון חלש הרדוקציה שגויה: הקלט $(1, 1)$ מקיים $a_1 = \frac{1}{2}T$ **וכן** שייך ל-$\mathrm{PARTITION}$, ואילו הפלט $\left(\frac{3}{4}, \frac{3}{4}, \frac{3}{4}, 2\right)$ אינו ב-$\mathrm{BIN\text{-}PACKING}$.

מקור: ההקלטה. **הפער:** ההשוואה נעשית בין S לבין $\frac{1}{2}\sum a_i$, כלומר בין שלם לבין מספר שעלול להיות חצי-שלם. **ההכרעה:** בגוף הקובץ ההשוואה נכתבת מחדש כ-$2S$ מול T. זהו אותו תנאי בדיוק, אך הוא נשאר בשלמים גם כאשר T אי-זוגי, וכך אין צורך להסביר מה פירוש "S שווה לחצי" כשהחצי אינו שלם.

מקור: ההקלטה ([00:18:52]–[00:28:47]). **הפער:** מתוך שלושת המקרים בהוכחת הנכונות של משפט 2, בהרצאה נעשה רק המקרה $S > T/2$ בשני הכיוונים; המקרים $S = T/2$ ו-$S < T/2$ הושארו כשיעורי בית. **ההכרעה:** שני המקרים נכתבים כאן במלואם. מקרה $S < T/2$ **אינו** העתקה סימטרית — בו הצד המסתכם לחצי הוא המשלים של I ולא I עצמה.

מקור: ההקלטה ([00:37:33]–[00:39:04]) מול [01:05:32]. **הפער:** הוכחת השייכות של $\mathrm{BIN\text{-}PACKING}$ ל-NP תוארה כמעבר על $\ell = 1, \ldots, k$, בעוד שבהמשך אותו שיעור המרצה עצמו הסביר שלולאה באורך k היא מעריכית באורך הקלט. **ההכרעה:** בגוף הקובץ נוסף תיקון מפורש (הערה למשפט 3): לסרוק רק תאים לא ריקים, או להניח בלי הגבלת הכלליות $k \leq n$ כי אחרת הקלט הוא בהכרח כן-קלט. הסתירה בין שני החלקים של ההרצאה היא כנראה קיצור בעל פה ולא טעות מהותית.

מקור: ההקלטה ([00:44:31], [00:46:45]) והסיכום. **הפער:** לא נאמר במפורש מדוע מותר לרדוקציה להחזיר "קלט מומצא" במקרה הראשון. **ההכרעה:** ההנמקה נכתבה במלואה: התנאי $2a_i > T$ ניתן לבדיקה בזמן פולינומי ומכריע לבדו שהקלט אינו ב-$\mathrm{PARTITION}$, ולכן מותר להחזיר עבורו כל אי-קלט קבוע של בעיית היעד.

מקור: ההקלטה ([01:27:31]–[01:29:06]). **הפער:** המרצה החליף בכוונה משקלים $\{0, 1\}$ עם $K = 0$ במשקלים $\{1, 2\}$ עם $K = |V|$, ואמר שהסיבה היא תת-בעיה עתידית — בלי לומר מהי. **ההכרעה:** בגוף הקובץ נוספה ההשלמה שהתת-בעיה היא ככל הנראה TSP המטרי, ושמשקלים ב-$\{1, 2\}$ מקיימים את אי-שוויון המשולש בעוד ש-$\{0, 1\}$ שוברים אותו. סומן כהשלמה שלי.

מקור: ההקלטה ([01:16:34]–[01:18:11]). **הפער:** נאמר שדי בארבע רדוקציות במקום 12 בגלל טרנזיטיביות, אך המעגל הקונקרטי לא נרשם. **ההכרעה:** המעגל $DHP \le_p DHC \le_p UHP \le_p UHC$ נכתב כאן במפורש; כל מעגל אחר על ארבע הבעיות שווה ערך.
מקור: הסיכום, עמוד 4 מול ההקלטה [01:14:51]. **הפער:** הסיכום כותב $3\mathrm{SAT} \le_p DHP$, ובהקלטה נאמר "רדוקציה מ-SAT או מ-$3\mathrm{SAT}$, זה לא באמת משנה". **ההכרעה:** נכתב $3\mathrm{SAT} \le_p DHP$ לפי הסיכום, עם ציון שההוכחה אינה חלק מהקורס. נרשם ב- `open_questions`.
מקור: הסיכום, עמוד 6. **הפער:** העמוד עוסק כולו בטבלת ההשוואה בין בעיות הכרעה/חיפוש/אופטימיזציה, בהגדרה הפורמלית של בעיית אופטימיזציה ובהגדרת אלגוריתם קירוב עם יחס α — כלומר, אינו שייך ל-TSP/$\mathrm{BIN\text{-}PACKING}$/$\mathrm{PARTITION}$ כלל. הוא מקביל ל-[01:40:43]–[02:08:24] בהקלטה. **ההכרעה:** החומר **אינו** נכתב כאן, למעט הפניה בסוף "הערות מהשיעור", מכיוון שהוא פותח את שיעור 13 (אלגוריתמי קירוב), הנכתב מתמליל 19. אם קובץ שיעור 13 אינו מכסה את הטבלה של עמוד 6 — יש לוודא זאת.
מקור: חלוקת החומר בין הסיכומים. **הפער:** קרוב לשליש מהשיעור ([01:09:20]–[01:40:43]) עוסק בבעיות המילטוניות ובּ-TSP, ואלה אינם מופיעים בשם הקובץ ובעיקר לא ב-slug. **ההכרעה:** החומר נכתב כאן במלואו, שכן הוא **כן** מופיע בעמודים 4–5 של סיכום שיעור 12 — זהו השיעור שבו הוא נלמד. שם הקובץ לא שונה, כנדרש בספציפיקציה; ההיקף האמיתי מופיע ב- `title_he`.
מקור: הקצאת התמלילים במשימה. **הפער:** תמליל 19 ($KZcJEmx19BU$) הוגדר כתמליל הקשר. בפועל אין בו ולו אזכור אחד של $\mathrm{PARTITION}$, $\mathrm{BIN\text{-}PACKING}$, מעגל המילטוני או TSP; הוא נפתח באמצע דיון על גרסאות VC וממשיך לאלגוריתם הקירוב. **ההכרעה:** סומן `coverage: none` עם הערה, ולא נעשה בו שימוש.

סיכום ונקודות למבחן

התוצאות שצריך לזכור

$\mathrm{PARTITION}$: בהינתן $a_1, \dots, a_n$ טבעיים, האם קיימת I עם $\sum_{i \in I} a_i = \frac{1}{2}\sum_{i=1}^{n} a_i$. NP-complete.

$\mathrm{BIN\text{-}PACKING}$: בהינתן $a_1, \dots, a_n \in (0,1]$ ו-k, האם קיימת $f : \{1,\dots,n\} \to \{1,\dots,k\}$ עם $\sum_{i:f(i)=\ell} a_i \le 1$ לכל ℓ. NP-complete, **וגם עבור $k = 2$ קבוע**.

הרדוקציה $\mathrm{SUBSET\text{-}SUM} \le_p \mathrm{PARTITION}$: מוסיפים איבר יחיד $2S - T$ אם $T > 2S$, ו-$T - 2S$ אם $2S < T$, וכלום אם $2S = T$.

הרדוקציה $\mathrm{PARTITION} \le_p \mathrm{BIN\text{-}PACKING$: אם קיים $2a_i > T$ מחזירים $\left(\frac{3}{4}, \frac{3}{4}, \frac{3}{4}, 2\right)$; אחרת $b_i = \frac{2a_i}{T}$ ו-$k = 2$. הסכום החדש הוא 2 בדיוק.

DHP, DHC, UHP, UHC: כולן NP-complete, שקולות פולינומית. $3\mathrm{SAT} \le_p DHP$ — התוצאה נדרשת, ההוכחה לא.

TSP: גרף מלא, משקלים, K; האם קיים מעגל המילטוני במשקל $\le K$. NP-complete, דרך $UHC \le_p TSP$ עם משקלים $1/2$ ו-$K = |V|$.

המלכודות הסטנדרטיות

כיוון החץ. $A \leq_p B$ פירושו ש-B קשה יותר. בכל תשובה כתבו את הכיוון גם במילים.

"הרדוקציה מוצאת פתרון". לא. הרדוקציה אינה מקבלת ואינה מחפשת תת-קבוצה, אריזה, מעגל או צביעה. כל התייחסות לפתרון שייכת אך ורק להוכחת הנכונות.

שכחת המשלים. בכיוון השני של $\text{SUBSET-SUM} \leq_p \text{PARTITION}$ **חובה** לומר "בלי הגבלת הכלליות $n+1 \notin J$, אחרת נעבור למשלים". בלי זה ההוכחה שגויה, כי J עלולה להכיל אינדקס שאינו קיים בקלט המקורי.

מקרה $S < T/2$ אינו העתקה של $S > T/2$. בו הצד ה"טוב" הוא המשלים.

אי-שוויון חלש במקום חד. בתנאי הראשון של רדוקציית BIN-PACKING חייבים $>$ ולא $\geq$.

ערך מול אורך ייצוג. "יש תכנון דינמי" אינה תשובה. טבלה בגודל S או k היא מעריכית באורך הקלט. זו הסיבה שהמספרים נתונים בבסיס ≥ 2 וזה חשוב.

חסימת זמן ריצה במונחי הפלט. ב-$UHC \leq_p TSP$ אסור לומר "לינארי ב-$|\hat{E}|$" ולעצור; צריך $|\hat{E}| \leq |V|^2 \leq |x|^2$.

קיבוע k. אינו מוריד קושי אוטומטית. CLIQUE ו-IS נופלות ל-P; 3COL ו-BIN-PACKING_2 נשארות NP-hard.

רשימת יכולות אחרי השיעור

אחרי השיעור צריך לדעת:

לנסח פורמלית את PARTITION, BIN-PACKING, ארבע הבעיות ההמילטוניות ו-TSP, כולל הקידודים המדויקים ($[0,1]$ ולא שלמים; גרף מלא ולא כל גרף).

להוכיח שכל אחת מהן ב-NP, עם certificate מפורש ועם נימוק שאורכו פולינומי.

לגזור את $2S - T$ ו-$T - 2S$ מתוך המשוואה $\sum_{i \notin I} a_i + b = S$ — לא לצטט אותם.

לכתוב את שלושת המקרים של רדוקציית PARTITION ואת שני הכיוונים בכל אחד, כולל טיעון המשלים.

לכתוב את רדוקציית BIN-PACKING כולל הטיפול במקרה החריג, ולהסביר למה מותר להחזיר קלט שלילי מומצא.

להסביר למה אותה רדוקציה מוכיחה קושי גם עבור $k = 2$ קבוע, ולהשוות ל-CLIQUE ול-3COL.

לחסום זמן ריצה של רדוקציה בגודל הקלט — לא בגודל הפלט ולא בערך המספרים.

לכתוב את $UHC \leq_p TSP$ בשני הכיוונים, בשתי הגרסאות (ישירה ובשלילה), ולהסביר את בחירת המשקלים.

להסביר במשפט אחד למה תכנון דינמי בגודל S או k אינו אלגוריתם פולינומי.

שאלות שנשארו פתוחות

עמוד 1 בסיכום, מקרה 3 של הרדוקציה: קראתי את האיבר המוחזר כ-$\sum_{i=1}^n a_i$ בלבד, בלי ה-$2S$ שנאמר בהקלטה ב-[00:15:28]; ייתכן שזו קריאה חלקית שלי של הכתב ולא השמטה בסיכום.

עמוד 2 בסיכום, תנאי 1 של רדוקציית BIN PACKING: הכתב נקרא כ-$a_i \ge \frac{1}{2}\sum a_j$, בעוד שבהקלטה ב-[00:44:31] נאמר במפורש 'גדול מ'. כאן נכתב אי-שוויון חד, שהוא הנכון מתמטית.

בהקלטה ב-[01:14:51] נאמר שהרדוקציה הידועה היא מ-SAT או מ-$3SAT$ ל-DHP ובסיכום נכתב $3SAT \le_p DHP$; ההוכחה לא נעשתה בקורס ולכן לא ניתן היה לאמת איזו משתי הגרסאות נלמדת.

עמוד 6 בסיכום (בעיות הכרעה/חיפוש/אופטימיזציה והגדרת אלגוריתם קירוב) מקביל ל-[01:40:43]–[02:08:24] בהקלטה, אך מבחינת התוכן הוא פתיחת שיעור 13; כאן ניתנת רק הפניה, והחומר עצמו שייך לקובץ שיעור 13.

ה-slug 'partition-bin-packing' מתאר בחסר: כשליש מהשיעור עוסק בבעיות המילטוניות וב-TSP (עמודים 4–5 בסיכום). ההיקף המלא נמצא ב-title_he; שם הקובץ לא שונה, כנדרש.

13 אלגוריתמי קירוב א׳: 2-קירוב ל-VC, ½-קירוב ל-MAXCUT ואי-קירוב של TSP

השיעור הראשון על אלגוריתמי קירוב: אלגוריתם 2-קירוב לכיסוי בקודקודים והוכחת ההידוק שלו, אלגוריתם חיפוש מקומי בעל יחס קירוב ½ ל-MAXCUT, והוכחה שקירוב בכל יחס קבוע לבעיית הסוכן הנוסע הכללית שקול ל-P=NP.

ביטחון: high

בקצרה

לפני הכול, **שלוש גרסאות של אותה בעיה**: הכרעה (שאלת כן/לא — שפה), חיפוש (מצא עד או דווח שאין) ואופטימיזציה (מצא את הערך/הפתרון הטוב ביותר — פונקציה, לא שפה). NP-קושי מוגדר פורמלית רק לגרסת ההכרעה, ולכן טענות אי-קירוב מנוסחות כתוצאות מותנות.

זהו השיעור הראשון שבו אנחנו **מוותרים על אופטימליות** במקום לוותר על זמן ריצה פולינומי. אלגוריתם קירוב חייב תמיד להחזיר **פתרון אפשרי** (feasible), רץ בזמן פולינומי, ומבטיח שהערך שלו רחוק מהאופטימום לכל היותר בפקטור α.

הטכניקה המרכזית של כל השיעור: האלגוריתם אינו יודע לחשב את OPT — הרי זו בדיוק הבעיה הקשה. לכן מוצאים גודל *עזר* שהאלגוריתם כן שולט בו, מוכיחים שהוא חוסם את OPT (מלמטה בבעיית מינימום, מלמעלה בבעיית מקסימום), ומשווים אליו את הפלט.

2-קירוב ל-VC: בחר קשת, הכנס את **שני** קצותיה לכיסוי, מחק את שניהם, חזור. גודל העזר הוא הזיווג F של הקשתות שנבחרו: $|F| \le |C_{\mathrm{opt}}|$ ו-$|C| = 2|F|$, ולכן $|C| \le 2|C_{\mathrm{opt}}|$.

להוסיף **קצה אחד** במקום שניים נשמע חסכוני יותר — ואינו נותן קירוב ביחס קבוע כלל. הדוגמה הנגדית היא כוכב.

הניתוח הדוק ביחס לאלגוריתם: על גרף שהוא זיווג מושלם האלגוריתם מחזיר את **כל** הקודקודים בעוד שהאופטימום הוא חצי מהם. שאלה אחרת לגמרי, ופתוחה עד היום, היא האם *לבעיה* יש אלגוריתם קירוב טוב מ-2.

½-קירוב ל-MAXCUT בחיפוש מקומי: כל עוד יש קודקוד שהעברתו לצד השני מגדילה את החתך — העבר אותו. בסיום מתקיים $\mathrm{cut}(v) \ge \mathrm{other}(v)$ לכל v, וספירה כפולה נותנת $|F| \ge \frac{1}{2}|E| \ge \frac{1}{2}K$.

תוצאת קושי מותנית: לכל $\alpha \ge 1$, אלגוריתם קירוב ביחס α לבעיית הסוכן הנוסע הכללית גורר $\mathrm{P} = \mathrm{NP}$ — ולמעשה שקול לכך. זו הדגמה של איך הופכים אלגוריתם קירוב לאלגוריתם הכרעה.

שני הכלים החדשים למבחן: **הוכחת פיזביליות בנפרד מהוכחת היחס**, ו**חסימת OPT באמצעות גודל עזר**.

רקע ותלויות

מ־שיעור 12 (הסוף שלו) — בעיית אופטימיזציה ואלגוריתם קירוב. הסיכום של שיעור 13 נפתח ישירות באלגוריתם, כי ההגדרות ניתנו בדקות האחרונות של המפגש הקודם ונרשמו בעמוד 6 של סיכום שיעור 12. **העמוד ההוא שייך מבחינת התוכן לשיעור הזה, ולכן הוא מטופל כאן במלואו —**

הטבלה המשולשת שבו בהגדרה 1, ההגדרה הפורמלית של בעיית אופטימיזציה בהגדרה 2, והגדרת אלגוריתם הקירוב בהגדרה 3. להלן תמצית קצרה של מה שנדרש כדי לקרוא את המשפטים; הניסוחים המלאים והדוגמאות נמצאים בפרק ההגדרות.

בעיית אופטימיזציה מורכבת מ־(א) קבוצת קלטים אפשריים $\mathcal{I}$ — למשל, עבור כיסוי בקודקודים, אוסף כל הגרפים הלא מכוונים; (ב) לכל קלט $I \in \mathcal{I}$, קבוצת **פתרונות אפשריים** X_I — עבור VC, כל הכיסויים בקודקודים של G; (ג) פונקציית ערך $v : X_I \to \mathbb{R}$ — עבור VC, גודל הקבוצה. המטרה: למצוא $x \in X_I$ שעבורו $v(x)$ מינימלי (או מקסימלי, תלוי בבעיה).

> **הערה על שני צירים [02:01:23] בתמלול 18:** יש כאן שני צירים שאפשר "להתפשר" עליהם — האם הפתרון אפשרי, ומה ערכו. **בקורס הזה מתפשרים רק על הערך.** אלגוריתם קירוב ל-VC שמקבל גרף חייב להחזיר כיסוי בקודקודים; לא כיסוי "כמעט". יש תחום מחקר שלם שמתפשר גם על זה, ואיננו עוסקים בו.

הגדרת אלגוריתם הקירוב לבעיית מינימיזציה (מילה במילה כפי שניתנה): עבור $\alpha \geq 1$, אלגוריתם קירוב לבעיית מינימיזציה עם יחס קירוב α הוא אלגוריתם שעבור כל קלט I לבעיה — (1) רץ בזמן פולינומי ב-$|I|$; (2) מחזיר פתרון אפשרי $x \in X_I$; (3) מקיים $\mathrm{OPT}(I) \;\leq\; v(x) \;\leq\; \alpha \cdot \mathrm{OPT}(I)$, כאשר $\mathrm{OPT}(I) = \min_{y \in X_I} v(y)$. אי-השוויון השמאלי טריוויאלי — פתרון אפשרי לא יכול להיות זול מהמינימום מבין הפתרונות האפשריים; **כל העבודה היא באי-השוויון הימני**.

הבעיה שהמרצה השאיר כ־cliffhanger בסוף שיעור 12 [02:07:08]: אם האלגוריתם אינו יודע לחשב את OPT — הרי חישובו הוא בדיוק הבעיה הקשה — איך בכלל הוא יכול לדעת שמה שהחזיר אינו גדול מפי 2 מ-OPT? התשובה ניתנת בשיעור הזה, והיא ליבת משפט 1.

מ־שיעור 10 — הבעיות עצמן. $U \subseteq V$ היא **כיסוי בקודקודים** של $G = (V, E)$ אם לכל קשת $xy \in E$ מתקיים $x \in U$ או $y \in U$. גרסת האופטימיזציה: בהינתן G, מצא כיסוי בקודקודים בגודל מינימלי. בעיית MAXCUT: בהינתן G, חלק את V לשתי קבוצות כך שמספר הקשתות ה"חוצות" יהיה מקסימלי. שתיהן NP-קשות בגרסת ההכרעה שלהן.

מ־שיעור 12 — מעגל המילטוני ובעיית הסוכן הנוסע. UHC (Undirected Hamiltonian Cycle) — האם קיים בגרף לא מכוון מעגל העובר בכל קודקוד בדיוק פעם אחת — היא NP-שלמה. בשיעור 12 נראתה גם הרדוקציה $\mathrm{UHC} \leq_p \mathrm{TSP}$, שבה נתנו לקשתות המקוריות משקל 1 ולשאר משקל 2. נזכיר את כיוון הסימון: $A \leq_p B$ פירושו ש-A ניתנת לרדוקציה ל-B, כלומר B **קשה לפחות כמו** A.

מאלגוריתמים / מתמטיקה בדידה — שני כלים שנשתמש בהם במפורש:

משפט הדרגות (lemma of handshakes): בכל גרף $G = (V, E)$ מתקיים $\sum_{v \in V} \deg_G(v) = 2|E|$, כי כל קשת תורמת 1 לדרגת כל אחד משני קצותיה.

עקרון שובך היונים בניסוח של פונקציות [00:26:19]: אם קיימת פונקציה חד-חד-ערכית $f : A \to B$ אז $|A| \leq |B|$. בקונטרפוזיציה: אם ב-A יש יותר איברים מאשר ב-B, אז אף פונקציה מ-A ל-B אינה חד-חד-ערכית — זהו בדיוק שובך היונים.

הגדרות

הגדרה 1: שלוש הגרסאות של בעיה — הכרעה, חיפוש ואופטימיזציה

לבעיות רבות יש **שלוש גרסאות שונות**, ואת ההבחנה ביניהן צריך לעשות לפני שמדברים על קירוב בכלל. הטבלה הבאה היא הטבלה שבעמוד 6 של סיכום שיעור 12, בדוגמה של VC:

הגרסה	הקלט	מה נדרש
בעיית הכרעה	גרף $G=(V,E)$ ומספר k	שאלה: האם קיים כיסוי בקודקודים בגודל k?
בעיית חיפוש	גרף $G=(V,E)$ ומספר k	מטרה: מצא כיסוי בקודקודים בגודל k, או דווח שאין כזה
בעיית אופטימיזציה	גרף $G=(V,E)$ בלבד	מטרה: החזר את הגודל המינימלי של כיסוי בקודקודים, או מצא כיסוי בקודקודים בגודל מינימלי

הבחנה טכנית שהמרצה הדגיש [01:52:35]–[01:53:07]. רק לבעיית ההכרעה יש "שאלה"; לשתי האחרות יש "מטרה". ההבדל אינו סמנטי בלבד: בעיית הכרעה היא **שפה** (קבוצה), כי היא שאלת כן/לא, ולכן אפשר לדבר עליה במונחים של P, NP ורדוקציות. בעיית אופטימיזציה אינה שפה אלא **פונקציה** — מקבלים גרף וצריך להחזיר מספר (או פתרון). זו הסיבה שאמרנו בשיעור 12 [01:55:13] ש-**NP-קושי מוגדר פורמלית לבעיות הכרעה בלבד**, כי הוא מוגדר באמצעות רדוקציות בין שפות; ובכל זאת גרסת האופטימיזציה של בעיה NP-קשה היא "קשה" במובן המעשי, ולכן משפט 4 בקובץ הזה מנוסח כתוצאת קושי **מותנית** ולא כטענת NP-קושי.

שתי תת-גרסאות של האופטימיזציה [01:51:32], [01:52:05]. אפשר לדרוש רק את **הערך** האופטימלי (הגודל המינימלי של כיסוי), ואפשר לדרוש את **הפתרון** עצמו (כיסוי בגודל מינימלי). שתיהן נקראות "בעיית אופטימיזציה", וההבדל דומה להבדל בין "מהו משקל המסלול הקל ביותר" לבין "מהו המסלול הקל ביותר". **הדרישה חייבת להיות חלק מהגדרת הבעיה** — זו בדיוק הנקודה שבה נפתחה ההקלטה של שיעור 13 [00:00:00]. בקורס הזה מתמקדים בגודל.

הקשר בין הגרסאות. הסדר הוא מהקל לכבד:

בעיית החיפוש היא הקשחה של בעיית ההכרעה [01:50:54]: לא מספיק לומר "כן", צריך גם להציג עד. **פותר יעיל לגרסת האופטימיזציה נותן פותר יעיל לגרסת ההכרעה** [01:54:42]. ההוכחה, שהמרצה נתן במפורש: בהינתן $\langle G, k\rangle$, הרץ את פותר האופטימיזציה על G, קבל את הגודל המינימלי m, והחזר "כן" אם ורק אם $m \le k$. זו קריאה אחת ובדיקה אחת, ולכן פולינומית. במילותיו: "אם אני יודע לפתור את זה, אני יודע לפתור את זה."

מכאן נובעת המסקנה שמעניינת אותנו: אם את גרסת ההכרעה איננו יודעים לפתור ביעילות, אז בוודאי לא את גרסת האופטימיזציה. **זו הסיבה שבשיעור הזה מוותרים על אופטימליות.**

הערה על הכיוון ההפוך. המרצה לא טען בשיעור את הכיוון ההפוך (בנייה של פותר אופטימיזציה מפותר הכרעה, למשל בחיפוש בינארי על k ואז self-reducibility), ולכן הוא אינו נטען כאן כתוצאה של השיעור. הוא כן משתמש בגרסה חלשה שלו במסקנת השקילות של משפט 4 [01:25:28], שם די בכך שאם $\mathrm{P} = \mathrm{NP}$ אפשר לפתור במדויק.

אינטואיציה כללית — למה בכלל התחלנו בזה [01:43:50]–[01:47:27]. זהו הפרק השלישי בקורס, "התמודדות עם NP-קושי". עד היום כל האלגוריתמים שראיתם (דייקסטרה, קרוסקל) החזירו תשובה **מדויקת**. כאן, לראשונה, מוותרים על משהו כדי לקבל זמן ריצה פולינומי: אלגוריתמי קירוב מוותרים על **אופטימליות**, ואלגוריתמים אקראיים (השיעורים הבאים) מוותרים על **ודאות**. בשני המקרים מתעקשים על גרנטי כמותי — "טועה, אבל לא יותר מדי" / "לא אופטימלי, אבל לא רחוק מדי".
והמרצה הוסיף אזהרה: זה **לא** אומר שהבעיה באמת קשה; ייתכן ש-VC בכלל ב-P — פשוט איננו יודעים לפתור אותה [01:45:24].
אי-מופע: "האם קיים כיסוי בקודקודים בגודל k" אינה בעיית אופטימיזציה, גם אם k קטן מאוד — אין בה פונקציית ערך למזער; היא שפה.
הגדרה 2: בעיית אופטימיזציה (הגדרה פורמלית)
בעיית אופטימיזציה מורכבת מארבעה רכיבים (עמוד 6 בסיכום שיעור 12; [01:57:00]–[02:00:51] בתמלול 18):
קבוצה $\mathcal{I}$ של **קלטים אפשריים**;
לכל קלט $I \in \mathcal{I}$, אוסף X_I של **פתרונות אפשריים** (feasible);
פונקציית **ערך** $v : X_I \to \mathbb{R}$;
המטרה: מבין הפתרונות האפשריים, למצוא פתרון אפשרי $x \in X_I$ שעבורו $v(x)$ אופטימלי — מינימלי או מקסימלי, לפי הבעיה.
המופע של VC (העמודה הכחולה בעמוד 6):
$\mathcal{I}$ היא אוסף כל הגרפים הלא מכוונים;
לכל גרף $G = (V, E)$, כל כיסוי בקודקודים ב-G נקרא פתרון אפשרי;
הערך של פתרון אפשרי הוא **גודלו**;
מבין כל הכיסויים בקודקודים מחפשים מינימלי.
אינטואיציה — שני צירים, מתפשרים רק על אחד [02:01:23]. הרכיב (2) והרכיב (3) הם שני צירים נפרדים: האם הפתרון אפשרי, ומה ערכו. אלגוריתם קירוב ל-VC **חייב** להחזיר כיסוי; על הערך הוא רשאי להתפשר. יש קו מחקר שלם שמתפשר גם על הפיזביליות — לא בקורס הזה.
אי-מופע: למה דווקא **מינימום** ב-VC ולא מקסימום [02:02:24]? כי כיסוי מקסימלי הוא טריוויאלי — כל קבוצת הקודקודים היא תמיד כיסוי. באופן סימטרי, ב-CLIQUE ו-Independent Set מחפשים מקסימום כי כל קודקוד בודד הוא קליק, וב-MAXCUT מחפשים מקסימום כי $U = \emptyset$ נותן תמיד חתך בגודל 0. "יש היגיון בטירוף": מגדירים תמיד את הכיוון המעניין, כי בכיוון השני התשובה ידועה מראש.

הגדרה 3: אלגוריתם קירוב ביחס α

(א) בעיית מינימיזציה (הניסוח שבעמוד 6 בסיכום שיעור 12, [02:05:02] בתמלול 18). עבור $\alpha \geq 1$, אלגוריתם קירוב לבעיית מינימיזציה עם יחס קירוב α הוא אלגוריתם שעבור כל קלט I לבעיה: רץ בזמן פולינומי ב-$|I|$, מחזיר פתרון אפשרי $x \in X_I$, ומקיים $\mathrm{OPT}(I) \leq v(x) \leq \alpha \cdot \mathrm{OPT}(I)$, $\mathrm{OPT}(I) = \min_{y \in X_I} v(y)$.

(ב) בעיית מקסימיזציה (לא בעמוד 6; נאמר בעל פה בשיעור הזה [00:36:24]). עבור $0 < \alpha \leq 1$, אלגוריתם קירוב לבעיית מקסימיזציה עם יחס קירוב α הוא אלגוריתם שעבור כל קלט I: רץ בזמן פולינומי ב-$|I|$, מחזיר פתרון אפשרי $x \in X_I$, ומקיים $\alpha \cdot \mathrm{OPT}(I) \leq v(x) \leq \mathrm{OPT}(I)$, $\mathrm{OPT}(I) = \max_{y \in X_I} v(y)$.

אינטואיציה. בשני המקרים **שלושה** דברים צריך לוודא [02:06:37]: זמן פולינומי, פיזביליות, וחסם על הערך. אחד משני אי-השוויונות הוא תמיד טריוויאלי — במינימיזציה זה $v(x) \geq \mathrm{OPT}$ (פתרון אפשרי לא יכול להיות זול מהמינימום), ובמקסימיזציה זה $v(x) \leq \mathrm{OPT}$ (אי אפשר להחזיר פתרון טוב מהמקסימלי). **כל העבודה היא באי-השוויון השני.**

מופע: אלגוריתם שמחזיר חתך בגודל לפחות חצי מהחתך המקסימלי הוא אלגוריתם קירוב ביחס $\frac{1}{2}$ (משפט 3); האלגוריתם של משפט 1 הוא אלגוריתם קירוב ביחס 2.

אי-מופע חשוב [00:36:24]: אלגוריתם ל-Independent Set שמחזיר תמיד קודקוד בודד הוא אמנם פולינומי ואמנם מחזיר פתרון אפשרי — אבל אין שום $\alpha > 0$ קבוע שעבורו הוא אלגוריתם קירוב ביחס α, כי OPT יכול לגדול עם הגרף בעוד הפלט נשאר 1. פתרון אפשרי כשלעצמו אינו מספיק; היחס חייב להיות **קבוע שאינו תלוי בקלט**.

> **שימו לב לקונבנציה של הקורס.** כאן $\alpha \geq 1$ לבעיות מינימום ו-$\alpha \leq 1$ לבעיות מקסימום — כלומר α הוא תמיד היחס $\mathrm{ALG}/\mathrm{OPT}$ בכיוון שבו הוא נמדד. הסיכום כותב בהתאם "אלגוריתם קירוב פי 2" ל-VC ו"אלגוריתם קירוב פי $\frac{1}{2}$" ל-MAXCUT. ספרים אחרים מנרמלים גם בעיות מקסימום ל-$\alpha \geq 1$ וכותבים $\mathrm{OPT}/\mathrm{ALG} \leq \alpha$; בקובץ הזה נשמרת הקונבנציה של הקורס.

> **הקושי שהמרצה השאיר כשאלה פתוחה בסוף שיעור 12 [02:07:08]:** האלגוריתם אינו יודע את $\mathrm{OPT}(I)$ — חישובו הוא בדיוק הבעיה הקשה. אז איך הוא בכלל יכול להתחייב ש-$v(x) \leq \alpha \cdot \mathrm{OPT}(I)$? "זה הקסם, אבל זה כמו הקסם של רדוקציה." התשובה נמצאת במשפט 1: גודל עזר שחוסם את OPT.

הגדרה 4: זיווג (קשתות זרות בזוגות)

קבוצת קשתות $F \subseteq E$ נקראת **זרה בזוגות** (זיווג, matching) אם לכל $e, \hat{e} \in F$ עם $e \neq \hat{e}$ מתקיים $e \cap \hat{e} = \emptyset$, כלומר אין להן קודקוד משותף.

אינטואיציה. זהו אוסף קשתות שאפשר "לצבוע" בלי ששתיים ייגעו זו בזו. הרעיון בהוכחת משפט 1 הוא שכיסוי בקודקודים חייב "לשלם" קודקוד נפרד עבור כל קשת בזיווג.

מופע: בגרף המעגל C_6 עם קודקודים $1, \ldots, 6$, הקבוצה $\{12, 34, 56\}$ היא זיווג. **אי-מופע:** $\{12, 23\}$ אינה זיווג, כי $12 \cap 23 = \{2\}$.

הגדרה 5: החתך המושרה, ו-$\mathrm{cut}(v)$ מול $\mathrm{other}(v)$
יהי $G=(V,E)$ ותהי $U \subseteq V$, ונסמן $\bar{U} = V \setminus U$. **החתך המושרה על ידי** U הוא קבוצת הקשתות $F = \{\, xy \in E \mid |\{x,y\} \cap U| = 1 \,\}$, כלומר כל הקשתות שיש להן **בדיוק קצה אחד** ב-U. לכל $v \in V$ נסמן:
$\mathrm{cut}(v)$ — מספר הקשתות הסמוכות ל-v ששייכות לחתך (הקצה השני שלהן בצד הנגדי);
$\mathrm{other}(v)$ — מספר הקשתות הסמוכות ל-v שאינן בחתך (הקצה השני שלהן באותו צד).
קשת נקראת **סמוכה** ל-v אם v הוא אחד מקצותיה.
אינטואיציה. כל קשת הנוגעת ב-v היא או "חוצה" או "פנימית", ולכן באופן מיידי $\mathrm{cut}(v) + \mathrm{other}(v) = \deg_G(v) \qquad \text{for all } v \in V.$
מופע: בגרף המשולש $\{a,b,c\}$ עם $U=\{a\}$: החתך הוא $\{ab, ac\}$, ומתקיים $\mathrm{cut}(a)=2;\ \mathrm{other}(a)=0$, $\mathrm{cut}(b)=1,\ \mathrm{other}(b)=1$ (הקשת bc פנימית). **אי-מופע:** עבור $U=\emptyset$ החתך ריק ו-$\mathrm{cut}(v)=0$ לכל v — קבוצה ריקה היא פתרון אפשרי לגמרי, פשוט גרוע.
הגדרה 6: גרסת האופטימיזציה של בעיית הסוכן הנוסע
קלט: גרף שלם $\hat{G}=(V,\hat{E})$ ופונקציית משקלים $w:\hat{E}\to\mathbb{Q}_{\geq 0}$. **פתרונות אפשריים:** כל המעגלים ההמילטוניים ב-$\hat{G}$ (מעגל שעובר בכל קודקוד בדיוק פעם אחת). שימו לב שבגרף שלם תמיד קיים כזה. **ערך:** $w(C)=\sum_{e\in C} w(e)$. **מטרה:** מינימיזציה.
אינטואיציה [01:21:14]. נקודת בלבול נפוצה מהכיתה: המשקל שמעניין אותנו הוא של **המעגל**, לא של הגרף. במעגל המילטוני יש בדיוק $|V|$ קשתות, לא משנה כמה קשתות יש בגרף השלם עצמו.
מופע: על K_4 עם משקל 1 לקשתות $12, 23, 34, 41$ ומשקל 9 לאלכסונים, המעגל $1-2-3-4-1$ הוא פתרון אפשרי בערך 4, וזהו האופטימום.

משפטים והוכחות
משפט 1: קיים אלגוריתם קירוב ביחס 2 לבעיית הכיסוי בקודקודים
האלגוריתם (עמוד 1 בסיכום). על קלט $G=(V,E)$:
אתחל $C \leftarrow \emptyset$, וכן $F \leftarrow \emptyset$.
כל עוד יש בגרף קשת $e = xy$:
הוסף את x ואת y ל-C; הוסף את e ל-F.
מחק מהגרף את x ואת y ואת כל הקשתות המחוברות ל-x או ל-y.
החזר את C.

> **הערה [00:03:12]–[00:03:43]:** בגרסה הראשונה שנכתבה על הלוח שלב 2.2 היה "מחק את הקשת e ואת כל הקשתות המחוברות ל-x ול-y". סטודנט העיר שמחיקת הקשת e מיותרת — ברגע שמוחקים את הקודקודים x, y, כל הקשתות הנוגעות בהם, ובכללן e עצמה, נעלמות. המרצה קיבל את התיקון ("אתה צודק ב-100%"), וזו הגרסה שנרשמה. הקובץ הזה משתמש בגרסה המתוקנת.

הערה: השורה $F \leftarrow \emptyset$ ותוספת e ל-F **אינן חלק אמיתי מהאלגוריתם** [00:30:04]. האלגוריתם אינו צריך את F כדי לרוץ, והיא לא משפיעה על הפלט. היא קיימת אך ורק לצורך הניתוח, ולכן נכתבה בסיכום בצבע אחר. זהו דפוס שחוזר בכל השיעור: מוסיפים לאלגוריתם "משתנה רפאים" שנותן לנו נקודת ייחוס להשוואה מול האופטימום.

טענה א (זמן ריצה). האלגוריתם רץ בזמן $O(|E|^2)$, ובפרט בזמן פולינומי בגודל הקלט.
הוכחה. נבחן מה "מתקדם" בכל איטרציה. בכל איטרציה של הלולאה נבחרת קשת e ונמחקים שני קצותיה, ולכן **נמחקת לפחות קשת אחת** (הקשת e עצמה). מספר הקשתות אינו גדל אף פעם, ולכן מספר האיטרציות קטן או שווה ל-$|E|$. בכל איטרציה, מציאת קשת ומחיקת הקודקודים והקשתות הסמוכות עולה לכל היותר מעבר על כל הגרף, כלומר $O(|E| + |V|)$, ובחסם גס לכל היותר $|E|$ מחיקות. סך הכל $O(|E|^2)$ — פולינומי בגודל הקלט. ■

הערה מתודית [00:06:53]–[00:10:53]: סטודנט נתן ניתוח הדוק בהרבה — כל קשת "נוגעים" בה לכל היותר פעם אחת (או שעוברים עליה ואז מוחקים אותה, או שהיא נמחקת כתוצאה ממחיקת שכן), ולכן זמן הריצה הוא $O(|E|)$. המרצה אישר שהניתוח נכון ומעולה, אך העדיף בכוונה את הניתוח הגס: "כל מה שמעניין אותי זה שזה פולינומי; אם אני לא חייב, אני לא עושה עבודות יזומות". במבחן — החסם הגס מספיק, ובלבד שהוא נכון.

טענה ב (פיזביליות). יהי $G = (V, E)$ ותהי C הקבוצה המוחזרת על ידי האלגוריתם. אז C היא כיסוי בקודקודים של G.
הוכחה. ראשית נבחין באינוריאנטה: **קודקוד נמחק מהגרף אם ורק אם הוא הוכנס ל-C**. אכן, המחיקה היחידה מתבצעת בשלב 2.2 ומתייחסת בדיוק לשני הקודקודים שהוכנסו ל-C בשלב 2.1. תהי $e = xy \in E$ קשת שרירותית של הגרף המקורי. האלגוריתם עוצר רק כשאין קשתות בגרף, ולכן בסיום הריצה e אינה בגרף — כלומר e נמחקה במהלך הריצה (אחרת האלגוריתם לא היה עוצר). קשת נמחקת רק בשלב 2.2, וזה קורה באחד משלושה מקרים:
מקרה 1: e הייתה הקשת שהאלגוריתם בחר באיטרציה. אז לפי שלב 2.1 מתקיים $x \in C$ **וגם** $y \in C$, ובפרט $x \in C$ או $y \in C$.
מקרה 2: e נמחקה כתוצאה ממחיקת x (כלומר x היה קצה של קשת אחרת שנבחרה). לפי האינוריאנטה $x \in C$, ולכן $x \in C$ או $y \in C$.
מקרה 3: e נמחקה כתוצאה ממחיקת y. באופן סימטרי $y \in C$, ולכן $x \in C$ או $y \in C$.
בכל המקרים לפחות אחד מקצות e שייך ל-C. מכיוון ש-e הייתה שרירותית, C מכסה את כל קשתות G. ■

הערה: מקרה 1 הוא למעשה מקרה פרטי של מקרים 2–3 בגרסה המתוקנת של האלגוריתם (הקשת הנבחרת נמחקת בדיוק בגלל מחיקת קצותיה). הסיכום מונה את שלושתם בנפרד, וכך גם נשמר כאן, כי בגרסה שעל הלוח בתחילת השיעור המחיקה של e הייתה מפורשת ולכן המקרה היה נפרד באמת.

שימו לב לניסוח [00:14:01]: גם כשמקבלים "$x \in C$ וגם $y \in C$", המרצה התעקש לסיים את המשפט ב"ובפרט $x \in C$ או $y \in C$" — כי זה בדיוק מה שההגדרה של כיסוי דורשת. "זה הקורד שאני חייב לסיים איתו את הדבר הזה."

טענה ג (יחס הקירוב). יהי C_{opt} פתרון אופטימלי (כיסוי בקודקודים בגודל מינימלי) עבור G. אז $|C_{\text{opt}}| \le |C| \le 2\,|C_{\text{opt}}|$.

הוכחה. אי-השוויון השמאלי מיידי: לפי טענה ב, C הוא כיסוי בקודקודים, ואין כיסוי בקודקודים קטן מהמינימלי.

לאי-השוויון הימני נשתמש ב-F. תהי $e \in F$ קשת כלשהי שהאלגוריתם בחר. מכיוון ש-C_{opt} הוא כיסוי בקודקודים של G, ומכיוון ש-$e \in E$, חייב להיות לפחות אחד מקצותיה של e ב-C_{opt}. נגדיר פונקציה $\varphi : F \to C_{\text{opt}}$, $\qquad \varphi(e) = \text{one endpoint of } e \text{ that lies in } C_{\text{opt}}$ (אם שני הקצוות ב-C_{opt} נבחר אחד מהם באופן שרירותי — לא משנה איזה). הפונקציה מוגדרת היטב בדיוק בזכות היות C_{opt} כיסוי.

φ חד-חד-ערכית. יהיו $e, \hat{e} \in F$ עם $e \neq \hat{e}$. לפי מבנה האלגוריתם, ברגע שקשת נכנסת ל-F שני קצותיה נמחקים מהגרף יחד עם כל הקשתות הנוגעות בהם; לכן שום קשת שתיבחר אחר כך לא תיגע בהם. נובע ש-$e \cap \hat{e} = \emptyset$, כלומר F **היא קבוצת קשתות זרות בזוגות** (זיווג). ומכיוון ש-$\varphi(e)$ הוא קצה של e ו-$\varphi(\hat{e})$ הוא קצה של $\hat{e}$, ושתי הקשתות זרות, בהכרח $\varphi(e) \neq \varphi(\hat{e})$.

לפי עקרון שובך היונים בניסוח של פונקציות, קיום פונקציה חד-חד-ערכית מ-F ל-C_{opt} נותן $|F| \le |C_{\text{opt}}|$.

מצד שני, בכל איטרציה הכנסנו קשת אחת ל-F **ושני** קודקודים חדשים ל-C (חדשים, כי אחרי המחיקה הם לא יופיעו שוב), ולכן $|C| = 2\,|F|$.

בשילוב: $|C| = 2|F| \le 2|C_{\text{opt}}|$. ■

הערה: זו ליבת השיעור [00:18:45]. האלגוריתם אינו יודע לחשב את $|C_{\text{opt}}|$, ואפילו לא לדבר עליו. הפתרון הוא לקחת גודל אחר, $|F|$, שנוח לעבוד איתו, להראות שהוא **חוסם מלמטה** את האופטימום, ולהראות שהפלט אינו גדול מפי 2 ממנו. זהו התבנית הכללית לכל בעיית מינימיזציה: מצא חסם תחתון על OPT שהאלגוריתם שולט בו.

הערה: כאן מתברר למה מוחקים את שני הקודקודים [00:24:10]. אילו היינו מוחקים רק קודקוד אחד, שתי קשתות ב-F היו יכולות לחלוק קודקוד, φ לא הייתה בהכרח חד-חד-ערכית, וכל ההוכחה קורסת. ראו תרגיל 3 בהמשך לדוגמה נגדית מפורשת.

משפט 2: הניתוח של משפט 1 הדוק ביחס לאלגוריתם

ניסוח. קיימת משפחה אינסופית של גרפים שעליהם האלגוריתם של משפט 1 מחזיר כיסוי בגודל **בדיוק** $2|C_{\text{opt}}|$. לכן לא ניתן לשפר את הקבוע 2 בטענה ג עבור האלגוריתם הזה.

הוכחה. לכל $n \ge 1$ נגדיר את M_n: גרף על $2n$ קודקודים $x_1, y_1, \dots, x_n, y_n$ שקשתותיו הן $x_i y_i$ לכל i — כלומר n קשתות זרות בזוגות (זיווג מושלם, ולא גרף רדוקיבילי במובן כלשהו; המרצה הדגיש שזה בדיוק "זיווג" [00:34:16]).

התנהגות האלגוריתם: בכל איטרציה נבחרת אחת מהקשתות $x_i y_i$; שני קצותיה נכנסים ל-C ונמחקים; אף קשת אחרת אינה נוגעת בהם, ולכן כל שאר הקשתות נשארות. לאחר n איטרציות $C = \{x_1, y_1, \ldots, x_n, y_n\}$, כלומר $|C| = 2n = |V|$ — **כל** הגרף.
האופטימום: הקשתות זרות בזוגות, ולכן כל כיסוי חייב להכיל לפחות קודקוד אחד מכל קשת, ומכאן $|C_{\text{opt}}| \geq n$. מצד שני, בחירת קצה אחד מכל קשת נותנת כיסוי בגודל n. לכן $|C_{\text{opt}}| = n$, ומספר הפתרונות האופטימליים הוא $2^n = 2^{|V|/2}$ (שתי בחירות לכל קשת) [00:35:19].
מכאן $|C| = 2n = 2|C_{\text{opt}}|$. ■

> **למה צריך משפחה אינסופית ולא גרף בודד [00:34:16]:** אם מציגים דוגמה נגדית קטנה אחת, אפשר לטעון "על גרף כזה אני פשוט פותר ידנית". כדי לומר משהו על האלגוריתם צריך אינסטנס גדול כרצוננו — לכן M_n לכל n.

> **שתי שאלות שונות לחלוטין [00:31:09]–[00:33:12].** (א) האם *ההוכחה* הדוקה ביחס *לאלגוריתם*? כן — זה משפט 2. (ב) האם *האלגוריתם* הדוק ביחס *לבעיה*, כלומר האם קיים אלגוריתם קירוב טוב מ-2 ל-VC? **זו בעיה פתוחה** ותחום מחקר חי. שאלה (א) היא שאלה על הניתוח שלנו; שאלה (ב) היא שאלה על טבע הבעיה, ואיננו עונים עליה בקורס. שימו לב גם: כל אלגוריתם 2-קירוב הוא בפרט אלגוריתם 4-קירוב — אי-השוויון רק נחלש [00:35:19].

משפט 3: קיים אלגוריתם קירוב ביחס $\frac{1}{2}$ לבעיית MAXCUT
האלגוריתם (עמוד 3 בסיכום) — חיפוש מקומי. על קלט $G = (V, E)$:
אתחל $U \leftarrow \emptyset$ (ולכן $\bar{U} \leftarrow V$).
כל עוד יש קודקוד v שהעברתו מ-U ל-$\bar{U}$, או מ-$\bar{U}$ ל-U, מגדילה את גודל החתך המושרה:
העבר את הקודקוד.
החזר את U.
טענה א (פיזביליות). האלגוריתם מחזיר קבוצת קודקודים $U \subseteq V$, וכל קבוצת קודקודים היא פתרון אפשרי ל-MAXCUT. לכן הפלט אפשרי, תמיד. ■

> **הערה [00:38:30]:** כאן, בניגוד ל-VC, אין שום תנאי על הקבוצה המוחזרת — "מקסימלי" הוא חלק מפונקציית המטרה, לא מהגדרת הפתרון האפשרי. לכן כל ההתעקבות תהיה על יחס הקירוב.

טענה ב (עצירה וזמן ריצה). האלגוריתם עוצר לאחר לכל היותר $|E| + 1$ סריקות, וזמן הריצה הכולל הוא $O(|G|^2)$ — פולינומי בגודל הקלט.
הוכחה. החשש האמיתי כאן אינו הזמן אלא **העצירה** [00:41:59]: לכאורה קודקוד יכול לעבור לצד אחד ואז לחזור, ולהיתקע בלולאה אינסופית. ואכן, קודקוד *יכול* לחזור (ראו דוגמה 4 בהמשך) — אבל זה לא משנה, כי יש לנו "חוש התקדמות" מונוטוני:
בכל איטרציה שבה מבוצעת העברה, גודל החתך המושרה על ידי U **גדל בלפחות** 1 — זה בדיוק תנאי הלולאה, ולכן החתך לעולם אינו קטן. גודל החתך מתחיל ב-0 (כי $U = \emptyset$), ובאף חתך אין יותר מ-$|E|$ קשתות. לכן מספר ההעברות הוא לכל היותר $|E|$, ומספר הסריקות (כולל הסריקה האחרונה

שבה לא נמצא קודקוד משפר ולכן האלגוריתם עוצר) הוא לכל היותר $|E|+1$.
עלות סריקה אחת: עוברים על כל קודקוד v, ולכל אחד על כל שכניו, וסופרים כמה מהם בצד שלו וכמה בצד הנגדי; אם בצד שלו יש יותר — מעבירים אותו. בייצוג ברשימת שכנויות זהו מעבר על כל הגרף, כלומר $O(|V|+|E|)$. סך הכל $O(|E|\cdot(|V|+|E|)) = O(|G|^2)$, פולינומי בגודל הקלט. ■

טענה ג (יחס הקירוב). נסמן ב-K את גודלו של חתך מקסימלי ב-G, וב-F את קבוצת הקשתות בחתך המושרה על ידי ה-U שהאלגוריתם החזיר. אז $|F| \geq \frac{1}{2}|E| \geq \frac{1}{2}K$.

הוכחה. נתחיל מהחסם העליון הפשוט על האופטימום: כל חתך הוא תת-קבוצה של E, ולכן $K \leq |E|$. זהו גודל העזר בבעיית מקסימיזציה — בדיוק המראה של $|F| \leq |C_{\text{opt}}|$ ממשפט 1, רק שכאן צריך חסם **מלמעלה** על OPT [00:50:01].

כעת שלושה מרכיבים:

(1) פירוק הדרגה. לכל $v \in V$, כל קשת סמוכה ל-v היא או בחתך או לא, ולכן $\mathrm{cut}(v) + \mathrm{other}(v) = \deg_G(v)$. סכימה על כל הקודקודים ושימוש במשפט הדרגות: $\sum_{v\in V}\big(\mathrm{cut}(v)+\mathrm{other}(v)\big) = \sum_{v\in V}\deg_G(v) = 2|E|$.

(2) תנאי האופטימליות המקומית. האלגוריתם עצר. נסמן ב-$\mathrm{cut}(v), \mathrm{other}(v)$ את הערכים **ברגע העצירה** [01:00:37]. אילו היה קיים v עם $\mathrm{cut}(v) < \mathrm{other}(v)$, אז העברת v לצד הנגדי הייתה הופכת את כל הקשתות הפנימיות שלו לקשתות חתך ולהפך, ומשנה את גודל החתך ב- $\mathrm{other}(v) - \mathrm{cut}(v) > 0$ — כלומר מגדילה אותו, והאלגוריתם לא היה עוצר. סתירה. לכן $\mathrm{cut}(v) \geq \mathrm{other}(v) \quad \text{for all } v \in V$.

(3) ספירה כפולה של קשתות החתך. כל קשת בחתך היא בעלת קצה אחד בדיוק ב-U וקצה אחד בדיוק ב-$\bar{U}$. לכן בסכימה על צד אחד בלבד, כל קשת חתך נספרת בדיוק פעם אחת: $\sum_{v\in U}\mathrm{cut}(v) = |F|, \qquad \sum_{v\in \bar{U}}\mathrm{cut}(v) = |F|$. חיבור שתי המשוואות נותן $\sum_{v\in V}\mathrm{cut}(v) = 2|F|$.

החיבור (ה"גרנד פינלה" [00:57:07]). נשתמש ב-(1), ואז ב-(2) איבר-איבר, ואז ב-(3): $2|E| = \sum_{v\in V}\big(\mathrm{cut}(v)+\mathrm{other}(v)\big) \leq \sum_{v\in V} 2\,\mathrm{cut}(v) = 2\sum_{v\in V}\mathrm{cut}(v) = 4|F|$. מכאן $|F| \geq \frac{1}{2}|E|$, ומכיוון ש-$K \leq |E|$ מתקיים גם $|F| \geq \frac{1}{2}K$. יחד עם טענה א וטענה ב, זהו אלגוריתם קירוב ביחס $\frac{1}{2}$ ל-MAXCUT. ■

הערה [00:57:53]: בהרצאה נאמר לרגע "גדול שווה" ומיד תוקן ל"קטן שווה". הכיוון הנכון הוא זה שכתוב כאן: מחליפים $\mathrm{other}(v)$ ב-$\mathrm{cut}(v)$ שהוא **גדול** ממנו, ולכן הסכום רק גדל.

הערה: היכן ההפסד בניתוח. החסם $|F| \geq |E|$ הוא גס. על גרף המשולש למשל $|E| = 3$ ו-$K = 2$, כך שהניתוח מבטיח רק $|F| \geq 1.5$ בעוד שהאלגוריתם למעשה מוצא חתך בגודל 2, כלומר אופטימלי. שאלת ההידוק של $\frac{1}{2}$ לא נדונה בהרצאה ואינה בסיכום.

משפט 4: לכל $\alpha \geq 1$ — אם ניתן לקרב את בעיית הסוכן הנוסע הכללית ביחס α, אז $\mathrm{P} = \mathrm{NP}$

רקע לניסוח [01:03:27]: אין באמת "קושי" מוכח בעולם ה-NP. לא הוכחנו שאי אפשר לפתור בעיה NP-קשה ביעילות; הוכחנו רק שהיא קשה **ביחס** לשאר בעיות NP. לכן, ובפרט לבעיות אופטימיזציה שעבורן NP-קושי לא מוגדר פורמלית (הוא מוגדר דרך רדוקציות בין שפות, כלומר בעיות הכרעה), התוצאות שאנחנו יכולים לנסח הן **תוצאות קושי מותנות**: "אם אפשר לעשות X, אז $\mathrm{P} = \mathrm{NP}$" — ומכיוון שאיננו מצפים ל-$\mathrm{P} = \mathrm{NP}$, איננו מצפים ש-X אפשרי.

הוכחה. יהי $\alpha \geq 1$, ונניח בשלילה שקיים אלגוריתם קירוב A ביחס α לגרסת האופטימיזציה של בעיית הסוכן הנוסע. נבנה את האלגוריתם הבא, שמקבל גרף לא מכוון $G = (V, E)$:
בנה גרף שלם $\hat{G} = (V, \hat{E})$ על אותה קבוצת קודקודים, ולכל $e \in \hat{E}$ הגדר $w(e) = \begin{cases} 1 & e \in E \\ \alpha|V| + 1 & e \notin E \end{cases}$
הרץ את אלגוריתם הקירוב A על $(\hat{G}, w)$.
אם ערך הפתרון שחזר קטן או שווה $\alpha|V|$ — **קבל**; אחרת — **דחה**.

הערה [01:11:40]: זו כמעט אותה בנייה כמו הרדוקציה $\mathrm{UHC} \leq_p \mathrm{TSP}$ משיעור 12, אבל שם המשקלים היו 1 ו-2 וכאן המשקל של "קשת שלא הייתה" הוא ענק. הענק הזה הוא מה שקונה לנו את הפער מול α.

הערה [01:16:56]: האובייקט שבנינו אינו רדוקציית מיפוי. זה **אלגוריתם** שקורא לאלגוריתם אחר כתת-שגרה ואז מפרש את התשובה — בדיוק סוג ה"רדוקציה" שמכירים מקורסי אלגוריתמים ומבני נתונים. לכן הניסוח הוא "האלגוריתם מכריע את UHC", ולא "יש רדוקציה".

ניתוח זמן ריצה. יהי $G = (V, E)$.
שלב 1 דורש $O(|V|^2)$ צעדים: יש $\binom{|V|}{2}$ קשתות בגרף השלם, ולכל אחת בדיקה אם היא ב-E וכתיבת משקל. המשקל $\alpha|V| + 1$ ניתן לכתיבה ב-$O(\log(\alpha|V|))$ ביטים — זה מספר גדול, אבל **קצר** [01:12:10]; זה בדיוק ההבדל בין "מספר גדול" ל"מספר שאי אפשר לכתוב".
שלב 2 דורש זמן פולינומי ב-$|(\hat{G}, w)|$, כי אלגוריתם קירוב הוא **מעצם ההגדרה** אלגוריתם פולינומי [01:14:18]. מכיוון ש-$|(\hat{G}, w)| \leq O(|G|^2)$, ומכיוון שפולינום בפולינום הוא פולינום, שלב 2 פולינומי ב-$|G|$.
שלב 3 דורש זמן קבוע: השוואת שני מספרים.
סך הכל: זמן ריצה פולינומי ב-$|G|$.
ניתוח נכונות. יהי $G = (V, E)$ ונסמן $n = |V|$.
כיוון ראשון: $G \in \mathrm{UHC}$. אז קיים ב-G מעגל המילטוני C_0. אותו מעגל קיים גם ב-$\hat{G}$ (כי $E \subseteq \hat{E}$), וכל קשתותיו הן קשתות של E ולכן במשקל 1 כל אחת. במעגל המילטוני יש בדיוק n קשתות, ולכן $w(C_0) = n$. יתרה מזו, כל מעגל המילטוני מורכב מ-n קשתות שמשקל כל אחת הוא לפחות 1, ולכן

α יחד, $\mathrm{OPT}(\hat{G}, w) \geq n$; בדיוק. מכיוון ש-$\mathrm{OPT}(\hat{G}, w) = n$ הוא אלגוריתם קירוב ביחס A לבעיית מינימיזציה, הפתרון שהוא מחזיר מקיים $w(A(\hat{G}, w)) \leq \alpha \cdot \mathrm{OPT}(\hat{G}, w) = \alpha n.$
לכן שלב 3 **מקבל** את G — כנדרש.

כיוון שני: $G \notin \mathrm{UHC}$. אז אין ב-G מעגל המילטוני. יהי C מעגל המילטוני **כלשהו** ב-$\hat{G}$ (קיים כזה, כי $\hat{G}$ שלם). מכיוון ש-C אינו מעגל המילטוני של G, בהכרח יש בו קשת $e^* \notin E$, ולכן $w(e^*) = 1$. שאר $n - 1$ הקשתות של C תורמות לפחות 1 כל אחת, ולכן $w(C) \geq (n-1) + (\alpha n + 1) = \alpha n + n > \alpha n.$
זה נכון ל**כל** מעגל המילטוני ב-$\hat{G}$, ובפרט למעגל המינימלי, ולכן $\mathrm{OPT}(\hat{G}, w) > \alpha n$. אלגוריתם הקירוב מחזיר פתרון אפשרי, ופתרון אפשרי אינו יכול להיות זול מהאופטימום, ולכן גם $w(A(\hat{G}, w)) \geq \mathrm{OPT}(\hat{G}, w) > \alpha n$. לכן שלב 3 **דוחה** את G — כנדרש.

> **הערה [01:23:52]:** שימו לב שהשתמשנו בשני צדדיו של אי-השוויון שבהגדרת אלגוריתם הקירוב. בכיוון הראשון השתמשנו בצד ה"מעניין" ($\mathrm{ALG} \leq \alpha\,\mathrm{OPT}$), ובכיוון השני דווקא בצד הטריוויאלי ($\mathrm{ALG} \geq \mathrm{OPT}$), שנובע מכך שהפלט הוא פתרון אפשרי. בלי הדרישה שהפלט יהיה פיזבילי, הכיוון השני היה נופל.

סיום. האלגוריתם שבנינו מכריע את UHC בזמן פולינומי, ולכן $\mathrm{UHC} \in \mathrm{P}$. אך UHC היא NP-קשה (שיעור 12), ולכן לכל $L \in \mathrm{NP}$ מתקיים $L \leq_p \mathrm{UHC} \in \mathrm{P}$, כלומר $\mathrm{NP} \subseteq \mathrm{P}$. יחד עם ההכלה הטריוויאלית $\mathrm{P} \subseteq \mathrm{NP}$ נקבל $\mathrm{P} = \mathrm{NP}$. ■

> **הערה טכנית (לא נאמרה בהרצאה):** אם α אינו שלם, $\alpha n + 1$ אינו מספר שלם. אפשר לעבוד עם משקלים רציונליים (ואז חייב להיות רציונלי כדי שנוכל בכלל לכתוב אותו בזמן פולינומי), או להשתמש במשקל $\lceil \alpha n \rceil + 1$; אז $w(C) \geq \lceil \alpha n \rceil + 1 + (n-1) > \alpha n$ וההוכחה עוברת מילה במילה.

> **הערה (לא נאמרה בהרצאה):** המשקלים שבנינו מפרים בגסות את אי-שוויון המשולש — קשת "יקרה" בין שני קודקודים שיש ביניהם מסלול זול. לכן המשפט אומר דבר על TSP **הכללי** בלבד, ואינו סותר את קיומם של אלגוריתמי קירוב לגרסה המטרית.

מסקנה: שקילות [01:25:28]. למעשה מתקיים: $\exists\, \alpha \geq 1$ approximation for general TSP $\iff \mathrm{P} = \mathrm{NP}.$
הכיוון שהוכחנו הוא ($\Rightarrow$). הכיוון ($\Leftarrow$) מיידי: אם $\mathrm{P} = \mathrm{NP}$ אז אפשר להכריע את גרסת ההכרעה של TSP בזמן פולינומי, ובאמצעות חיפוש בינארי על ערך המטרה גם לפתור את גרסת האופטימיזציה **במדויק** — כלומר לקרב אותה בפקטור 1; ואם אפשר לקרב בפקטור 1, אז בפרט אפשר בפקטור 3 או בכל $\alpha \geq 1$ אחר.

דוגמאות ותרגילים מהשיעור

דוגמה 1: הרצת אלגוריתם ה-VC על מסלול באורך 3 — הסדר קובע

יהי G המסלול $a - b - c - d$, כלומר $E = \{ab, bc, cd\}$. הכיסוי המינימלי הוא $\{b, c\}$ בגודל 2.

סדר א' (הקשת הנבחרת ראשונה היא bc): $C = \{b, c\}$, $F = \{bc\}$; מוחקים את b, c ואיתם את ab, bc, cd. לא נשארו קשתות. הפלט: $C = \{b, c\}$, גודל 2. יחס: $2/2 = 1$.

סדר ב' (הקשת הנבחרת ראשונה היא ab): $C=\{a,b\}$, $F=\{ab\}$; מוחקים את a,b ואיתם את ab,bc. נשארה cd. איטרציה שנייה: $C=\{a,b,c,d\}$, $F=\{ab,cd\}$. הפלט בגודל 4. יחס: $4/2=2$.

מה למדנו: האלגוריתם אינו קובע איזו קשת לבחור, והפלט תלוי בבחירה — אבל **בשני המקרים** מתקיים $|F|\le|C_{\text{opt}}|$ ו-$|C|=2|F|$, ולכן החסם $|C|\le 2|C_{\text{opt}}|$ נשמר תמיד.

דוגמה 2: הרצה על המעגל C_6

$V=\{1,\dots,6\}$, $E=\{12,23,34,45,56,16\}$. הכיסוי המינימלי הוא $\{1,3,5\}$ בגודל 3.

איטרציה 1: בוחרים 12. $C=\{1,2\}$, $F=\{12\}$. מוחקים $1,2$ ואיתם $12,23,16$. נשאר $E'=\{34,45,56\}$.

איטרציה 2: בוחרים 34. $C=\{1,2,3,4\}$, $F=\{12,34\}$. מוחקים $3,4$ ואיתם $34,45$. נשאר $E'=\{56\}$.

איטרציה 3: בוחרים 56. $C=\{1,\dots,6\}$, $F=\{12,34,56\}$. אין קשתות.

פלט: כל ששת הקודקודים. בדיקה: $|F|=3\le|C_{\text{opt}}|=3$ ✓, $|C|=6=2|F|$ ✓, $6\le 2\cdot 3$ ✓ — היחס כאן הדוק בדיוק.

תרגיל 3 (שאלת סטודנט, [00:16:38]–[00:18:13]): למה לא להוסיף רק קצה אחד?

השאלה. האלגוריתם "מבזבז": הוא מכניס שני קודקודים לכל קשת. למה לא לבחור קשת $e=xy$, להוסיף רק את x ל-C, ולמחוק רק את x (ואיתו את הקשתות הנוגעות בו)?

התשובה המלאה. קודם כל, הווריאנט הזה **כן** מחזיר כיסוי בקודקודים: כל קשת נמחקת רק כשאחד מקצותיה נכנס ל-C. הבעיה היא ביחס הקירוב — והוא לא רק גרוע מ-2, הוא **אינו קבוע כלל**.

נתבונן בכוכב $K_{1,n}$: קודקוד מרכזי c ו-n עלים $x_1,\dots,x_n$, כאשר $E=\{cx_i\}$. הכיסוי המינימלי הוא $\{c\}$, כלומר $|C_{\text{opt}}|=1$.

מכיוון שהאלגוריתם דטרמיניסטי אך אינו מגדיר את סדר בחירת הקשתות, אפשר לבנות קלט (או מימוש) שבו הבחירה תמיד "רעה": בכל איטרציה נבחרת קשת cx_i ומוסיפים דווקא את **העלה** x_i. מחיקת x_i מסלקת רק את הקשת cx_i, ושאר הקשתות נשארות. לאחר n איטרציות $C=\{x_1,\dots,x_n\}$, כלומר $|C|=n=|V|-1$ היחס הוא $|C|/|C_{\text{opt}}|=n/1=|V|-1$, שגדל עם הקלט — כלומר אין α **קבוע** שהאלגוריתם הזה מקיים.

המסקנה המבנית. מחיקת שני הקצוות אינה בזבוז; היא בדיוק מה שהופך את F לזיווג, ובלעדיה הפונקציה φ שבהוכחת משפט 1 מפסיקה להיות חד-חד-ערכית. המרצה הוסיף שאותה תופעה מופיעה גם על מסלול ארוך [00:17:09].

תרגיל 4 (מהשיעור, [00:33:12]): הראו שהאלגוריתם ל-VC אינו יכול להשיג יחס טוב מ-2.

זהו בדיוק משפט 2 לעיל: משפחת הזיווגים המושלמים M_n. פתרון מלא ניתן שם.

דוגמה 5: הרצת אלגוריתם ה-MAXCUT — קודקוד שעובר וחוזר

החשש שהמרצה העלה [00:41:59] הוא שקודקוד יעבור הלוך ושוב לנצח. הנה גרף שבו קודקוד באמת חוזר, ובכל זאת האלגוריתם עוצר:

$V=\{v,a,b,p_1,p_2,q_1,q_2\}$, $E=\{va,\ vb,\ ap_1,\ ap_2,\ bq_1,\ bq_2\}$ — עץ עם $|E|=6$.

התחלה: $U=\emptyset$, גודל החתך 0.

איטרציה	הקודקוד המועבר	other / cut שלו לפני ההעברה	U אחרי	גודל החתך
1	v	$0/2$	$\{v\}$	2
2	a	$1/2$	$\{v,a\}$	3
3	b	$1/2$	$\{v,a,b\}$	4
4	v	$0/2$	$\{a,b\}$	6

באיטרציה 4 הקודקוד v **חוזר** ל-$\bar{U}$: אחרי ש-a ו-b עברו, שתי הקשתות va, vb הפכו לפנימיות, ולכן משתלם להחזיר את v. בסיום: $U=\{a,b\}$, כל שש הקשתות חוצות, ואין קודקוד משפר ($\mathrm{cut}(a)=3,\mathrm{other}(a)=0$; $\mathrm{cut}(p_1)=1,\mathrm{other}(p_1)=0$ וכו').

מה למדנו: אי אפשר לטעון "קודקוד לא יחזור"; **אפשר** לטעון שגודל החתך $0\to2\to3\to4\to6$ עולה ממש בכל צעד, וזה לבדו מבטיח עצירה תוך $\le|E|$ העברות. סדרת החתכים היא ה"חוש התקדמות" של האלגוריתם.

בדיקת ההבטחה: $|F|=6\ge\frac{1}{2}|E|=3$ ✓ (וכאן אפילו נמצא האופטימום, $K=6$, כי העץ דו-צדדי).

דוגמה 6: ספירת החתך משני צדדיו [01:01:41]

הדוגמה שהמרצה צייר כדי להסביר את שלב (3) בהוכחת משפט 3: חתך שבו קשתותיו נספרות מצד U כ-$1+1+1+1+1=5$, ומצד $\bar{U}$ כ-$1+2+2=5$. אותו חתך, שתי ספירות שונות, אותו מספר — כי כל קשת חוצה נספרת בדיוק פעם אחת בכל אחד מהסכומים, לפי הגדרת החתך. זהו גם ההסבר לכך ש-$\sum_{v\in V}\mathrm{cut}(v)=2|F|$ ולא $|F|$.

דוגמה 7: הרצת אלגוריתם ההכרעה של משפט 4 עם $\alpha=2$

מופע חיובי. G = המעגל $1-2-3-4-1$, כלומר $V=\{1,2,3,4\}$, $E=\{12,23,34,41\}$. בונים $\hat{G}=K_4$; המשקלים: $w(12)=w(23)=w(34)=w(41)=1$, $w(13)=w(24)=\alpha|V|+1=2\cdot4+1=9$. המעגל $1-2-3-4-1$ במשקל 4, וזהו OPT. אלגוריתם קירוב ביחס 2 חייב להחזיר מעגל במשקל ≤ 8. סף ההכרעה הוא $\alpha|V|=8$, ולכן האלגוריתם **מקבל** — נכון, כי $G\in\mathrm{UHC}$.

מופע שלילי. G = המסלול $1-2-3-4$, כלומר $E=\{12,23,34\}$; אין בו מעגל המילטוני. שוב $\hat{G}=K_4$ ו-$w(12)=w(23)=w(34)=1$, $w(13)=w(14)=w(24)=9$. שלושת המעגלים ההמילטוניים ב-K_4:

$1-2-3-4-1$: $1+1+1+9=12$;

$1-2-4-3-1$: $1+9+1+9=20$;

$1-3-2-4-1$: $9+1+9+9=28$.

$\mathrm{OPT}=12>8$, וכל פתרון שיוחזר יהיה לפחות 12. לכן האלגוריתם **דוחה** — נכון, כי $G\notin\mathrm{UHC}$.

.

שימו לב לפער: בכיוון החיובי הערך המקסימלי האפשרי הוא 8, ובכיוון השלילי הערך המינימלי האפשרי הוא 12. הפער הזה הוא כל תפקידו של המשקל הענק $\alpha|V|+1$ — הוא נבנה כך שאפילו אלגוריתם קירוב גרוע ככל האפשר לא יוכל "לחצות" את הסף.

הערות מהשיעור

[00:03:43]–[00:05:49] — "למה דווקא זה?" היא לא השאלה הנכונה עכשיו. המרצה הקדיש כמה דקות לנקודה מתודית: כשרואים אלגוריתם או רדוקציה, סדר הפעולות הוא (1) להבין **איך** הוא עובד — הרצה יבשה על גרף; (2) להוכיח **למה** הוא מקיים את מה שדרוש; ורק אחר כך, אם בכלל, לשאול איך מישהו חשב עליו. "זה יכול לקחת חודשים של מחקר. אם אין לכם את החודשים לשבת על זה, לא תגיעו לזה — ואתם גם לא צריכים לצורך הקורס."

[00:09:33] — ניתוח גס מכוון. "אני קצת הורס את כל מה שלימדו אתכם באלגוריתמים ומבני נתונים": כאן לא מחפשים את זמן הריצה הטוב ביותר אלא רק פולינומיות, ולכן ניתוח גס עדיף כי הוא קצר ובטוח יותר. הניתוח ההדוק ($O(|E|)$ ל-VC) נכון ואף "מעולה", פשוט מיותר.

[00:20:56]–[00:21:59] — "פתרון אופטימלי", לא "הפתרון האופטימלי". יש **גודל** אופטימלי אחד (מינימום קיים תמיד בקבוצה לא ריקה של טבעיים), אבל **פתרונות** אופטימליים יכולים להיות רבים. לכן הסימון הוא "פתרון אופטימלי", ובניתוח לא מסתמכים על יחידות. משפט 2 מדגים זאת: שם יש $2^{|V|/2}$ פתרונות אופטימליים.

[00:26:19]–[00:28:25] — שובך היונים. סטודנטים ביקשו לחזור על המעבר $|F| \le |C_{\text{opt}}|$. הניסוח שהוסכם: אם ב-A יש יותר איברים מב-B, אז אף פונקציה מ-A ל-B אינה חד-חד-ערכית (שובך היונים); בקונטרפוזיציה — אם קיימת פונקציה חד-חד-ערכית מ-A ל-B אז $|A| \le |B|$. "אתם צריכים לדעת את זה."

[00:29:31]–[00:30:04] — $|C| = 2|F|$ אינו "כמו קודם". סטודנט שאל מתי אמרנו ש-$|C| = 2|F|$. התשובה: זו **טענה חדשה**, ולא משהו שנאמר קודם; היא כמעט מיידית מהבנייה (כל קשת שנכנסה ל-F הכניסה שני קודקודים ל-C), אבל היא עדיין טענה שצריך לומר.

[00:30:36]–[00:31:09] — האם 2 הוא הקירוב הטוב ביותר ל-VC? שאלה שנשאלה בשיעור הקודם. התשובה: להוכיח שקירוב מסוים הוא הטוב ביותר האפשרי הוא נושא קשה מלא בבעיות פתוחות, ועבור VC זו בעיה פתוחה לגמרי. תיאורטית ייתכן שקיים אלגוריתם עם יחס $2-\varepsilon$ לכל $\varepsilon > 0$. "התחום עדיין חי — עדיין מוצאים אלגוריתמי קירוב טובים יותר לכל מיני בעיות."

[00:35:19] — יחס קירוב הוא חסם, לא ערך. אלגוריתם 2-קירוב הוא בפרט 4-קירוב; אי-השוויון פשוט נחלש. לכן ההצהרה "יחס הקירוב הוא 2" משמעה "לכל היותר 2".

[00:36:24] — מקסימיזציה: היחס בין 0 ל-1. אזהרה מפורשת: להחזיר פתרון חוקי אבל זעיר (למשל קודקוד בודד ל-Independent Set) אינו קירוב.

[00:41:59]–[00:44:32] — החשש הראשון בחיפוש מקומי הוא תמיד עצירה. "בדרך כלל כשרואים את האלגוריתם הזה, הדבר הראשון שעולה זה: איך אני יודע שזה עוצר?" והתשובה תמיד: מהו ה-sense of progress, והאם ההתקדמות הזו גוררת חסם על מספר האיטרציות.

[00:47:19]–[00:48:20] — מה בדיוק עושים בסריקה. לכל קודקוד עוברים על כל שכניו וסופרים כמה מהם בצד שלו וכמה בצד הנגדי; אם בצד שלו יש יותר — מעבירים. בייצוג ברשימת שכנויות זה מעבר על כל הגרף. המרצה ציין שאפשר גם ניתוח מדויק יותר ($|V| \cdot |E|$ או $|G|^3$) — לא משנה, כל אלה פולינומיים.

[01:03:27]–[01:04:33] — למה בכלל "תוצאות קושי מותנות". "אנחנו קוראים לבעיה NP-קשה, אבל לא באמת הוכחתי שהיא קשה — הוכחתי שהיא קשה ביחס לבעיות ב-NP." לכן כל טענת אי-קירוב בקורס היא מהצורה "אם ניתן לקרב, אז $\mathrm{P} = \mathrm{NP}$".

[01:08:26]–[01:09:32] — איך מוכיחים $\mathrm{P} = \mathrm{NP}$ תחת הנחה. אפשרות א': לקחת $A \in \mathrm{NP}$ שרירותית ולהראות $A \in \mathrm{P}$ — קשה. אפשרות ב', והדרך שנבחרה: לקחת בעיה **אחת** שידועה כ-NP-קשה ולהראות שהיא ב-P; מהגדרת NP-קושי נובע מיד ש-$\mathrm{NP} \subseteq \mathrm{P}$. "עכשיו העניין הוא רק לבחור נכון את הבעיה ה-NP-קשה שנוח לעבוד איתה" — וכאן בחרנו את UHC, כי גרסת האופטימיזציה של TSP נבנתה עליה מלכתחילה.

[01:12:10] — מספר גדול אינו מספר ארוך. המשקל $\alpha|V| + 1$ הוא ענק, אבל אורכו $O(\log(\alpha|V|))$ ביטים. זו נקודה שחוזרת בכל הקורס (ראו גם SUBSET-SUM בשיעור 11): מה שמגביל אותנו הוא אורך הייצוג, לא הערך.

[01:19:36]–[01:21:45] — בלבול נפוץ שהמרצה פתר בכיתה. ב-$\hat{G}$ תמיד קיים מעגל המילטוני (הוא גרף שלם) — זה לא מה שמעניין; מה שמעניין הוא **המשקל** שלו. ובנוסף: משקל המעגל הוא סכום על $|V|$ קשתות בלבד, ולא על כל קשתות הגרף השלם.

[01:25:28] — למה חשוב לומר "שקול". התוצאה אינה רק "קירוב $\Longleftarrow \mathrm{P} = \mathrm{NP}$" אלא שקילות, כי אם $\mathrm{P} = \mathrm{NP}$ אפשר לפתור את הבעיה במדויק ובפרט לקרב אותה בכל פקטור. הכיוון הזה מיידי, ובכל זאת צריך לומר אותו כדי לטעון שקילות.

פערים בין הסיכום להקלטה

מקור: סיכום שיעור 12, עמוד 6 (מול סיכום שיעור 13, עמוד 1). **הפער:** עמוד 6 של סיכום השיעור **הקודם** אינו שייך לתוכן שיעור 12 (המילטוני/TSP) אלא הוא **פתיחת נושא הקירוב**: טבלת ההשוואה הכרעה/חיפוש/אופטימיזציה, ההגדרה הפורמלית של בעיית אופטימיזציה עם המופע של VC, והגדרת אלגוריתם קירוב ביחס α לבעיית מינימיזציה. סיכום שיעור 13 מתחיל ישירות באלגוריתם ומניח את כל זה כידוע. **ההכרעה:** העמוד נכתב **כאן** במלואו — הגדרות 1, 2 ו-3 — כולל הטבלה, ארבעת רכיבי בעיית האופטימיזציה, המופע של VC בארבעה סעיפים, וההגדרה לבעיית מינימיזציה. קובץ שיעור 12 מחזיק לגבי העמוד מצביע בלבד; הבעלות על התוכן היא של הקובץ הזה, וכך נרשם גם ב- `sources.pdf.note` .

מקור: עמוד 6 בסיכום שיעור 12 מול ההקלטה של שיעור 13. **הפער:** עמוד 6 מגדיר אלגוריתם קירוב **לבעיית מינימיזציה בלבד** ($\alpha \geq 1$); הגרסה למקסימיזציה ($0 < \alpha \leq 1$) נאמרה רק בעל פה בשיעור 13 [00:36:24] ואינה בשום סיכום. **ההכרעה:** הגדרה 3 מנוסחת בשני סעיפים — (א) מינימיזציה לפי עמוד 6, (ב) מקסימיזציה לפי ההקלטה — ומקורו של כל סעיף מצוין בגוף ההגדרה.

מקור: תמלול 18, [01:40:43]–[02:08:24]. **הפער:** קטע זה — פתיחת הפרק "התמודדות עם NP-קושי", ההבחנה בין שאלה (שפה) לבין מטרה (פונקציה), ההסבר ש-NP-קושי מוגדר לבעיות הכרעה בלבד, והטיעון שפותר אופטימיזציה יעיל נותן פותר הכרעה יעיל — אינו מכוסה בשום סיכום.
ההכרעה: נכתב בהגדרה 1, והתמלול נוסף ל- `sources.transcripts` עם `coverage: partial` וטווח מפורש, במקום להיות מצוטט בלי להופיע ב-frontmatter.

מקור: ההקלטה [00:03:12]–[00:03:43]. **הפער:** הגרסה הראשונה של שלב 2.2 כללה "מחק את הקשת e", מה שמיותר; סטודנט תיקן והמרצה קיבל. הסיכום מכיל כבר את הגרסה המתוקנת.
ההכרעה: נכתבה הגרסה המתוקנת, והאפיזודה תועדה כהערה כי היא מסבירה למה בסיכום מופיעים שלושה מקרים בהוכחת הפיזביליות ולא שניים.

מקור: הסיכום (עמוד 3), שורת פתיחת ניתוח זמן הריצה. **הפער:** כתוב "יהי $G = (E, V)$ גרף" — היפוך סדר הרכיבים בזוג. **ההכרעה:** תוקן ל-$G = (V, E)$, כמו בכל שאר העמודים; פליטת קולמוס ברורה.

מקור: הסיכום (עמוד 4). **הפער:** נכתב $|F| \geq \frac{1}{2}|K|$ למרות ש-K הוגדר כמספר (גודל חתך מקסימלי), כך שסימני הערך המוחלט מיותרים. **ההכרעה:** נכתב $|F| \geq \frac{1}{2}K$.

מקור: הסיכום (עמוד 4), הפרמטר $|E| + 1$ למספר האיטרציות ב-MAXCUT. **הפער:** מספר ההעברות בפועל חסום ב-$|E|$; ה-$+1$ נובע מהסריקה האחרונה שבה לא נמצא קודקוד משפר. הסיכום אינו מסביר זאת. **ההכרעה:** נשמר החסם $|E| + 1$ של הסיכום, עם ההסבר המפורש שהתוספת היא סריקת העצירה.

מקור: ההקלטה [00:57:53]. **הפער:** המרצה אמר "גדול שווה" ותיקן מיד ל"קטן שווה" בשרשרת אי-השוויונות $2|E| \leq \sum 2\,\mathrm{cut}(v)$. **ההכרעה:** נכתב הכיוון הנכון (החלפת $\mathrm{other}(v)$ ב-$\mathrm{cut}(v)$ הגדול ממנו מגדילה את הסכום).

מקור: ההקלטה בלבד. **הפער:** חומר מהותי שאינו בסיכום כלל — (א) הדוגמה הנגדית של הכוכב לוריאנט שמוסיף קצה אחד [00:16:38]; (ב) ההבחנה בין "ההוכחה הדוקה ביחס לאלגוריתם" לבין "האלגוריתם הדוק ביחס לבעיה", והיות השאלה השנייה פתוחה עבור VC [00:31:09]; (ג) הדיון בעצירת החיפוש המקומי וההדגמה שקודקוד יכול לחזור [00:41:59]; (ד) ההבחנה שזו אינה רדוקציית מיפוי אלא אלגוריתם שקורא לאלגוריתם [01:16:56]; (ה) השקילות ל-$\mathrm{P} = \mathrm{NP}$ ולא רק הגרירה [01:25:28]. **ההכרעה:** כל אלה נכללו — (א) כתרגיל 3, (ב) כמשפט 2 והערותיו, (ג) כטענה ב של משפט 3 ודוגמה 5, (ד)–(ה) כהערות במשפט 4.

מקור: הסיכום בלבד. **הפער:** משפט 2 (הידוק הניתוח) מופיע בהקלטה בלבד ולא בסיכום; לעומת זאת, הסיכום מנסח את שלושת המקרים בהוכחת הפיזביליות של VC בצורה מסודרת יותר משנאמר בעל פה. **ההכרעה:** שני המקורות מוזגו; הניסוח והסימונים (C, F, C_{opt}, cut, other, K) נלקחו מהסיכום.

מקור: קונבנציות. **הפער:** הסיכום כותב "Max-Cut" ו-"UHC"/"TSP"/"VC" כטקסט; המסמך המנחה דורש עטיפת שמות בעיות ב- `\mathrm{}` בצורה MAXCUT. **ההכרעה:** אומצה הקונבנציה של המסמך המנחה לשמות בעיות ומחלקות ($\mathrm{VC}, \mathrm{MAXCUT}, \mathrm{TSP}, \mathrm{UHC}, \mathrm{P}, \mathrm{NP}$), ונשמרו שמות המשתנים והאינדקסים של הסיכום ($G, V, E, C, F, C_{\mathrm{opt}}, U, \bar{U}, K, \alpha, w, \hat{G}, \hat{E}$).

מקור: תמלול 20. **הפער:** התמלול הוקצה כהקשר אך עוסק כולו באלגוריתמים אקראיים (בעיית המזכיר, אימות כפל מטריצות) ואינו נוגע בחומר של שיעור זה. **ההכרעה:** נרשם ב-frontmatter עם `coverage: none` והערה. חשוב לציין: אין בקורפוס הקלטה נוספת של חומר קירוב — תמלול 19 מסתיים ב-[01:26:00] בדיוק בסוף עמוד 5, ואינו חורג לחומר של שיעור 14.

סיכום ונקודות למבחן

שלושת הדברים שצריך להוכיח על כל אלגוריתם קירוב — ותמיד בנפרד ובסדר הזה:

זמן ריצה פולינומי. ניתוח גס מספיק: כמה איטרציות (מה ה-sense of progress?) כפול כמה עבודה באיטרציה.

פיזביליות. הפלט חייב להיות פתרון אפשרי לבעיה — כיסוי, ולא "כמעט כיסוי". על זה לא מתפשרים.

יחס הקירוב. דרך גודל עזר: בבעיית מינימיזציה — חסם **תחתון** על OPT ($|F| \le |C_{\mathrm{opt}}|$); בבעיית מקסימיזציה — חסם **עליון** על OPT ($|E| \le K$).

התוצאות שכדאי לזכור בעל פה:

$$|C_{\mathrm{opt}}| \le |C| = 2|F| \le 2|C_{\mathrm{opt}}| \qquad (\mathrm{VC}),\ |F| \ge \tfrac{1}{2}|E| \ge \tfrac{1}{2}K \qquad (\mathrm{MAXCUT}),$$

$$\text{approximating general TSP within any } \alpha \ge 1 \iff \mathrm{P} = \mathrm{NP}.$$

המלכודות הסטנדרטיות:

לבלבל בין "ההוכחה הדוקה" ל"האלגוריתם אופטימלי". הצגת משפחת M_n מוכיחה רק שהניתוח שלנו לא ניתן לשיפור עבור **האלגוריתם הזה**. השאלה אם ל-VC יש קירוב טוב מ-2 פתוחה.

לשכוח שדוגמה נגדית בודדת אינה מספיקה. צריך משפחה אינסופית.

לכתוב יחס קירוב לבעיית מקסימום כגדול מ-1. בקונבנציה של הקורס: מינימיזציה $\alpha \ge 1$, מקסימיזציה $0 < \alpha \le 1$.

לוותר על צד ה"טריוויאלי" של אי-השוויון. בהוכחת משפט 4, הכיוון השלילי נשען דווקא על $\mathrm{ALG} \ge \mathrm{OPT}$, שנובע מהפיזביליות.

לחשוב שמשקל גדול הוא בעיה. $\alpha|V| + 1$ נכתב ב-$O(\log(\alpha|V|))$ ביטים.

להתבלבל בין משקל הגרף למשקל המעגל. במעגל המילטוני יש בדיוק $|V|$ קשתות.

צ׳ק־ליסט: אחרי השיעור סטודנט צריך לדעת

לנסח את שלוש הגרסאות של בעיה נתונה (הכרעה / חיפוש / אופטימיזציה), ולהסביר למה רק הראשונה היא שפה ולמה פותר אופטימיזציה יעיל גורר פותר הכרעה יעיל.

לכתוב את ארבעת רכיבי של בעיית אופטימיזציה ואת שלוש הדרישות מאלגוריתם קירוב, ולדעת איזה משני אי-השוויונות טריוויאלי בכל אחד משני סוגי הבעיות.

לכתוב את אלגוריתם ה-2-קירוב ל-VC מהזיכרון, ולהוכיח את שלוש טענותיו במלואן.

להסביר בדיוק היכן ההוכחה נשברת אם מוחקים רק קצה אחד, ולתת את הכוכב כדוגמה נגדית.

להראות שהניתוח הדוק באמצעות זיווג מושלם.

לכתוב את אלגוריתם החיפוש המקומי ל-MAXCUT, להוכיח שהוא עוצר, ולהריץ את שרשרת הספירה הכפולה $|F| = \sum 2\,\mathrm{cut}(v) \le 2|E|$ עד הסוף.

לבנות מתוך אלגוריתם קירוב ל-TSP אלגוריתם הכרעה ל-UHC, כולל בחירת המשקל הענק וניתוח שני הכיוונים.

להסביר במילים למה כל תוצאות אי-הקירוב בקורס הן מותנות.

שאלות שנשארו פתוחות

הסיכום של שיעור 13 נפתח באמצע הנושא: הגדרות הפתיחה נמצאות בעמוד 6 של סיכום שיעור 12 ובתמלול 18 ([01:40:43]–[02:08:24]); העמוד ההוא נכתב כאן ולא בקובץ שיעור 12, ויש לוודא בסקירה שאין כפילות בין שני הקבצים.

עמוד 6 בסיכום שיעור 12, שורת בעיית ההכרעה בטבלה: נקרא "כיסוי בקודקודים בגודל k" בלי סימן אי-שוויון; בהקלטה [01:49:49] נאמר אותו נוסח. ייתכן שהכוונה "בגודל לכל היותר k" כמקובל, ובגוף הקובץ נשמר נוסח המקור.

עמוד 4 בסיכום: הסוגריים אחרי TSP נקראו כ-"הסוכן הנוסע"; ייתכן שכתוב שם "המקרה הכללי". שתי הקריאות אינן משנות את הטענה.

עמוד 4 בסיכום: כתוב |F| ≥ ½|K| למרות ש-K כבר מסמן מספר; סימני הערך המוחלט מיותרים ונכתב כאן K.

המשקל α|V|+1 מניח בשתיקה ש-α רציונלי (אחרת אי אפשר לכתוב אותו); בהקלטה זה לא נאמר, וכאן צוינה החלופה ⌈α|V|⌉+1.

הידוק יחס הקירוב ½ עבור MAXCUT לא נדון בהרצאה ואינו בסיכום; נכתבה כאן רק ההערה מהיכן ההפסד בניתוח.

14 אלגוריתמי קירוב ב׳: ½-קירוב חמדני ל-MAXCUT, 2-קירוב ל-TSP המטרי ו-2-קירוב לאריזה למכלים

שלושה אלגוריתמי קירוב פולינומיים, כל אחד עם הוכחת פיזביליות, ניתוח זמן ריצה והוכחת יחס: אלגוריתם חמדני חד-מעברי ביחס ½ ל-MAXCUT, אלגוריתם עץ פורש מינימלי + DFS ביחס 2 לבעיית הסוכן הנוסע כשהמשקלים מקיימים את אי-שוויון המשולש, ואלגוריתם First-Fit ביחס 2 לבעיית האריזה למכלים.

ביטחון: medium | ללא הקלטה

בקצרה

זהו השיעור השני על אלגוריתמי קירוב, והוא כולו **אלגוריתמים ובניית חסמים** — אין בו אף תוצאת קושי. שלושה אלגוריתמים, שלוש הוכחות יחס, ואותה טכניקה בדיוק בכל אחת.

הטכניקה החוזרת (מ־שיעור 13): האלגוריתם אינו יודע לחשב את OPT. לכן בונים *גודל עזר* שהאלגוריתם שולט בו, מוכיחים שהוא חוסם את OPT מהצד הנכון, ומשווים אליו את הפלט. כאן שלושת גדלי העזר הם: $|E|$ עבור MAXCUT, משקל העץ הפורש המינימלי עבור TSP, וסכום האיברים $\sum a_i$ עבור בעיית האריזה.

½-קירוב חמדני ל-MAXCUT: מעבר יחיד על הקודקודים לפי סדר; כל קודקוד נכנס לצד שבו יש לו **פחות** שכנים שכבר הוצבו. ההוכחה מפרקת את E לקבוצות $E_1, \dots, E_n$ לפי הקצה בעל האינדקס הגבוה, ומראה $|F \cap E_j| \geq \frac{1}{2}|E_j|$ **בנפרד לכל** j. זהו אלגוריתם שונה מהחיפוש המקומי של שיעור 13, ומשיג את אותו יחס — במעבר אחד ובלי איטרציות.

2-קירוב לבעיית הסוכן הנוסע כשהמשקלים מטריים: חשב עץ פורש מינימלי T, הרץ עליו DFS, והחזר את הקודקודים לפי סדר הגילוי. שלושה אי-שוויונות מרכיבים את ההוכחה: $w(T) \leq w(C_{\mathrm{opt}})$, ואז $w(P) = 2w(T)$ עבור הסיור שעובר על כל קשת פעמיים, ואז $w(C) \leq w(P)$ בזכות אי-שוויון המשולש (״קיצורי דרך״).

שימו לב לניגוד מול שיעור 13: שם הוכחנו שלבעיית הסוכן הנוסע ה**כללית** אין קירוב ביחס קבוע אלא אם $\mathrm{P} = \mathrm{NP}$. כאן, בתוספת הנחה אחת בלבד — אי-שוויון המשולש — יש קירוב ביחס 2. ההנחה הזו היא כל ההבדל.

2-קירוב לבעיית האריזה למכלים (First-Fit): הכנס כל פריט לתא הראשון שהוא נכנס אליו. הלמה המרכזית: בפלט יש **לכל היותר תא אחד** שסכום איבריו $\leq \frac{1}{2}$. מכאן $\sum a_i > \frac{1}{2}(m-1)$, ומכיוון ש-$m_{\mathrm{opt}} \geq \sum a_i$ מקבלים $m \leq 2m_{\mathrm{opt}}$.

שני טריקים כלליים שכדאי לזכור מכאן: **חלוקת קבוצת האילוצים לחלקים שהאלגוריתם מכריע עליהם אחד-אחד** (הפירוק ל-E_j), ו**מעבר משלמים לחסם** — האי-שוויון $m < 2m_{\mathrm{opt}} + 1$ הופך ל-$m \leq 2m_{\mathrm{opt}}$ רק כי m שלם.

רקע ותלויות

מ־שיעור 13 — הגדרת אלגוריתם הקירוב. נחזור עליה במלואה, כי כל השיעור הזה הוא שלוש הפעלות שלה.

עבור בעיית **מינימיזציה** ו-$\alpha \geq 1$, אלגוריתם A הוא אלגוריתם קירוב ביחס α אם לכל קלט I:
A רץ בזמן פולינומי ב-$|I|$;
$A(I)$ הוא **פתרון אפשרי** (feasible) לקלט I;
$\mathrm{OPT}(I) \;\leq\; v(A(I)) \;\leq\; \alpha \cdot \mathrm{OPT}(I)$.
עבור בעיית **מקסימיזציה** ו-$0 < \alpha \leq 1$ הכיוון מתהפך: $\alpha \cdot \mathrm{OPT}(I) \;\leq\; v(A(I)) \;\leq\; \mathrm{OPT}(I)$.
בשני המקרים אחד משני אי-השוויונות טריוויאלי (פתרון אפשרי לעולם אינו טוב מהאופטימום), וכל העבודה היא בשני. זו הסיבה שכל שלושת הניתוחים בשיעור בנויים באותו סדר: **פיזביליות** $\to$ **זמן ריצה** $\to$ **יחס**. אל תוותרו על השלב הראשון במבחן; הוא נבדק.

> **הערה:** הסיכום של שיעור 14 כותב "ביחס קירוב $\frac{1}{2}$" עבור MAXCUT ו"ביחס קירוב 2" עבור שתי בעיות המינימום, כלומר משתמש בקונבנציה שבה $\alpha \leq 1$ לבעיות מקסימום ו-$\alpha \geq 1$ לבעיות מינימום. זו הקונבנציה שנשמרת כאן לאורך כל הקובץ. ספרים אחרים כותבים $\mathrm{OPT}/\mathrm{ALG}$ גם לבעיות מקסימום ואז אותו אלגוריתם הוא "2-קירוב"; שימו לב לכיוון לפני שאתם מצטטים תוצאה.

מ־שיעור 13 — MAXCUT. בהינתן גרף לא מכוון $G = (V, E)$, יש למצוא חלוקה של V לשתי קבוצות כך שמספר הקשתות שקצה אחד שלהן בכל צד יהיה מקסימלי. בשיעור 13 ראינו אלגוריתם **חיפוש מקומי**: כל עוד יש קודקוד שהעברתו לצד השני מגדילה את החתך — העבר אותו. הוא נותן יחס $\frac{1}{2}$. האלגוריתם של השיעור הזה משיג את אותו יחס בשיטה אחרת לגמרי.
מ־שיעור 13 ומ־שיעור 12 — בעיית הסוכן הנוסע. בשיעור 12 ראינו את הרדוקציה $\mathrm{UHC} \leq_p \mathrm{TSP}$ (הזכרה: $A \leq_p B$ פירושו ש-A ניתנת לרדוקציה פולינומית ל-B, כלומר B **קשה לפחות כמו** A). בשיעור 13 הוכחנו, על גבי אותה רדוקציה, שאם קיים אלגוריתם קירוב ביחס α כלשהו ל-TSP הכללית אז $\mathrm{P} = \mathrm{NP}$. התוצאה הזו היא הרקע ההכרחי למשפט 3 כאן: היא מסבירה למה מוסיפים את הנחת אי-שוויון המשולש, ולמה בלעדיה אין מה לחפש.
מקורס אלגוריתמים — שני כלים שמשמשים אותנו כקופסה שחורה.
עץ פורש מינימלי (MST). לכל גרף לא מכוון קשיר ממושקל אפשר למצוא בזמן פולינומי עץ פורש שמשקלו מינימלי מבין כל העצים הפורשים (Prim ב-$O(|V|^2)$, Kruskal ב-$O(|E| \log |V|)$).
התכונה היחידה שנשתמש בה: אם T עץ פורש מינימלי ו-T' עץ פורש כלשהו, אז $w(T) \leq w(T')$.
DFS. סריקה לעומק של עץ מנוהלת ב-$O(|V| + |E|)$ ומייצרת שני דברים שנצטרך: **סדר הגילוי** (preorder) של הקודקודים, ו**הסיור הסגור** שבו כל קשת של העץ נחצית בדיוק פעמיים — פעם "ברדת" ופעם "בעלייה".

הגדרות

הגדרה 1: החתך המושרה על ידי קבוצת קודקודים

יהי $G = (V, E)$ גרף לא מכוון, ותהי $U \subseteq V$. **החתך המושרה** על ידי U הוא $F = \{\, xy \in E \;:\; x \in U,\; y \in \bar{U} \,\}$, כאשר $\bar{U} = V \setminus U$. ערך הפתרון הוא $|F|$, ובעיית MAXCUT היא למקסם אותו.

אינטואיציה. צובעים כל קודקוד בשחור או בלבן, וסופרים כמה קשתות מחברות בין צבעים שונים. כל קבוצה U היא פתרון אפשרי — גם $U = \emptyset$ (חתך ריק) וגם $U = V$. אין כאן שום אילוץ פיזביליות מלבד "U היא תת-קבוצה של V", ולכן הוכחת הפיזביליות של אלגוריתם ל-MAXCUT היא כמעט טריוויאלית — כל התוכן הוא ביחס.

דוגמה. ב-K_3 עם $V = \{v_1, v_2, v_3\}$: עבור $U = \{v_1\}$ מתקבל $F = \{v_1v_2, v_1v_3\}$ ו-$|F| = 2$, וזהו האופטימום. *אי-דוגמה לרווח:* עבור $U = V$ מתקבל $F = \emptyset$ — פתרון אפשרי לחלוטין, וערכו 0.

הגדרה 2: משקלים המקיימים את אי-שוויון המשולש

יהי $G = (V, E)$ גרף שלם עם משקלים $w : E \to \mathbb{R}^+$. נאמר ש-w **מקיימת את אי-שוויון המשולש** אם לכל $x, y, z \in V$. $w(xz) \;\le\; w(xy) + w(yz)$.

אינטואיציה. "קיצור דרך אינו מייקר": לעולם לא כדאי לעבור דרך תחנת ביניים כדי להגיע מ-x ל-z. כל מרחק גיאומטרי מקיים זאת, וגם מרחקי מסלול קצר בגרף.

דוגמה. ארבע נקודות במישור עם מרחק אוקלידי, למשל קודקודי מלבן 3×4: המשקלים הם $3, 4, 5$ והם מקיימים את אי-השוויון. *אי-דוגמה:* שלושה קודקודים עם $w(xy) = 1$, $w(yz) = 1$, $w(xz) = 5$ — כאן $5 > 1 + 1$, ולכן משפט 3 אינו חל. זה בדיוק סוג המשקלים שהרדוקציה של שיעור 13 מייצרת, וזו הסיבה שהיא מצליחה לייצר אי-קירוב.

הגדרה 3: בעיית הסוכן הנוסע עם משקלים מטריים

נתון: גרף שלם $G = (V, E)$ עם משקלים $w : E \to \mathbb{R}^+$ המקיימים את אי-שוויון המשולש.
מטרה: למצוא מעגל המילטוני (מעגל העובר בכל קודקוד של G בדיוק פעם אחת וחוזר לנקודת ההתחלה) שמשקלו מינימלי.

אינטואיציה. זו בעיית הסוכן הנוסע הרגילה, בהגבלה למופעים "הגיוניים גיאומטרית". שימו לב שהגרף חייב להיות **שלם** — אחרת אין ערובה שקיים מעגל המילטוני בכלל, והבעיה חוזרת להיות בעיית קיום.

אי-דוגמה חשובה. מופע TSP שבו המשקלים הם 1 ו-2 בשרירותיות אינו בהכרח מטרי, אף שכל מופע כזה שנוצר מהרדוקציה של שיעור 12 **כן** מקיים את אי-השוויון (כי $2 \ge 1 + 1$). זו נקודה שכדאי לבדוק לפני שמכריזים שמשפט 3 סותר את שיעור 13 — הוא אינו סותר; שיעור 13 השתמש במשקלים 1 ו-$1 + \alpha|V|$, שאינם מטריים.

הגדרה 4: בעיית האריזה למכלים (Bin Packing)

נתון: מספרים $a_1, \dots, a_n \in (0, 1]$. **מטרה:** לחלק את $a_1, \dots, a_n$ למספר מינימלי של קבוצות, כך שסכום האיברים בכל קבוצה אינו עולה על 1.

פורמלית, פתרון אפשרי הוא פונקציה $f : [n] \to [m]$ (הקצאת פריט לתא) המקיימת $\sum_{i:\, f(i) = j} a_i \le 1$ לכל $j \in [m]$, וערך הפתרון הוא m.

אינטואיציה. n חפצים בגדלים שונים ומכלים בעלי קיבולת 1 — כמה מכלים צריך. התנאי $a_i \le 1$ הכרחי: פריט גדול מ-1 לא היה נכנס לשום תא, ואז לא היה קיים פתרון אפשרי כלל.

דוגמה. $a = (0.4,\ 0.7,\ 0.3,\ 0.6)$: החלוקה $\{a_1, a_4\}$ (סכום 1.0) ו-$\{a_2, a_3\}$ (סכום 1.0) היא פתרון אפשרי בעל ערך 2, וזה האופטימום כי $\sum a_i = 2.0 > 1$. *אי-דוגמה.* החלוקה $\{a_1, a_2\}$ אינה פתרון אפשרי, כי $0.4 + 0.7 = 1.1 > 1$.

משפטים והוכחות

משפט 1: אלגוריתם חמדני הוא אלגוריתם קירוב ביחס ½ ל-MAXCUT

האלגוריתם (כפי שהוא בסיכום). לכל גרף $G = (V, E)$, נסמן $V = \{v_1, \ldots, v_n\}$.

אתחל $U = \bar{U} = \emptyset$.

לכל $1 \leq i \leq n$:

אם ל-v_i יש **יותר** שכנים ב-U מאשר ב-$\bar{U}$ — הכנס את v_i ל-$\bar{U}$; אחרת הכנס את v_i ל-U.

החזר את U.

שימו לב: בזמן הריצה U ו-$\bar{U}$ הן שתי קבוצות נפרדות שנבנות במקביל, ורק בסוף הריצה מתקיים $\bar{U} = V \setminus U$. הספירה בשלב 2.1 מתייחסת **רק לשכנים שכבר הוצבו**, כלומר לשכנים עם $k < i$; שכנים עתידיים אינם נמצאים באף אחת מהקבוצות ולכן אינם נספרים.

טענת פיזביליות. האלגוריתם מחזיר תמיד קבוצת קודקודים $U \subseteq V$, וכל תת-קבוצה של V היא פתרון אפשרי לפי הגדרה 1. בנוסף, כל v_i מוכנס בדיוק לאחת משתי הקבוצות בדיוק פעם אחת, ולכן בסוף אכן $U \dot{\cup} \bar{U} = V$. $\square$

ניתוח זמן ריצה (כפי שהוא בסיכום). שלב 1 דורש $O(1)$ פעולות. שלב 2 מתבצע ב-$|V|$ איטרציות, ובכל איטרציה עוברים על לא יותר מ-$|E|$ קשתות כדי לספור את השכנים בשני הצדדים. סך הכול $O(|V| \cdot |E|)$, שהוא פולינומי בגודל הקלט. $\square$

> **הערה:** הסיכום מסתפק בחסם הרופף $O(|V| \cdot |E|)$, וזה מספיק לחלוטין למטרה (להראות פולינומיות). לשלמות: אם באיטרציה i סורקים רק את הקשתות **הנוגעות ב-**v_i, כל קשת נסרקת פעמיים לאורך כל הריצה (פעם לכל קצה), והזמן הכולל הוא $O(|V| + |E|)$ — כלומר האלגוריתם הוא ליניארי, במעבר יחיד.

ניתוח יחס הקירוב. יהי $G = (V, E)$ גרף, ונסמן $V = \{v_1, \ldots, v_n\}$. יהי U הפלט של האלגוריתם ויהי $F \subseteq E$ החתך המושרה על ידי U.

הפירוק המרכזי. לכל $1 \leq j \leq n$ נסמן ב-E_j את קבוצת הקשתות ש-v_j הוא הקצה שלהן בעל **האינדקס הגבוה** מבין שני הקצוות: $E_j = \{ v_i v_j \in E \ : \ i < j \}$.

> **אינטואיציה (מופיעה בסיכום בכחול):** E_j היא קבוצת הקשתות ש-v_j "יקבע את גורלן". כשהאלגוריתם מגיע ל-v_j, כל הקצוות השניים של קשתות E_j כבר הוצבו, ולכן ההחלטה על v_j קובעת סופית עבור כל קשת ב-E_j אם היא בחתך או לא. הקשתות שיוכרעו מאוחר יותר שייכות ל-E_k עבור $k > j$ ואינן מושפעות.

למה 1.1. $\bigcup_{j=1}^{n} E_j = E$, והקבוצות $E_1, \ldots, E_n$ זרות בזוגות; לכן $|E| = \sum_{j=1}^{n} |E_j|$.

הוכחה. תהי $e = v_i v_j \in E$ קשת כלשהי. הגרף פשוט ואין בו לולאות עצמיות, ולכן $i \neq j$, ולקשת יש קצה יחיד בעל אינדקס גבוה יותר — נניח $j > i$. אז $e \in E_j$, ומכאן שהאיחוד הוא כל E. מצד שני, e אינה יכולה להשתייך ל-E_k עבור $k \neq j$: לפי ההגדרה, $e \in E_k$ מחייב ש-v_k הוא הקצה בעל האינדקס הגבוה של e, וקצה כזה יחיד. לכן הקבוצות זרות בזוגות, והשוויון בגדלים נובע מכלל החיבור. $\square$

(שימו לב ש-$E_1 = \emptyset$ תמיד, כי אין קודקוד עם אינדקס קטן מ-1.)

למה 1.2. לכל $1 \le j \le n$ מתקיים $|F \cap E_j| \ge \frac{1}{2}|E_j|$.

הוכחה. נתבונן ברגע שבו האלגוריתם מטפל ב-v_j. נסמן ב-p את מספר השכנים של v_j שכבר נמצאים ב-U וב-q את מספר השכנים שכבר נמצאים ב-$\bar{U}$. כל שכן של v_j בעל אינדקס $i < j$ כבר הוצב (האלגוריתם עובר על האינדקסים בסדר עולה), וכל שכן כזה מגדיר קשת של E_j; להפך, כל קשת של E_j מגיעה משכן כזה. לכן $|E_j| = p + q$.

יש שני מקרים, לפי תנאי שלב 2.1:

אם $p > q$, האלגוריתם מכניס את v_j ל-$\bar{U}$. אז כל אחת מ-p הקשתות אל השכנים שב-U הופכת לקשת חתך, ולכן $|F \cap E_j| \ge p$. מכיוון ש-$p > q$ מתקיים $|E_j| = p + q < 2p$, ובפרט $p \ge \frac{1}{2}|E_j|$.

אחרת $p \le q$, והאלגוריתם מכניס את v_j ל-U. אז כל אחת מ-q הקשתות אל השכנים שב-$\bar{U}$ הופכת לקשת חתך, ולכן $|F \cap E_j| \ge q$. מכיוון ש-$q \ge p$ מתקיים $|E_j| = p + q \le 2q$, כלומר $q \ge \frac{1}{2}|E_j|$.

> **הערה:** נקודה עדינה שמותר לפספס בקריאה ראשונה — למה מותר לכתוב "הופכת לקשת חתך" בזמן עתיד ולא לחשוש שהחלטה מאוחרת יותר תקלקל אותה? כי שני הקצוות של קשת ב-E_j כבר סופיים ברגע שבו v_j מוצב: קצה אחד הוא v_j עצמו, והשני הוצב קודם. האלגוריתם לעולם אינו מזיז קודקוד שכבר הוצב, ולכן החברות של קשת ב-F נקבעת סופית ברגע ההצבה של הקצה המאוחר יותר. זו בדיוק הסיבה שהפירוק מוגדר לפי האינדקס **הגבוה** ולא הנמוך. □

סיום ההוכחה. לפי למה 1.1 החתך F מתפרק לפי אותה חלוקה, ולפי למה 1.2: $|F| = \sum_{j=1}^{n} |F \cap E_j| \ge \frac{1}{2}\sum_{j=1}^{n} |E_j| = \frac{1}{2}|E|$.

מצד שני, כל חתך הוא תת-קבוצה של E, ובפרט האופטימלי: $|E| \le \mathrm{OPT}(G)$. לכן $|F| \ge \frac{1}{2}|E| \ge \frac{1}{2} \cdot \mathrm{OPT}(G)$, והאלגוריתם הוא אלגוריתם קירוב ל-MAXCUT ביחס קירוב $\frac{1}{2}$. ■

> **הערה:** גודל העזר כאן הוא $|E|$ — כמות שהאלגוריתם "שולט בה" במובן שהוא סופר אותה חלק-חלק (E_j אחרי E_j), והיא חוסמת את OPT **מלמעלה** כי הבעיה היא בעיית מקסימום. השוו לשיעור 13: שם, בבעיית המינימום VC, גודל העזר (הזיווג) חסם את OPT **מלמטה**. זהו אותו רעיון בשני הכיוונים.

משפט 2: אי-שוויון המשולש המוכלל

יהי $G = (V, E)$ גרף שלם עם משקלים $w : E \to \mathbb{R}^+$ המקיימים את אי-שוויון המשולש. אז לכל $v_1, \ldots, v_k \in V$ מתקיים $w(v_1, v_k) \le \sum_{j=1}^{k-1} w(v_j, v_{j+1})$.

הסיכום מציג את הטענה הזו כ"תזכורת" ואינו מוכיח אותה. היא הכלי היחיד שמאפשר את שלב "קיצורי הדרך" במשפט 3, ולכן נוכיח אותה.

> **הערה:** ההוכחה הבאה אינה מופיעה בסיכום; היא ההשלמה הסטנדרטית באינדוקציה.

הוכחה. באינדוקציה על $k \ge 2$.

בסיס, $k = 2$: הטענה היא $w(v_1, v_2) \le w(v_1, v_2)$ — נכון.

צעד: נניח שהטענה נכונה עבור $k-1$ ($k \geq 3$). לפי אי-שוויון המשולש (הגדרה 2) עם $x = v_1$, $y = v_{k-1}$, $z = v_k$: $w(v_1, v_k) \leq w(v_1, v_{k-1}) + w(v_{k-1}, v_k)$. לפי הנחת האינדוקציה על הסדרה $v_1, \ldots, v_{k-1}$: $w(v_1, v_{k-1}) \leq \sum_{j=1}^{k-2} w(v_j, v_{j+1})$. נחבר את שני האי-שוויונות: $w(v_1, v_k) \leq \sum_{j=1}^{k-2} w(v_j, v_{j+1}) + w(v_{k-1}, v_k) = \sum_{j=1}^{k-1} w(v_j, v_{j+1})$. ■

הערה טכנית: הקודקודים בסדרה אינם חייבים להיות שונים, וזה חיוני — במשפט 3 נפעיל את הטענה על סיור שחוזר לקודקודים. אם $v_j = v_{j+1}$ מפרשים $w(v_j, v_{j+1}) = 0$; זה רק מקטין את האגף הימני, כלומר מחזק את הטענה, והבסיס $k = 2$ נשאר נכון גם כאשר $v_1 = v_2$.

משפט 3: MST + DFS הוא אלגוריתם קירוב ביחס 2 לבעיית הסוכן הנוסע המטרית

האלגוריתם (כפי שהוא בסיכום). לכל קלט $G = (V, E)$, $w : E \to \mathbb{R}^+$:

מצא עץ פורש מינימלי T של G.

הרץ DFS על T.

החזר את הקודקודים לפי סדר גילוים ב-DFS.

טענת פיזביליות. DFS על עץ פורש מגלה כל קודקוד של V בדיוק פעם אחת, ולכן רשימת הגילוי היא תמורה של V. הגרף G שלם, ולכן כל שתי תמורות עוקבות מחוברות בקשת, וגם האחרון מחובר לראשון. לכן הרשימה מגדירה מעגל המילטוני — פתרון אפשרי לבעיה. □

ניתוח זמן ריצה. שלב 1 פולינומי (Prim/Kruskal). שלב 2 הוא $O(|V| + |E|)$, ולמעשה $O(|V|)$ כי T עץ ויש בו $|V| - 1$ קשתות. שלב 3 דורש רק את הפלט של השלב הקודם. סך הכול פולינומי בגודל הקלט. □

ניתוח יחס הקירוב. יהי $G = (V, E)$ עם $w : E \to \mathbb{R}^+$ המקיימת את אי-שוויון המשולש. נסמן ב-T עץ פורש מינימלי של G, וב-C_{opt} את המעגל ההמילטוני בעל המשקל האופטימלי (המינימלי) ב-G.

הבחנה 1 (כלשונה בסיכום). נסמן ב-$\hat{T}$ את הגרף המתקבל מ-C_{opt} על ידי הסרת קשת אחת כלשהי. אז $w(T) \leq w(\hat{T}) \leq w(C_{\text{opt}})$.

הוכחה. אי-השוויון הימני: $\hat{T}$ מתקבל מ-C_{opt} בהסרת קשת, ומשקל כל קשת אי-שלילי, ולכן ההסרה רק מקטינה את המשקל. אי-השוויון השמאלי: C_{opt} הוא מעגל העובר בכל קודקוד; הסרת קשת ממעגל משאירה **מסלול** העובר בכל הקודקודים, ומסלול כזה הוא בפרט עץ פורש של G (קשיר, פורש, ובעל $|V| - 1$ קשתות). מכיוון ש-T עץ פורש **מינימלי**, משקלו קטן או שווה למשקל של כל עץ פורש, ובפרט של $\hat{T}$. □

הבחנה 2. אם נרשום את הקודקודים לפי **סדר הביקורים** של ה-DFS על T — כלומר את הסיור הסגור המלא, שבו כל קשת של העץ נחצית פעמיים, פעם "ברדת" ופעם "בעלייה" — נקבל סיור P בגרף המקיים $w(P) = 2\,w(T)$.

הוכחה. DFS על עץ, המתחיל בשורש כלשהו r ומסתיים בחזרה ל-r, חוצה כל קשת של העץ בדיוק פעמיים: פעם אחת בכיוון מהאב אל הבן ברגע גילוי הבן, ופעם אחת בכיוון ההפוך ברגע שהתת-עץ של הבן הסתיים. מכיוון שאלה כל צעדי הסיור, המשקל הכולל הוא $\sum_{e \in T} 2w(e) = 2w(T)$. □

הערה: הסיכום כותב את שלב 3 של האלגוריתם כ"סדר הגילוי" ואת הבחנה 2 כ"סדר הביקורים". אלה שני עצמים שונים ואסור לבלבל ביניהם: **סדר הביקורים** הוא הסיור P באורך $2(|V|-1)$ צעדים, שבו קודקוד יכול להופיע כמה פעמים; **סדר הגילוי** (preorder) הוא רשימת ההופעות **הראשונות** בלבד, שבה כל קודקוד מופיע בדיוק פעם אחת. P אינו פתרון אפשרי לבעיה (הוא חוזר לקודקודים) — הוא רק גודל עזר.

הבחנה 3 (קיצורי הדרך). נסמן ב-C את המעגל המתקבל מרשימת הקודקודים לפי סדר הגילוי — כלומר, מוחקים מ-P את כל ההופעות החוזרות ומשאירים רק את ההופעה הראשונה של כל קודקוד. אז $w(C) \le w(P)$.

הוכחה. נסמן את סדר הגילוי $u_1 = r, u_2, \dots, u_n$, ואת הסיור P כרשימת קודקודים $p_0 = r, p_1, \dots, p_{2(n-1)} = r$. לכל t, נסמן ב-$\pi(t)$ את המיקום ב-P שבו u_t מופיע לראשונה. לפי הגדרת סדר הגילוי, $\pi(1) < \pi(2) < \cdots < \pi(n)$.

המעגל C מורכב מ-n קשתות: $u_1u_2, u_2u_3, \dots, u_{n-1}u_n$, ולבסוף u_nu_1. לכל $1 \le t \le n-1$, הקטע של P בין המיקום $\pi(t)$ למיקום $\pi(t+1)$ הוא סדרת קודקודים המתחילה ב-u_t ומסתיימת ב-u_{t+1}; לפי משפט 2, $w(u_t, u_{t+1}) \le \sum_{s=\pi(t)}^{\pi(t+1)-1} w(p_s, p_{s+1})$. באופן דומה, עבור הקשת הסוגרת u_nu_1: הקטע של P מהמיקום $\pi(n)$ ועד סוף הסיור מתחיל ב-u_n ומסתיים ב-$p_{2(n-1)} = r = u_1$, ולכן $w(u_n, u_1) \le \sum_{s=\pi(n)}^{2(n-1)-1} w(p_s, p_{s+1})$. הקטעים $[\pi(1), \pi(2)], [\pi(2), \pi(3)], \dots, [\pi(n), 2(n-1)]$ הם רצופים, זרים בצעדיהם, ומכסים את כל הסיור מהמיקום $\pi(1) = 0$ ועד סופו. לכן סכום האגפים הימניים הוא בדיוק $w(P)$, וסכום האגפים השמאליים הוא בדיוק $w(C)$. $\square$

הערה: בסיכום הבחנה 3 מקוצרת ל"אז מאי-שוויון המשולש $w(C) \le w(P)$". הפירוט שלמעלה הוא מה שהקיצור הזה מייצג. הנקודה הלא-טריוויאלית היא שהקטעים **זרים ומכסים** — בלי זה היינו סופרים צעדים של P יותר מפעם אחת ומקבלים חסם חלש יותר.

סיום ההוכחה. נשרשר את שלוש ההבחנות: $C\,w(C) \overset{(3)}{\le} w(P) \overset{(2)}{=} 2\,w(T) \overset{(1)}{\le} 2\,w(C_{\text{opt}})$. הוא בדיוק הפלט של האלגוריתם, והוא פתרון אפשרי; לכן האלגוריתם הוא אלגוריתם קירוב ביחס 2 לבעיית הסוכן הנוסע כשהמשקלים מקיימים את אי-שוויון המשולש. $\blacksquare$

הערה: אי-שוויון המשולש נחוץ **רק** בהבחנה 3. הבחנות 1 ו-2 נכונות בכל גרף ממושקל אי-שלילי. זו הסיבה שהאלגוריתם עצמו ניתן להרצה על כל מופע TSP — אבל אין לו שום ערובת יחס בלי ההנחה, ולפי שיעור 13 גם לא יכולה להיות לו כזו אלא אם $\mathrm{P} = \mathrm{NP}$.

משפט 4: First-Fit הוא אלגוריתם קירוב ביחס 2 לבעיית האריזה למכלים

האלגוריתם (כפי שהוא בסיכום). לכל קלט $a_1, \dots, a_n$:

לכל $1 \le j \le n$:

הכנס את a_j לקבוצה **הראשונה** שניתן להכניס אליה את a_j; אם אין כזו — פתח קבוצה חדשה.

החזר את החלוקה.

טענת פיזביליות. האלגוריתם מכניס כל a_j לקבוצה אחת בדיוק, ולכן הפלט הוא חלוקה של $\{a_1, \dots, a_n\}$ לקבוצות זרות. פריט מוכנס לקבוצה קיימת רק אם הסכום שלה נשאר ≤ 1, ואם נפתחת קבוצה חדשה — סכומה הוא $a_j \le 1$ (כאן נדרש התנאי $a_j \in (0, 1]$ מהגדרה 4). לכן כל הקבוצות חוקיות והפלט הוא פתרון אפשרי. $\square$

ניתוח זמן ריצה. באיטרציה j יש לכל היותר $j - 1 \le n$ קבוצות פתוחות, וסריקתן לפי הסדר עולה $O(n)$ (החזקת הסכום הנוכחי של כל קבוצה מאפשרת בדיקה ב-$O(1)$ לקבוצה). לכן זמן הריצה הוא $O(n^2)$, פולינומי בגודל הקלט. $\square$

ניתוח יחס הקירוב. יהיו $a_1, \dots, a_n \in (0, 1]$. נסמן ב-$m$ את מספר הקבוצות שהחזיר האלגוריתם וב-$f : [n] \to [m]$ את החלוקה שהוא מחזיר. נסמן ב-m_{opt} את מספר הקבוצות המינימלי האפשרי לקלט הזה, וב-$f_{\mathrm{opt}} : [n] \to [m_{\mathrm{opt}}]$ חלוקה אופטימלית.

למה 4.1 (חסם תחתון על האופטימום). $\displaystyle\sum_{i=1}^{n} a_i \;\le\; m_{\mathrm{opt}}$.

הוכחה. נחלק את הסכום לפי הקבוצות של החלוקה האופטימלית — זו חלוקה של קבוצת האינדקסים, ולכן החלוקה חוקית: $\sum_{i=1}^{n} a_i \;=\; \sum_{j=1}^{m_{\mathrm{opt}}} \sum_{i:\, f_{\mathrm{opt}}(i) = j} a_i \;\le\; \sum_{j=1}^{m_{\mathrm{opt}}} 1 \;=\; m_{\mathrm{opt}}$, כאשר אי-השוויון האמצעי הוא בדיוק אילוץ הפיזביליות: הסכום הפנימי הוא סכום האיברים שנכנסו לקבוצה j בחלוקה האופטימלית, והוא חסום על ידי 1. $\square$

זהו גודל העזר של המשפט: $\sum a_i$ הוא מספר שהאלגוריתם "רואה" ישירות, והוא חוסם את OPT **מלמטה** — כנדרש בבעיית מינימיזציה.

למה 4.2 (ההבחנה המרכזית). בחלוקה שמחזיר האלגוריתם יש לכל היותר **קבוצה אחת** שסכום האיברים בה הוא $\le \frac{1}{2}$.

הוכחה. נניח בשלילה שקיימים $1 \le \ell < j \le m$ כך שגם בקבוצה ה-ℓ וגם בקבוצה ה-j סכום האיברים (בסוף הריצה) אינו יותר מ-$\frac{1}{2}$.

הקבוצה ה-j נפתחה בשלב כלשהו של הריצה; נסמן ב-i_0 את האינדקס של הפריט שבעטיו היא נפתחה, כלומר a_{i_0} הוא הפריט הראשון שהוכנס אליה. מכיוון שסכום כל איברי הקבוצה ה-j בסוף הריצה הוא $\le \frac{1}{2}$, וכל האיברים חיוביים, בפרט $a_{i_0} \;\le\; \frac{1}{2}$.

כעת נתבונן ברגע שבו האלגוריתם טיפל ב-a_{i_0}, ונסמן ב-S_ℓ את סכום האיברים שהיו בקבוצה ה-ℓ באותו רגע. מכיוון ש-$\ell < j$, הקבוצה ה-ℓ כבר הייתה פתוחה (הקבוצות נפתחות לפי הסדר), והאלגוריתם בדק אותה **לפני** שפתח קבוצה חדשה. מכיוון שהאלגוריתם לעולם אינו מוציא איבר מקבוצה, S_ℓ קטן או שווה לסכום הסופי של אותה קבוצה, כלומר $S_\ell \le \frac{1}{2}$. לכן $S_\ell + a_{i_0} \;\le\; \frac{1}{2} + \frac{1}{2} \;=\; 1$, כלומר a_{i_0} **כן** היה נכנס לקבוצה ה-ℓ, והאלגוריתם היה מכניס אותו אליה במקום לפתוח קבוצה חדשה — בסתירה להנחה ש-a_{i_0} פתח את הקבוצה ה-j. $\square$

> **הערה:** בעמוד 4 בסיכום שורת "סכום האיברים בקבוצה ה-ℓ באותו הרגע" נקראת בקושי וסימן אי-השוויון אינו חד-משמעי. הכיוון היחיד שנותן סתירה הוא $\le \frac{1}{2}$ (כלומר: הקבוצה ה-ℓ הייתה ריקה מספיק כדי לקלוט את a_{i_0}), וכך נכתב כאן. הכיוון ההפוך היה סותר את הנחת השלילה עצמה ומייתר את הטיעון.

סיום ההוכחה. לפי למה 4.2, לפחות $m-1$ מהקבוצות שהחזיר האלגוריתם הן בעלות סכום **גדול ממש** מ-$\frac{1}{2}$. לכן, בשילוב עם למה 4.1: $m_{\text{opt}} \geq \sum_{i=1}^{n} a_i = \sum_{j=1}^{m} \sum_{i:\, f(i)=j} a_i > \frac{1}{2}(m-1)$. (אי-השוויון האחרון חזק ממש: לפחות $m-1$ מהמחוברים גדולים ממש מ-$\frac{1}{2}$, והנותר אי-שלילי. גם במקרה $m=1$ הוא נכון, כי $\sum a_i > 0 = \frac{1}{2}\cdot 0$.)
מכאן $2m_{\text{opt}} > m-1$, כלומר $m < 2m_{\text{opt}}+1$. וכיוון שמדובר במספרים שלמים, נקבל $m \leq 2m_{\text{opt}}$. לכן First-Fit הוא אלגוריתם קירוב ביחס 2 לבעיית האריזה למכלים. $\blacksquare$

> **הערה:** הצעד האחרון הוא הצעד היחיד בשיעור שמשתמש בשלמות. בלעדיו היינו נשארים עם החסם החלש יותר $m \leq 2m_{\text{opt}}+1$, שהוא "קירוב ביחס 2 עד כדי תוספת קבועה" ולא קירוב ביחס 2. שווה לזכור את התרגיל הזה — הוא חוזר.

> **הערה (מחוץ לסיכום):** ההוכחה מראה שהיחס של First-Fit הוא לכל היותר 2; היא אינה טוענת שהחסם הדוק. ידוע שהניתוח האסימפטוטי המדויק של First-Fit טוב יותר, וגם ידוע שלבעיית האריזה אין אלגוריתם קירוב ביחס טוב מ-$\frac{3}{2}$ אלא אם $\mathrm{P}=\mathrm{NP}$ (רדוקציה מ-$\mathrm{PARTITION}$: קירוב טוב מ-$\frac{3}{2}$ היה מבחין בין $m_{\text{opt}}=2$ ל-$m_{\text{opt}}=3$). שני הדברים האלה **אינם** בסיכום ואינם נדרשים למבחן; הם מובאים כאן רק כדי שלא תסיקו מהמשפט שהאלגוריתם "גרוע פי 2" בפועל.

דוגמאות ותרגילים מהשיעור

הסיכום עצמו אינו כולל דוגמאות מספריות. הדוגמאות הבאות הן מעקב מלא אחרי כל אחד משלושת האלגוריתמים, והן חובה כדי לוודא שהבנתם את הסדר שבו כל אחד מהם מקבל החלטות.

> **הערה:** כל הדוגמאות בסעיף זה נבנו כאן, לא בשיעור. הן מכוונות בדיוק לנקודות שההוכחות נשענות עליהן.

דוגמה 1: האלגוריתם החמדני ל-MAXCUT על מעגל באורך 5

יהי C_5 עם $V=\{v_1,\dots,v_5\}$ וקשתות $v_1v_2,\ v_2v_3,\ v_3v_4,\ v_4v_5,\ v_5v_1$. הפירוק לפי האינדקס הגבוה: $E_1=\emptyset,\quad E_2=\{v_1v_2\},\quad E_3=\{v_2v_3\},\quad E_4=\{v_3v_4\},\quad E_5=\{v_4v_5,\ v_5v_1\}$.

מעקב אחר הריצה (p = שכנים ב-U, q = שכנים ב-$\bar{U}$, בזמן הטיפול):

i	**שכנים שכבר הוצבו**	p	q	$p>q$**?**	**היעד**	U	$\bar{U}$
1	—	0	0	לא	U	$\{v_1\}$	$\emptyset$
2	$v_1\in U$	1	0	כן	$\bar{U}$	$\{v_1\}$	$\{v_2\}$
3	$v_2\in\bar{U}$	0	1	לא	U	$\{v_1,v_3\}$	$\{v_2\}$

i	שכנים שכבר הוצבו	p	q	$p > q$?	היעד	U	$\bar{U}$
4	$v_3 \in U$	1	0	כן	$\bar{U}$	$\{v_1, v_3\}$	$\{v_2, v_4\}$
5	$v_4 \in \bar{U},\ v_1 \in U$	1	1	לא	U	$\{v_1, v_3, v_5\}$	$\{v_2, v_4\}$

הפלט: $U = \{v_1, v_3, v_5\}$. החתך המושרה הוא $F = \{v_1v_2,\ v_2v_3,\ v_3v_4,\ v_4v_5\}$, כלומר $|F| = 4$ (הקשת v_5v_1 אינה בחתך, כי שני קצותיה ב-U).

בדיקת הלמות: $|E| = \sum_j |E_j| = 0 + 1 + 1 + 1 + 2 = 5$ ✓. לכל j: $|F \cap E_2| = 1 \geq \frac{1}{2}$, $|F \cap E_3| = 1 \geq \frac{1}{2}$, $|F \cap E_4| = 1 \geq \frac{1}{2}$, ו-$|F \cap E_5| = 1 \geq \frac{1}{2} \cdot 2 = 1$ ✓ — כאן הלמה **הדוקה**, וזה בדיוק המקרה $p = q$ בצעד 5. סך הכול $|F| = 4 \geq \frac{1}{2} \cdot 5 = 2.5$ ✓.

מהו האופטימום? ב-C_5 (מעגל אי-זוגי) אי אפשר לחתוך את כל 5 הקשתות, כי חתך של גרף לא-דו-צדדי אינו יכול להכיל את כל הקשתות; לכן $\mathrm{OPT} = 4$, והאלגוריתם החזיר את האופטימום.

תרגיל. הריצו את אותו אלגוריתם על K_3 עם הסדר v_1, v_2, v_3. *פתרון.* $v_1 \to U$; v_2: $p = 1, q = 0 \Rightarrow \bar{U}$; v_3: $p = 1$ (בגלל v_1), $q = 1$ (בגלל v_2), לא $p > q$, ולכן $v_3 \to U$. מתקבל $U = \{v_1, v_3\}$, $F = \{v_1v_2, v_2v_3\}$, $|F| = 2$. גם כאן $\mathrm{OPT} = 2$ והבטחת הקירוב $2 \geq \frac{1}{2} \cdot 3$ מתקיימת בהפרש גדול.

דוגמה 2: DFS + MST על מלבן

$V = \{a, b, c, d\}$ בנקודות $a = (0,0)$, $b = (0,3)$, $c = (4,0)$, $d = (4,3)$ עם מרחקים אוקלידיים — ולכן המשקלים מטריים: $w(ac) = 4,\quad w(bd) = 4,\quad w(ad) = 5,\quad w(bc) = 5.$ $w(ab) = 3,\quad w(cd) = 3,$

שלב 1 — עץ פורש מינימלי. Kruskal לפי סדר עולה: $ab\,(3)$ ✓, $cd\,(3)$ ✓, $ac\,(4)$ ✓ (מחבר את שני הרכיבים), ואז עוצרים עם 3 קשתות. לכן $T = \{ab,\ cd,\ ac\}$ ו-$w(T) = 10$.

שלב 2 — DFS. נתחיל ב-a; שכניו ב-T הם b ו-c. נניח שמבקרים ב-b ראשון. סדר הביקורים המלא (הסיור P): $a \to b \to a \to c \to d \to c \to a$, ומשקלו $3 + 3 + 4 + 3 + 3 + 4 = 20 = 2w(T)$ ✓ (הבחנה 2).

שלב 3 — סדר הגילוי. ההופעות הראשונות: $a,\ b,\ c,\ d$. המעגל המוחזר: $C = a \to b \to c \to d \to a$, $w(C) = 3 + 5 + 3 + 5 = 16.$ בדיקה: $w(C) = 16 \leq w(P) = 20$ ✓

(קיצור הדרך $b \to c$ החליף את הקטע $b \to a \to c$ שמשקלו $3 + 4 = 7$, במחיר 5).

האופטימום. המעגל $a \to b \to d \to c \to a$ במשקל $4 + 3 + 4 + 3 = 14$ הוא המינימלי. אכן $16 \leq 2 \cdot 14 = 28$ ✓, ובפועל היחס הוא $16/14 \approx 1.14$ — הרבה יותר טוב מהערובה.

בדיקת הבחנה 1: הסרת הקשת ca מ-C_{opt} נותנת את המסלול $a - b - d - c$ במשקל 10, ואכן $w(T) = 10 \leq w(\hat{T}) = 10 \leq w(C_{\mathrm{opt}}) = 14$ ✓.

תרגיל: כמה חשוב סדר ה-DFS? הריצו שוב עם ביקור ב-c לפני b. *פתרון.* סדר הגילוי הוא a, c, d, b, והמעגל המוחזר הוא $a \to c \to d \to b \to a$ במשקל $4 + 3 + 4 + 3 = 14$ — בדיוק האופטימום. **מסקנה:** האלגוריתם אינו דטרמיניסטי ביחס לסדר הסריקה, וההוכחה מבטיחה את היחס 2 עבור **כל** סדר. אין צורך לבחור סדר "נכון".

דוגמה 3: First-Fit על ארבעה פריטים

יהי הקלט $a = (0.4,\ 0.7,\ 0.3,\ 0.6)$.

j	a_j	קבוצות פתוחות (סכומים)	ההחלטה	אחרי
1	0.4	—	אין קבוצה, פותח קבוצה 1	(0.4)
2	0.7	(0.4)	$0.4 + 0.7 = 1.1 > 1$, פותח קבוצה 2	$(0.4),\ (0.7)$
3	0.3	$(0.4),\ (0.7)$	$0.4 + 0.3 = 0.7 \le 1$ ✓ לקבוצה 1	$(0.7),\ (0.7)$
4	0.6	$(0.7),\ (0.7)$	$0.7 + 0.6 > 1$ בשתיהן, פותח קבוצה 3	$(0.7),\ (0.7),\ (0.6)$

הפלט: $m = 3$ קבוצות — $\{0.6\},\ \{0.7\},\ \{0.4, 0.3\}$.

האופטימום. $\{0.4, 0.6\}$ (סכום 1.0) ו-$\{0.7, 0.3\}$ (סכום 1.0) — לכן $m_{\text{opt}} = 2$, וזהו מינימום כי $\sum a_i = 2.0 > 1$ מחייב לפחות שתי קבוצות.

בדיקת ההוכחה על הדוגמה. סכומי הקבוצות של האלגוריתם הם $0.6,\ 0.7,\ 0.7$ — כולם $> \frac{1}{2}$, ולכן ההבחנה של למה 4.2 ("לכל היותר קבוצה אחת עם סכום $\le \frac{1}{2}$") מתקיימת בשופי. השרשרת: $m = 3 < 2 \cdot 2 + 1 = 5$, כלומר $m \le 4$ — נכון, אם כי כאן רופף. היחס בפועל הוא $3/2$.

תרגיל: מתי בכל זאת נוצרת קבוצה "קלה"? *פתרון.* קחו $a = (0.6,\ 0.7,\ 0.4)$. First-Fit מחזיר $\{0.4\}, \{0.7\}, \{0.6\}$, והקבוצה השלישית בעלת סכום $0.4 \le \frac{1}{2}$ — והיא **היחידה** כזו, וגם האחרונה שנפתחה. זה לא במקרה: הטיעון של למה 4.2 מראה שקבוצה "קלה" אינה יכולה להיפתח כאשר כבר קיימת קבוצה "קלה" לפניה.

הערות מהשיעור

אין הקלטה לשיעור הזה בקורפוס (ראו את הסעיף הבא לפירוט מלא), ולכן אין ולא יכולות להיות כאן חותמות זמן, ציטוטים מהמרצה או שאלות סטודנטים. הסעיף הזה מכיל את מה שהסיכום הכתוב עצמו מדגיש — ההערות שגיא סופר רשם בשוליים ובצבע — ואת ההצלבות בין השיעור הזה לקודמיו.

ההערה הכחולה בעמוד 1: ליד הגדרת E_j רשום "E_j קבוצת הקשתות ש-v_j יקבע את גורלן". זו לא הערת נוי — היא ההסבר למה הפירוק **חייב** להיות לפי האינדקס הגבוה. אם היינו מפרקים לפי האינדקס הנמוך, כשהאלגוריתם היה מטפל ב-v_j עוד לא היה ידוע לאן ילכו הקצוות השניים, ואי אפשר היה להסיק דבר.

ההערה הכחולה בעמוד 2: ליד הגדרת בעיית הסוכן הנוסע רשום במפורש "לכל $x, y, z \in V$: $w(xz) \le w(xy) + w(yz)$" — כלומר, אי-שוויון המשולש הוא **חלק מהגדרת הקלט**, לא הנחה נוספת שנוסיף בניתוח. מופע שאינו מקיים אותו אינו קלט חוקי לבעיה הזו.

ההערות הכחולות בעמוד 3: מתחת לשרשרת $w(T) \le w(\hat{T}) \le w(C_{\text{opt}})$ רשומות שתי ההצדקות בנפרד — "כי T מינימלי" ו"כי w אי-שלילי". זכרו ששניהם נדרשים; רבים כותבים במבחן רק את הראשון.

ההערה הכחולה בעמוד 3, בבעיית האריזה: מתחת לסכום הפנימי רשום "סכום האיברים שנכנסו לקבוצה j" עם החסם 1 — כלומר הפיזביליות של האופטימום היא שנותנת את למה 4.1.

הצלבה עם שיעור 13 — הנקודה שהכי כדאי להבין מהשיעור: בשיעור 13 הוכח שקירוב ביחס קבוע ל-TSP הכללית שקול ל-$\mathrm{P} = \mathrm{NP}$, וכאן מתקבל קירוב ביחס 2. אלה אינם סותרים, כי המופעים שהרדוקציה של שיעור 13 בונה (משקל 1 לקשתות המקוריות ו-$\alpha|V| + 1$ לשאר) **מפרים** את אי-שוויון המשולש בגסות. הנחת המטריות אינה קוסמטית — היא בדיוק מה שמפרק את בניית הקושי.

הצלבה עם שיעור 13 — שני קירובים ½ ל-MAXCUT: חיפוש מקומי (שיעור 13) ואלגוריתם חמדני חד-מעברי (כאן). שניהם נותנים $|F| \ge \frac{1}{2}|E|$, אבל בדרכים שונות: החיפוש המקומי משתמש בתנאי אופטימליות מקומית וספירה כפולה על **הקודקודים**, והחמדן משתמש בפירוק ל-E_j וספירה על **הקשתות**. במבחן שאלה יכולה לבקש כל אחד מהם בשמו; שימו לב מה בדיוק נשאלתם.

פערים בין הסיכום להקלטה

לשיעור הזה אין הקלטה בקורפוס — זו העובדה החשובה ביותר בקובץ הזה, והיא נבדקה ולא הונחה.

מקור: תמלול 19 (המפגש הקודם). **הפער:** התמלול נגמר ב-$[01{:}26{:}00]$ בדיוק בסוף עמוד 5 של הסיכום של **שיעור 13** — על שקילות TSP ל-$\mathrm{P} = \mathrm{NP}$ — וחותם ב"שאלות?". הוא אינו גולש אל החומר של שיעור 14. **ההכרעה:** אינו נרשם כמקור.

מקור: תמלול 20 (המפגש הבא). **הפער:** התמלול הוא כולו אלגוריתמים אקראיים — בעיית המזכיר ואימות כפל מטריצות — ואינו נוגע באלגוריתמי קירוב מלבד אמירה צופה פני עתיד ב-$[00{:}34{:}34]$ ("נשלב אלגוריתמים אקראיים עם אלגוריתמי קירוב"). **ההכרעה:** אינו נרשם כמקור.

מקור: הקורפוס בכללותו. **הפער:** קיים פער אמיתי בהקלטות בין שני המפגשים הללו, כלומר המפגש שהסיכום הזה מתעד מעולם לא הוקלט. **ההכרעה:** `sources.transcripts` נשאר רשימה ריקה, `confidence` נקבע ל- `medium` , וכל תוכן הקובץ נשען על ארבעת עמודי הסיכום בתוספת השלמה מתמטית סטנדרטית — המסומנת לאורך כל הקובץ ב- `**הערה:**` .

מה בדיוק מגיע מהסיכום, ומה הושלם כאן.

מקור: עמודים 1–4 בסיכום. **הפער:** — . **ההכרעה:** מהסיכום, מילה במילה מבחינת התוכן: שלושת האלגוריתמים (החמדני ל-MAXCUT, First-Fit, MST+DFS) על כל שלביהם; הגדרת E_j וההערה הכחולה עליה; טענות $\bigcup E_j = E$, הזרות, ו-$|E| = \sum |E_j|$; אי-השוויון $|F \cap E_j| \geq \frac{1}{2}|E_j|$; ניתוח זמן הריצה $O(|V| \cdot |E|)$; ניסוח אי-שוויון המשולש והצורה המוכללת שלו; הבחנה 1 עם שתי ההצדקות; $w(P) = 2w(T)$; $w(C) \leq w(P) = 2w(T) \leq 2w(C_{\mathrm{opt}})$; הגדרת בעיית האריזה; למה 4.1 על שרשרת הסכומים; למה 4.2 והוכחתה בשלילה; והמעבר $m < 2m_{\mathrm{opt}} + 1 \Rightarrow m \leq 2m_{\mathrm{opt}}$.

מקור: הסיכום מציג את אי-השוויון המוכלל כ"תזכורת" בלי הוכחה. **הפער:** אין הוכחה. **ההכרעה:** נוספה הוכחה באינדוקציה (משפט 2) המסומנת כהשלמה, כולל הטיפול במקרה $v_j = v_{j+1}$ הנדרש לשימוש בסיור.

מקור: הסיכום כותב "אז מאי-שוויון המשולש $w(C) \leq w(P)$". **הפער:** המעבר מקוצר ואינו מסביר למה קטעי הסיור זרים ומכסים. **ההכרעה:** הבחנה 3 כתובה כאן במלואה עם מיפוי ההופעות הראשונות $\pi(t)$ וטיעון הכיסוי; מסומן כהשלמה.

מקור: עמוד 4 בסיכום, בשורה על סכום הקבוצה ה-ℓ "באותו הרגע". **הפער:** סימן אי-השוויון אינו קריא באופן חד-משמעי. **ההכרעה:** נכתב $\leq \frac{1}{2}$, שכן זהו הכיוון היחיד שמייצר את הסתירה; צוין ב-`open_questions`.

מקור: הסיכום, ניתוח זמן הריצה של האלגוריתם החמדני. **הפער:** $O(|V| \cdot |E|)$ הוא חסם נכון אך רופף. **ההכרעה:** נשמר כלשונו כניתוח "של השיעור", ונוסף חסם הדוק $O(|V| + |E|)$ בהערה מסומנת — בלי לתקן את הסיכום, כי הוא אינו שגוי.

מקור: הסיכום אינו מגדיר מחדש "יחס קירוב" לבעיית מקסימום. **הפער:** ההגדרה ניתנה בשיעור 13 לבעיית מינימיזציה בלבד. **ההכרעה:** ההגדרה למקסימיזציה ($\alpha \leq 1$, $v(A(I)) \geq \alpha \, \mathrm{OPT}$) שוחזרה בסעיף הרקע והותאמה לניסוח "ביחס קירוב $\frac{1}{2}$" שבעמוד 2.

מקור: הסיכום. **הפער:** אין בסיכום אף דוגמה מספרית, אף מופע מפורט ואף תרגיל. **ההכרעה:** סעיף הדוגמאות כולו נבנה כאן ומסומן ככזה בראשו; כל מופע נבחר כדי לבדוק נקודה ספציפית בהוכחה (הידוק למה 1.2, השפעת סדר ה-DFS, ומקרה שבו First-Fit מפסיד לאופטימום).

מקור: מחוץ לשני המקורות. **הפער:** אין בסיכום דיון בהידוק היחס. **ההכרעה:** נוספה הערה קצרה ומסומנת שמציינת שהיחס 2 אינו נטען כהדוק ושידועה גם תוצאת אי-קירוב $\frac{3}{2}$ לבעיית האריזה; מודגש שם שזה מחוץ לחומר.

מקור: קונבנציות הכתיבה של הסדרה. **הפער:** — . **ההכרעה:** שמות בעיות ומחלקות נכתבים ב-MAXCUT, TSP, P, NP), ואילו שמות המשתנים והאינדקסים ($U, \bar{U}, E_j, F, T, \hat{T}, P, C, C_{\mathrm{opt}}, m, m_{\mathrm{opt}}, f, f_{\mathrm{opt}}, a_i$) נשמרו בדיוק כפי שהם בסיכום.

סיכום ונקודות למבחן

שלוש התוצאות שיש לזכור.

בעיה	סוג	אלגוריתם	יחס	גודל העזר
MAXCUT	מקסימום	חמדני חד-מעברי: כל קודקוד לצד עם פחות שכנים שהוצבו	$\frac{1}{2}$	$\|E\| \geq \mathrm{OPT}$
TSP מטרי	מינימום	MST, ואז DFS, ואז סדר הגילוי	2	$w(T) \leq w(C_{\mathrm{opt}})$
אריזה למכלים	מינימום	First-Fit	2	$\sum a_i \leq m_{\mathrm{opt}}$

המבנה הקבוע של תשובה מלאה. לכל שאלה מהסוג הזה, כתבו שלושה סעיפים נפרדים ומסומנים: (1) **פיזביליות** — למה הפלט הוא פתרון חוקי לבעיה; (2) **זמן ריצה** — למה פולינומי, עם ספירה; (3) **יחס** — הצד הטריוויאלי, ואז החסם האמיתי דרך גודל העזר. ניתוח שמדלג על (1) אינו שלם גם אם (3) מושלם.

מלכודות סטנדרטיות.

כיוון האי-שוויון. בבעיית מקסימום $\alpha \leq 1$ ומוכיחים $\mathrm{ALG} \geq \alpha \cdot \mathrm{OPT}$; בבעיית מינימום $\alpha \geq 1$ ומוכיחים $\mathrm{ALG} \leq \alpha \cdot \mathrm{OPT}$. חצי מהשגיאות בשאלות קירוב הן היפוך הכיוון.

חסימת OPT מהצד הלא נכון. בבעיית מקסימום צריך חסם **עליון** על OPT (כאן $|E|$); בבעיית מינימום חסם **תחתון** (כאן $w(T)$ ו-$\sum a_i$).

סדר הגילוי מול סדר הביקורים. P (הסיור, כל קשת פעמיים) הוא גודל עזר בלבד ואינו פתרון אפשרי; C (סדר הגילוי) הוא הפלט. אל תחזירו את P.

שכחת אי-שוויון המשולש. בלעדיו אין שום ערובה על $w(C)$ מול $w(P)$, ולפי שיעור 13 גם לא יכולה להיות. אם בשאלה לא נאמר שהמשקלים מטריים — אל תשתמשו במשפט 3.

הפירוק לפי האינדקס הגבוה. לפי הנמוך ההוכחה נשברת. אם התבקשתם להוכיח את למה 1.2, אמרו במפורש למה שני הקצוות של קשת ב-E_j סופיים ברגע ההצבה של v_j.

שלמות ואי-שוויון חזק ממש. $m < 2m_{\mathrm{opt}} + 1$ גורר $m \leq 2m_{\mathrm{opt}}$ רק כי m שלם — אמרו את זה. ובאותה נשימה: אם תכתבו $\sum a_i \geq \frac{1}{2}(m-1)$ במקום $>$, תקבלו רק $m \leq 2m_{\mathrm{opt}} + 1$ ותפסידו את המשפט.

צ׳ק-ליסט אחרי השיעור. אחרי השיעור הזה צריך לדעת: לרוץ ידנית על שלושת האלגוריתמים על מופע קטן; להוכיח את שלוש הלמות המרכזיות (הפירוק ל-E_j; $w(T) \leq w(C_{\mathrm{opt}})$; "לכל היותר תא אחד עם סכום $\leq \frac{1}{2}$"); להסביר במשפט אחד למה משפט 3 אינו סותר את תוצאת האי-קירוב של שיעור 13; ולזהות, בשאלה חדשה, מהו גודל העזר שיחסום את OPT מהצד הנכון.

שאלות שנשארו פתוחות

לשיעור הזה אין הקלטה בקורפוס: תמלול 19 נגמר בסוף עמוד 5 של הסיכום של שיעור 13, ותמלול 20 הוא כולו אלגוריתמים אקראיים. כל הקובץ נשען על ארבעת עמודי הסיכום בלבד.

אין חותמות זמן בשום מקום בקובץ, ולכן אי אפשר לצטט הערות מרצה, שאלות סטודנטים או מוטיבציה שנאמרה בעל פה.

הסיכום אינו מגדיר במפורש את יחס הקירוב לבעיית מקסימום; ההגדרה כאן שוחזרה משיעור 13 והותאמה לניסוח "ביחס קירוב ½" שבעמוד 2.

עמוד 4 בסיכום: בשורת "סך האיברים בתא ה-ℓ באותו הרגע" סימן אי-השוויון נקרא בקושי; ההקשר מחייב ≥ ½ (אחרת אין סתירה), וכך נכתב כאן.

עמוד 2 בסיכום: ניסוח המטרה של בעיית הסוכן הנוסע נקרא כ"מעגל המילטוני במשקל מינימלי"; מילת התואר המדויקת בכתב היד אינה חד-משמעית.

הסיכום כותב את ניתוח זמן הריצה של האלגוריתם החמדני כ-O(|V|·|E|); זהו חסם נכון אך רופף, והחסם ההדוק O(|V|+|E|) נוסף כאן כהערה.

15 אלגוריתמים אקראיים: מבוא, בעיית המזכיר ואלגוריתם Freivalds

השיעור מציג את הרעיון של אלגוריתם שמטיל מטבעות — כאשר ההסתברות נלקחת אך ורק על המטבעות הפנימיים של האלגוריתם והקלט נשאר שרירותי ובמקרה הגרוע — ומדגים אותו בשני אלגוריתמים המנותחים עד הסוף: אלגוריתם לבעיית המזכיר שמצליח בהסתברות $\ge \tfrac14$ שם ששום אלגוריתם דטרמיניסטי אינו מבטיח דבר, ואלגוריתם Freivalds לווידוא כפל מטריצות ב-$O(n^2)$ עם טעות חד-צדדית $\le \tfrac12$ שניתן להגבירה ל-2^{-t} ב-t חזרות בלתי תלויות.

ביטחון: high

בקצרה

אלגוריתם אקראי הוא אלגוריתם שרשאי, בנוסף לקלט, להטיל מטבעות הוגנים ובלתי תלויים ולהשתמש בתוצאתם. כל טענה הסתברותית בשיעור הזה נלקחת **אך ורק על המטבעות של האלגוריתם** — הקלט נשאר שרירותי, נבחר על ידי "אויב אכזר" שמכיר את קוד האלגוריתם אך לא את תוצאות ההטלות, והערובה נדרשת **לכל קלט**, לא לקלט אקראי. זו הנקודה שהכי קל להתבלבל בה, וזה הדבר היחיד שחייבים לקחת מהשיעור אם לוקחים ממנו דבר אחד.

בעיית המזכיר מדגימה מדוע אקראיות עוזרת בכלל: לכל אלגוריתם **דטרמיניסטי** קיים קלט שעליו הוא נכשל באופן קטסטרופלי, בעוד אלגוריתם אקראי פשוט מוצא את המועמד הטוב ביותר בהסתברות $\ge \frac{1}{4}$ **על כל קלט**.

אלגוריתם Freivalds לווידוא $A \cdot B = C$ רץ בזמן $O(n^2)$ במקום $O(n^3)$ ומחזיר תשובה נכונה בהסתברות $\ge \frac{1}{2}$; הטעות שלו היא **חד-צדדית** — הוא לעולם לא דוחה קלט נכון.

הגברה (amplification): t הרצות בלתי תלויות עם קבלה רק אם *כל* ההרצות קיבלו מורידות את הסתברות הטעות ל-$\le 2^{-t}$ במחיר זמן ריצה $O(t \cdot n^2)$. גורם **ליניארי** בזמן קונה ירידה **אקספוננציאלית** בשגיאה. עם $t = \log n$ מקבלים זמן $O(n^2 \log n)$ ושגיאה $\le 1/n$.

כל ההסתברויות בשיעור **מוכחות** בספירה קומבינטורית מפורשת על מרחב המדגם, ולא נטענות. מרחב המדגם הוא אוסף תוצאות הניסוי האקראי (כל התמורות; כל הווקטורים ב-$\{0,1\}^n$) — לא אוסף הפלטים האפשריים של האלגוריתם.

השיעור **אינו** מגדיר את המודל הפורמלי ואינו מגדיר מחלקות סיבוכיות אקראיות. מכונת טיורינג אקראית והמחלקות RP, coRP ו-BPP מוגדרות בשיעור הבא; שם גם ייאמר שבעיית וידוא כפל המטריצות שייכת ל-coRP.

הערה על היקף: המרצה אמר במפורש ([00:00:00]) שבעיית המזכיר **אינה חלק מחומר המבחן** והיא מוצגת בשביל העקרונות; אלגוריתם Freivalds וההגברה **כן** חלק מהחומר ([00:29:45]).

רקע ותלויות

מהיכן הגענו לכאן. שיעורים 12–14 עסקו בהתמודדות עם קושי חישובי דרך אלגוריתמי קירוב: כאשר בעיה היא NP-hard, במקום לוותר על יעילות מוותרים על אופטימליות ומסתפקים בערובה על יחס הקירוב. השיעור הזה פותח כלי שני מאותה משפחה — ויתור על **ודאות** במקום ויתור על איכות. המרצה הדגיש ([00:00:00], [00:34:34]) ששני האלגוריתמים שיוצגו כאן אינם קשורים כלל לבעיות NP-קשות; שילוב האקראיות עם אלגוריתמי קירוב יגיע בהמשך.

הסתברות בדידה — כל מה שנשתמש בו. אלה הכלים היחידים הנדרשים, וכולם מהקורס המקדים: **מרחב מדגם** Ω הוא אוסף התוצאות האפשריות של ניסוי אקראי. **מאורע** הוא תת-קבוצה $E \subseteq \Omega$. אם הדגימה **אחידה** מ-Ω סופי, אז $\Pr[E] = \dfrac{|E|}{|\Omega|}$. כלומר חישוב הסתברות מתחת להתפלגות אחידה הוא בדיוק תרגיל בקומבינטוריקה ([00:27:02]).

מונוטוניות: אם $E \subseteq F$ אז $\Pr[E] \le \Pr[F]$. זהו הכלי שבו נחסום הסתברויות משני הכיוונים: פעם אחת כדי לחסום **מלמטה** הסתברות הצלחה (משפט 2), ופעם אחת כדי לחסום **מלמעלה** הסתברות כישלון (משפט 3).

אי-תלות: מאורעות $E_1, \dots, E_t$ בלתי תלויים אם $\Pr\left[\bigcap_{i} E_i\right] = \prod_{i} \Pr[E_i]$. אצלנו אי-התלות לעולם אינה מונחת — היא **נבנית** בכך שכל הרצה משתמשת בהטלות מטבע טריות.

ספירה: מספר התמורות של $[n]$ הוא $n!$; מספר הווקטורים ב-$\{0,1\}^n$ הוא 2^n.

המרצה ביקש במפורש ([00:31:20], [01:21:06]) לחזור לקראת השיעור הבא על **תוחלת**, **ליניאריות התוחלת** ו**פירוק לאינדיקטורים**. בשיעור הזה תוחלת מופיעה רק בהערה אחת קצרה (מסקנה 2.1).

אלגברה ליניארית. לכל מטריצות A, B מסדר $n \times n$ ולכל וקטור $r \in \mathbb{R}^n$:

$$(A \cdot B) \cdot r = A \cdot (B \cdot r), \qquad (A - C) \cdot r = A \cdot r - C \cdot r.$$

הזהות הראשונה (אסוציאטיביות) היא לב האלגוריתם של Freivalds; השנייה (דיסטריביוטיביות) היא לב הניתוח. כמו כן, הקואורדינטה ה-i של $D \cdot r$ היא

$$(D \cdot r)_i = \sum_{j=1}^{n} D_{ij}\, r_j.$$

חישוב מכפלת **מטריצה בווקטור** עולה $\Theta(n^2)$ פעולות אריתמטיות; חישוב מכפלת **מטריצה במטריצה** בשיטה הנאיבית עולה $\Theta(n^3)$. בהקלטה [00:35:46] עלה שקיימים אלגוריתמים מהירים יותר לכפל מטריצות (מעריך כ-$n^{2.37}$), אך הקורס לא נכנס לזה ומשווה מול n^3.

המקרה הגרוע ביותר והאויב האכזר. מקורס האלגוריתמים: ניתוח במקרה הגרוע ביותר שקול לחשוב על יריב שמכיר את האלגוריתם ובוחר עבורו את הקלט המזיק ביותר ([00:07:06]). ההבדל המרכזי שנוסף כאן: היריב מכיר את **הקוד**, אך **לא** את תוצאות ההטלות, שנבחרות אחרי שהקלט כבר נקבע ([00:08:08]). זהו כל ההסבר לשאלה "למה אקראיות עוזרת".

הגדרות

הגדרה 1: אלגוריתם אקראי

ניסוח. אלגוריתם אקראי $\mathcal{A}$ מקבל שני קלטים: את הקלט "האמיתי" x, ומחרוזת ביטים r שכל ביט בה נדגם באופן אחיד ובלתי תלוי מ-$\{0,1\}$. בהינתן x ו-r, הריצה של $\mathcal{A}$ **דטרמיניסטית לחלוטין**, והפלט הוא פונקציה $\mathcal{A}(x, r)$. כל אמירה הסתברותית על $\mathcal{A}$ היא אמירה על

$$\Pr_r\left[\,\mathcal{A}(x,r)\text{ has some property}\,\right]\quad\text{for a }\mathbf{fixed}\text{, arbitrary }x.$$

אינטואיציה. תחשבו על x כעל דבר שנתון לנו מבחוץ, ועל r כעל הדבר היחיד שאנחנו מגרילים. המרצה ניסח זאת פעמיים ([00:11:18], [00:16:35]): "האקראיות לא תגיע לי מהקלט. הקלט הוא שרירותי, אני חושב על הקלט הגרוע ביותר, האלגוריתם הוא זה שאקראי". הניסוח האינטואיטיבי שהמרצה נתן בפתיחה ([00:00:34]) הוא: אלגוריתם אקראי הוא אלגוריתם שיכול, בכל רגע ובכמה פעמים שירצה, "לדגום באקראי ביט $0/1$", בלתי תלוי בקודמים.

מופע. האלגוריתם של Freivalds (הגדרה 5 להלן) דוגם וקטור $r\in\{0,1\}^n$; זהו בדיוק n ביטים אקראיים.

אי-מופע (חשוב). משפט מהצורה "v_1 הוא המועמד הטוב ביותר" **אינו** מאורע אקראי בהקשר הזה, כי הוא תלוי רק בקלט ולא ב-r. המרצה עצר על כך במפורש ([00:20:16]): "לא לדבר על הסתברות של משהו שהוא לא אקראי — זה חסר משמעות". לעומת זאת "$\sigma(1)$ הוא המועמד הטוב ביותר" **כן** מאורע אקראי, כי σ הוא האובייקט שהוגרל.

> **הערה (מינוח שלא נאמר בשיעור):** בספרות מבחינים בין אלגוריתם **Las Vegas** — תמיד מחזיר תשובה נכונה, וזמן הריצה שלו הוא משתנה מקרי — לבין אלגוריתם **Monte Carlo** — זמן הריצה חסום תמיד, אך התשובה עשויה להיות שגויה בהסתברות קטנה. שני האלגוריתמים בשיעור הזה הם מטיפוס Monte Carlo: זמן הריצה שלהם חסום בוודאות והתשובה עשויה להיות שגויה. המונחים האלה **אינם** מופיעים לא בסיכום ולא בהקלטה, והם נכתבים כאן רק כדי לקשר לחומר חיצוני.

הגדרה 2: מרחב המדגם של ריצה אקראית

ניסוח. מרחב המדגם Ω של אלגוריתם אקראי הוא אוסף **תוצאות הניסוי האקראי** שהאלגוריתם מבצע — לא אוסף הפלטים האפשריים שלו.

אינטואיציה ומדוע זה קריטי. זו הייתה שאלת סטודנטית שהמרצה ציין כשאלה מצוינת ([00:23:52]), כי כאן נופלים הכי הרבה. באלגוריתם המזכיר הניסוי הוא "הגרלת תמורה", ולכן $\Omega=S_n$, קבוצת כל התמורות $\sigma:[n]\to[n]$, ו-$|\Omega|=n!$. **לא** $\{1,\dots,n\}$, שהיא קבוצת הפלטים. באלגוריתם Freivalds הניסוי הוא "הגרלת וקטור", ולכן $\Omega=\{0,1\}^n$ ו-$|\Omega|=2^n$.

מופע ואי-מופע (הדוגמה שהמרצה נתן, [00:24:55]). מטילים שתי קוביות הוגנות ושואלים מה ההסתברות שהסכום הוא 5. מרחב המדגם הוא

$$\Omega=\{(x,y):x,y\in\{1,\dots,6\}\},\qquad |\Omega|=36,$$

כלומר **זוגות סדורים**. תשובה שגויה נפוצה היא ש-Ω הוא קבוצת הסכומים האפשריים $\{2,\dots,12\}$ — אבל הסכום הוא **מאורע**, לא תוצאה של הניסוי. הפתרון המלא מופיע בסעיף הדוגמאות.

הגדרה 3: טעות חד-צדדית, ומטריצת הבלבול

ניסוח. נתבונן באלגוריתם הכרעה אקראי לשפה L. לכל קלט x מוגדרים שני סוגי טעות:

	האלגוריתם מקבל	**האלגוריתם דוחה**
$x\in L$ (yes-instance)	נכון	**false negative**
$x\notin L$ (no-instance)	**false positive**	נכון

זוהי **מטריצת הבלבול** (confusion matrix) של האלגוריתם ([01:02:43]). לאלגוריתם יש **טעות חד-צדדית** אם אחת משתי משבצות הטעות ריקה — כלומר הוא יכול לטעות רק לכיוון אחד. אם שתיהן אפשריות, הטעות **דו-צדדית**.

אינטואיציה. אין תשובה כללית לשאלה איזו טעות גרועה יותר — זה תלוי ביישום ([01:03:14]): בבדיקה אפידמיולוגית עדיף false positive (מישהו יישאר בבית לחינם) על false negative; לפני ניתוח מוח לא רוצים אף אחד מהם.

מופע. אלגוריתם Freivalds: כאשר $AB = C$ הוא **תמיד** מקבל, ולכן אין לו false negative כלל — טעות חד-צדדית מסוג false positive בלבד ([01:03:46]). זו בדיוק התכונה שתאפשר את ההגברה הפשוטה במשפט 4.

אי-מופע. אלגוריתם שמכריע לפי הצבעת רוב על הרצות שכל אחת מהן טועה בהסתברות $\leq 1/3$ בשני הכיוונים הוא בעל טעות דו-צדדית. גם אותו אפשר להגביר, אך לא בכלל "קבל רק אם כולם קיבלו" אלא בהצבעת רוב; המרצה ציין זאת ([01:04:52]) והשאיר לשיעור הבא.

הגדרה 4: בעיית המזכיר (Secretary Problem)

ניסוח (המודל). נתונים n מועמדים, $[n] = \{1, \dots, n\}$, שלמועמד i ערך ממשי $v_i \geq 0$. הערכים **שונים זה מזה** ו-n **זוגי** (ראו פערים). המועמדים מרואיינים אחד-אחד, בסדר שהאלגוריתם קובע. הכללים:

הערך v_i מתגלה **רק** בזמן הראיון של מועמד i, ולא לפניו.

מיד בתום הראיון יש להחליט: לקבל או לדחות.

אם קיבלנו — התהליך נעצר, שאר המועמדים הולכים הביתה.

אם דחינו — המועמד הולך הביתה ולא ניתן לחזור אליו.

המטרה: לבחור את המועמד בעל הערך המקסימלי.

אינטואיציה. בלי כללים 1–4 זו בעיית "מציאת מקסימום במערך", והאלגוריתם המוכר (שמור את המקסימום עד כה, החלף אם ראית גדול יותר) פותר אותה בוודאות ([00:04:56]). הכללים הופכים את הקלט מ**מערך** ל**רשימה מקושרת חד-כיוונית שאי אפשר לחזור בה אחורה** ([00:14:29]) — מה שנקרא היום בעיה **online**. כל הקושי נובע מכך שההחלטה חייבת להתקבל לפני שנראתה יתרת הקלט.

מופע. $n = 4$ עם ערכים $v = (10, 40, 20, 30)$: המועמד הטוב ביותר הוא 2 (ערך 40), השני הכי טוב הוא 4 (ערך 30).

אי-מופע (מה שאינו הבעיה). "לבחור את המקסימום מתוך מערך נתון" — שם אין החלטה בלתי הפיכה, ולכן אין קושי.

הגדרה 5: וידוא כפל מטריצות ואלגוריתם Freivalds

ניסוח הבעיה. הקלט הוא שלוש מטריצות A, B, C מסדר $n \times n$, והשאלה היא האם $A \cdot B = C$. זו בעיית **הכרעה** ("בעיית אחר?" — כן/לא), והיא **אינה** NP-קשה: אפשר לפתור אותה דטרמיניסטית בזמן $O(n^3)$ פשוט על ידי חישוב $A \cdot B$ והשוואה ל-C. נסמן את השפה ב-MATMUL (סימון שלנו; בסיכום הבעיה אינה מקבלת שם).

המטרה אינה להוציא את הבעיה מ-P — היא כבר שם — אלא **להוריד את המעריך** ([00:36:51]).

האלגוריתם (Freivalds). על קלט A, B, C:

בחר באקראי, באופן אחיד, וקטור $r \in \{0,1\}^n$.
חשב $A \cdot (B \cdot r)$ ו-$C \cdot r$.
אם $A \cdot (B \cdot r) = C \cdot r$ — **קבל**; אחרת — **דחה**.
אינטואיציה. במקום להשוות שתי מטריצות (יקר), משווים את פעולתן על וקטור אקראי אחד (זול). ההצדקה לזמן הריצה היא האסוציאטיביות $(A \cdot B) \cdot r = A \cdot (B \cdot r)$: אף פעם לא כופלים מטריצה במטריצה, רק מטריצה בווקטור ([00:38:59]).
מופע ואי-מופע. אם $AB = C$ אז לכל r ההשוואה מצליחה. אם $AB \neq C$ עדיין ייתכנו וקטורים r ספציפיים שעבורם $ABr = Cr$ — מהאלגברה הליניארית ידוע ששתי מטריצות שונות יכולות להסכים על וקטור מסוים ([00:43:20]). כל מה שצריך להוכיח הוא ש**אין יותר מדי** כאלה.

משפטים והוכחות
משפט 1: אין אלגוריתם דטרמיניסטי עם ערובה כלשהי לבעיית המזכיר
ניסוח. לכל אלגוריתם **דטרמיניסטי** $\mathcal{D}$ לבעיית המזכיר קיים קלט (סדרת ערכים) שעליו $\mathcal{D}$ מחזיר את המועמד בעל הערך **הנמוך ביותר**. בפרט, לכל $\alpha > 0$ קיים קלט שעליו הערך שנבחר קטן מ-α כפול המקסימום.
הוכחה. נבנה יריב שמייצר את הערכים תוך כדי ריצה. הנקודה המרכזית: מאחר ש-$\mathcal{D}$ דטרמיניסטי, ההחלטה שלו בשלב j היא **פונקציה של הרישא** $v_1, \dots, v_j$ בלבד. לכן אם היריב שינה רק ערכים שטרם נחשפו, התנהגות $\mathcal{D}$ על הרישא אינה משתנה.
היריב מזין ערכים עולים: $v_1 = 1,\ v_2 = 2,\ v_3 = 3, \dots$. נבחין בשני מקרים.
מקרה א': $\mathcal{D}$ מקבל בשלב כלשהו $j \le n-1$. בזמן הזה הוא ראה רק את $v_1, \dots, v_j$. עכשיו היריב "משנה את דעתו" לגבי ההמשך וקובע $v_{j+1} = \dots = v_n = M$ עבור M גדול כרצוננו. הרישא לא השתנתה, ולכן $\mathcal{D}$ עדיין מקבל בשלב j ומחזיר ערך j, בעוד המקסימום הוא M. היחס j/M קטן מכל $\alpha > 0$ עבור M גדול מספיק. אם בפרט $j = 1$, המועמד שנבחר הוא גם בעל הערך הנמוך ביותר.
מקרה ב': $\mathcal{D}$ דוחה את כל $n-1$ הראשונים. אז הוא חייב לקחת את המועמד האחרון (או להחזיר כלום, מה שגרוע אף יותר). היריב קובע כעת $v_n = 0$, כלומר הנמוך מכולם. שוב הרישא $v_1, \dots, v_{n-1}$ לא השתנתה, ולכן ההתנהגות זהה, ו-$\mathcal{D}$ מחזיר את הגרוע ביותר. ■

> **הערה:** בהרצה זה נאמר בקיצור — "לכל אלגוריתם דטרמיניסטי אני יכול לייצר קלט שבו הוא יבחר לא נכון... יותר מזה, אני יכול לדאוג שהוא ימצא מועמד ממש גרוע" ([00:05:28]–[00:06:33]) — בלי לפרט את שני המקרים. הפירוט כאן.

מדוע הניסיון הנאיבי לאקראיות אינו עוזר. סטודנט הציע ([00:07:06]) להגריל את **הסף**: לצפות במספר אקראי של מועמדים ואז לקחת את הראשון שעובר את המקסימום שנצפה. המרצה הראה מיד שזה נכשל: היריב פשוט ישים את המועמד הטוב ביותר **במקום הראשון**. אז לא משנה מה הסף שהוגרל (כל עוד הוא לפחות 1), המועמד הטוב ביותר נמצא בשלב התצפית ונדחה בוודאות, ולכן קיים

קלט שעליו האלגוריתם טועה **בהסתברות** 1. המסקנה, שהיא הלקח האמיתי של המשפט: לא מספיק "להוסיף אקראיות" — צריך להוסיף אותה **במקום הנכון**, כלומר לטשטש בדיוק את הדבר שהיריב שולט בו. היריב שולט ב**סדר**, ולכן את הסדר צריך להגריל ([00:09:42]).

משפט 2: האלגוריתם האקראי לבעיית המזכיר

האלגוריתם. על קלט של n מועמדים (n זוגי, ערכים שונים):

הגרל תמורה $\sigma : [n] \to [n]$ באופן אחיד מתוך כל $n!$ התמורות.

לכל $1 \le j \le \frac{n}{2}$: ראיין את המועמד $\sigma(j)$ **ודחה** אותו.

סמן ב-V את הערך המקסימלי שנצפה עד כה, כלומר $V = \max_{1 \le j \le n/2} v_{\sigma(j)}$.

לכל $\frac{n}{2}+1 \le j \le n-1$: אם $v_{\sigma(j)} > V$ אז **קבל** את $\sigma(j)$ ועצור.

אם הגעת לכאן — **קבל** את $\sigma(n)$.

ניסוח המשפט. לכל קלט (כלומר לכל וקטור ערכים שונים $v_1, \dots, v_n$), אם A הוא המאורע "האלגוריתם מחזיר את המועמד בעל הערך המקסימלי", אז

$$\Pr_{\sigma}[A] \;\ge\; \frac{n}{4(n-1)} \;>\; \frac{1}{4}.$$

ההסתברות נלקחת **רק על התמורה** σ, והחסם תקף **לכל** קלט.

למה שלב 5 קיים. שאלת סטודנט ([00:17:06]): מדוע הלולאה בשלב 4 נעצרת ב-$n-1$? כי כאשר מגיעים למועמד האחרון אין עוד ברירה — חייבים לקבל אותו, בלי תנאי. אלמלא שלב 5 האלגוריתם היה עלול לא להחזיר דבר ([00:12:22]).

הוכחה. ראשית נשים לב לנקודה המתודולוגית: לאחר שהוגרלה σ, כל שאר הריצה **דטרמיניסטית** ([00:19:45]). לכן כל מאורע שאנחנו מגדירים חייב להיות פונקציה של σ בלבד, ומרחב המדגם הוא $\Omega = S_n$ עם $|\Omega| = n!$.

נגדיר מאורע שני:

$$B = \Big\{ \sigma \;:\; \sigma^{-1}(\text{best}) \in \{\tfrac{n}{2}+1, \dots, n\} \;\text{ and }\; \sigma^{-1}(\text{2nd best}) \in \{1, \dots, \tfrac{n}{2}\} \Big\},$$

כלומר: התמורה שמה את המועמד הטוב ביותר איפשהו בחצי השני, ואת השני-הכי-טוב איפשהו בחצי הראשון.

שלב 1: $B \subseteq A$. נניח ש-B מתרחש. המועמד השני-הכי-טוב נמצא בחצי הראשון, והמועמד הטוב ביותר אינו שם; לכן המקסימום של החצי הראשון הוא בדיוק ערכו של השני-הכי-טוב, כלומר $V = v_{(2)}$ (כאן $v_{(1)} > v_{(2)} > \dots$ הם הערכים בסדר יורד). כעת בחצי השני: המועמד היחיד בכל הקלט שערכו גדול מ-$v_{(2)}$ הוא המועמד הטוב ביותר. לכן בשלב 4 האלגוריתם דוחה כל מי שאינו הטוב ביותר, ומקבל אותו ברגע שהוא מגיע אליו. שני מקרי קצה:

אם הטוב ביותר יושב במקום j עבור $\frac{n}{2}+1 \le j \le n-1$ — הוא ייבחר בשלב 4.

אם הטוב ביותר יושב דווקא במקום n — אז שלב 4 לא קיבל אף אחד (איש לא עבר את V), ושלב 5 מקבל את $\sigma(n)$, שהוא הטוב ביותר.

בשני המקרים האלגוריתם מחזיר את הטוב ביותר, כלומר A מתרחש. לכן $B \subseteq A$ כקבוצות של תמורות. מכאן, לפי מונוטוניות, $\Pr[A] \ge \Pr[B]$ ([00:22:19]).

שלב 2: ספירת $|B|$. נבנה תמורה ב-B בשלושה שלבים בלתי תלויים:

בוחרים מקום לשני-הכי-טוב בחצי הראשון: $\frac{n}{2}$ אפשרויות.

בוחרים מקום לטוב ביותר בחצי השני: $\frac{n}{2}$ אפשרויות.
מסדרים את $n-2$ הנותרים ב-$n-2$ המקומות הנותרים: $(n-2)!$ אפשרויות.
כל תמורה ב-B מתקבלת בדיוק פעם אחת בבנייה הזאת, ולכן
$$|B| = \frac{n}{2} \cdot \frac{n}{2} \cdot (n-2)! = \frac{n^2}{4}\,(n-2)!.$$
שלב 3: החשבון. מאחר שהדגימה אחידה,
$$\Pr[B] = \frac{|B|}{|\Omega|} = \frac{\frac{n^2}{4}(n-2)!}{n!}.$$
נשתמש ב-$n! = n\,(n-1)\,(n-2)!$, כלומר $\dfrac{(n-2)!}{n!} = \dfrac{1}{n(n-1)}$, ונקבל
$$\Pr[B] = \frac{n^2}{4} \cdot \frac{1}{n(n-1)} = \frac{n}{4(n-1)} = \frac{1}{4} \cdot \frac{n}{n-1} \;\geq\; \frac{1}{4},$$
שכן $\frac{n}{n-1} > 1$ לכל $n \geq 2$. בשילוב עם שלב 1: $\Pr[A] \geq \Pr[B] \geq \frac{1}{4}$. ■
מסקנה 2.1 (תוחלת). לכל קלט, הערך של המועמד שנבחר מקיים בתוחלת
$$\mathbb{E}[\,v_{\text{chosen}}\,] \;\geq\; \Pr[A] \cdot v_{(1)} \;\geq\; \frac{v_{(1)}}{4},$$
כלומר לפחות רבע מהמקסימום. הנימוק: כל הערכים אי-שליליים, ולכן התוחלת חסומה מלמטה על ידי התרומה של המאורע A בלבד. המרצה ציין זאת ב-[00:31:20] בלי חישוב; זהו החישוב.
מדוע $\frac{1}{4}$ אינו "גרוע" (שאלת סטודנט, [00:29:45]–[00:30:50]). יש להשוות למשפט 1, לא ל-1. דטרמיניסטית **אין שום ערובה** — קיים קלט שעליו הכישלון ודאי. כאן $\frac{1}{4}$ מתקבל **לכל קלט**, כולל הגרוע ביותר; האקראיות "פיזרה את הסיכון". יתרה מזו, אם מחליפים את הסף $\frac{n}{2}$ ב-$\frac{n}{e}$ מקבלים הסתברות הצלחה $\frac{1}{e} \approx 0.37 \to$, וזהו האופטימום — אין אלגוריתם טוב יותר ([00:12:54], [00:17:38]). הבחירה ב-$\frac{n}{2}$ נעשתה רק כדי שההוכחה תהיה בת שלוש שורות.
משפט 3: נכונות וזמן ריצה של אלגוריתם Freivalds
ניסוח. יהיו A, B, C מטריצות $n \times n$ **קבועות** (חלק מהקלט, לא אקראיות). האלגוריתם של הגדרה 5 רץ בזמן $O(n^2)$ פעולות אריתמטיות ומקיים:
אם $A \cdot B = C$ אז $\Pr_r[\text{the algorithm accepts}] = 1$;
אם $A \cdot B \neq C$ אז $\Pr_r[\text{the algorithm accepts}] \leq \frac{1}{2}$, ולכן $\Pr_r[\text{rejects}] \geq \frac{1}{2}$.
ההסתברות נלקחת **רק על** r, והחסם תקף **לכל שלשת מטריצות**.

> **הערה מתודולוגית חשובה ([00:41:47]–[00:42:19]):** אסור לכתוב "$\Pr[\text{the algorithm is correct}]$" בלי לפצל למקרים. הפיצול ל-yes-instance ו-no-instance הוא פיצול **לפי הקלט**, והקלט אינו אקראי; לכן הוא חייב להיעשות **מחוץ** לסימן ההסתברות. זו טעות נפוצה למבחן.

זמן ריצה. מחשבים $B \cdot r$ ($\Theta(n^2)$ כפלים), אחר כך $A \cdot (B \cdot r)$ (שוב $\Theta(n^2)$), כי זו מטריצה כפול וקטור), ובנפרד $C \cdot r$ ($\Theta(n^2)$), ולבסוף משווים שני וקטורים באורך n ($O(n)$). סך הכול $O(n^2)$.
הנקודה: **בזכות האסוציאטיביות לעולם לא מבצעים כפל מטריצה במטריצה** ([00:38:59]).
הוכחת סעיף 1 (שלמות). נניח $A \cdot B = C$. אז לכל r **בלי יוצא מן הכלל** מתקיים $A \cdot (B \cdot r) = (A \cdot B) \cdot r = C \cdot r$, ולכן התנאי בשלב 3 מתקיים והאלגוריתם מקבל. זהו מאורע שמכיל את כל Ω, ולכן הסתברותו 1. שימו לב שכאן לא נעשה שום שימוש באקראיות — הטענה נכונה **פוינטווייז** לכל r.

הוכחת סעיף 2 (נאותות). נניח $A \cdot B \neq C$ ונסמן
$$D := A \cdot B - C \neq 0.$$
צעד א' — *תרגום תנאי הקבלה.* מדיסטריביוטיביות, $A \cdot (B \cdot r) = C \cdot r$ אם ורק אם $(A \cdot B) \cdot r - C \cdot r = 0$. לכן $D \cdot r = 0$ אם ורק אם
$$\Pr_r[\text{accept}] = \Pr_r[\, D \cdot r = 0 \,].$$
צעד ב' — *בחירת איבר לא אפסי.* מאחר ש-$D \neq 0$, יש בה לפחות איבר אחד שונה מאפס. **ללא הגבלת הכלליות** נניח שזהו D_{11}. הבחירה הזו לגיטימית בתוך חישוב הסתברות משום ש-A, B, C (ולכן D) **אינן אקראיות** — האינדקסים נקבעים לפני ההגרלה ואינם תלויים ב-r. אילו היה מדובר באיבר D_{ik} כללי, ההוכחה הייתה זהה מילה במילה עם גרירת שני אינדקסים ([00:45:29]).
צעד ג' — *מעבר לקואורדינטה אחת.* מתקיימת הכלת מאורעות: אם $D \cdot r$ הוא וקטור האפס אז בפרט הקואורדינטה הראשונה שלו אפס. כלומר
$$\{r : D \cdot r = 0\} \subseteq \{r : (D \cdot r)_1 = 0\},$$
ולכן, ממונוטוניות, וזה **הכיוון הנכון** כי אנחנו חוסמים מלמעלה ([00:48:43]):
$$\Pr_r[D \cdot r = 0] \leq \Pr_r[(D \cdot r)_1 = 0] = \Pr_r\left[\sum_{j=1}^{n} D_{1j} r_j = 0\right].$$
צעד ד' — *בידוד* r_1. מעבירים אגפים ומבודדים:
$$\sum_{j=1}^{n} D_{1j} r_j = 0 \iff D_{11} r_1 = -\sum_{j=2}^{n} D_{1j} r_j \iff r_1 = \frac{-\sum_{j=2}^{n} D_{1j} r_j}{D_{11}}.$$
החלוקה חוקית **בדיוק** משום שדאגנו ש-$D_{11} \neq 0$; זו כל המטרה של צעד ב' ([00:53:37]).
צעד ה' — *ספירה.* מרחב המדגם הוא $\Omega = \{0,1\}^n$ עם $|\Omega| = 2^n$, בהתפלגות אחידה. נספור כמה וקטורים מקיימים את השוויון האחרון. נקבע ערכים כלשהם ל-$r_2, \ldots, r_n$; יש 2^{n-1} קביעות כאלה. עבור כל קביעה, האגף הימני הוא **מספר קבוע** c, ולכן קיים **לכל היותר** ערך אחד של r_1 שמקיים את השוויון: אם $c \in \{0,1\}$ יש בדיוק אפשרות אחת, ואם $c \notin \{0,1\}$ (למשל $c = -3$ או c לא שלם או אפילו אי-רציונלי) אין אף אפשרות ([00:55:47], [00:56:19]). לכן
$$\left|\{r \in \{0,1\}^n : \; D \cdot r = 0\}\right| \leq 2^{n-1} \cdot 1 = 2^{n-1},$$
ומכאן
$$\Pr_r[\text{accept}] \leq \frac{2^{n-1}}{2^n} = \frac{1}{2}. \qquad \blacksquare$$
האופן שבו כדאי לחשוב על צעד ה'. $r_2, \ldots, r_n$ הם $n-1$ "משתנים חופשיים" ו-r_1 הוא "משתנה תלוי" שנקבע (לכל היותר) על ידם ([01:00:36]). זהו בדיוק תרגיל ספירה, לא טיעון הסתברותי עמוק.
מסקנה 3.1 (טעות חד-צדדית). לפי סעיף 1 אין לאלגוריתם false negative כלל: הוא לעולם אינו דוחה קלט שבו $AB = C$. לכן כל הטעות שלו היא false positive, והיא חד-צדדית ([01:03:46]). זו התכונה שמפעילה את משפט 4.
משפט 4: הגברה בשתי חזרות
האלגוריתם המשופר. על קלט A, B, C:
הרץ את האלגוריתם של הגדרה 5 **פעמיים**, כל פעם עם הגרלה **טרייה ובלתי תלויה** של r.
אם בשתי ההרצות האלגוריתם קיבל — **קבל**; אחרת — **דחה**.
ניסוח. אם $AB = C$ אז $\Pr[\text{accept}] = 1$; אם $AB \neq C$ אז $\Pr[\text{accept}] \leq \frac{1}{4}$, ולכן $\Pr[\text{correct}] \geq \frac{3}{4}$. זמן הריצה נשאר $O(n^2)$ אסימפטוטית.

הוכחה. יהיו E_1, E_2 המאורעות "ההרצה הראשונה קיבלה" ו"ההרצה השנייה קיבלה".
מקרה $AB = C$: לפי משפט 3.1, $\Pr[E_1] = \Pr[E_2] = 1$, ולכן שתי ההרצות מקבלות בוודאות והאלגוריתם המשופר מקבל בהסתברות 1. **זה בדיוק מה שהטעות החד-צדדית קונה לנו:** הצד הזה לא נפגע מההחזרה ([01:12:25]).
מקרה $AB \neq C$: לפי הגדרת האלגוריתם, האלגוריתם המשופר מקבל **אם ורק אם** **וגם** E_1 E_2. המאורעות E_1, E_2 בלתי תלויים, כי הם פונקציות של שתי מחרוזות אקראיות נפרדות שהוגרלו באופן בלתי תלוי — אי-התלות אינה הנחה, היא **מובנית באלגוריתם** ([01:06:25]). לכן
$$\Pr[\text{accept}] = \Pr[E_1 \cap E_2] = \Pr[E_1] \cdot \Pr[E_2] \;\leq\; \tfrac{1}{2} \cdot \tfrac{1}{2} = \tfrac{1}{4},$$
ומכאן $\Pr[\text{reject}] \geq 1 - \frac{1}{4} = \frac{3}{4}$. ■

> **הערה על שם התהליך:** מרגע שנאמר "באופן בלתי תלוי", אפשר לחשוב על שתי ההרצות כאילו נעשו במקביל; זה נקרא גם ([01:06:25]) **parallel repetition**.

משפט 5: הגברה כללית ל-t חזרות
האלגוריתם. על קלט A, B, C:
הרץ את האלגוריתם של הגדרה 5 t **פעמים** עם הגרלות טריות ובלתי תלויות.
קבל אם ורק אם **בכל** ההרצות האלגוריתם קיבל.
ניסוח. זמן הריצה הוא $O(t \cdot n^2)$, ולכל A, B, C:
אם $AB = C$: $\Pr[\text{accept}] = 1$;
אם $AB \neq C$: $\Pr[\text{accept}] \leq \dfrac{1}{2^t}$, ולכן $\Pr[\text{correct}] \geq 1 - \dfrac{1}{2^t}$.
הוכחה. זמן הריצה: t הרצות של $O(n^2)$ כל אחת. שימו לב ש-t עצמו רשאי להיות פונקציה של n, ולכן הגורם t נשאר מפורש בחסם ([01:11:39]).
נכונות במקרה $AB = C$: כל הרצה מקבלת בהסתברות 1 (משפט 3.1), ולכן חיתוך של t מאורעות ודאיים הוא מאורע ודאי.
נכונות במקרה $AB \neq C$: יהי E_i המאורע "ההרצה ה-i קיבלה". המאורעות $E_1, \ldots, E_t$ בלתי תלויים, שכן כל אחד מהם תלוי בבלוק ביטים אקראיים נפרד וזר לאחרים. האלגוריתם מקבל אם ורק אם $\bigcap_{i=1}^{t} E_i$, ולכן
$$\Pr[\text{accept}] = \Pr\left[\bigcap_{i=1}^{t} E_i\right] = \prod_{i=1}^{t} \Pr[E_i] \;\leq\; \left(\tfrac{1}{2}\right)^t = \tfrac{1}{2^t}. \qquad \blacksquare$$
המקרה המעניין: $t = \log n$ (בסיס 2). אז
$$\Pr[\text{failure}] \;\leq\; \tfrac{1}{2^{\log n}} = \tfrac{1}{n}, \qquad \text{running time} \;= O(n^2 \log n).$$
זהו הלקח הכמותי המרכזי של השיעור ([01:15:16]): **גורם ליניארי בזמן הריצה קונה ירידה אקספוננציאלית בהסתברות הכישלון**, וזה בדיוק בגלל שהסתברויות של מאורעות בלתי תלויים **מוכפלות**. ככל ש-n גדל, הסתברות ההצלחה $1 - \frac{1}{n}$ שואפת ל-1.
מסקנה 5.1 (טרייד-אוף). יש כאן שתי מטרות מתחרות ([01:10:37]): הגדלת t משפרת את הסתברות ההצלחה אך מגדילה את זמן הריצה, וגם צורכת יותר ביטים אקראיים ($t \cdot n$ במקום n). אין ערך "נכון" ל-t — הוא נקבע לפי היישום.

משפט 6: הגרלה מאלפבית גדול יותר, וחשבון הביטים

רקע. שאלת סטודנט ([01:14:05]): למה להגריל r מ-$\{0,1\}^n$ ולא מ-$\{0,1,2\}^n$?

ניסוח. נריץ את האלגוריתם של הגדרה 5 כאשר r נדגם באופן אחיד מ-Σ^n עבור $\Sigma = \{0,1,\dots,k-1\}$. אז אם $AB \neq C$ מתקיים $\Pr_r[\text{accept}] \le \dfrac{1}{k}$.

הוכחה. ההוכחה של משפט 3 עוברת מילה במילה עד צעד ה'. שם, $|\Omega| = k^n$; לכל קביעה של $r_2,\dots,r_n$ (יש k^{n-1} כאלה) יש לכל היותר ערך אחד של r_1 שמקיים $r_1 = -\left(\sum_{j\ge 2} D_{1j} r_j\right)/D_{11}$. לכן $\Pr_r[\text{accept}] \le \frac{k^{n-1}}{k^n} = \frac{1}{k}$. $\blacksquare$

בפרט: $\Sigma=\{0,1,2\}$ נותן $\frac{1}{3}$, ו-$\Sigma=\{0,\dots,7\}$ נותן $\frac{1}{8}$ ([01:17:22]).

החשבון שמראה שזה לא בהכרח משתלם ([01:18:25]–[01:19:30]). ביטים אקראיים אמיתיים הם משאב שעולה כסף — ה-`random` של המחשב אינו אקראי באמת, ואם רוצים ביטים בלתי תלויים באיכות גבוהה משלמים עליהם; זה משאב שכלל **לא** נכלל בחשבון זמן הריצה שלנו. נשווה שתי דרכים להוציא הסתברות טעות טובה יותר מ-$\frac{1}{2}$:

שיטה	ביטים אקראיים	הסתברות טעות	זמן ריצה
הרצה אחת מ-$\{0,1,2\}^n$	$2n$ (שני ביטים לקואורדינטה)	$\le \frac{1}{3}$	$O(n^2)$
שתי הרצות מ-$\{0,1\}^n$	$2n$	$\le \frac{1}{4}$	$2\cdot O(n^2)$

באותו מחיר בביטים אקראיים, החזרה הכפולה על האלפבית הבינארי נותנת **טעות קטנה יותר** ($\frac{1}{4} < \frac{1}{3}$) אך משלמת פי שניים בזמן. אין כאן זוכה מוחלט — יש טרייד-אוף, וההחלטה תלויה במה יקר יותר במערכת הספציפית (זמן מעבד, ביטים אקראיים, זמן מתכנתים). המרצה סיכם: "זה כמו פלסטלינה, צריך לשחק עם זה".

הערה נוספת: הבחירה ב-$\{0,1\}$ בהוכחה המקורית נעשתה מסיבה דידקטית בלבד — כך היה קל למנות את כל האפשרויות על הלוח ([01:17:22]).

דוגמאות ותרגילים מהשיעור

דוגמה 1: שתי קוביות — תרגיל החימום על מרחב מדגם

השאלה ([00:24:55]). מטילים שתי קוביות הוגנות. מה ההסתברות שהסכום הוא 5?

פתרון מלא. מרחב המדגם הוא אוסף התוצאות של הניסוי, כלומר זוגות סדורים:

$$\Omega = \{(x,y) : x,y \in \{1,\dots,6\}\}, \qquad |\Omega| = 6\cdot 6 = 36.$$

ההתפלגות אחידה על 36 הזוגות. המאורע המבוקש הוא

$$E = \{(1,4),(2,3),(3,2),(4,1)\}, \qquad |E| = 4.$$

לכן $\Pr[E] = \dfrac{4}{36} = \dfrac{1}{9}$.

הלקח. התשובה הנפוצה והשגויה היא ש-$\Omega=\{2,3,\dots,12\}$ ולכן ההסתברות היא $\frac{1}{11}$. הסכום הוא **מאורע**, לא תוצאת ניסוי; אילו היה מרחב המדגם, כל הסכומים היו שווי הסתברות, וזה שקר. אותה בדיוק טעות ממתינה בבעיית המזכיר: מרחב המדגם הוא S_n ולא $\{1,\dots,n\}$.

דוגמה 2: מעקב מלא אחר אלגוריתם המזכיר עבור $n = 4$

הקלט. $n = 4$, ערכים $v = (10, 40, 20, 30)$. הטוב ביותר: מועמד 2 (ערך 40). השני-הכי-טוב: מועמד 4 (ערך 30).

האלגוריתם על הקלט הזה. מגרילים σ מתוך $4! = 24$ תמורות; מראיינים ודוחים את $\sigma(1), \sigma(2)$ וקובעים $V = \max(v_{\sigma(1)}, v_{\sigma(2)})$; בשלב $j = 3$ מקבלים אם $v_{\sigma(3)} > V$; אחרת מקבלים את $\sigma(4)$.

החסם מהמשפט. $\frac{n}{4(n-1)} = \frac{4}{12} = \frac{1}{3}$. בהתאמה מלאה $|B| = \frac{4}{2} \cdot \frac{4}{2} \cdot 2! = 2 \cdot 2 \cdot 2 = 8$, ולכן $\Pr[B] = \frac{8}{24} = \frac{1}{3}$.

חישוב מדויק של $\Pr[A]$ (מעבר לנדרש, כדי לראות שההכלה $B \subseteq A$ ממש). נסמן את דירוגי המועמדים 1 (הטוב ביותר) עד 4 (הגרוע ביותר) ונספור לפי מיקום הטוב ביותר בתמורה:

הטוב ביותר במקום 3: אז $v_{\sigma(3)} > V$ תמיד, והאלגוריתם מקבל אותו. הצלחה. מספר תמורות: $3! = 6$.

הטוב ביותר במקום 4: מצליחים אם ורק אם המועמד במקום 3 **אינו** עובר את V, כלומר אם הוא אינו הטוב מבין השלושה הראשונים. שלושת המקומות הראשונים מכילים את הדירוגים $\{2, 3, 4\}$ ב-$3! = 6$ סידורים; הכישלון הוא בדיוק כאשר דירוג 2 יושב במקום 3, וזה קורה ב-2 סידורים. לכן $6 - 2 = 4$ הצלחות.

הטוב ביותר במקום 1 או במקום 2: אז V שווה לערך המקסימלי בכל הקלט, איש בחצי השני לא יעבור אותו, והאלגוריתם ייקח את $\sigma(4)$ שאינו הטוב ביותר. כישלון בכל $2 \cdot 3! = 12$ התמורות.

סך הצלחות: $6 + 4 = 10$, כלומר

$$\Pr[A] = \frac{10}{24} = \frac{5}{12} \approx 0.4167.$$

ואכן $\frac{5}{12} > \frac{1}{3} = \Pr[B] > \frac{1}{4}$. ההכלה $B \subseteq A$ אמיתית וממש — יש הצלחות שאינן ב-B (למשל: הטוב ביותר במקום 3 בעוד השני-הכי-טוב במקום 4) — ולכן החסם $\frac{1}{4}$ אינו הדוק, אבל הוא זול מאוד להוכחה.

דוגמה 3: מעקב מלא אחר Freivalds, כולל מקרה שבו החסם $\frac{1}{2}$ הדוק

ניקח

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \text{so } A \cdot B = \begin{pmatrix} 2 & 1 \\ 4 & 3 \end{pmatrix}.$$

מקרה yes-instance. אם $C = \begin{pmatrix} 2 & 1 \\ 4 & 3 \end{pmatrix}$ אז לכל אחד מארבעת הווקטורים $r \in \{0,1\}^2$ מתקיים $A(Br) = Cr$, והאלגוריתם מקבל. $\Pr[\text{accept}] = 1$, כמובטח.

מקרה no-instance. ניקח $C = \begin{pmatrix} 2 & 1 \\ 4 & 0 \end{pmatrix}$, שנבדל מ-$A \cdot B$ רק באיבר $(2,2)$. אז

$$D = A \cdot B - C = \begin{pmatrix} 0 & 0 \\ 0 & 3 \end{pmatrix}.$$

כאן $D_{11} = 0$, ולכן ה"ללא הגבלת הכלליות" של ההוכחה מחייב לבחור את האיבר הלא-אפסי $D_{22} = 3$ ולהריץ את הטיעון על **השורה השנייה** — בדיוק כפי שנאמר בהקלטה שהיה קורה עם אינדקסים כלליים ([00:45:29]).

נבדוק את ארבעת הווקטורים ידנית:

r	$A(Br)$	Cr	החלטה	נכונות
$(0,0)^\top$	$(0,0)^\top$	$(0,0)^\top$	קבל	**טעות** (false positive)
$(1,0)^\top$	$(2,4)^\top$	$(2,4)^\top$	קבל	**טעות** (false positive)
$(0,1)^\top$	$(1,3)^\top$	$(1,0)^\top$	דחה	נכון
$(1,1)^\top$	$(3,7)^\top$	$(3,4)^\top$	דחה	נכון

לכן $\Pr[\text{accept}] = \frac{2}{4} = \frac{1}{2}$ **בדיוק** — הדוגמה מראה שהחסם של משפט 3 הדוק ואי אפשר לשפרו במקרה הגרוע. ואכן, לפי הניתוח: $(Dr)_2 = 3r_2$, שמתאפס אם ורק אם $r_2 = 0$, ויש $2^{n-1} = 2$ וקטורים כאלה מתוך $2^n = 4$.

מה עושה ההגברה כאן. על אותו קלט, t הרצות בלתי תלויות טועות רק אם בכל ההרצות הוגרל $r_2 = 0$, כלומר בהסתברות $\left(\frac{1}{2}\right)^t = 2^{-t}$ בדיוק — התאמה מושלמת למשפט 5.

דוגמה 4: החשבון הכמותי שמצדיק את כל התרגיל

ניקח $n = 1024$ ו-$t = \log_2 n = 10$:

דטרמיניסטי נאיבי: $n^3 = 1024^3 \approx 1.07 \cdot 10^9$ פעולות, תשובה ודאית.

Freivalds עם $t = 10$: $t \cdot n^2 = 10 \cdot 1024^2 \approx 1.05 \cdot 10^7$ פעולות — חיסכון של פי ≈ 100 — והסתברות טעות $2^{-10} = \frac{1}{1024} \approx 0.1\%$, וגם זו רק לכיוון אחד.

זהו הטיעון המלא לטובת האלגוריתם: מוותרים על ודאות מוחלטת תמורת שיפור של סדר גודל בזמן, ומחיר הוויתור יורד אקספוננציאלית בעוד המחיר בזמן עולה רק ליניארית.

תרגיל (נשאל בכיתה, [01:14:05]) — פתרון מלא

השאלה. מה קורה אם דוגמים r מ-$\{0,1,2\}^n$ במקום מ-$\{0,1\}^n$, והאם זה עדיף?

פתרון. לפי משפט 6, הסתברות הטעות יורדת ל-$\leq \frac{1}{3}$. אבל צריך לספור **ביטים אקראיים**: כל קואורדינטה ב-$\{0,1,2\}$ דורשת שני ביטים, כלומר $2n$ ביטים לעומת n. באותם $2n$ ביטים אפשר במקום זאת להריץ פעמיים את הגרסה הבינארית ולקבל טעות $\leq \frac{1}{4}$, שהיא **טובה יותר** מ-$\frac{1}{3}$ — במחיר של פי שניים בזמן הריצה. מסקנה: מבחינת ניצול ביטים אקראיים, חזרה על האלגוריתם הבינארי עדיפה; מבחינת זמן ריצה, האלפבית הגדול עדיף. אין תשובה אחת נכונה — יש טרייד-אוף.

הערות מהשיעור

[00:00:00] היקף למבחן. בעיית המזכיר "אינה למבחן ואינה חלק מהחומר של הקורס" — המרצה מציג אותה כי היא מדגימה בדיוק את העקרונות שיחזרו בכל השיעור: הקלט הגרוע ביותר, האויב האכזר, מה אקראי ומה שרירותי, ומהו מרחב המדגם. לעומת זאת, מ-[00:29:45] ואילך ("אלגוריתם שהוא כבר כן חלק מהקורס") החומר הוא חומר מבחן מלא.

[00:08:08] הסדר שבו הדברים נקבעים. "אני מכיר את האלגוריתם שלך כשאני בונה את הקלט, אבל האקראיות נבחרת אחר כך." זו כל הסיבה שאקראיות עוזרת. אם האויב היה רואה גם את המטבעות, לא היה יתרון.

[00:10:47] מאיפה מגיעה האקראיות. סטודנט שאל מה ההבדל בין "המנהלת מראיינת בסדר אקראי" לבין "המועמדים מגיעים בסדר אקראי". התשובה: הבדל מהותי. הקלט מגיע בסדר **שרירותי** ואיננו שולטים בו; רק המנהלת רשאית לערבב. הנחה על התפלגות הקלט היא הנחה שאין לנו זכות להניח.

[00:20:16] מאורעות חייבים להיות פונקציה של האקראיות. "v_1 הוא הטוב ביותר" אינו מאורע אקראי; "$\sigma(1)$ הוא הטוב ביותר" כן. אין משמעות להסתברות של דבר שאינו אקראי. שווה לבדוק את זה לפני כל חישוב הסתברות במבחן.

[00:31:51] למה זה חשוב. שאלת סטודנט "למה צריך את זה?" קיבלה את התשובה המפורשת ביותר בשיעור: "אם אתה שואל אותי מה מכל הקורס לקחת איתך הלאה — זה החלק הזה של אלגוריתמים אקראיים." הנימוק: היום גם זמן ריצה ליניארי עשוי להיות יקר מדי; אם אין תקציב לקרוא את כל הקלט, בהכרח בודקים רק חלק ממנו — ואם בוחרים את המקומות באופן קבוע, יבוא אויב ויקלקל. לכן בוחרים אותם באקראי.

[00:39:29] אזהרה מפני "שיפור" ריק. "להוריד את זמן הריצה זה לא חוכמה — יכולתי גם להגיד: תזרוק מטבע, יצא אפס תחזיר כן, יצא אחד תחזיר לא." העניין אינו בזמן הריצה לבדו אלא בזמן ריצה **יחד עם ערובת נכונות מוכחת**.

[00:46:38] מתודולוגיה של חסמים. "יש לי הרבה יותר כלים לחסום הסתברות מלמעלה מאשר מלמטה. לכן כשאני מנתח אלגוריתם אקראי אני אחסום מלמעלה את הסתברות הכישלון, ומכך אקבל חסם מלמטה על הסתברות ההצלחה." זה מסביר למה כל הניתוח של Freivalds מנוסח על "האלגוריתם מקבל" ולא על "האלגוריתם צודק".

[01:13:29] מבנה קבוע לניתוח. כמעט תמיד מפצלים ל-yes-instance ו-no-instance, כי האלגוריתם עשוי להתנהג אחרת לגמרי בשני המקרים — אבל זהו פיצול **של הקלטים**, לא של הדגימה האקראית.

[01:17:53] ביטים אקראיים עולים כסף. ה- `random` של המחשב אינו אקראי ואפילו לא קרוב לזה; ביטים אקראיים איכותיים ובלתי תלויים הם מוצר שמשלמים עליו. זהו משאב שהניתוח שלנו כלל לא תמחר.

[01:20:34] כמה שגיאה מותרת? אין תשובה מוחלטת: 10% שגיאה בחלוקת עיתונים היא זניחה; 10% שגיאה בניתוח מוח היא בלתי נסבלת. "שערה אחת על הראש זה מעט, שערה אחת במרק זה המון."

[01:21:06] לקראת השיעור הבא. לחזור על תוחלת, ליניאריות התוחלת, ופירוק לאינדיקטורים. השיעור הבא מגדיר את המודל הפורמלי (מכונת טיורינג אקראית) ואת המחלקות; שם ייאמר ([00:40:58] בהקלטה 21) שבעיית וידוא כפל המטריצות שייכת ל-coRP, בדיוק בגלל הטעות החד-צדדית שהוכחנו כאן.

פערים בין הסיכום להקלטה

מקור: ההקלטה, [00:04:56]–[00:09:42]. **הפער:** כל הטיעון שאין אלגוריתם דטרמיניסטי עם ערובה לבעיית המזכיר, כולל טיעון האויב האכזר והניסיון הכושל להגריל את הסף, אינו מופיע בסיכום כלל. **ההכרעה:** נכתב כאן במלואו כמשפט 1, כולל שני מקרי היריב שנאמרו בעל-פה בקיצור.

מקור: ההקלטה, [00:23:52]–[00:26:31]. **הפער:** כל הדיון במרחב המדגם ודוגמת שתי הקוביות אינם בסיכום. **ההכרעה:** נכתבו כהגדרה 2 וכדוגמה 1, כולל הפתרון המספרי $(1/9)$ שלא נאמר בהקלטה.

מקור: ההקלטה, [01:01:40]–[01:04:52]. **הפער:** המושגים confusion matrix, false positive/false negative וטעות חד-צדדית אינם מופיעים בסיכום, אף שהם המצדיקים את כלל ההגברה "קבל רק אם כולם קיבלו". **ההכרעה:** נכתבו כהגדרה 3 וכמסקנה 3.1.

מקור: ההקלטה, [01:14:05]–[01:19:30]. **הפער:** ניתוח האלפבית $\{0,1,2\}$ וחשבון הביטים האקראיים אינם בסיכום. **ההכרעה:** נכתבו כמשפט 6 וכתרגיל בסוף סעיף הדוגמאות; ההוכחה הכללית ל-Σ בגודל k היא הכללה שלנו של הטיעון שנאמר עבור $k=3$ ו-$k=8$.

מקור: עמוד 1 בסיכום. **הפער:** האות V מופיעה בשלוש משמעויות — קבוצת המועמדים ($V = [1,\dots,n]$), ערכי המועמדים (V_i), והסף המקסימלי בשלב 3. **ההכרעה:** הופרדו כאן ל-$[n]$ (המועמדים), v_i (הערכים) ו-V (הסף). זהו תיקון סימון, לא תיקון מתמטי.

מקור: עמוד 1 בסיכום, שלב 4. **הפער:** נכתב "אם $\sigma[j] > V$" — השוואה בין **אינדקס** לבין **ערך**. **ההכרעה:** הכוונה ברורה מן ההקשר ומההקלטה ([00:16:03]) והתנאי נכתב כאן $v_{\sigma(j)} > V$.

מקור: עמוד 1 בסיכום. **הפער:** לא נאמר ש-n זוגי (אחרת $\frac{n}{2}$ אינו שלם) ולא שהערכים שונים זה מזה (אחרת "המועמד הטוב ביותר" ו"השני הכי טוב" אינם מוגדרים היטב, וההכלה $B \subseteq A$ עלולה להיכשל). **ההכרעה:** שתי ההנחות נוספו במפורש בהגדרה 4 ובמשפט 2.

מקור: ההקלטה, [00:51:55]. **הפער:** על הלוח נכתב לרגע $\sum_j D_{1j} r_1$ (עם r_1 בתוך הסכום); סטודנטית תיקנה והמרצה אישר "טעיתי". הסיכום כותב נכון $\sum_j D_{1j} r_j$. **ההכרעה:** הסיכום נכון ומופיע כאן; מדובר בפליטת לוח רגעית ולא בפער אמיתי.

מקור: עמוד 3 בסיכום. **הפער:** $t = \log n$ נרשם ללא ציון בסיס. **ההכרעה:** פורש כ-$\log_2$, שכן רק כך $2^{-t} = 1/n$ כפי שרשום מיד אחריו ונאמר ב-[01:14:46].

מקור: משימת הכתיבה מול שני המקורות. **הפער:** ההבחנה Las Vegas מול Monte Carlo אינה מופיעה בשום מקום בסיכום או בשתי ההקלטות. **ההכרעה:** נכתבה כהערת מינוח מסומנת בלבד, בתוך הגדרה 1, כדי לא לייחס לקורס מונחים שלא נאמרו בו.

מקור: הסיכום וההקלטה מול המוסכמות של הסדרה. **הפער:** שני המקורות מדברים על "האלגוריתם" ולא על שפות ומחלקות, ולכן אין בשיעור הזה שמות מחלקות או רביעיית מכונה. **ההכרעה:** שמות המחלקות שכן מוזכרים בהפניות קדימה (P, RP, coRP, BPP) נכתבים לפי מוסכמת הסדרה, ולשפת וידוא כפל המטריצות ניתן כאן השם MATMUL שאינו מופיע במקורות. סימוני המשתנים (σ, V, r, D) נלקחו מהסיכום.

מקור: שם קובץ ההקלטה. **הפער:** הקובץ מתויג "שיעור 14" בעוד תוכנו הוא בדיוק שיעור 15 בסיכומים; ההקלטה שמתאימה לשיעור 14 (השיעור השני על קירוב) חסרה. **ההכרעה:** התיוג התעלם ממנו; ההקלטה מכסה את שלושת עמודי הסיכום מתחילתה ועד סופה, ואינה פותחת בחזרה על

חומר הקירוב.

סיכום ונקודות למבחן

מה חייבים לזכור.

על מה ההסתברות. בכל טענה על אלגוריתם אקראי, ההסתברות היא על **המטבעות של האלגוריתם בלבד**, לקלט **קבוע ושרירותי**, והערובה נדרשת **לכל** קלט. "בהסתברות $\geq \frac{1}{4}$" פירושו: לכל קלט, לפחות רבע מהגרלות σ מובילות להצלחה. זה **לא** אומר "לרבע מהקלטים", ו**לא** אומר משהו על קלט אקראי.

בעיית המזכיר: דטרמיניסטית אין ערובה כלל; אקראית — הצלחה בהסתברות $\geq \frac{n}{4(n-1)} > \frac{1}{4}$, עם הסף $\frac{n}{2}$. הסף $\frac{n}{e}$ נותן $\frac{1}{e}$ וזה אופטימלי.

Freivalds: $O(n^2)$; אם $AB = C$ מקבל בהסתברות 1; אם $AB \neq C$ מקבל בהסתברות $\leq \frac{1}{2}$. טעות חד-צדדית.

הגברה: t הרצות בלתי תלויות $\Rightarrow$ שגיאה $\leq 2^{-t}$ בזמן $O(t \cdot n^2)$. $t = \log n$ שגיאה $\leq 1/n$.

המלכודות הסטנדרטיות.

מלכודת מרחב המדגם. לזהות את Ω עם קבוצת הפלטים במקום עם תוצאות הניסוי. בבעיית המזכיר $|\Omega| = n!$, לא n.

מלכודת "הסתברות שהאלגוריתם צודק". אסור לכתוב ביטוי כזה בלי לפצל קודם לפי סוג הקלט; הפיצול הוא **מחוץ** להסתברות, כי הקלט אינו אקראי.

מלכודת "לכל היותר אחד". בספירה של משפט 3, לכל קביעת $r_2, \ldots, r_n$ יש **לכל היותר** ערך אחד תקין ל-r_1 — ולא בהכרח בדיוק אחד, כי הערך המבוקש עלול כלל לא להיות ב-$\{0,1\}$. כתיבת "בדיוק אחד" היא טעות (אם כי במקרה הזה היא לא מקלקלת את החסם, כי אנחנו חוסמים מלמעלה).

מלכודת ה-WLOG. מותר לקבוע ש-$D_{11} \neq 0$ בתוך חישוב הסתברות **רק** משום ש-D קבועה ואינה תלויה ב-r. אילו D הייתה אקראית, "ללא הגבלת הכלליות" היה טיעון פסול.

מלכודת ההגברה. הכלל "קבל רק אם כל ההרצות קיבלו" נכון **רק** כשהטעות חד-צדדית מסוג false positive. עם טעות דו-צדדית הוא הורס את צד ה-yes-instance, וצריך הצבעת רוב.

מלכודת מאורע לא אקראי. לא לדבר על הסתברות של מאורע שאינו פונקציה של האקראיות.

צ'ק-ליסט: אחרי השיעור צריך לדעת

לנסח מהו אלגוריתם אקראי ולציין במדויק, לגבי כל טענה, על מה נלקחת ההסתברות ולאילו קלטים היא תקפה.

לזהות את מרחב המדגם של אלגוריתם אקראי נתון ולחשב בו הסתברות בספירה קומבינטורית.

לבנות טיעון אויב שמראה שאלגוריתם דטרמיניסטי נכשל, ולהסביר מדוע האקראיות שוברת אותו.

לכתוב את אלגוריתם Freivalds, לנמק את זמן הריצה $O(n^2)$ דרך האסוציאטיביות, ולשחזר את שרשרת החסמים $\Pr[Dr = 0] \leq \Pr[(Dr)_1 = 0] \leq 2^{n-1}/2^n = \frac{1}{2}$ על כל צעדיה.

לחשב את הסתברות הטעות אחרי t חזרות בלתי תלויות, ולבחור t שמשיג יעד שגיאה נתון (למשל $1/n$ או $1/n^c$).

להסביר מה טעות חד-צדדית, למה היא הופכת את ההגברה לטריוויאלית, ומה משתנה בלעדיה.

שאלות שנשארו פתוחות

המונחים Las Vegas ו-Monte Carlo אינם מופיעים כלל לא בסיכום ולא בשתי ההקלטות; ההבחנה ביניהם נכתבה כאן כהערת מינוח בלבד ומסומנת ככזו.

עמוד 1 בסיכום: האות V משמשת גם לקבוצת המועמדים ($V=[1,\dots,n]$), גם לסף המקסימלי בשלב 3 וגם לערכי המועמדים (V_i); כאן הופרדו הסימונים ($[n]$, v_i, V).

עמוד 1 בסיכום: לא נאמר במפורש ש-n זוגי ושערכי המועמדים שונים זה מזה; שתי ההנחות נדרשות לניסוח האלגוריתם ולהוכחה, ונוספו כאן.

עמוד 3 בסיכום: $t=\log n$ נרשם ללא בסיס; פורש כבסיס 2, שכן רק כך מתקבל $1/n={t-}^2$ כמצוין בסיכום ובהקלטה [01:14:46].

בסיכום ובהקלטה בעיית וידוא כפל המטריצות אינה מקבלת שם פורמלי של שפה; הסימון MATMUL כאן הוא תוספת שלנו לצורך הפניה.

ההקלטה [00:12:54] מזכירה שהסף האופטימלי הוא n/e ונותן הסתברות $1/e$, ושזה חסם עליון הדוק; ההוכחה לאופטימליות לא נאמרה ואינה נכתבת כאן.

16 מכונות טיורינג אקראיות — הגדרה פורמלית, ומחלקות הסיבוכיות RP, coRP ו-BPP

מגדירים פורמלית את מודל החישוב האקראי בשתי צורות שקולות, מגדירים דרכו את משפחת המחלקות $\mathrm{BPP}(\alpha,\beta)$ ואת $\mathrm{RP},\mathrm{coRP},\mathrm{BPP}$, ומוכיחים $\mathrm{RP}\subseteq\mathrm{NP}$, $\mathrm{BPP}\subseteq\mathrm{PSPACE}$ ואת העצמת ההסתברות בטעות חד-צדדית.

ביטחון: high

בקצרה

עד עכשיו האקראיות בקורס הייתה **תכונה של אלגוריתם** ("נדגום וקטור באקראי"), ולא של מודל חישוב. השיעור הזה סוגר את הפער ומגדיר **מכונת טיורינג אקראית** באופן פורמלי, בשתי צורות שקולות: אקראיות **בתוך** המכונה, או מכונה דטרמיניסטית שקוראת **סרט אקראי** מבחוץ.

ההבחנה המרכזית של השיעור: מכונה אקראית היא מודל **לא דטרמיניסטי** (הקלט אינו קובע ביחידות את הפלט), אבל היא **אינה** מכונה **אי-דטרמיניסטית**. באי-דטרמיניזם המכונה "בוחרת" ואיננו יודעים איך; באקראיות אנחנו יודעים בדיוק איך — הטלת מטבע הוגן. זה כל ההבדל, והוא מהותי.

מגדירים משפחת מחלקות אחת, $\mathrm{BPP}(\alpha,\beta)$, שממנה נגזרות שלוש מחלקות בשמות מוכרים: $\mathrm{BPP}=\mathrm{BPP}(\frac{2}{3},\frac{2}{3})$, $\mathrm{RP}=\mathrm{BPP}(\frac{1}{2},1)$, $\mathrm{coRP}=\mathrm{BPP}(1,\frac{1}{2})$.

ההסתברות היא **תמיד ורק על מטבעות המכונה, עבור כל קלט קבוע בנפרד**. אין כאן שום התפלגות על הקלטים. זו הנקודה שבה נופלים הכי הרבה, ובגללה $\Pr[\text{accept}]$ ו-$\Pr[\text{reject}]$ אינם מאורעות משלימים כשמדובר בקלטים שונים — אבל **כן** משלימים כשהקלט קבוע.

מוכיחים שלוש תוצאות: מונוטוניות ההכלה במשפחה $\mathrm{BPP}(\alpha,\beta)$; $\mathrm{RP}\subseteq\mathrm{NP}$ (המחרוזת האקראית משמשת כ-witness); ו-$\mathrm{BPP}\subseteq\mathrm{PSPACE}$ (מריצים את המכונה על **כל** המחרוזות האקראיות, וסופרים).

מוכיחים את **ההעצמה החד-צדדית**: לכל פולינום q, $\mathrm{RP}=\mathrm{BPP}\left(1-\frac{1}{2^{q(n)}},1\right)$ — ולכן בפרט גם $\mathrm{RP}=\mathrm{BPP}\left(1-\frac{1}{q(n)},1\right)$. הסף $\frac{1}{2}$ בהגדרת RP אינו חלק מהתוכן.

מסדרים סופית את מה שנשאר פתוח בשיעור 15: בעיית וידוא כפל המטריצות (MATMUL) שייכת ל-coRP, וההוכחה היא בדיוק התאמה בין הערבויות של Freivalds לבין ההגדרה של $\mathrm{BPP}(1,\frac{1}{2})$.

רקע ותלויות

מודלים לא דטרמיניסטיים (ראו שיעור 4). מכונת טיורינג אי-דטרמיניסטית היא שישייה $M=(Q,q_{start},F,\Sigma,\Gamma,\delta)$ שבה פונקציית המעברים מחזירה **קבוצה** של אפשרויות, $\delta(q,\alpha)\subseteq Q\times\Gamma\times\{L,R\}$, כך שממצב וקריאה נתונים ייתכנו כמה צעדים המשך. המכונה **מקבלת** את x אם קיימת ריצה מקבלת. חשוב לזכור את השישייה כולה, כולל q_{start} — בלעדיו אין בכלל מושג "הריצה של M על x".

למת הנרמול הבינארי (ראו שיעור 6, משפט 3). לכל מכונה אי-דטרמיניסטית N קיימת מכונה אי-דטרמיניסטית שקולה $\hat{N}$ שבה $|\hat{\delta}(q,\alpha)| \le 2$ לכל q, α, וזמן הריצה גדל רק בפקטור קבוע $2|Q||\Gamma|$. המשמעות: אפשר להניח שבכל צעד ההחלטה היא **בינארית**, ולכן ריצה שלמה מתוארת על ידי **ביט אחד לכל צעד**. זה בדיוק מה שיאפשר לנו להחליף "בחירה" ב"הטלת מטבע הוגן".

ההגדרה השקולה של NP (ראו שיעור 6, משפט 4). $A \in \mathrm{NP}$ אם ורק אם קיימים פולינומים p, q ומכונה **דטרמיניסטית** M כך ש-$\mathrm{time}_M(a) \le p(|a|)$ לכל קלט a, ולכל x $$x \in A \iff \exists\, w \in \{0,1\}^{q(|x|)} \ \text{s.t.}\ M \text{ accepts } (x, w).$$ בכיוון ה-yes יש **קיום** של עד, ובכיוון ה-no יש **לכל** — כל עד נדחה. השלד הזה הוא בדיוק מה שנחפש כשנוכיח $\mathrm{RP} \subseteq \mathrm{NP}$.

אלגוריתמים אקראיים (ראו שיעור 15). שם ראינו שני אלגוריתמים — בעיית המזכיר ואלגוריתם Freivalds לווידוא כפל מטריצות (MATMUL) — אבל, כדברי המרצה בפתיחה, "לא הגדרנו במדויק את המודל... נתנו אלגוריתם ואמרנו שהוא יכול לדגום באקראי" [00:00:00]–[00:01:34]. נזכיר את הערבות שהוכחה שם ונשתמש בה כלשונה: על קלט A, B, C מסדר $n \times n$, האלגוריתם הדוגם $r \in \{0,1\}^n$ באופן אחיד ובודק אם $A \cdot (B \cdot r) = C \cdot r$ רץ בזמן $O(n^2)$ ומקיים
אם $A \cdot B = C$ אז הוא מקבל בהסתברות 1 (למעשה לכל r בלי יוצא מן הכלל);
אם $A \cdot B \neq C$ אז הוא דוחה בהסתברות לפחות $\frac{1}{2}$.
שיעור 15 ציין שהבעיה "שייכת ל-coRP" ודחה את ההצדקה הפורמלית לכאן; משפט 3 להלן הוא ההצדקה.

הכלים ההסתברותיים. מרחב מדגם סופי עם התפלגות אחידה; מונוטוניות ההסתברות; אי-תלות של מאורעות ($\Pr[\bigcap E_i] = \prod \Pr[E_i]$); והתרגום היסודי שהמרצה חזר עליו במפורש [00:51:42]–[00:54:30]: **כשההתפלגות אחידה, הסתברות היא קומבינטוריקה**, כלומר "רצוי חלקי הכול", ולכן $$|\{\text{good outcomes}\}| \;=\; \Pr[\text{good}] \cdot |\Omega|.$$

סגירות הפולינומים. משתמשים בזה לאורך כל הקורס וגם כאן: הפולינומים סגורים לחיבור, לכפל **ולהרכבה**. לכן אם $|r|$ פולינומי ב-$|x|$ אז $|(x,r)|$ פולינומי ב-$|x|$, ומכונה שרצה בזמן פולינומי באורך הקלט שלה רצה בזמן פולינומי ב-$|x|$. המרצה הדגיש שזו תכונה שהפונקציות המעריכיות **אינן** מקיימות [01:19:41].

הגדרות

הגדרה 1: מכונת טיורינג אקראית — המודל הפנימי

ניסוח. מכונת טיורינג אקראית היא שישייה $M = (Q, q_{start}, F, \Sigma, \Gamma, \delta)$ שבה, בהינתן מצב q ותו נקרא α, יש **שתי** אפשרויות לצעד הבא: $\delta(q,\alpha) = \{(q_1,\beta_1,d_1),\ (q_2,\beta_2,d_2)\}$, והבחירה ביניהן נעשית על ידי **הטלת מטבע הוגן** — כל אפשרות בהסתברות $\frac{1}{2}$, בלתי תלוי בכל שאר ההטלות בריצה. אם $|\delta(q,\alpha)| = 1$ הצעד דטרמיניסטי לגמרי.

אינטואיציה, ומדוע דווקא שתיים. מבחינת האובייקט הסינטקטי, זו **בדיוק** מכונת טיורינג אי-דטרמיניסטית מנורמלת של שיעור 6: אותה שישייה, אותו δ רב-ערכי, אותה הנחת בינאריות. מה שהשתנה הוא **כלל הקריאה** של הריצה. באי-דטרמיניזם אמרנו "המכונה בוחרת", ולא אמרנו איך — ולכן דיברנו על **קיום** ריצה מקבלת. כאן אנחנו אומרים בדיוק איך: מטבע הוגן. ולכן אפשר לדבר על

הסתברות שהמכונה מקבלת. ההנחה שיש בדיוק שתי אפשרויות אינה מגבילה בזכות למת הנרמול (שיעור 6, משפט 3), והיא זו שמאפשרת לתאר את כל האקראיות של ריצה באורך t כמחרוזת של t ביטים אחידים ובלתי תלויים.

> **הערה:** בסיכום ובהקלטה [00:04:00]–[00:04:34] ההגדרה נמסרת מילולית — "מכונה שבה יש אפשרות לעבור למצב הבא ממצב נתון על ידי בחירה אקראית או הטלת מטבע" — בלי לרשום שישייה. המרצה עצמו אמר "זה לא מרגיש לגמרי פורמלי, ובצדק" ולא הידק יותר. השישייה כאן נלקחת משיעור 4 לשם אחידות הסדרה.

האזהרה המרכזית של השיעור [00:05:05]–[00:06:43]. יש להבחין בין שני מונחים שקל לבלבל ביניהם:

מודל לא דטרמיניסטי (non-deterministic במובן הרחב) הוא **כל** מודל שבו הקלט אינו קובע ביחידות את הפלט. מכונה אי-דטרמיניסטית היא כזו; מכונה אקראית היא כזו.

מודל אי-דטרמיניסטי (nondeterministic במובן הצר של שיעור 4) הוא מודל **ספציפי** שבו המכונה "מחליטה" ואין לנו שום תיאור של איך.

המרצה הדגיש שהוא נזהר לאורך כל הקורס לומר על מכונה אי-דטרמיניסטית "**תנחש** באופן אי-דטרמיניסטי", ולא "תגריל" — "כי אני יודע איפה טעויות הולכות לקרות" [00:14:42]. במכונה אקראית מותר ורצוי לומר תגריל, תדגום, תטיל מטבע. סטודנט שאל אם אפשר לקרוא למודל האקראי "מודל אי-דטרמיניסטי עם בחירה אקראית", והמרצה השיב שזה "לא שגוי לגמרי, אבל זה ייצור בלבול — תשמור מרחק בין שני המודלים" [00:14:09]–[00:15:12].

מופע. האלגוריתם של Freivalds משיעור 15, כשמממשים אותו כמכונה: בכל אחד מ-n הצעדים שבהם נבחרת קואורדינטה של הווקטור r, המכונה מטילה מטבע.

אי-מופע. המכונה האי-דטרמיניסטית של שיעור 6 שמכריעה את SAT על ידי ניחוש השמה **אינה** מכונה אקראית — לא כי המבנה שלה שונה, אלא כי המשמעות שאנחנו נותנים ל-δ רב-ערכי שונה. אם נקרא אותה כמכונה אקראית, היא כבר לא מכריעה את SAT: על נוסחה ספיקה עם השמה מספקת יחידה מתוך 2^n, ההסתברות שהיא תקבל היא 2^{-n} ולא 1.

הגדרה 2: מכונת טיורינג אקראית — מודל הסרט האקראי

ניסוח. מכונת טיורינג אקראית היא מכונה **דו-סרטית** M שבה:

סרט 1 הוא סרט עבודה רגיל (עליו מגיע הקלט, ועליו המכונה קוראת וכותבת חופשית);

סרט 2 מכיל מחרוזת **אינסופית** של ביטים; המכונה יכולה רק **לקרוא** ממנו, ולא לכתוב, והראש עליו זז **רק ימינה**;

סרט 2 נקרא **הסרט האקראי**.

המכונה עצמה **דטרמיניסטית לחלוטין**: ברגע שקבענו את x ואת תוכן הסרט האקראי, כל הריצה נקבעת.

אינטואיציה. חשבו על הסרט השני כעל אינסוף הטלות מטבע שמישהו הטיל מראש והניח לפנינו [00:07:50]. המכונה "מתייעצת" איתו. שימו לב שהמרצה הדגיש: הסרט הזה **אינו באמת אקראי** — הוא מגיע מבחוץ, ואיננו יודעים מאיפה. הוא נקרא "אקראי" רק כי **בניתוח** נשאל: אילו התוכן שלו היה נבחר באקראי אחיד, מה ההסתברות שהמכונה צודקת? [00:12:04], [00:13:38].

חשבון זמן ומקום. למרות שהמכונה דו-סרטית, אין צורך בתרגום "דו-סרטי לחד-סרטי": הסרט השני מוגבל מאוד — קריאה בלבד, תנועה ימינה בלבד — ולכן כל צעד קורא לכל היותר ביט אחד ממנו, וזמן הריצה אינו מושפע [00:08:54]. המרצה תיאר את המכונה כ"חצי דו-סרטית".

הצורה שנשתמש בה. אם המכונה רצה בזמן פולינומי, היא קוראת לכל היותר פולינום ביטים מהסרט האקראי (קריאת ביט עולה צעד). לכן נסמן: קיים פולינום p כך שבריצה על x המכונה קוראת לכל היותר $p(|x|)$ ביטים, נסמן אותם $r \in \{0,1\}^{p(|x|)}$, ונכתוב $M(x,r)$. שאר הביטים על הסרט אינם משפיעים כלל, ולכן אפשר להגריל רק את $p(|x|)$ הראשונים [00:27:17].

מתי משתמשים בכל מודל — זו נקודת המפתח של השיעור.

מודל 1 (אקראיות בפנים) נוח כשרוצים **להציג אלגוריתם** ולהראות תוצאה חיובית. "זה מודל שיותר נוח לתכנת בו, פשוט ככה" [00:10:57].

מודל 2 (סרט אקראי, מכונה דטרמיניסטית) נוח כשרוצים **לדבר על קשר בין מחלקות** — למשל להראות שמחלקה אקראית מוכלת במחלקה דטרמיניסטית. "תמיד נוח לי לעבוד עם מכונות דטרמיניסטיות... המעברים הרבה יותר קלים כשהמכונה היא מראש דטרמיניסטית" [00:11:28]–[00:13:07].

בקורס לא מוכיחים את שקילות שני המודלים [00:10:26]; היא מונחת. אנחנו נשתמש בכל אחד מהם היכן שנוח, בדיוק כפי שנעשה בשיעור עם NP מול NP' (ראו שיעור 6) — וזו הייתה ההקבלה המפורשת שהמרצה בנה עליה את כל המבנה [00:02:22]–[00:02:55].

הגדרה 3: משפחת המחלקות $\mathrm{BPP}(\alpha,\beta)$

יהיו $\alpha,\beta \in [0,1]$. המחלקה $\mathrm{BPP}(\alpha,\beta)$ היא קבוצת השפות A עבורן מתקיים אחד משני התנאים השקולים הבאים.

נוסח א (מכונה אקראית). קיימת מכונת טיורינג **אקראית** M הרצה בזמן פולינומי בגודל הקלט, כך שלכל x: $x \notin A \implies \Pr\left[M \text{ rejects } x\right] \geq \beta$ $\quad x \in A \implies \Pr\left[M \text{ accepts } x\right] \geq \alpha$.

נוסח ב (מכונה דטרמיניסטית וסרט אקראי). קיימת מכונת טיורינג **דטרמיניסטית** M הרצה בזמן פולינומי בגודל הקלט, וקיים פולינום p, כך שלכל x בריצתה על x המכונה M קוראת לכל היותר $p(|x|)$ ביטים מהסרט האקראי, ומתקיים

$$x \in A \implies \Pr_{r\in\{0,1\}^{p(|x|)}}\left[M \text{ accepts } (x,r)\right] \geq \alpha,$$
$$x \notin A \implies \Pr_{r\in\{0,1\}^{p(|x|)}}\left[M \text{ rejects } (x,r)\right] \geq \beta.$$

מרחב ההסתברות — לקרוא לאט. בנוסח א האקראיות היא **המטבעות שהמכונה מטילה**; בנוסח ב היא **המחרוזת** r, הנדגמת אחידה מתוך $\{0,1\}^{p(|x|)}$. בשני המקרים:

$$\Omega = \Omega(x) = \{0,1\}^{p(|x|)}, \qquad |\Omega| = 2^{p(|x|)}.$$

הקלט x **אינו** חלק מהניסוי האקראי. הוא נתון, שרירותי, ואפשר לחשוב עליו כעל הקלט הגרוע ביותר. המרצה חזר על זה כלל אצבע: "תמיד כשאתם מחשבים הסתברות, שאלו את עצמכם מה האקראי פה. מאיפה האקראיות? זה הדבר הראשון שאני בודק" [00:25:13].

המסקנה החשובה מכך (שאלת סטודנטית, [00:21:01] ו-[00:29:23]). אסור לחשוב על "$x \in A$" ועל "$x \notin A$" כעל **מאורעות משלימים**, ואסור לצפות ש-$\alpha+\beta$ יסתכם ל-1. אלה שני **תרחישים** שונים לגמרי, עם שני קלטים שונים, ולכן עם שני מרחבי מדגם שונים — ואם $p(|x_1|) \neq p(|x_2|)$ אז

אפילו גודל מרחב המדגם שונה. אבל — וזה הצד השני של אותו מטבע — **ברגע שקיבענו x אחד**, המאורעות "M מקבלת את (x,r)" ו-"M דוחה את (x,r)" הם כן מאורעות משלימים באותו מרחב, כי המכונה דטרמיניסטית ועוצרת, ולכן $\Pr_r\left[M \text{ accepts } (x,r)\right] = 1 - \Pr_r\left[M \text{ rejects } (x,r)\right]$. בהוכחת משפט 4 נשתמש בעובדה הזו במפורש, ובדיוק שם היא נחוצה [01:23:54]–[01:24:56].

איך לזכור את ההגדרה. "אני תמיד בודק מה ההסתברות שהמכונה **צודקת**, ואני רוצה לחסום אותה **מלמטה**" [00:28:51]. על yes-instance להיות צודק פירושו לקבל; על no-instance פירושו לדחות. לכן שני התנאים נראים שונים אך אומרים אותו דבר.

מופע. $A = \emptyset$ שייכת ל-$\mathrm{BPP}(\alpha, 1)$ לכל α: המכונה "דחה תמיד" עונה על התנאי השני בשוויון 1, והתנאי הראשון ריק.

אי-מופע מאלף. $\mathrm{BPP}(\frac{1}{2}, \frac{1}{2})$ מכילה **כל** שפה: המכונה שמטילה מטבע אחד ומקבלת על "עץ" מקיימת את שני התנאים בשוויון עבור כל A, בלי להסתכל בכלל בקלט. כלומר סף של בדיוק $\frac{1}{2}$ בשני הצדדים הוא חסר תוכן לחלוטין. באותו אופן $\mathrm{BPP}(0, 1)$ מכילה כל שפה (המכונה "דחה תמיד"), ו-$\mathrm{BPP}(1, 0)$ מכילה כל שפה (המכונה "קבל תמיד"). לכן הערכים בסוגריים אינם קישוט: הם כל התוכן.

הגדרה 4: המחלקות בשמותיהן, והסף המדויק בכל אחת

$$\boxed{\mathrm{BPP} = \mathrm{BPP}\left(\tfrac{2}{3}, \tfrac{2}{3}\right), \qquad \mathrm{RP} = \mathrm{BPP}\left(\tfrac{1}{2}, 1\right), \qquad \mathrm{coRP} = \mathrm{BPP}\left(1, \tfrac{1}{2}\right)}$$

נפרט כל אחת: הכמתים המדויקים, מדוע דווקא הקבוע הזה, ומה נשבר בקבוע אחר.

BPP — טעות דו-צדדית (bounded-error probabilistic polynomial time). קיימת מכונה אקראית פולינומית M כך ש**לכל** x: אם $x \in A$ אז $\Pr[\text{accept}] \geq \frac{2}{3}$, ואם $x \notin A$ אז $\Pr[\text{reject}] \geq \frac{2}{3}$. הטעות אפשרית **משני הכיוונים**, ולכן שום תשובה יחידה של המכונה אינה אמינה במאת האחוזים. הפירוש של השם, כפי שהמרצה שחזר אותו בכיתה [00:42:01]: ה-P הראשונה — probabilistic, השנייה — polynomial, וה-B — bounded, כי הסתברות הטעות חסומה **משני הכיוונים**.

למה $\frac{2}{3}$? משום ש**כל** קבוע בין $\frac{1}{2}$ ל-1 נותן את אותה מחלקה בדיוק — זה בדיוק תוכנו של שיעור 17 — ולכן בוחרים ערך נוח לכתיבה. *מה נשבר בערך אחר?* אם מורידים ל-$\frac{1}{2}$ בדיוק מקבלים את המחלקה חסרת התוכן שראינו לעיל, שמכילה כל שפה. אם מעלים ל-1 מקבלים את P (מכונה שצודקת בהסתברות 1 על מרחב מדגם סופי צודקת לכל r, ואפשר להריץ אותה עם $r = 0^{p(|x|)}$). ואם מסתפקים בפער אקספוננציאלית קטן, $\frac{1}{2} + \frac{1}{2^{q(n)}}$, לא ידוע שההעצמה עובדת.

RP — טעות חד-צדדית, הצד ה"בטוח" הוא ה-no. קיימת מכונה אקראית פולינומית M כך שלכל x: אם $x \in A$ אז $\Pr[\text{accept}] \geq \frac{1}{2}$; ואם $x \notin A$ אז $\Pr[\text{reject}] \geq 1$, כלומר **שווה** 1, כלומר לכל r בלי יוצא מן הכלל המכונה דוחה. במילים: **אין תשובות "כן" שגויות**. אם המכונה אמרה "כן" — $x \in A$ בוודאות; אם אמרה "לא" — ייתכן שהיא טועה, בהסתברות עד $\frac{1}{2}$.

למה $\frac{1}{2}$? אותה סיבה — משפט 5 להלן מראה שאפשר להעלות עד $1 - \frac{1}{2^{q(n)}}$, ושיעור 17 מראה שאפשר גם להתחיל מ-$\frac{1}{q(n)}$ זעיר. *מה נשבר בערך אחר?* $\alpha = 0$ הורס הכול: $\mathrm{BPP}(0, 1)$ מכילה כל שפה. לעומת זאת אסור לוותר על ה-1 בצד ה-no — זה מה שהופך את המחלקה לחד-צדדית, וזה מה

שמאפשר את כל ההעצמות הפשוטות.

coRP — טעות חד-צדדית, הצד ה"בטוח" הוא ה-yes. לכל x: אם $x \in A$ אז $\Pr[\text{accept}] = 1$; אם $x \notin A$ אז $\Pr[\text{reject}] \geq \frac{1}{2}$. **אין תשובות "לא" שגויות**. שקול לכך ש-$\overline{A} \in \mathrm{RP}$, ומכאן השם.

אזהרה על השם "co" [00:42:34]–[00:43:40]. coRP **אינה** המשלימה של RP כקבוצת שפות; היא **קבוצת המשלימות** של שפות ב-RP. שתי המחלקות אינן זרות (כל שפה ב-P שייכת לשתיהן) ואינן ממצות את הכול. סטודנט ביקש דוגמה לשפה שבוודאות אינה ב-RP, והתשובה: בעיית העצירה — כי כל המחלקות שאנחנו מסתכלים עליהן כאן מורכבות משפות כריעות, ובעיית העצירה אינה כריעה.

למה דווקא ה-yes קיבל את הצד ה"לא ודאי" ב-RP? [00:58:48]–[01:00:24]. סטודנט שאל, והמרצה נתן תשובה מבנית: זו אותה חוסר-סימטריה שכבר הייתה ב-NP. שם $x \in A$ פירושו **קיים** עד, ו-$x \notin A$ פירושו **שלכל** עד המכונה דוחה. הבעיות הקומבינטוריות "המעניינות" מנוסחות היסטורית עם קיום (קיימת השמה מספקת, קיימת קליקה בגודל k), ולכן המחלקות נבנו סביב הצורה הזו, ו-RP ירשה את המבנה. משפט 2 להלן מראה שההקבלה אינה רק אסתטית — היא הוכחה.

משפטים והוכחות

משפט 1: מונוטוניות במשפחה $\mathrm{BPP}(\alpha, \beta)$

ניסוח. יהיו $\alpha, \beta, \hat{\alpha}, \hat{\beta} \in [0,1]$ ונניח $\hat{\alpha} \geq \alpha$ וגם $\hat{\beta} \geq \beta$. אזי $\mathrm{BPP}(\hat{\alpha}, \hat{\beta}) \subseteq \mathrm{BPP}(\alpha, \beta)$.

הוכחה. תהא $A \in \mathrm{BPP}(\hat{\alpha}, \hat{\beta})$. לפי נוסח א של הגדרה 3, קיימת מכונה אקראית M הרצה בזמן פולינומי בגודל הקלט כך שלכל x: $x \in A \implies \Pr[M \text{ accepts } x] \geq \hat{\alpha}$, ו$x \notin A \implies \Pr[M \text{ rejects } x] \geq \hat{\beta}$. נתבונן ב-$M$ עצמה — לא בונים דבר. M רצה בזמן פולינומי, וזה כל מה שנדרש מבחינת המשאב. יהי x קלט כלשהו. *מקרה $x \in A$:* $\Pr[M \text{ accepts } x] \geq \hat{\alpha} \geq \alpha$. *מקרה $x \notin A$:* $\Pr[M \text{ rejects } x] \geq \hat{\beta} \geq \beta$. בשני המקרים התנאי של $\mathrm{BPP}(\alpha, \beta)$ מתקיים עם אותה מכונה, ולכן $A \in \mathrm{BPP}(\alpha, \beta)$. ■

איך לזכור את כיוון ההכלה [01:34:25]. המרצה הדגיש שהוא לעולם אינו זוכר בעל פה מי מוכל במי, אלא שואל: **לאן קשה יותר להיכנס?** דרישת הצלחה גדולה יותר היא דרישה חמורה יותר, ולכן היא מגדירה מחלקה **מצומצמת** יותר, שמוכלת במחלקה עם הדרישה הרפויה. זה בדיוק מה שמאפשר לקבל "חינם" את הכיוון הקל בכל אחת משתי טענות ההעצמה.

שימוש מיידי. $\mathrm{RP} = \mathrm{BPP}(\frac{1}{2}, 1) \subseteq \mathrm{BPP}(\frac{1}{2}, \frac{1}{2})$ ו-$\mathrm{coRP} \subseteq \mathrm{BPP}(\frac{1}{2}, \frac{1}{2})$ — אך זו הכלה חסרת ערך, כי אגף ימין הוא כל השפות. לעומת זאת $\mathrm{RP} \subseteq \mathrm{BPP}(\frac{1}{2}, \frac{2}{3})$ **אינה** נובעת מהמשפט (הכיוון הפוך), ואכן היא אינה טענה טריוויאלית.

משפט 2: $\mathrm{RP} \subseteq \mathrm{NP}$

ניסוח. כל שפה ב-RP שייכת ל-NP.

מדוע ההוכחה בנויה כך. אנחנו רוצים לסיים עם השלד של NP' (שיעור 6): מכונה **דטרמיניסטית** שמקבלת זוג (x, w), כמת קיום בכיוון אחד וכמת "לכל" בכיוון השני. לכן כדאי להתחיל כבר עם **נוסח ב** של הגדרה 3 — המכונה שם דטרמיניסטית ומקבלת זוג (x, r), כלומר בדיוק אותו ממשק. "לעבור

מאקראית לאי-דטרמיניסטית — אני לא בטוח; אבל אם אני עובד עם מכונה דטרמיניסטית פה ומכונה דטרמיניסטית שם, לפחות את המכונות אני יודע איך להתאים" [00:45:10]–[00:45:42]. זה לקח מתודי כללי בשיעור: **בוחרים את הנוסח לפי הממשק שאליו רוצים להגיע.**

הוכחה. תהא $A \in \mathrm{RP} = \mathrm{BPP}(\frac{1}{2}, 1)$. לפי נוסח ב קיימת מכונה **דטרמיניסטית** M הרצה בזמן פולינומי בגודל הקלט וקיים פולינום p כך שלכל x:

$$\begin{aligned} x \in A &\implies \Pr_{r \in \{0,1\}^{p(|x|)}}\left[M \text{ accepts } (x, r)\right] \geq \tfrac{1}{2}, \\ x \notin A &\implies \Pr_{r \in \{0,1\}^{p(|x|)}}\left[M \text{ rejects } (x, r)\right] \geq 1. \end{aligned}$$

נתבונן ב-M; היא כבר מכונה דטרמיניסטית פולינומית המקבלת זוג, ולא נבנה מכונה חדשה. יהי x קלט.

מקרה $x \in A$. מרחב המדגם $\{0,1\}^{p(|x|)}$ סופי והתפלגותו אחידה, ולכן הסתברות היא "רצוי חלקי הכול". נבודד את המונה: $\left|\left\{r \in \{0,1\}^{p(|x|)} \;:\; M \text{ accepts } (x,r)\right\}\right|$ $= \Pr_r\left[M \text{ accepts } (x,r)\right] \cdot 2^{p(|x|)} \geq \frac{1}{2} \cdot 2^{p(|x|)} = 2^{p(|x|)-1} \geq 1$. המעבר האחרון דורש $p(|x|) \geq 1$. זה מתקיים לכל x ארוך מספיק, שכן p פולינום שאינו זהותית אפס ולכן שואף לאינסוף; ומספר הקלטים x שעבורם $p(|x|) < 1$ הוא **סופי**, ואפשר לצרוב את התשובות עליהם בטבלה בתוך המכונה [00:57:44]–[00:58:16]. לכן קיים r שעבורו M מקבלת את (x, r).

מקרה $x \notin A$. הסתברות הדחייה היא 1, ומכיוון שמרחב המדגם סופי ואחיד פירוש הדבר שהמאורע הוא כל המרחב: $\left|\left\{r \in \{0,1\}^{p(|x|)} \;:\; M \text{ rejects } (x,r)\right\}\right| = 2^{p(|x|)}$, כלומר **לכל** $r \in \{0,1\}^{p(|x|)}$ המכונה M דוחה את (x, r).

חיברנו: קיימת מכונה דטרמיניסטית M הרצה בזמן פולינומי, וקיים פולינום p, כך שלכל x $A \iff \exists r \in \{0,1\}^{p(|x|)} \text{ s.t. } M \text{ accepts } (x, r)$, וזו בדיוק ההגדרה של NP' (שיעור 6, הגדרה 1), שהיא לפי משפט 4 שם שקולה ל-NP. לכן $A \in \mathrm{NP}$. ■

> **הערה:** בהרצאה זה נאמר בקיצור — "לכן קיים r" — והמרצה **עצר במכוון** וביקש לעבור דרך שלב הספירה [00:50:59]–[00:54:30], כדי להדגיש שההסתברות מתורגמת לקומבינטוריקה. גם הטיפול ב-x-ים הקצרים נאמר רק בעל פה בתשובה לשאלה; הפירוט כאן.

מה תופס את מקומו של מה. המרצה שאל את הכיתה ישירות [00:55:00]: "ה-r הזה תופס את התפקיד של מי?" התשובה — של ה-**witness**. המחרוזת האקראית ב-RP היא בדיוק העד ב-NP: היא מגיעה מבחוץ, אורכה פולינומי, והמכונה רק **מאמתת** בעזרתה. ההבדל היחיד הוא שב-NP די בכך ש**קיים** עד אחד, ואילו ב-RP נדרש שלפחות **מחצית** מהמחרוזות יהיו עדים. זו דרישה חזקה **יותר**, ולכן ההכלה היא בכיוון הזה ולא בהפוך.

מסקנה 2.1. $\mathrm{coRP} \subseteq \mathrm{coNP}$. אכן, $A \in \mathrm{coRP}$ פירושו $\overline{A} \in \mathrm{RP} \subseteq \mathrm{NP}$, ולכן $A \in \mathrm{coNP}$ לפי ההגדרה של coNP.

משפט 3: $\mathrm{MATMUL} \in \mathrm{coRP}$

ניסוח. תהא $\mathrm{MATMUL} = \{\langle A, B, C\rangle \;:\; A, B, C \text{ are } n \times n \text{ matrices and } A \cdot B = C\}$. אזי $\mathrm{MATMUL} \in \mathrm{coRP}$.

הוכחה. לפי הגדרה 4, $\mathrm{coRP} = \mathrm{BPP}(1, \frac{1}{2})$, ולכן צריך מכונה אקראית פולינומית שמקבלת כל yes-instance בהסתברות 1 ודוחה כל no-instance בהסתברות לפחות $\frac{1}{2}$.

ניקח את אלגוריתם Freivalds של שיעור 15 ונכתוב אותו בנוסח ב. תהא M המכונה הדטרמיניסטית שעל קלט $\langle A, B, C\rangle$ ומחרוזת אקראית r:

קוראת n ביטים מהמחרוזת האקראית ומפרשת אותם כווקטור $r \in \{0,1\}^n$;

מחשבת $A \cdot (B \cdot r)$ ואת $C \cdot r$;

מקבלת אם שני הווקטורים שווים, ודוחה אחרת.

הפולינום של הביטים. $p(|x|) = n$. הקלט $x = \langle A, B, C\rangle$ מקודד $3n^2$ ערכים, ולכן $n \le |x|$, ובפרט p פולינום ב-$|x|$ כנדרש.

זמן הריצה. שיעור 15, משפט 3: $O(n^2)$ פעולות אריתמטיות, ולכן פולינומי ב-$|x|$.

תנאי ה-yes ($\alpha = 1$). אם $\langle A, B, C\rangle \in \mathrm{MATMUL}$, כלומר $A \cdot B = C$, אז לפי האסוציאטיביות לכל r **בלי יוצא מן הכלל** $A \cdot (B \cdot r) = (A \cdot B) \cdot r = C \cdot r$, ולכן M מקבלת. המאורע הוא כל מרחב המדגם, ולכן $\Pr_r[M \text{ accepts } (x, r)] = 1 \ge \alpha = 1$.

תנאי ה-no ($\beta = \frac{1}{2}$). אם $A \cdot B \neq C$, שיעור 15 משפט 3 נותן $\Pr_r[M \text{ accepts } (x, r)] \le \frac{1}{2}$. מכיוון שהקלט x **קבוע**, המאורעות "מקבלת" ו"דוחה" משלימים באותו מרחב מדגם, ולכן שני התנאים מתקיימים, ולכן $\mathrm{MATMUL} \in \mathrm{BPP}(1, \frac{1}{2}) = \mathrm{coRP}$. ■

> **הערה:** בהקלטה [00:41:30] המרצה רק שאל את הכיתה "כפל מטריצות — לאן היא שייכת?", קיבל את התשובה "coRP", ונימק במשפט: "אם היה yes-instance תמיד החזרתי כן, ואם לא — האלגוריתם צדק בהסתברות לפחות חצי". ההתאמה המלאה לנוסח ב, כולל חשבון הביטים ומעבר המשלים, היא הפירוט כאן.

למה זה coRP ולא RP — מלכודת. התשובה תלויה בשאלה **איך ניסחנו את השפה**. אם היינו מגדירים את השפה כ-$\{\langle A, B, C\rangle : A \cdot B \neq C\}$ היינו מקבלים RP. הכיוון שבו יש ודאות הוא הכיוון שבו האלגוריתם **לא יכול** לטעות, וזה תמיד הכיוון שבו הזהות מתקיימת פוינטווייז.

משפט 4: $\mathrm{BPP} \subseteq \mathrm{PSPACE}$

ניסוח. כל שפה ב-BPP מוכרעת על ידי מכונה דטרמיניסטית במקום פולינומי.

מדוע ההוכחה בנויה כך. כדי להוכיח שייכות ל-PSPACE צריך מכונה דטרמיניסטית ש**מכריעה** את השפה במקום פולינומי — הכרעה רגילה, כמו בחישוביות [01:08:44]. הממשק של מכונה כזו מקבל **רק את** x. לכן שוב מתחילים מנוסח ב, אבל כאן יש קושי נוסף: המכונה שבידינו מקבלת זוג (x, r) והמכונה שנבנה תקבל רק x. סטודנט הציע לשרשר x ואחריו r — והמרצה פסל מיד [01:06:38]: "הקלט שקיבלתי הוא הקלט שאני צריך לבדוק אם הוא שייך; אני לא יכול לשרשר לו שום דבר". הפתרון היחיד הוא **לא להגריל את r בכלל, אלא לעבור על כולם**.

ההוכחה. תהא $A \in \mathrm{BPP} = \mathrm{BPP}(\frac{2}{3}, \frac{2}{3})$. לפי נוסח ב קיימת מכונה דטרמיניסטית M הרצה בזמן פולינומי בגודל הקלט וקיים פולינום p כך שלכל x:

x\notin A\ \Longrightarrow\ \Pr_{r\in\{0,1\}^{p(|x|)}}\big[M \text{ rejects } (x,r)\big]\ \ge\ \tfrac23

$$.$$ נבנה מכונה דטרמיניסטית $\hat M$ שעל קלט x פועלת כך: 1. חשב את $p(|x|)$. אתחל 2.

M על (x,r); 2. אם M קיבלה — $\text{count}\leftarrow \text{count}+1$. 4. אם $\text{count}\ge \tfrac23\cdot 2^{p(|x|)}$ — **קבל**; אחרת — **דחה**. > **הערה:** הסף בשלב 4 אינו בהכרח מספר שלם. המבחן השקול בשלמים הוא $\text{count}\ge \tfrac23\cdot 2^{p(|x|)+1}$, וכך יש לממש אותו; הסיכום כותב את השבר. זו השלמה פורמלית שלנו ואינה משנה דבר בהוכחה. **ניתוח סיבוכיות המקום.** יהי x קלט, ונסמן $n=|x|$. - **שלבים 1 ו-4.** p פונקציה אלמנטרית, ולכן חישובה חסום במקום; שלב 1 דורש $O(p(n))$ תאים ושלב 4 (השוואה בין שני מספרים באורך $O(p(n))$ ביט) דורש $O(p(n))$ תאים. חשוב: את המספר $2^{p(n)}$ כותבים ב**בינארי** ולא באונרי — באונרי הוא היה תופס $2^{p(n)}$ תאים ומהרס את החסם. הטריק הזה כבר נעשה במשפט ההיררכיה (ראו שיעור 3), והמרצה הזכיר אותו במפורש [01:13:03]–[01:13:37]. פעולות הגדלה באחת והשוואה על מספרים בינאריים נעשות במקום ליניארי בייצוג. - **שלב 2.** המונה מגיע לכל היותר ל-$2^{p(n)}$, ולכן בייצוג בינארי הוא תופס $p(n)+1$ תאים. - **שלב 3.** בכל איטרציה שומרים את r, שאורכו $p(n)$ ביט. M רצה בזמן פולינומי באורך הקלט שלה, ומכונה שרצה בזמן t מבקרת לכל היותר t תאים, ולכן היא משתמשת במקום פולינומי באורך הקלט שלה. אורך הקלט הוא $|(x,r)|=n+p(n)$, שהוא פולינומי ב-n (סגירות הפולינומים לחיבור), ולכן — מסגירות הפולינומים ל**הרכבה** — המקום שמשמש להרצה הוא פולינומי ב-n. - **הנקודה המכרעת** [01:11:01]–[01:12:03].** האיטרציות **חוזרות על אותו מקום**. בין שתי איטרציות מוחקים את r ואת כל שטח העבודה של M ומשתמשים בהם מחדש. לכן המקום הכולל של הלולאה הוא המקום של **איטרציה אחת** בלבד, ולא מספר האיטרציות כפול המקום. זהו בדיוק ההבדל בין זמן למקום: בזמן היינו חייבים לכפול במספר האיטרציות, במקום לא. סך הכול $\mathrm{space}_{\hat M}(x)$ פולינומי ב-$|x|$. **ניתוח הזמן — הערה.** זמן הריצה של $\hat M$ הוא $2^{p(n)}$ כפול פולינום, כלומר **מעריכי**. זה בסדר גמור, כי טוענים שייכות ל-PSPACE ולא ל-P. סטודנט שאל אם ההוכחה אינה נותנת גם $\mathrm{BPP}\subseteq\mathrm{P}$, והמרצה השיב בשלילה מפורשת: "אני לא יודע אם BPP מוכלת ב-P או לא — זו בעיה פתוחה" [01:12:33]. **נכונות:** $\hat M$ מכריעה את A.** יהי x; נסמן $N=2^{p(|x|)}$. *מקרה $x\in A$.* לפי ההנחה $\Pr_r[M \text{ accepts } (x,r)]\ge\frac23$. תרגום לספירה: $$\Big|\big\{r\in\{0,1\}^{p(|x|)}: M \text{ accepts } (x,r)\big\}\Big| \;=\; \Pr_r[M \text{ accepts } (x,r)]\cdot N \;\ge\; \tfrac23 N.$$ הלולאה בשלב 3 מגדילה את המונה בדיוק פעם אחת עבור כל r בקבוצה הזו, ולכן בסיום הריצה $\text{count}\ge\frac23 N$, ולכן $\hat M$ **מקבלת** את x. *מקרה $x\notin A$.* לפי ההנחה $\Pr_r[M \text{ rejects } (x,r)]\ge\frac23$. כאן נחוצה הנקודה שהודגשה בהגדרה 3: **הקלט x קבוע**, ולכן שני המאורעות משלימים באותו מרחב מדגם, ומכאן $$\Pr_r\big[M \text{ accepts } (x,r)\big] \;=\; 1-\Pr_r\big[M \text{ rejects } (x,r)\big] \;\le\; 1-\tfrac13 \;=\; \tfrac23.$$ שימו לב שאי-השוויון נשאר **חלש**: זו השלמה של קבוצה, לא שלילה לוגית [01:25:27]–[01:26:31]. לכן $$\text{count} \;=\; \Big|\big\{r: M \text{ accepts } (x,r)\big\}\Big| \;\le\; \tfrac13 N \;<\; \tfrac23 N,$$ כאשר אי-השוויון האחרון **חזק** כי $N=2^{p(|x|)}>0$. התנאי בשלב 4 בודק "האם $\text{count}\ge\frac23N$", ואנחנו הראינו שהוא קטן ממש, כלומר השלילה הלוגית של התנאי מתקיימת, ולכן $\hat M$ **דוחה** את x. $\hat M$

עוצרת תמיד (הלולאה סופית ו-M פולינומית), ולכן היא מכריעה את A במקום פולינומי, כלומר $A\in\mathrm{PSPACE}$. $\blacksquare$ **הערה על ההבדל בין שני סוגי "היפוך" [01:27:35]–[01:29:17].** בהוכחה הופיעו שני מעברים שנראים דומים ואינם: (א) מ-$\Pr[\text{reject}]\ge\frac23$ ל-$\Pr[\text{accept}]\le\frac13$ — זו **השלמה של קבוצה**, ואי-השוויון נשאר חלש; (ב) מ"לא מתקיים $\text{count}\ge\frac23N$" ל-"$\text{count}<\frac23N$" — זו **שלילה לוגית**, ואי-השוויון הופך לחזק. המרצה הקדיש לזה זמן ואמר שאם לא זוכרים — לבדוק על מקרה פרטי: אם $\Pr[\text{reject}]$ היה **שווה** $\frac23$, אז $\Pr[\text{accept}]$ היה שווה $\frac13$, ולכן ההיפוך חייב להשאיר שוויון אפשרי. ### משפט 5: העצמת ההסתברות בטעות חד-צדדית **ניסוח.** יהי q פולינום עם $q(n)\ge 1$. אזי $$\boxed{\mathrm{RP}\;=\;\mathrm{BPP}\!\left(1-\frac{1}{2^{q(n)}},\,1\right)}$$ במילים: בטעות חד-צדדית, הסף $\frac12$ שבהגדרת RP אינו חלק מהתוכן — אפשר להעלות את ההסתברות ההצלחה על yes-instances עד קרוב **אקספוננציאלית** ל-1, בלי לצאת מהמחלקה ובלי לוותר על הוודאות בצד ה-no. **הוכחת ההכלה $\mathrm{RP}\subseteq\mathrm{BPP}\!\left(1-\frac{1}{2^{q(n)}},1\right)$.** מכיוון ש-$q(n)\ge1$ מתקיים $2^{q(n)}\ge2$ ולכן $\frac{1}{2^{q(n)}}\ge\frac12$. כמו כן $1\ge1$. לפי משפט 1 (מונוטוניות), עם $\alpha=1-\hat\alpha$ ו-$\beta=\hat\beta=1$, מתקבלת ההכלה. $\square$ **הוכחת ההכלה $\mathrm{BPP}\subseteq\mathrm{RP}$.** תהא $A\in\mathrm{RP}$. נעבוד בנוסח ב **במכוון**, למרות ששני האגפים אקראיים — כדי לעקוב במפורש אחרי מספר הביטים האקראיים, שהוא לב העניין [01:32:47], [01:49:33]. לכן: קיימת מכונה דטרמיניסטית M הרצה בזמן פולינומי בגודל הקלט וקיים פולינום p כך שלכל x: $$x\in A \Longrightarrow \Pr_{r\in\{0,1\}^{p(|x|)}}\big[M \text{ accepts } (x,r)\big] \ge \tfrac12,\qquad x\notin A \Longrightarrow \Pr_{r\in\{0,1\}^{p(|x|)}}\big[M \text{ rejects } (x,r)\big] \ge 1 .$$ נבנה מכונה דטרמיניסטית $\hat M$ שהממשק שלה הוא זוג (x,r), שכן זה הממשק הנדרש כדי להוכיח שייכות למחלקה מהמשפחה $\mathrm{BPP}(\alpha,\beta)$ [01:39:55]–[01:40:27]. אורך המחרוזת האקראית שלה יהיה $|r| \;=\; p(|x|)\cdot q(|x|).$$ $\hat M$ על קלט x ומחרוזת $r\in\{0,1\}^{p(|x|)\cdot q(|x|)}$: חלק את r ל-$q(|x|)$ מחרוזות **זרות** באורך $p(|x|)$ כל אחת: $r_1,r_2,\dots,r_{q(|x|)}$. לכל $1 \le j\le q(|x|)$: הרץ את M על (x,r_j); 2. אם M **קיבלה** — **קבל** ועצור. 3. **דחה**. **מדוע דווקא הכלל הזה — הניסיון הראשון שנכשל [01:42:03]–[01:42:34].** המרצה כתב תחילה "אם M **דחתה** — דחה", ומיד תיקן. הסיבה: ב-RP הוודאות היא בצד ה-no. תשובת "לא" של M אינה מלמדת דבר (היא ייתכנה גם על yes-instance, בהסתברות עד $\frac12$), אבל תשובת "כן" היא **חד-משמעית**: אילו x היה M, no-instance הייתה דוחה לכל r. לכן מספיקה **הצלחה אחת** מתוך כל ההרצות, ואין צורך במונה כמו בהוכחת משפט 4 — במפורש: "בגלל שהטעות חד-צדדית אני לא צריך counter". **מדוע המחרוזות חייבות להיות זרות [01:43:05]–[01:43:37].** אנחנו רוצים $q(|x|)$ הרצות **בלתי תלויות**, כי רק אי-תלות מתירה להכפיל הסתברויות. סטודנט הציע לחסוך ביטים ולהזיז את החלון ביט אחד בכל פעם; המרצה פסל: "שונה זה לא מספיק לי — אם אני זז ביט אחד יש המון תלות בין המחרוזות". דגימה אחידה של r באורך $p(|x|)q(|x|)$ ופירוקה למקטעים **זרים** נותנת בדיוק

$q(|x|)$ מחרוזות אחידות ובלתי תלויות באורך $p(|x|)$, כי לכל ביט בנפרד הדגימה אחידה ובלתי תלויה. **ניתוח זמן ריצה.** - החלוקה של r לתת-מחרוזות: פולינומית ב-$|x|$ (חישוב $p(|x|)$ ו-$q(|x|)$ וסימון גבולות). - כל הרצה של M על (x,r_j): M פולינומית באורך הקלט שלה, שהוא $|x|+p(|x|)$, ולכן פולינומית ב-$|x|$ (סגירות להרכבה). - מספר האיטרציות: $q(|x|)$, פולינומי ב-$|x|$. מכפלת פולינום בפולינום היא פולינום, ולכן סך זמן הריצה של $\hat M$ פולינומי ב-$|x|$. $\square$ **ניתוח הסתברותי — מקרה $x\notin A$.** מהנתון $\Pr_{r\in\{0,1\}^{p(|x|)}}[M \text{ rejects } (x,r')]\ge 1$, כלומר שווה 1, כלומר **לכל** $r\in\{0,1\}^{p(|x|)}$ המכונה M דוחה את (x,r'). בפרט זה נכון לכל אחד מהמקטעים $r_1,\dots,r_{q(|x|)}$ של כל r שהוא. לכן בשלב 2.2 אף פעם לא מתקבל "קבל", ו-$\hat M$ מגיעה לשלב 3 ודוחה — **לכל** $r\in\{0,1\}^{p(|x|)q(|x|)}$. מכאן $$\Pr_{r\in\{0,1\}^{p(|x|)q(|x|)}}\big[\hat M \text{ rejects } (x,r)\big]\;=\;1\;\ge\;\beta=1 .\qquad\checkmark$$ **ניתוח הסתברותי — מקרה $x\in A$.** מהנתון $\Pr_{r'}[M \text{ accepts } (x,r')]\ge\frac12$, ומכיוון ש-$x$ **קבוע** והמאורעות משלימים באותו מרחב, $$\Pr_{r\in\{0,1\}^{p(|x|)}}\big[M \text{ rejects } (x,r')\big]\ \le\ \tfrac12$$ לכל j המכונה M דחתה את (x,r_j). כמות סופית של "לכל" מתורגמת ל"וגם" [01:59:34], ולכן $$\Pr_r\big[\hat M \text{ rejects } (x,r)\big] \;=\; \Pr_r\Big[\ \bigcap_{j=1}^{q(|x|)}\big\{M \text{ rejects } (x,r_j)\big\}\ \Big] \;\overset{(\ast)}{=}\;\prod_{j=1}^{q(|x|)}\Pr_{r_j}\big[M \text{ rejects } (x,r_j)\big]\;\le\;\left(\tfrac12\right)^{q(|x|)} = \frac{1}{2^{q(|x|)}}$$, כאשר $(\ast)$ הוא בדיוק המקום שבו נדרשת אי-התלות, שהובטחה בזכות הזרות של המקטעים. שוב מהשלמה במרחב מדגם קבוע: $$\Pr_r\big[\hat M \text{ accepts } (x,r)\big]\;=\;1-\Pr_r\big[\hat M \text{ rejects } (x,r)\big]\;\ge\;1-\frac{1}{2^{q(|x|)}}\;=:\;\alpha .\qquad\checkmark$$ שני התנאים מתקיימים עם המכונה $\hat M$ והפולינום $\hat p(n)=p(n)\cdot q(n)$, ולכן $A\in\mathrm{BPP}\!\left(1-\frac{1}{2^{q(n)}},1\right)$. יחד עם הכיוון הראשון, $\mathrm{RP}=\mathrm{BPP}\!\left(1-\frac{1}{2^{q(n)}},1\right)$. $\blacksquare$

מסקנה 5.1: הצורה שמצוטטת בשיעור 17

ניסוח. לכל פולינום q עם $q(n)\ge 2$ מתקיים $\mathrm{RP}\;=\;\mathrm{BPP}\!\left(1-\frac{1}{q(n)},\,1\right)$. **הוכחה.** לכל מספר טבעי $m\ge1$ מתקיים $m\ge m^2$, ולכן $\frac{1}{q(n)}\le\frac{1}{2^{q(n)}}$, כלומר $1-\frac{1}{2^{q(n)}}\ \ge\ 1-\frac{1}{q(n)}\ \ge\ \tfrac12$. כעת: לפי משפט 1, $\mathrm{BPP}\!\left(1-\frac{1}{2^{q(n)}},1\right)\subseteq\mathrm{BPP}\!\left(1-\frac{1}{q(n)},1\right)$. ולפי משפט 5, האגף השמאלי ביותר שווה ל-RP. לכן כל ההכלות בשרשרת הן שוויונות, ובפרט $\mathrm{RP}=\mathrm{BPP}\!\left(1-\frac{1}{q(n)},1\right)$. $\blacksquare$

מדוע שתי הצורות. הסיכום וההקלטה מנסחים את המשפט עם $\frac{1}{2^{q(n)}}$ — הצורה החזקה יותר. שיעור 17 מצטט את הצורה עם $\frac{1}{q(n)}$. מסקנה 5.1 מראה שאלו אותה טענה, ושהצורה החלשה נובעת מן החזקה בשורה אחת. **מה עולה בהעצמה — "זה לא קסם" [ב׳ 00:01:04]–[ב׳ 00:02:08].** ההעצמה אינה חינם. זמן הריצה גדל (מ-T ל-$q\cdot T$ בקירוב), ומספר הביטים האקראיים גדל מ-$p(n)$ ל-$p(n)q(n)$. הסיבה שהמחלקות בכל זאת **שוות** היא הרזולוציה שבה

אנחנו מסתכלים: "אם פה זה היה n^2 ופה העליתי את זה ל-n^{50} — זה עדיין פולינומי". כלומר מה שמסתתר מאחורי המשפט הוא בדיוק סגירות הפולינומים לחיבור, כפל והרכבה. **שלושה פולינומים שונים — האזהרה שהמרצה חזר עליה שלוש פעמים [01:55:24]–[01:58:33].** בכל טענה מהסוג הזה מסתובבים שלושה פולינומים נפרדים: 1. **זמן הריצה** של המכונה; 2. **מספר הביטים האקראיים** שהיא קוראת, כאן $p(n)$ ואחר כך $3p(n)q(n)$; 3. **הפולינום שבתוך ההסתברות**, כאן $q(n)$. באופן כללי **אין ביניהם שום קשר**, למעט העובדה הכמעט-מיידית שמספר הביטים האקראיים אינו יכול לעלות על זמן הריצה (קריאת ביט עולה צעד). המרצה בחר במכוון בדרך הארוכה, עם המכונה הדטרמיניסטית ועם r מפורש, רק כדי שיהיה אפשר לראות בעיניים שהפולינום של האורך גדל מ-p ל-$p\cdot q$ בעוד שהפולינום בהסתברות נשאר q. מסקנה מעשית שנאמרה כרמז לבחינה [01:58:33]: **אם בשאלה מופיע אותו p בשני התפקידים — זו הגדרה אחרת ממה שהוכחנו כאן, ויש לשים לב.** --- ## דוגמאות ותרגילים מהשיעור ### דוגמה 1: מעקב מלא אחרי ניקח $\mathrm{MATMUL}\in\mathrm{coRP}$ על מופע $\$2$times2\$

$$A=\begin{pmatrix}1&0\\0&1\end{pmatrix},\qquad B=\begin{pmatrix}1&0\\0&1\end{pmatrix},\qquad C=\begin{pmatrix}1&0\\0&0\end{pmatrix}.$$

כאן $A\cdot B=I\ne C$, ולכן $\langle A,B,C\rangle\notin\mathrm{MATMUL}$ — זהו **no-instance**, ובו מותרת טעות. נסמן $$D:=A\cdot B-C=\begin{pmatrix}0&0\\0&1\end{pmatrix}\ne 0.$$ מרחב המדגם הוא $Omega=\{0,1\}^2$ ו-$|Omega|=4$. נעבור על כל ארבע המחרוזות האקראיות: | r | $D\cdot r$ | תשובת המכונה | נכונה? | |---|---|---|---| | $(0,0)$ | $(0,0)$ | מקבלת ("$AB=C$") | לא — טעות | | $(1,0)$ | $(0,1)$ | דוחה | כן | לכן $(0,0)$ | מקבלת | לא — טעות | | $(0,1)$ | $(0,1)$ | דוחה | כן | | $(1,1)$ | $(0,1)$ | דוחה | כן | לכן $\Pr_r[\text{reject}]=\frac24=\frac12$ — בדיוק על גבול הדרישה $beta=\frac12$. שימו לב שהמופע הזה **הדוק**: אי אפשר לשפר את $frac12$ בניתוח, כי כאן הוא מושג בשוויון. עכשיו נבדוק **yes-instance**: נחליף את C ב-$C'=I$. אז $D=0$, ולכן $D\cdot r=0$ לכל אחת מארבע המחרוזות, והמכונה מקבלת **בכל** מקרה: $\Pr_r[\text{accept}]=1=\alpha$. זהו הצד החד-צדדי, והוא נכון **פוינטווייז** — בלי שום שימוש באקראיות. ### דוגמה 2: מה ההעצמה עושה במספרים ניקח את המופע מדוגמה 1 בתפקיד הפוך: השפה $overline{\mathrm{MATMUL}}$ (כלומר "$AB\ne C$") שייכת ל-RP עם $alpha=\frac12$. נפעיל את משפט 5 עם $q(n)=10$ (פולינום קבוע): - המכונה $\hat M$ דוגמת r באורך $p(|x|)\cdot 10$, מפצלת ל-10 מקטעים זרים, ומריצה את 10 Freivalds פעמים. - על (no-instance ($AB=C$: כל הרצה דוחה בוודאות, ולכן $\hat M$ דוחה בוודאות. אין false positive. - על yes-instance ($AB\ne C$): $\Pr[\hat M \text{ rejects}]\le\left(\frac12\right)^{10}=\frac{1}{1024}$, ולכן $\Pr[\hat M \text{ accepts}]\ge 1-\frac{1}{1024}\approx 0.999$. עם $q(n)=n$ נקבל הסתברות שגיאה 2^{-n} — קטנה מסיכוי הכשל של החומרה — במחיר n הרצות, כלומר עדיין זמן פולינומי. ### תרגיל 1 (החימום שהמרצה נתן בכיתה, [00:34:04]) **השאלה.** יהיו $\alpha,\beta,\hat\alpha,\hat\beta\in[0,1]$ עם $\hat\alpha\ge\alpha,\ \hat\beta\ge\beta$. מה אפשר לומר על היחס בין $\mathrm{BPP}(\hat\alpha,\hat\beta)$ ל-$\mathrm{BPP}(\alpha,\beta)$? **פתרון.** $\mathrm{BPP}(\hat\alpha,\hat\beta)\subseteq\mathrm{BPP}(\alpha,\beta)$ — זה משפט 1, וההוכחה היא

"אותה מכונה בדיוק". המרצה הדגיש שזה תרגיל **ניסוח** ותו לא: אין בו רעיון, רק פתיחת ההגדרה משני צדדיה [00:39:14]. הערך שלו הוא בהרגל: כל טענה על מחלקות מתחילה ב"תהא $A\in\dots$ ולכן קיימת מכונה". ### תרגיל 2: מדוע $\mathrm{BPP}\left(\frac12,\frac12\right)$ חסרת תוכן **השאלה.** הוכיחו ש-$\mathrm{BPP}\left(\frac12,\frac12\right)$ מכילה כל שפה $A\subseteq\Sigma^*$, גם שפות שאינן כריעות. **פתרון.** תהא A שפה כלשהי. נגדיר מכונה אקראית M שעל כל קלט x מתעלמת מ-x לגמרי, מטילה מטבע אחד, ומקבלת אם יצא "עץ" ודוחה אם יצא "פלי". זמן הריצה קבוע, ובפרט פולינומי. לכל x מתקיים $\Pr[M \text{ accepts } x]=\frac12$ ו-$\Pr[M \text{ rejects } x]=\frac12$; לכן אם $x\in A$ מתקיים $\Pr[\text{accept}]\ge\frac12$, ואם $x\notin A$ מתקיים $\Pr[\text{reject}]\ge\frac12$. שני התנאים מתקיימים לכל שפה. $\blacksquare$ **המסקנה.** בטעות דו-צדדית **חייבים** לדרוש יותר מ-$\frac12$. זה מסביר למה ההגדרה של BPP בחרה $\frac23$ ולא $\frac12$, ולמה בהגדרת RP מותר $\frac12$ — שם הצד השני הוא 1, ולכן המכונה שמטילה מטבע נפסלת מיד. ### תרגיל 3: מדוע $\mathrm{BPP}(0,1)$ ו-$\mathrm{BPP}(1,0)$ חסרות תוכן **פתרון.** $\mathrm{BPP}(0,1)$: המכונה "דחה תמיד" מקיימת $\Pr[\text{reject}]=1\ge\beta$ לכל no-instance, ואת התנאי $\Pr[\text{accept}]\ge 0$ **כל** מכונה מקיימת. לכן כל שפה בפנים. סימטרית ל-$\mathrm{BPP}(1,0)$ עם "קבל תמיד". **הלקח:** ב-$\mathrm{BPP}(\frac12,1)$ הקבוע $\frac12$ אינו חשוב (משפט 5 ושיעור 17), אבל **אסור** שיהיה 0 — הגבול התחתון האמיתי הוא "משהו שאינו זניח". ### תרגיל 4 (מהתרגיל שהמרצה הודיע עליו, [01:29:50]) **השאלה.** בתרגיל הבית תופיע מחלקה C_1 שמוגדרת כ"קבוצת כל השפות שעבורן קיימת מכונה כך ש...", עם ערבויות מעט שונות מאלו של הגדרה 3, ותידרשו למקם אותה ביחס ל-NP ו-BPP — בדיוק כמו התרגיל המקביל על NP מוקדם יותר בסמסטר. **איך ניגשים.** לפי ההוכחות בשיעור, יש רק שלוש שאלות שכדאי לשאול על הגדרה כזו: 1. **מה הממשק של המכונה** — האם היא מקבלת x בלבד או זוג (x,r)? זה קובע איזה נוסח של הגדרה 3 נוח, ומה אפשר בכלל להוכיח (משפט 4 נבנה סביב זה). 2. **מה מרחב המדגם, וכמה ביטים אקראיים** — האם הפולינום שבאורך r הוא אותו פולינום שבהסתברות? אם כן, זו הגדרה **חזקה יותר** ממה שהוכחנו. 3. **האם הטעות חד-צדדית או דו-צדדית** — כלומר האם אחד מ-α,β שווה 1. אם כן, ההעצמה היא "לפחות פעם אחת" ואין צורך במונה; אם לא, נדרשת הצבעת רוב (שיעור 17). --- ## הערות מהשיעור - **[00:01:02] למה בכלל צריך מודל פורמלי.** כשכותבים אלגוריתם, "חוקי המשחק נובעים מתוך האלגוריתם" — אם כתוב "נדגום וקטור באקראי", ברור מה מותר. אבל כדי **להוכיח דברים על מחלקות סיבוכיות** חייבים להגדיר את המודל קודם. זו כל ההצדקה לשיעור. - **[00:25:13] כלל האצבע החשוב ביותר בשיעור.** "תמיד כשאתם מחשבים הסתברות, שאלו את עצמכם מה האקראי פה. מאיפה האקראיות? זה הדבר הראשון שאני בודק." - **[00:21:01], [00:29:23] שאלת סטודנטית שחשפה את הנקודה העדינה.** "אם $x\in A$ ו-$x\notin A$ הם מקרים משלימים, למה $\alpha+\beta$ לא חייב להיות 1?" התשובה: כי x **אינו** חלק מהניסוי האקראי. "יש לי את x, ואז אני דוגם את r — זה הניסוי האקראי." שני התרחישים חיים במרחבי מדגם שונים לגמרי; אלה שני ניסויים שונים, לא שני מאורעות משלימים באותו ניסוי. זו הטעות מספר אחת בנושא הזה. - **[01:23:54] הצד השני של

אותה נקודה.** ברגע ש-x **קבוע**, המאורעות "מקבלת" ו"דוחה" כן משלימים, כי הכול תלוי רק ב-r. שני הכיוונים נחוצים: הראשון כדי לא לחבר $\alpha+\beta$, השני כדי להסיק $\Pr[\text{accept}]\le\frac13$ בהוכחת משפט 4. - **[00:49:25] "אל תחמקו מהשלד של ההוכחה."** סטודנט קפץ ישר לפואנטה, והמרצה עצר: "אתה אומר דברים נכונים אבל you jump the gun. אם אני לא כותב את המסגרת של ההוכחה, אני הולך לאיבוד — כי אתה מתחיל לדבר על x ואין לך x." הכוונה: לפני כל טיעון הסתברותי צריך לכתוב "תהא $A\in\dots$, לכן קיימת מכונה M..., יהי x..., נניח $x\in A$..." — ורק אז לחשב. - **[01:39:55] הלקח המתודי המרכזי.** "אני מתאים את הממשק למה שאני רוצה להוכיח." להוכחת PSPACE בונים מכונה שמקבלת רק x (ולכן עוברים על כל ה-r-ים בלולאה); להוכחת שייכות ל-BPP (α,β) בונים מכונה שמקבלת (x,r) (ולכן אין לולאה על r). זו אותה שאלה שהמרצה ציין כ"שאלה חשובה". - **[01:13:03] טריק שחוזר מהקורס.** את $2^{|x|}$ כותבים בבינארי ולא באונרי. באונרי היינו רושמים $|x|$ אפסים ואחריהם אחד — ייצוג לגיטימי, אך גדול מדי כאן. הטריק ההפוך נעשה במשפט ההיררכיה (ראו שיעור 3), ושם דווקא האונרי היה הנוח. "מתי אכתוב באונרי ומתי בבינארי? מתי שנוח לי." - **[01:12:33] מה שלא הוכחנו.** ההוכחה של משפט 4 אינה נותנת $\mathrm{BPP}\subseteq\mathrm{P}$, כי זמן הריצה של $\hat M$ מעריכי. השאלה אם $\mathrm{BPP}=\mathrm{P}$ היא **בעיה פתוחה**. - **[00:30:24] "יש לזה שימוש במציאות?"** כן, ובגדול — בניגוד לאי-דטרמיניזם, שאינו מודל ישים בשום צורה. אקראיות מפזרת סיכונים; כשהקלטים ענקיים לא רוצים לעבור על כולו אלא לדגום ממנו, ואת הדגימה עושים באקראי כדי להימנע מהטיה (bias). המרצה נתן כדוגמה אלגוריתמי למידת מכונה, שדוגמים מדגם אקראי לאימון ומאתחלים באקראי. - **[01:29:17] נקודה קטנה שחוזרת בבחינות.** ההבדל בין **שלילה לוגית** ($x\ge$-מ-y) לבין **השלמה של קבוצה** (שמשאירה $x\ge$ כ-y). שניהם הופיעו בהוכחה אחת. - **[02:02:52] הכיוון שנשאר לשיעור הבא.** המרצה סיים בהצגת הטענה $\mathrm{RP}=\mathrm{BPP}\!\left(\frac{1}{q(n)},1\right)$ בלי להוכיחה, וקרא לה "קאונטר-אינטואיטיבית": מתחילים מהסתברות הצלחה ששואפת ל-0 ומגיעים להסתברות ששואפת ל-1 — **בזמן פולינומי**. ראו שיעור 17. > **הערה (מינוח שלא נאמר בשיעור).** בספרות מקובל לכנות אלגוריתם שזמן הריצה שלו חסום תמיד אך תשובתו עשויה להיות שגויה — **Monte Carlo**, ואלגוריתם שתשובתו תמיד נכונה אך זמן הריצה שלו משתנה מקרי — **Las Vegas**. כל המכונות בשיעור הזה הן מטיפוס Monte Carlo. המונחים האלה **אינם** מופיעים לא בסיכום ולא בשתי ההקלטות, והם נכתבים כאן רק לצורך קישור לחומר חיצוני (אותה הערה מופיעה גם בשיעור 15). --- ## פערים בין הסיכום להקלטה - **מקור:** עמוד 5 בסיכום מול שיעור 17. **הפער:** הסיכום וההקלטה מנסחים את משפט ההעצמה כ-$\mathrm{RP}=\mathrm{BPP}(1-\frac{1}{2^{q(n)}},1)$, ואילו שיעור 17 מצטט $\mathrm{RP}=\mathrm{BPP}(1-\frac{1}{q(n)},1)$. **ההכרעה:** נכתבו שתיהן — משפט 5 בצורת המקור, ומסקנה 5.1 בצורה שמצוטטת בשיעור 17, עם הוכחה בת שורה שהשנייה נובעת מהראשונה. - **מקור:** עמוד 4 בסיכום. **הפער:** שלב 4 בפסאודו-קוד משווה $\text{count}\ge\frac23\cdot2^{p(|x|)}$, ערך שאינו שלם בהכרח, ולא נאמר איך ממשים זאת. **ההכרעה:** נכתב במפורש שהמבחן השקול בשלמים הוא $\text{count}\ge2^{p(|x|)+1}$; ההוכחה אינה מושפעת. - **מקור:** עמוד 1 בסיכום. **הפער:** הסיכום אינו נותן שישייה למכונה

האקראית אלא הגדרה מילולית; גם ההקלטה [00:04:34] מודה במפורש ש"זה לא מרגיש לגמרי פורמלי". **ההכרעה:** נרשמה השישייה $M=(Q,q_{start},F,\Sigma,\Gamma,\delta)$ בעקבות שיעור 4, עם הערה שההידוק הוא שלנו. - **מקור:** עמוד 1 בסיכום, שתי ההערות בכחול בשוליים. **הפער:** קצרות מדי מכדי לקרוא בוודאות. **ההכרעה:** פוענחו לפי ההקלטה [00:10:57]–[00:11:28] כ"מודל 1 נוח לכתיבת אלגוריתמים, מודל 2 נוח להשוואה בין מחלקות", וכך נכתבו. - **מקור:** ההקלטה מול הסיכום. **הפער:** ההקלטה מכילה חומר מהותי שאין בסיכום כלל — ההבחנה בין "לא דטרמיניסטי" ל"אי-דטרמיניסטי" [00:05:05]–[00:06:43]; ההסבר למה RP מוגדרת עם 1 דווקא בצד ה-no [00:58:48]; האזהרה על שלושת הפולינומים [01:55:24]; והתיקון החי של כלל העצירה בלולאה מ"אם דחתה" ל"אם קיבלה" [01:42:03]. **ההכרעה:** כל אלה נכללו בגוף, עם חותמות זמן. - **מקור:** הסיכום מול ההקלטה, בסיווג MATMUL. **הפער:** הסיכום אינו מזכיר את בעיית וידוא כפל המטריצות בכלל; בהקלטה [00:41:30] הסיווג ב-coRP נאמר בעל פה כשאלה לכיתה, בלי אימות מול ההגדרה. **ההכרעה:** נכתב כמשפט 3 עם הוכחה מלאה, כולל חשבון הביטים, כדי לסגור את מה שנדחה לכאן משיעור 15. השם MATMUL הוא סימון של הסדרה ואינו מופיע במקורות. - **מקור:** עמוד 2 בסיכום. **הפער:** שם המחלקה RP כתוב בכתב יד באופן שאפשר לקרוא כ-"BP" בכמה מקומות ($\mathrm{BP}=\mathrm{BPP}(\frac12,1)$, $\mathrm{BP}\subseteq\mathrm{NP}$). **ההכרעה:** מההקלטה ברור שהכוונה ל-RP בכל המופעים; נכתב RP. - **מקור:** ההקלטה בלבד. **הפער:** המרצה תיאר את ההוכחה של משפט 5 כ"מעגל פינות" בניתוח הזמן [01:46:20], [01:46:51]. **ההכרעה:** ניתוח הזמן נכתב כאן במלואו — חלוקת r, זמן כל הרצה, מספר האיטרציות, וסגירות הפולינומים — במקום ה"עיגול". - **מקור:** המוסכמות של הסדרה. **ההכרעה:** שמות המחלקות והשפות נכתבים ב-$\mathrm{ }$ לפי מוסכמת הסדרה; סימוני המשתנים ($\alpha,\beta,\hat\alpha,\hat\beta,p,q,r,M,\hat M,\text{count}$) נלקחו כלשונם מהסיכום. --- ## סיכום ונקודות למבחן **להכיר בעל פה.**

$$\mathrm{BPP}=\mathrm{BPP}\!\left(\tfrac23,\tfrac23\right),\qquad$$

$$\mathrm{RP}=\mathrm{BPP}\!\left(\tfrac12,1\right),\qquad$$

$$\mathrm{coRP}=\mathrm{BPP}\!\left(1,\tfrac12\right),$$

$$\mathrm{RP}\subseteq\mathrm{NP},\qquad$$

$$\mathrm{coRP}\subseteq\mathrm{coNP},\qquad$$

$$\mathrm{BPP}\subseteq\mathrm{PSPACE},\qquad \mathrm{RP}=\mathrm{BPP}\!\left(1-\tfrac{1}{2^{q(n)}},1\right).$$ **המלכודות הסטנדרטיות.** 1. **הסתברות על מי.** לעולם לא על הקלט. הקלט קבוע ושרירותי; האקראיות היא מטבעות המכונה בלבד. כל משפט מתחיל ב"יהי x" ורק אחר כך פותחים $\alpha+\beta\ne1$. **אלה שני תרחישים במרחבי מדגם שונים. אבל **לקלט קבוע** כן מותר לכתוב $\Pr[\text{accept}]=1-\Pr[\text{reject}]$ — ובלי זה אי אפשר להוכיח את משפט 4. 3. **coRP אינה משלימת RP** אלא קבוצת המשלימות. אותה מלכודת כמו coNP. 4. **איזה צד ודאי.** ב-RP אין "כן" שגוי; ב-coRP אין "לא" שגוי. אם מתבלבלים — לחשוב על Freivalds: כשהזהות

מתקיימת, היא מתקיימת לכל r; לכן הצד הוודאי הוא ה-yes, ולכן $5\$ .mathrm{coRP}$. **שלושה פולינומים.** זמן ריצה, מספר ביטים אקראיים, והפולינום בהסתברות — אין קשר ביניהם. אם בשאלה מופיע אותו פולינום בשני תפקידים, זו הגדרה **אחרת**. 6. **שלילה לוגית מול השלמת קבוצה.** $neg(\text{count}\ge t)\$ נותן $<$ חזק; $Pr[\text{reject}]\ge\frac23$\$ נותן $Pr[\text{accept}]\le\frac13$\$ חלש. 7. **בחירת הנוסח.** מוכיחים שייכות למחלקה **דטרמיניסטית** — התחילו מנוסח ב (סרט אקראי), כי הממשק תואם. מציגים **אלגוריתם** — נוסח א נוח יותר. **צ'ק-ליסט: אחרי השיעור הזה צריך לדעת** - לכתוב את שני המודלים של מכונה אקראית ולהסביר במשפט מה ההבדל בין "לא דטרמיניסטי" ל"אי-דטרמיניסטי". - לפתוח את ההגדרה של $mathrm{BPP}(\alpha,\beta)\$ בשני הנוסחים, ולזהות מיד מהו מרחב המדגם וגודלו. - להוכיח את מונוטוניות ההכלה (משפט 1) בשלוש שורות, ולקבוע לבד לאיזה כיוון היא הולכת. - לשחזר את $mathrm{RP}\subseteq\mathrm{NP}\$ כולל שלב הספירה $Pr\cdot|\Omega|=2^{p(|x|)-1}\ge1$\$ והטיפול בקלטים הקצרים. - לשחזר את $mathrm{BPP}\subseteq\mathrm{PSPACE}\$ כולל: למה המכונה הבנויה מקבלת רק x, למה שימוש חוזר במקום בין איטרציות שומר על מקום פולינומי, ולמה הזמן מעריכי ואין מכאן $mathrm{BPP}\subseteq\mathrm{P}\$. - לבנות את מכונת ההעצמה החד-צדדית, להסביר למה עוצרים ב"קיבלה" ולא ב"דחתה", ולמה המקטעים חייבים להיות זרים. - לסווג בעיה נתונה ל-$\mathrm{BPP}\$ / coRP / RP לפי כיוון הוודאות, כפי שנעשה עבור $\mathrm{MATMUL}\$.

שאלות שנשארו פתוחות

בסיכום עמוד 5 המשפט נכתב $\mathrm{RP}=\mathrm{BPP}(1-1/2^{q(n)},1)\$, וכך גם בהקלטה; שיעור 17 מצטט את הצורה החלשה יותר $\mathrm{RP}=\mathrm{BPP}(1-1/q(n),1)\$. שתיהן נכונות והשנייה נובעת מהראשונה — כאן מופיעות שתיהן (משפט 5 ומסקנה 5.1) כדי שהציטוט בשיעור 17 יהיה מדויק.

בעמוד 1 בסיכום שתי ההערות בכחול בשוליים קצרות מאוד; פוענחו בעזרת ההקלטה כ'המודל הנוח לכתיבת אלגוריתמים' מול 'המודל הנוח להשוואה בין מחלקות'. אם הקריאה שגויה, מדובר רק בניסוח ההערה ולא בתוכן.

הסיכום אינו נותן רביעייה/שישייה למכונה האקראית אלא הגדרה מילולית בלבד; שישיית המכונה כאן הובאה משיעור 4 לצורך אחידות הסדרה.

שלב 4 בפסאודו-קוד שבסיכום (עמוד 4) משווה $\text{count}\ge\frac23\cdot2^{p(|x|)}\$ — ערך שאינו שלם בהכרח; כאן נכתבה ההשוואה השקולה בשלמים $\cdot\text{count}\ge2^{p(|x|)+1}\$3, וזו תוספת פורמלית שלנו.

17 העצמת/הקטנת ההסתברות ב-BPP וב-RP

מוכיחים שסף השגיאה בהגדרת RP ו-BPP הוא שרירותי: הרצה חוזרת בלתי-תלויה עם 'לפחות פעם אחת' (טעות חד-צדדית) או עם הצבעת רוב (טעות דו-צדדית) מרכזת את ההסתברות ומורידה את השגיאה, כל עוד יש פער של $1/\mathrm{poly}$ מהסף.

ביטחון: high

בקצרה

הסף שמופיע בהגדרת המחלקות ההסתברותיות **אינו חלק מהתוכן**: כל סף סביר נותן בדיוק את אותה מחלקה. זו כל התוצאה של השיעור.

בטעות **חד-צדדית** (one-sided error), ההעצמה חזקה במיוחד: גם הסתברות הצלחה זעירה של $1/q(n)$ מספיקה — $\mathrm{RP} = \mathrm{BPP}\left(\frac{1}{q(n)}, 1\right)$ לכל פולינום q. מריצים $q(|x|)$ פעמים בלתי-תלויות ומקבלים אם **לפחות פעם אחת** התקבל "כן".

בטעות **דו-צדדית** (two-sided error) אין תשובה שאפשר לסמוך עליה, ולכן מצביעים **רוב**. כאן חייב להיות פער של $1/\mathrm{poly}$ מעל $\frac{1}{2}$ — סף של בדיוק $\frac{1}{2}$ חסר-תוכן לגמרי, וסף של $\frac{1}{2} + \frac{1}{2^{q(n)}}$ אינו ידוע כניתן להעצמה.

הכלי המתמטי הוא **ריכוז** (concentration): משתנה בינומי מרוכז סביב התוחלת שלו. בקורס לא מוכיחים את זה בצ'רנוף אלא מחשבים בידיים זנב בינומי אחד קונקרטי.

ההוכחה המלאה שנעשתה בכיתה: $\mathrm{BPP} = \mathrm{BPP}\left(\frac{4}{5}, \frac{4}{5}\right)$, על ידי 7 הרצות והצבעת רוב, עם חישוב מפורש של $\sum_{k=4}^{7} \binom{7}{k} \left(\frac{2}{3}\right)^{k} \left(\frac{1}{3}\right)^{7-k} = \frac{1808}{2187}$.

מה שמניע את כל החשבון הוא **אי-התלות** בין ההרצות: היא זו שמאפשרת את המעבר מהסתברות של "וגם" למכפלה ואת נוסחת ההתפלגות הבינומית.

בסוף השיעור נפתחה בעיית **החתך המינימלי** ואלגוריתם הכיווץ האקראי; הניתוח שלו נדחה לשיעור 18.

רקע ותלויות

השיעור הזה יושב ישירות על שיעור 16, ולא ניתן לקרוא אותו בלעדיו. נזכיר במפורש את מה שנשתמש בו.

המודל. מכונת טיורינג הסתברותית M הרצה בזמן פולינומי. בשיעור 16 ראינו שתי דרכים שקולות למדל אותה: מכונה דטרמיניסטית $M(x, r)$ המקבלת מחרוזת אקראית r באורך $p(|x|)$ כקלט נוסף, או מכונה שבכל צעד מטילה מטבע. בשיעור זה המרצה עובד **במודל האקראי** (המכונה בוחרת בחירות אקראיות בעצמה), ולא במודל הדטרמיניסטי עם r — במפורש ומסיבה מוצהרת: ההוכחה יוצאת קצרה יותר, וההדגמה שהמחרוזת האקראית גדלה כבר נעשתה בשיעור הקודם [00:12:48].

המשפחה $\mathrm{BPP}(\alpha, \beta)$. בשיעור 16 הוגדרה משפחת מחלקות שהמחלקות המוכרות הן מקרים פרטיים שלה [00:00:01]. נזכיר אותה בהגדרה 1 להלן, כי כל ניסוחי השיעור כתובים בה.

שתי זהויות מוסכמות (שיעור 16): $\mathrm{BPP} = \mathrm{BPP}\left(\frac{2}{3}, \frac{2}{3}\right)$, $\qquad \mathrm{RP} = \mathrm{BPP}\left(\frac{1}{2}, 1\right)$

התוצאה שכבר הוכחה בשיעור 16 ואינה חוזרת כאן. ראו שיעור 16: לכל פולינום q מתקיים $\mathrm{RP} = \mathrm{BPP}\left(1 - \frac{1}{q(n)}, 1\right)$ כלומר, בטעות חד-צדדית אפשר להעלות את הסתברות ההצלחה מ-$\frac{1}{2}$ עד קרוב מאוד ל-1. השיעור הנוכחי הולך ל**כיוון ההפוך ולכן המפתיע יותר**: להתחיל מהסתברות הצלחה זעירה ולהגיע ל-$\frac{1}{2}$ [00:02:41]. אלה שני חצאים משלימים של אותה טענה, והצירוף שלהם הוא שנותן ש-RP עמידה לכל שינוי סביר של הסף.

מונוטוניות ההכלה — עיקרון עבודה. המרצה מדגיש שהוא לעולם לא זוכר מי מוכל במי, אלא בודק בכל פעם: *לאן קשה יותר להיכנס?* אם דורשים הסתברות הצלחה גדולה יותר, הדרישה חזקה יותר, ולכן המחלקה הזו מוכלת בזו עם הדרישה החלשה [00:07:58]. זהו הכיוון ה"קל" בכל אחת מהטענות למטה.

התקדים מהשיעורים הקודמים. ראו שיעור 15: באלגוריתם של Freivalds לאימות מכפלת מטריצות (MATMUL) התחלנו מאלגוריתם עם טעות חד-צדדית והסתברות הצלחה $\frac{1}{2}$, והגברנו אותה בדיוק באותה שיטה — הרצות חוזרות בלתי-תלויות ו"קבל רק אם התקבל לפחות פעם אחת" [00:36:02]. השיעור הנוכחי הוא ההכללה של אותו טריק לרמת המחלקה.

מה נדרש מהסתברות. אי-תלות של מאורעות, הסתברות של איחוד מאורעות זרים בזוגות, והתפלגות בינומית. שונות ואי-שוויוני ריכוז אינם נלמדים בקורס [00:45:04], ולכן המשפט הכללי יינתן ללא הוכחה.

הגדרות

הגדרה 1: המחלקה $\mathrm{BPP}(\alpha, \beta)$

תהיינה α, β פונקציות של n (או קבועים). שפה A שייכת ל-$\mathrm{BPP}(\alpha, \beta)$ אם קיימת מכונת טיורינג הסתברותית M הרצה בזמן פולינומי כך שלכל קלט x, כאשר $n = |x|$:

$$x \in A \implies \Pr[M \text{ accepts } x] \geq \alpha(n) \quad x \notin A \implies \Pr[M \text{ rejects } x] \geq \beta(n)$$

ההסתברות היא על פני המטבעות שהמכונה מטילה, ולא על פני הקלט. הקלט אינו אקראי — הוא נתון וקבוע, ואי-הוודאות היא כולה של האלגוריתם.

אינטואיציה. α הוא ה"ביטחון" שהאלגוריתם נותן על yes-instances ו-β הביטחון שהוא נותן על no-instances. שני הפרמטרים נפרדים, ולכן אפשר לתאר גם מצב א-סימטרי שבו לצד אחד יש ודאות מלאה ולצד השני כמעט כלום.

מופע. $\mathrm{BPP} = \mathrm{BPP}\left(\frac{2}{3}, \frac{2}{3}\right)$ — סימטרי, טעות דו-צדדית.

מופע גבולי חשוב. $\mathrm{BPP}\left(\frac{1}{2}, \frac{1}{2}\right)$ מכילה **כל שפה שהיא**, ולכן היא חסרת תוכן: המכונה "הטל מטבע, על עץ החזר accept ועל פלי החזר reject" מקיימת את שתי הדרישות בשוויון עבור כל שפה, בלי להסתכל על הקלט בכלל [00:05:18]. זהו בדיוק ה-non-instance שממחיש למה בטעות דו-צדדית חייבים לדרוש **יותר** מ-$\frac{1}{2}$, ולא רק $\frac{1}{2}$.

הערה: אזהרה על המונוטוניות — $\mathrm{BPP}(\alpha,\beta)\subseteq\mathrm{BPP}(\alpha',\beta')$ כאשר $\alpha'\le\alpha$ ו-$\beta'\le\beta$, כלומר ההכלה היא לכיוון הדרישה החלשה יותר. מכאן גם הטריק המעשי שהמרצה מלמד [00:48:45]: אם נתונה מכונה עם ערבויות א-סימטריות, למשל $\mathrm{BPP}\left(\frac{2}{3},\frac{9}{10}\right)$, אפשר תמיד "לרדת" לערך הקטן משניהם ולעבוד עם $\mathrm{BPP}\left(\frac{2}{3},\frac{2}{3}\right)$.

הגדרה 2: RP וטעות חד-צדדית

$$\mathrm{RP}=\mathrm{BPP}\left(\tfrac{1}{2},1\right)$$

כלומר: על $x\notin A$ המכונה דוחה בהסתברות 1 — לעולם אינה טועה; על $x\in A$ היא מקבלת בהסתברות $\ge\frac{1}{2}$.

האינטואיציה, ולמה היא מבלבלת. המרצה חוזר על כך שוב ושוב שהוא בעצמו מתבלבל כאן, ובונה טבלת בלבול (confusion matrix) על הלוח [00:20:46]. הכיוון הנכון לקרוא אותה:

האמת (הקלט)	תשובת האלגוריתם	שם המצב
yes-instance	accept	נכון
yes-instance	reject	**false negative**
no-instance	accept	**false positive**
no-instance	reject	נכון

ב-RP אין false positives: על no-instance המכונה דוחה בוודאות. מכאן המסקנה התפעולית — **אם המכונה החזירה accept, אפשר להאמין לה בוודאות**. הטעות היחידה האפשרית היא false negative: yes-instance שנדחה [00:22:21]. ב-coRP המצב הפוך בדיוק.

מופע. האלגוריתם של Freivalds ל-MATMUL (שיעור 15) — אם המכפלה שגויה הוא תמיד מזהה, ואם היא נכונה הוא עלול "לפספס"; זהו בדיוק המבנה החד-צדדי.

הגדרה 3: הצבעת רוב (majority vote)

בהינתן t הרצות בלתי-תלויות של M על אותו קלט x, שכל אחת מחזירה accept או reject, **הצבעת רוב** מחזירה את התשובה שהתקבלה במספר הרצות גדול ממש מ-$t/2$.

למה t חייב להיות אי-זוגי. אם t אי-זוגי, לא ייתכן תיקו, ולכן ה"רוב" **מוגדר היטב תמיד** ואין צורך בכלל שבירת-שוויון [00:55:19]. אם $t=2m$ זוגי, המאורע m מול m אפשרי, "רוב" אינו מוגדר, ויש להוסיף כלל שרירותי. בסעיף הדוגמאות נראה בחשבון שהמחיר איננו רק אסתטי: t זוגי עם שבירת תיקו במטבע הוגן נותן **בדיוק** את אותה הסתברות הצלחה כמו $t-1$ הרצות, כלומר ההרצה הזוגית האחרונה מבוזבזת לגמרי.

נקודה קריטית: מדוע אי-תלות. ההרצות חייבות להיות בלתי-תלויות — כל הרצה משתמשת במטבעות טריים משלה. אם היו תלויות (במקרה הקיצוני: אותה מחרוזת אקראית לכולן), כל ההרצות היו מחזירות את אותה תשובה ולא היינו מרוויחים דבר. אי-התלות היא בדיוק מה שמתיר את שני המעברים המרכזיים בשיעור: פירוק הסתברות של "וגם" למכפלה (משפט 1) ונוסחת ההתפלגות הבינומית (משפט 3).

הערה: המרצה מקדיש לכך דיון שלם [00:30:48] כי סטודנטית בלבלה בין מאורעות **זרים** למאורעות **בלתי-תלויים**. ההגדרה של אי-תלות היא $\Pr[X \cap Y] = \Pr[X] \cdot \Pr[Y]$, ולא $X \cap Y = \emptyset$. למעשה, שני מאורעות זרים בעלי הסתברות חיובית הם **תלויים מאוד**: $\Pr[X \cap Y] = 0 \neq \Pr[X]\Pr[Y]$, ואינטואיטיבית — אם אחד קרה, ידוע בוודאות שהשני לא. הכלל המעשי: אי-תלות עובדת טוב עם "וגם", זרות עובדת טוב עם "או".

הגדרה 4: בעיית החתך המינימלי (MIN CUT)

קלט: גרף $G = (V, E)$ (פשוט, לא מכוון). **מטרה:** למצוא חלוקה של הצמתים לשתי קבוצות $(U, \bar{U})$ עם $\emptyset \subsetneq U \subsetneq V$, כך שגודל החתך — מספר הקשתות שקצה אחד שלהן ב-U והשני ב-$\bar{U}$ — יהיה מינימלי.

מדוע התנאי $\emptyset \subsetneq U \subsetneq V$ הכרחי. בלעדיו הפתרון $U = \emptyset$ (או $U = V$) הוא טריוויאלי ונותן חתך בגודל 0 תמיד [01:12:37]. אנחנו דורשים חתך לא-מנוון.

מופע. בגרף מעגל על 4 צמתים, כל חתך לא-מנוון גוזר לפחות 2 קשתות, והמינימום הוא 2.

הערת סיווג. הבעיה **אינה** NP-קשה: היא ניתנת לפתרון בזמן פולינומי דטרמיניסטי, אך האלגוריתם הידוע מסובך, איטי וקשה למימוש [01:14:08]. זו בדיוק המוטיבציה לאלגוריתם האקראי הפשוט שלהלן.

הגדרה 5: כיווץ קשת (contraction)

בהינתן גרף G וקשת $\{x, y\} \in E$, **כיווץ** הקשת מייצר גרף חדש שבו x ו-y מוחלפים בצומת יחיד חדש, וכל הקשתות שהיו מחוברות ל-x או ל-y מחוברות עכשיו לצומת החדש. כל שאר הקשתות נשמרות.

התוצאה היא בדרך כלל **מולטי-גרף**: אם צומת z היה שכן של x וגם של y, יש עכשיו שתי קשתות מקבילות בין z לצומת החדש, ומספר הקשתות נשמר. הקשת המכווצת עצמה הופכת ללולאה עצמית; אפשר למחוק אותה או להשאיר אותה — היא אינה משפיעה על אף חתך, כי שני קצותיה יימצאו לעולם באותו צד [00:07:36 בהקלטה העוקבת].

משפטים והוכחות

משפט 1: העצמה בטעות חד-צדדית מהסתברות זניחה

טענה. לכל פולינום q: $\mathrm{BPP}\left(\frac{1}{2}, 1\right) = \mathrm{RP} = \mathrm{BPP}\left(\frac{1}{q(n)}, 1\right)$

זו התוצאה המרכזית של השיעור, והמרצה מציין שהיא מפתיעה יותר מזו של השיעור הקודם: הסתברות ההצלחה ההתחלתית **זניחה לחלוטין** — למשל $1/n^{50}$ — ובכל זאת אפשר להעלות אותה ל-$\frac{1}{2}$, ומשם (לפי שיעור 16) עד $1 - \frac{1}{q'(n)}$ [00:02:41]. כל זה מסתמך באופן חזק ביותר על החד-צדדיות.

הכיוון הקל: $\mathrm{RP} \subseteq \mathrm{BPP}\left(\frac{1}{q(n)}, 1\right)$

זהו הכיוון של הדרישה החלשה. מכונה המקיימת $\Pr[M \text{ accepts } x] \geq \frac{1}{2}$ על yes-instances מקיימת בפרט $\Pr[M \text{ accepts } x] \geq \frac{1}{q(n)}$, כי $\frac{1}{2} \geq \frac{1}{q(n)}$; דרישת ה-no-instances זהה בשתי המחלקות. $\square$

הערה: בהרצאה נאמר "עבור קלטים מגודל מסוים" [00:08:32] וזה נכון ומחייב פירוט. אי-השוויון $\frac{1}{2} \geq \frac{1}{q(n)}$ מתקיים רק כאשר $q(n) \geq 2$, ופולינום עשוי לקבל ערכים קטנים מ-2 עבור מספר **סופי** של קלטים קטנים. את הקלטים האלה מטפלים כרגיל: מקודדים לתוך המכונה טבלה סופית עם התשובה הנכונה לכל אחד מהם. טבלה סופית אינה משנה לא את הזמן האסימפטוטי ולא את הפולינומיות.

הכיוון העיקרי: $\mathrm{BPP}\left(\frac{1}{q(n)}, 1\right) \subseteq \mathrm{RP}$

יהי q פולינום ותהי $A \in \mathrm{BPP}\left(\frac{1}{q(n)}, 1\right)$. לפי ההגדרה קיימת מכונה הסתברותית M הרצה בזמן פולינומי כך שלכל x:

$$x \in A \implies \Pr[M \text{ accepts } x] \geq \frac{1}{q(n)} \quad x \notin A \implies \Pr[M \text{ rejects } x] \geq 1$$

(השורה השנייה אומרת כמובן שההסתברות **שווה** 1; היא נכתבת עם $\geq$ רק כדי להתאים לתבנית ההגדרה [00:29:17].)

האלגוריתם. נגדיר מכונה הסתברותית $\hat{M}$ באופן הבא. על קלט x:

$\hat{M}$ תחשב את $q(|x|)$.

$\hat{M}$ תריץ את M על x באופן **בלתי-תלוי** $q(|x|)$ פעמים.

$\hat{M}$ תקבל אם ורק אם M קיבלה **לפחות פעם אחת**.

הערה: שלב 1 נראה מיותר אך נכתב במפורש בכוונה [00:16:32]: כדי להריץ משהו $q(|x|)$ פעמים צריך קודם כל **לחשב** את המספר הזה, וזהו שלב חישובי שיש להצדיק את זמנו.

הערה: מדוע דווקא "לפחות פעם אחת" ולא "רוב הפעמים"? זו בדיוק הנקודה שבה החד-צדדיות נכנסת [00:18:40]. אילו היינו דורשים רוב, לא היינו יכולים להתמודד עם הסתברות התחלתית $1/q(n)$ בכלל, כי הרוב המצופה הוא reject. אבל מכיוון שאין false positives, תשובת accept בודדת היא **הוכחה חותכת** ש-$x \in A$, ולכן די בה. המרצה מציין שגם אם לא יודעים מראש כמה פעמים צריך להריץ, נכון להתחיל עם פרמטר t פתוח, לנתח, ורק בסוף לקבוע אותו — ולא להיתקע בבחירה [00:17:36].

ניתוח זמן ריצה. q פולינום, ולכן:

חישוב $q(|x|)$ (שלב 1) מתבצע בזמן פולינומי — חישוב ערך של פולינום על מספר בגודל $|x|$ הוא פולינומי.

$\hat{M}$ מריצה את M מספר **פולינומי** של פעמים, וכל הרצה בודדת של M רצה בזמן פולינומי.

מכפלה של פולינום בפולינום היא פולינום, ולכן סך הכל $\hat{M}$ רצה בזמן פולינומי. $\square$

הערה: הסגירות הזו — של הפולינומים לחיבור, לכפל ולהרכבה — היא כל ה"קסם" של המשפט, וכדאי לומר זאת במפורש [00:01:35]. אנחנו כן משלמים מחיר: אם M רצה בזמן n^2, $\hat{M}$ עשויה לרוץ בזמן n^{50}. פשוט הרזולוציה שבה אנחנו מסתכלים על זמן ריצה — "פולינומי או לא" — גסה מכדי לראות את ההפרש. במודל הדטרמיניסטי עם מחרוזת אקראית מפורשת (שיעור 16), המחיר נראה גם באורך המחרוזת: אם M צרכה $p(n)$ סיביות אקראיות, $\hat{M}$ צורכת $p(n) \cdot q(n)$ [00:09:39].

ניתוח הסתברותי. יהי x קלט, ונסמן $n = |x|$.

מקרה א': $x \notin A$. בכל הרצה בודדת של M על x, המכונה M דוחה בהסתברות 1. לכן בכל $q(n)$ ההרצות התקבל reject, ולכן $\hat{M}$ דוחה: $\Pr[\hat{M} \text{ rejects } x] = 1 \geq 1$ כלומר $\hat{M}$ שומרת על החד-צדדיות — אין לה false positives, כפי שנדרש עבור RP.

מקרה ב': $x \in A$. כאן מתחיל החשבון. המאורע "$\hat{M}$ מקבלת" הוא "**קיימת** הרצה j שבה M קיבלה". אי-תלות אינה מתמשקת יפה עם "קיים"/"או", אלא עם "לכל"/"וגם", ולכן עוברים למאורע המשלים [00:35:00]:

$$\hat{M} \text{ rejects } x \iff \text{in every iteration } j \in \{1, \dots, q(n)\},\ M \text{ rejects } x$$

מכיוון שקבוצת האיטרציות **סופית**, הכמת "לכל" מתורגם לשרשרת סופית של "וגם" — בדיוק כפי שעשינו בבעיית שמונה המלכות ובמשפט Cook–Levin [00:34:27]. עכשיו אפשר להפעיל אי-תלות:

$$\Pr[\hat{M} \text{ rejects } x] = \Pr\left[\bigwedge_{j=1}^{q(|x|)} M \text{ rejects } x \text{ in iteration } j\right] \overset{\text{independence}}{=} \prod_{j=1}^{q(|x|)} \Pr[M \text{ rejects } x \text{ in iteration } j]$$

נחסום כל גורם. ידוע ש-$\Pr[M \text{ accepts } x] \geq \frac{1}{q(|x|)}$, ולכן על המאורע המשלים:

$$\Pr[M \text{ rejects } x \text{ in iteration } j] \leq 1 - \frac{1}{q(|x|)}$$

הערה: המעבר הזה חשוב מספיק כדי לומר אותו במפורש [00:38:39]: אם $\Pr[B] \geq \alpha$ אז $\Pr[\bar{B}] \leq 1 - \alpha$ — אי-השוויון **מתהפך** במעבר למשלים. אנו מבצעים את ההיפוך פעמיים: פעם כאן כדי לחסום מלמעלה את הסתברות הדחייה, ופעם בסוף כדי לחזור לחסם מלמטה על הסתברות הקבלה. הסיבה שהחסם מלמעלה על הדחייה הוא ה"טוב" עבורנו היא שאותו אנחנו יודעים לפרק למכפלה.

מכיוון שכל הגורמים אי-שליליים, אפשר להציב את החסם בכל אחד מהם:

$$\prod_{j=1}^{q(|x|)} \Pr[M \text{ rejects } x \text{ in iteration } j] \leq \left(1 - \frac{1}{q(|x|)}\right)^{q(|x|)}$$

הלמה האנליטית. לכל $x \in \mathbb{R}$ מתקיים $1 + x \leq e^x$.

הערה: בהרצאה זה נאמר כעובדה מוכרת "בת מאתיים שנה" [00:40:24]; הנה ההצדקה. נגדיר $f(x) = e^x - 1 - x$. אז $f'(x) = e^x - 1$, ולכן $f'(x) < 0$ עבור $x < 0$ ו-$f'(x) > 0$ עבור $x > 0$; מכאן ש-f יורדת ואז עולה, ומקבלת מינימום גלובלי ב-$x = 0$, שם $f(0) = 0$. לכן $f(x) \geq 0$ לכל x, כלומר $1 + x \leq e^x$. שקילות: זהו בדיוק אי-השוויון האומר שהגרף של e^x נמצא מעל המשיק שלו בנקודה 0 (קמירות).

נציב $x = -\frac{1}{q(|x|)}$ ונקבל $1 - \frac{1}{q(|x|)} \le e^{-1/q(|x|)}$. שני האגפים אי-שליליים (עבור $q(|x|) \ge 1$), ולכן מותר להעלות בחזקה חיובית ולשמור על הכיוון:

$$\left(1 - \tfrac{1}{q(|x|)}\right)^{q(|x|)} \;\le\; \left(e^{-\frac{1}{q(|x|)}}\right)^{q(|x|)} = e^{-1} = \tfrac{1}{e} \le \tfrac{1}{2}$$

המעבר האחרון נכון כי $e > 2$.

לסיכום, עבור $x \in A$: $\Pr[\hat{M} \text{ accepts } x] \ge \frac{1}{2} \implies \Pr[\hat{M} \text{ rejects } x] \le \frac{1}{2}$

יחד עם מקרה א', $\hat{M}$ היא מכונה הסתברותית פולינומית עם $\Pr[\text{accept}] \ge \frac{1}{2}$ על yes-instances ו-$\Pr[\text{reject}] = 1$ על no-instances, כלומר $A \in \mathrm{BPP}\left(\frac{1}{2}, 1\right) = \mathrm{RP}$. ■

מדוע הבחירה $q(|x|)$ ולא משהו אחר

המרצה מדגיש שהמספר הזה **אינו קדוש** [00:27:36]: ההוכחה עובדת בדיוק באותו אופן עבור $q(|x|)^2$, $2q(|x|)$, $q(|x|) + 3$ וכן הלאה — כל דבר פולינומי ב-$|x|$ עובד, כי ניתוח זמן הריצה תלוי רק בפולינומיות, וניתוח ההסתברות רק משתפר. מה שכן קריטי הוא שהמספר יהיה **פולינומי** — כאן זה בדיוק המקום שבו נשבר הגבול.

מדוע $\mathrm{BPP}\left(\frac{1}{2^{q(n)}}, 1\right)$ אינה ניתנת להעצמה

זו הערה חשובה שנאמרה בכיתה [00:04:15] ואינה מופיעה בסיכום. שימו לב שהסף $\frac{1}{q(n)}$ **גדול** מהסף $\frac{1}{2^{q(n)}}$, כי מעריכי גדול מפולינומי; כלומר $\mathrm{BPP}\left(\frac{1}{2^{q(n)}}, 1\right)$ היא מחלקה גדולה יותר או שווה. עבורה **אין** לנו הוכחה שהיא שווה ל-RP.

הסיבה נראית מיד מהחשבון: כדי להוריד את הסתברות השגיאה מתחת ל-$\frac{1}{2}$ אנחנו צריכים בערך t הרצות עם $t \cdot \alpha \approx 1$, כלומר $t \approx 1/\alpha$. עם $\alpha = \frac{1}{q(n)}$ זה $q(n)$ הרצות — פולינומי, מצוין. עם $\alpha = \frac{1}{2^{q(n)}}$ זה $2^{q(n)}$ הרצות — **מעריכי**, ו-$\hat{M}$ כבר אינה רצה בזמן פולינומי. הפולינומיות של מספר החזרות היא המשאב שההוכחה צורכת, ומספר החזרות הדרוש הוא הופכי לסף.

משפט 2 (ללא הוכחה): העצמה בטעות דו-צדדית

טענה. לכל פולינום q: $\mathrm{BPP} = \mathrm{BPP}\left(1 - \frac{1}{2^{q(n)}}, 1 - \frac{1}{2^{q(n)}}\right) = \mathrm{BPP}\left(\frac{1}{2} + \frac{1}{q(n)}, \frac{1}{2} + \frac{1}{q(n)}\right)$

שתי השוויונות ביחד אומרות: **כל** סף בטווח שבין "מעט יותר מחצי בפער פולינומי" לבין "אחד פחות משהו זניח מעריכית" מגדיר את אותה מחלקה בדיוק, BPP.

מדוע זה נראה שונה מהמקרה החד-צדדי. בטעות דו-צדדית **אין אף תשובה שאפשר לסמוך עליה בוודאות**: גם accept עלול להיות שגוי וגם reject [00:46:04]. לכן הכלל "קבל אם התקבל accept ולו פעם אחת" חסר משמעות, ובמקומו יש להצביע רוב. ומכיוון שהחלטת הרוב היא סטטיסטית ולא לוגית, היא זקוקה לכך שרוב ההרצות **באמת** יהיו נכונות — כלומר להטיה של ממש מעל $\frac{1}{2}$.

שני גבולות שאסור לחצות:

סף של בדיוק $\frac{1}{2}$ חסר תוכן. ראו הגדרה 1: $\mathrm{BPP}\left(\frac{1}{2}, \frac{1}{2}\right)$ מכילה כל שפה, כי מטבע הוגן משיג את הסף בלי לחשב דבר [00:05:18]. אין שום מה להעצים כאשר האלגוריתם אינו מכיל אפילו טיפת אינפורמציה.

פער זניח מעריכית אינו מספיק. $\mathrm{BPP}\left(\frac{1}{2} + \frac{1}{2^{q(n)}}, \frac{1}{2} + \frac{1}{2^{q(n)}}\right)$ אינה ידועה כשווה ל-BPP [00:48:15]. הניסוח שהמרצה נתן: הפער מ-$\frac{1}{2}$ מותר להיות זניח, אבל **לא זניח מדי** — הוא חייב להיות $1/\mathrm{poly}$, ולא $1/\exp$.

זהו הניגוד המדויק למקרה החד-צדדי: שם מותר היה לסף עצמו להיות זעיר ($1/q(n)$), כאן מותר רק **לפער מהחצי** להיות זעיר.

מדוע אין הוכחה כאן. ההוכחה הכללית עוברת דרך אי-שוויון ריכוז — **אי-שוויון צ'רנוף** (Chernoff) — שאינו נלמד בקורס ההסתברות של הסטודנטים ולא בקורס הזה [00:50:56]. המרצה הבהיר במפורש את גבולות הדרישה: **את הטענה צריך לדעת, צריך לדעת להשתמש בה, וצריך לדעת שהיא נכונה — אך לא להוכיח אותה** [00:51:59]. במקום ההוכחה, נעשה בכיתה מקרה פרטי מחושב בידיים, והוא משפט 3.

הסיבה שזה עובד, בשורה אחת. משתנה מקרי בינומי מרוכז סביב התוחלת שלו [01:08:48]. אם מריצים t ניסויים בלתי-תלויים עם הסתברות הצלחה $\frac{2}{3}$, התוחלת של מספר ההצלחות היא $\frac{2}{3}t$ — שהיא מעל $\frac{t}{2}$ — וההסתברות לסטות ממנה כלפי מטה עד מתחת ל-$\frac{t}{2}$ דועכת **מעריכית** ב-t. זה מסביר גם את הצורה של המשפט: הפער בין $\frac{2}{3}$ (או $\frac{1}{2}+\frac{1}{q}$) לבין $\frac{1}{2}$ הוא בדיוק מרחק הסטייה שהריכוז צריך לכסות, ולכן הוא מה שההוכחה "אוכלת".

משפט 3: $\mathrm{BPP}=\mathrm{BPP}\left(\frac{4}{5},\frac{4}{5}\right)$ — המקרה המוכח

זו **גרסת הצעצוע** של משפט 2 [01:08:18], והיא ההוכחה המלאה היחידה של העצמה דו-צדדית בקורס. המטרה צנועה: להעלות את $\frac{2}{3}$ ל-$\frac{4}{5}$ בלבד.

הכיוון הקל

$\mathrm{BPP}\left(\frac{4}{5},\frac{4}{5}\right)\subseteq\mathrm{BPP}$, כי $\frac{4}{5}\geq\frac{2}{3}$ ולכן הדרישה חזקה יותר (הגדרה 1). $\square$

הכיוון העיקרי: $\mathrm{BPP}\subseteq\mathrm{BPP}\left(\frac{4}{5},\frac{4}{5}\right)$

תהי $A\in\mathrm{BPP}$. קיימת מכונה הסתברותית M הרצה בזמן פולינומי כך שלכל x: $x\in A\implies\Pr[M\text{ accepts }x]\geq\frac{2}{3}$, $\quad x\notin A\implies\Pr[M\text{ rejects }x]\geq\frac{2}{3}$

האלגוריתם. נגדיר $\hat{M}$: על קלט x,

$\hat{M}$ תריץ את M על x **שבע** פעמים, באופן בלתי-תלוי.

$\hat{M}$ תחזיר את התשובה שהתקבלה הכי הרבה פעמים (רוב מבין 7).

מדוע 7 אי-זוגי. ראו הגדרה 3: 7 אי-זוגי, ולכן קיים תמיד רוב חד-משמעי ($4\geq$ מול ≤ 3) ואין צורך בכלל שבירת-תיקו [00:55:19].

מדוע דווקא 7 ולא 5. המרצה סיפר במפורש שניסה 5 **וזה לא עבד** — ושבשנה קודמת הוא עשה את החישוב עם 5 על הלוח, טעה בחשבון, וחשב בטעות שקיבל $\geq\frac{4}{5}$ [00:56:27]. בסעיף הדוגמאות מובא החשבון שמראה בדיוק היכן 5 נופל.

זמן ריצה. $\hat{M}$ מריצה את M מספר **קבוע** של פעמים (7), וכל הרצה פולינומית; לכן $\hat{M}$ פולינומית. אין כאן אפילו צורך בחישוב מקדים של מספר החזרות כמו במשפט 1, כי 7 קבוע [00:56:58]. $\square$

ניתוח הסתברותי. יהי x. **היתרון של הטעות הדו-צדדית הוא הסימטריה** [00:57:33]: שני המקרים ($x\in A$ ו-$x\notin A$) זהים לחלוטין, ולכן די להוכיח אחד מהם.

נניח $x\in A$, ונסמן ב-$p=p_x=\Pr[M\text{ accepts }x]$ את הסתברות ההצלחה האמיתית של M על הקלט הזה; ידוע ש-$p\geq\frac{2}{3}$.

$\hat{M}$ מקבלת בדיוק כאשר M קיבלה לפחות 4 פעמים מתוך 7. שימו לב שכאן, בניגוד למשפט 1, **אין** טעם לעבור למאורע המשלים: אין כאן "קיים" שצריך להפוך ל"לכל", אלא ספירה [00:58:42].

$$\Pr[\hat{M}\text{ accepts }x] \;=\; \Pr[M\text{ accepted at least 4 times}] \;=\; \sum_{k=4}^{7}\Pr[M\text{ accepted exactly }k\text{ times}]$$

המעבר האחרון תקף כי המאורעות "בדיוק 4", "בדיוק 5", "בדיוק 6", "בדיוק 7" הם **זרים בזוגות** — לא ייתכן שהמכונה קיבלה בדיוק 4 פעמים וגם בדיוק 5 פעמים — ולכן הסתברות האיחוד היא סכום ההסתברויות [00:59:53]. (כאן זרות היא הכלי, ולא אי-תלות; ראו ההערה בהגדרה 3.)

חישוב האיבר הבודד. מהי ההסתברות ש-M קיבלה בדיוק k פעמים? זו התפלגות בינומית, אבל המרצה גוזר אותה מאפס [01:00:54]:

ראשית בוחרים **באילו** k מתוך 7 ההרצות תהיה הצלחה: $\binom{7}{k}$ אפשרויות.

באותן k הרצות שנבחרו נדרשת הצלחה: מכיוון שההרצות בלתי-תלויות, ההסתברות המשותפת היא מכפלה — p^k.

בשאר $7-k$ ההרצות נדרש כישלון: $(1-p)^{7-k}$.

$$\Pr[M\text{ accepted exactly }k\text{ times}] \;=\; \binom{7}{k}p^k(1-p)^{7-k}$$

ולכן $$\Pr[\hat{M}\text{ accepts }x] \;=\; \sum_{k=4}^{7}\binom{7}{k}p^k(1-p)^{7-k} \;=\; \Pr[\mathrm{Bin}(7,p)\ge 4]$$

המעבר ל-$p=\frac{2}{3}$. אנחנו רוצים לחסום מלמטה באמצעות $p=\frac{2}{3}$: $$\Pr[\mathrm{Bin}(7,p)\ge 4] \;\ge\; \sum_{k=4}^{7}\binom{7}{k}\left(\tfrac{2}{3}\right)^{k}\left(\tfrac{1}{3}\right)^{7-k}$$

> **הערה:** בהרצאה [01:03:02] ובסיכום ההצדקה שניתנה היא "כי הסתברות ההצלחה גדולה שווה $\frac{2}{3}$", והיא נאמרה כאילו היא פועלת **איבר-איבר**. איבר-איבר זה **לא נכון**, וזו נקודה שכדאי לשים אליה לב: עבור $k=4$ למשל, הפונקציה $p^4(1-p)^3$ מתאפסת ב-$p=1$, ולכן היא בהחלט אינה מונוטונית עולה ב-p. מה שנכון הוא אי-השוויון על **הסכום**, כלומר על זנב ההתפלגות. הנה ההצדקה המלאה, בשיטת הצמדה (coupling): יהיו $U_1,\dots,U_7$ משתנים בלתי-תלויים אחידים על $[0,1]$, ונגדיר "הצלחה i ברמה p" כמאורע $U_i\le p$. אז מספר ההצלחות ברמה p מתפלג $\mathrm{Bin}(7,p)$, ואם $p\le p'$ אז כל הצלחה ברמה p היא גם הצלחה ברמה p', ולכן מספר ההצלחות ברמה p' גדול או שווה **נקודתית**. מכאן $\Pr[\mathrm{Bin}(7,p')\ge 4] \ge \Pr[\mathrm{Bin}(7,p)\ge 4]$, כלומר זנב בינומי הוא מונוטוני עולה ב-p. הצבת $p\ge\frac{2}{3}$ נותנת בדיוק את אי-השוויון שרצינו.

החשבון. (הפירוט המספרי המלא של כל ארבעת האיברים מובא בסעיף הדוגמאות.)

$$\sum_{k=4}^{7}\binom{7}{k}\left(\tfrac{2}{3}\right)^{k}\left(\tfrac{1}{3}\right)^{7-k} \;=\; \frac{560+672+448+128}{2187} \;=\; \frac{1808}{2187} \;\approx\; 0.8267 \;\ge\; \frac{4}{5}$$

(אכן $1808 \le \frac{4}{5}\cdot 2187 = 1749.6$.)

לכן עבור $x\in A$ מתקיים $\Pr[\hat{M}\text{ accepts }x]\ge\frac{4}{5}$.

המקרה $x\notin A$. באופן זהה לחלוטין, בהחלפת התפקידים של accept ו-reject: $\Pr[M\text{ rejects }x]\ge\frac{2}{3}$, $\hat{M}$ דוחה בדיוק כאשר M דחתה לפחות 4 פעמים מתוך 7, ואותו חשבון בדיוק נותן $\Pr[\hat{M}\text{ rejects }x]\ge\frac{4}{5}$.

הערה: בהרצאה נכתב כאן "באופן דומה" [01:09:20], והמרצה עצמו העיר בבדיחות שהוא נמנע מזה בדרך כלל. במקרה הזה ההצדקה אמיתית ומלאה: המבנה של $\mathrm{BPP}(\alpha,\alpha)$ סימטרי לחלוטין תחת החלפת accept ב-reject ו-A במשלים שלה, ואף לא צעד אחד בחישוב משתמש בזהות של הצד. זהו בדיוק ההבדל ממשפט 1, שם המקרים היו א-סימטריים לגמרי.

מכאן $A \in \mathrm{BPP}\left(\frac{4}{5},\frac{4}{5}\right)$. ■

דוגמאות ותרגילים מהשיעור

דוגמה 1: החשבון הבינומי המלא של משפט 3

זהו החישוב שהמרצה הכין מראש בבית והעתיק ללוח [00:55:53]. נחשב תחילה $3^7 = 2187$, ונרשום את כל האיברים על מכנה משותף זה.

האיבר $k=4$: $\binom{7}{4}\left(\frac{2}{3}\right)^4\left(\frac{1}{3}\right)^3 = \frac{7!}{4!\,3!}\cdot\frac{16}{81}\cdot\frac{1}{27} = 35\cdot\frac{16}{2187} = \frac{560}{2187}$

האיבר $k=5$: $\binom{7}{5}\left(\frac{2}{3}\right)^5\left(\frac{1}{3}\right)^2 = 21\cdot\frac{32}{243}\cdot\frac{1}{9} = \frac{21\cdot 32}{2187} = \frac{672}{2187}$

האיבר $k=6$: $\binom{7}{6}\left(\frac{2}{3}\right)^6\left(\frac{1}{3}\right)^1 = 7\cdot\frac{64}{729}\cdot\frac{1}{3} = \frac{7\cdot 64}{2187} = \frac{448}{2187}$

האיבר $k=7$: $\binom{7}{7}\left(\frac{2}{3}\right)^7 = \frac{128}{2187}$

הסכום: $\frac{560+672+448+128}{2187} = \frac{1808}{2187} \approx 0.8267 \;\geq\; 0.8 = \frac{4}{5}$

הערות חשבון שהמרצה ביצע בכיתה: $\binom{7}{4} = \frac{7!}{4!\,3!} = \frac{7\cdot 6\cdot 5}{6} = 35$; $\binom{7}{5} = 21$; $\binom{7}{6} = 7$; $81\cdot$ $27 = 2187$; $35\cdot 16 = 560$.

דוגמה 2: מדוע 5 הרצות לא מספיקות

זו הדוגמה שהמרצה סיפר עליה כטעות של שנה שעברה [00:56:27], אך לא חישב על הלוח. הנה החשבון. עם 5 הרצות, רוב הוא ≥ 3, והמכנה הוא $3^5 = 243$:

$$\binom{5}{5}\left(\tfrac{2}{3}\right)^5 = \tfrac{32}{243} \quad \binom{5}{4}\left(\tfrac{2}{3}\right)^4\left(\tfrac{1}{3}\right)^1 = 5\cdot\tfrac{16}{81}\cdot\tfrac{1}{3} = \tfrac{80}{243} \quad \binom{5}{3}\left(\tfrac{2}{3}\right)^3\left(\tfrac{1}{3}\right)^2 = 10\cdot\tfrac{8}{27}\cdot\tfrac{1}{9} = \tfrac{80}{243}$$

סה"כ:

$$\frac{80+80+32}{243} = \frac{192}{243} \approx 0.7901$$

ואכן $0.7901 < 0.8$ — **חסר**, בהפרש קטן מאוד. זה ממחיש היטב עד כמה ההעצמה איטית כשעובדים בידיים, ולמה בפועל משתמשים באי-שוויון צ'רנוף.

דוגמה 3: מדוע מספר זוגי של הרצות מבוזבז

נניח שהיינו מריצים 6 פעמים. אז $3^6 = 729$, ורוב הוא ≥ 4: $\binom{6}{4}\left(\frac{2}{3}\right)^4\left(\frac{1}{3}\right)^2 = 15\cdot\frac{16}{81}\cdot\frac{1}{9} =$ $\binom{6}{6}\left(\frac{2}{3}\right)^6 = \frac{64}{729}$, $\binom{6}{5}\left(\frac{2}{3}\right)^5\left(\frac{1}{3}\right) = 6\cdot\frac{32}{243}\cdot\frac{1}{3} = \frac{192}{729}$, סכום: $\frac{240}{729}$, $\frac{496}{729} \approx 0.680$ — פחות אפילו מ-5 הרצות. הבעיה: המאורע "תיקו 3 מול 3" קיבל הסתברות $\binom{6}{3}\left(\frac{2}{3}\right)^3\left(\frac{1}{3}\right)^3 = \frac{160}{729}$ ואינו נספר.

אם נשבור את התיקו במטבע הוגן, נקבל $\frac{496}{729} + \frac{1}{2}\cdot\frac{160}{729} = \frac{496+80}{729} = \frac{576}{729} = \frac{192}{243} \approx 0.7901$ כלומר **בדיוק** התוצאה של 5 הרצות. ההרצה השישית לא תרמה דבר. זה מנמק את הבחירה במספר אי-זוגי לא רק כנוחות סימונית אלא כהימנעות מבזבוז ממשי.

דוגמה 4: חשבון הסיביות האקראיות במשפט 1

נניח ש-M המקורית משתמשת ב-$p(n) = n^2$ סיביות אקראיות ורצה בזמן $O(n^2)$, ונניח $q(n) = n^3$ (כלומר הסתברות ההצלחה ההתחלתית היא $1/n^3$). אז $\hat{M}$:

מריצה את M בדיוק n^3 פעמים,

זמן ריצה $O(n^3 \cdot n^2) = O(n^5)$ — פולינומי,

צורכת $n^3 \cdot n^2 = n^5$ סיביות אקראיות — פולינומי [00:09:39],

והסתברות הכישלון שלה על yes-instance היא לכל היותר $\left(1 - \frac{1}{n^3}\right)^{n^3} \leq \frac{1}{e} < 0.37$.

לעומת זאת, אילו הסתברות ההצלחה ההתחלתית הייתה 2^{-n}, היינו צריכים 2^n הרצות — ומיד יוצאים מהזמן הפולינומי. זה הקיר שתואר בסוף משפט 1.

דוגמה 5: אלגוריתם הכיווץ האקראי לחתך מינימלי (פתיחה בלבד)

בשלושים הדקות האחרונות נפתחה הבעיה הבאה, כמעבר לנושא של השיטה ההסתברותית [01:10:54]. הסיכום מקדיש לה את עמוד 3.

האלגוריתם. קלט: גרף $G = (V, E)$ לא מכוון (אפשר להניח שהוא **קשיר**; אחרת רכיב קשירות לא-טריוויאלי נותן חתך בגודל 0 ואפשר להחזירו מיד לאחר [01:15:17] BFS).

כל עוד יש בגרף יותר משני קודקודים:

בחר קשת באקראי, בהתפלגות **אחידה**, מבין הקשתות של הגרף **הנוכחי** (זה שמתעדכן תוך כדי).

כווץ את הקשת שנבחרה (הגדרה 5).

החזר את גודל החתך בין שני הקודקודים שנותרו.

מעקב אחר מופע. נניח $V = \{1, 2, 3, 4, 5\}$ עם הקשתות $\{1, 2\}, \{2, 3\}, \{1, 3\}, \{1, 5\}, \{2, 4\}, \{4, 5\}$, ונניח שנבחרה לכיווץ הקשת $\{1, 3\}$. אחרי הכיווץ מתקבל צומת חדש $\{1, 3\}$, ו:

ל-2 יש עכשיו **שתי** קשתות מקבילות אל הצומת החדש (אחת מ-$\{1, 2\}$ ואחת מ-$\{2, 3\}$),

קשת אחת מהצומת החדש אל 5 (מ-$\{1, 5\}$),

הקשת $\{1, 3\}$ עצמה הפכה ללולאה עצמית — אפשר להתעלם ממנה,

והקשתות $\{4, 5\}, \{2, 4\}$ נשארות כפי שהיו.

הגרף החדש הוא מולטי-גרף על 4 צמתים. בכל איטרציה מספר הצמתים יורד בדיוק באחד, ולכן האלגוריתם עוצר אחרי $|V| - 2$ איטרציות.

מה שהמרצה כבר גילה (spoiler מוצהר). האלגוריתם מצליח בהסתברות "לא משהו" — נמוכה — אבל **חוזרים עליו הרבה פעמים באופן בלתי-תלוי וזה עובד טוב** [01:20:06]. כלומר, בדיוק אותה טכניקת ההעצמה שהוכחנו בשיעור הזה תופעל שם. הניתוח המלא — כולל ההסתברות המדויקת להצלחה בהרצה בודדת וזמן הריצה — נעשה בשיעור 18; ראו שיעור 18.

הערות מהשיעור

[00:01:04] המחיר של ההעצמה אינו אפס. "זה לא קסם." זמן הריצה אכן גדל, ואיתו גם מספר הסיביות האקראיות. פשוט הרשת שבה אנחנו מודדים — פולינומי מול לא-פולינומי — גסה מדי מכדי לראות את ההפרש. אם המחלקות היו מוגדרות לפי זמן $O(n^2)$ מדויק, המשפט היה **שגוי**.

[00:06:22] "אני אף פעם לא זוכר את זה." המרצה חוזר שלוש פעמים על כך שהוא בעצמו מתבלבל בין false positive ל-false negative, ותמיד עוצר לצייר את טבלת הבלבול. ההמלצה המפורשת: אל תעשו את זה מהראש במבחן.

[00:17:36] אסטרטגיה לכתיבת הוכחה. אם אינכם יודעים כמה פעמים להריץ — כתבו t (המרצה הציע: באדום), המשיכו בניתוח, וקבעו את t בסוף כשהחשבון יגיד לכם. "אתם לא יכולים לראות איך זה ייגמר במעמד תחילת השאלה. לא לצפות לזה, לא לכוון לזה."

[00:27:05] נסו לשחרר את הקבוע. אחרי שההוכחה עובדת, שאלו את עצמכם על מה היא באמת נשענת. כאן: לא על הערך $q(|x|)$ אלא רק על כך שהוא פולינומי.

[00:30:48] מלכודת: זרים $\neq$ בלתי-תלויים. שאלת סטודנטית שחשפה סוגיה אמיתית. שני מאורעות זרים בעלי הסתברות חיובית הם **תלויים מאוד**, כי התרחשות אחד שוללת את השני. אי-תלות היא $\Pr[X \cap Y] = \Pr[X]\Pr[Y]$.

[00:33:54] מתי הופכים למאורע המשלים. כלל אצבע שנאמר במפורש: אי-תלות מתמשקת עם "וגם"; לכן אם המאורע שלכם הוא "קיים"/"או", הפכו למשלים כדי לקבל "לכל"/"וגם", חסמו, וחזרו. במשפט 1 עושים את ההיפוך פעמיים.

[00:35:32] "קיים" בקבוצה סופית. מכיוון שמספר האיטרציות סופי, אין צורך בכמת בכלל — פורסים אותו לשרשרת סופית של "או". באלגוריתמים אמיתיים מספר האיטרציות תמיד סופי, בניגוד למה שהיה בקורס חישוביות.

[00:48:45] טריק שימושי מאוד לתרגילים. אם נתונה מחלקה עם שני ספים שונים, למשל $\mathrm{BPP}\left(\frac{2}{3}, \frac{9}{10}\right)$, אפשר תמיד להכיל אותה במחלקה הסימטרית עם **הסף הקטן** מבין השניים, ולעבוד עם זה. תמיד עובד, לכל כיוון שצריך.

[00:50:26] "אני עושה הצבעה." שאלת סטודנט: "האם הרוב בהכרח נכון?" תשובה: אין "בהכרח" — יש רק **הסתברות**. הרוב אינו מבטיח דבר; הוא רק מגדיל את ההסתברות.

[00:51:28] גבולות החומר. את הטענה הכללית (משפט 2) צריך לדעת, צריך לדעת להשתמש בה, וצריך לדעת שהיא נכונה. את החישוב הבינומי של משפט 3 צריך **להבין** ולדעת לשחזר בעיקרון, אך לא לייצר מאפס תחת לחץ זמן במבחן.

[00:56:27] "המבוכה הייתה קשה." המרצה סיפר שבשנה שעברה עשה את החישוב עם 5 הרצות בכיתה, טעה, וחשב שקיבל $\geq \frac{4}{5}$. הלקח המעשי: בחישובים בינומיים בידיים, בדקו את הסכום עד הסוף.

[00:45:04] מה לא בקורס. שונות ואי-שוויוני ריכוז אינם נלמדים; אינדיקטורים ולינאריות התוחלת יגיעו בשיעור הבא (שיעור 18) ויידרשו לניתוח אלגוריתם החתך.

[00:41:26] הערת עידוד. "מקדם חיכוך קינטי תמיד קטן ממקדם חיכוך סטטי" — כלומר, במבחן עדיף לבחור ערך ולהתקדם מאשר להיתקע בשאלה מה הערך הנכון.

פערים בין הסיכום להקלטה

מקור: הסיכום, עמוד 2, החישוב של האיבר $k = 4$. **הפער:** נכתב $\frac{16}{31}$ במקום $\frac{16}{81}$ (שכן $\left(\frac{2}{3}\right)^4 = \frac{16}{81}$). **ההכרעה:** שגיאת כתיב; תוקן ל-$\frac{16}{81}$. התוצאה שהסיכום ממשיך אליה, $\frac{560}{2187}$, נכונה ומאשרת שזו שגיאת העתקה בלבד.

מקור: ההקלטה, [00:55:19]. **הפער:** התמלול אומר "מספר **זוגי** של פעמים", אך מיד נבחר 7 והנימוק שניתן הוא "שתמיד יהיה רוב". **ההכרעה:** התמלול האוטומטי החסיר את השלילה; הכוונה למספר **אי-זוגי**. הסיכום (7) מכריע. נוסף כאן חישוב מפורש (דוגמה 3) המראה שמספר זוגי מבזבז הרצה.

מקור: שני המקורות, המעבר $\Pr[\mathrm{Bin}(7,p)\ge 4] \ge \sum_{k\ge 4}\binom{7}{k}\left(\frac{2}{3}\right)^k\left(\frac{1}{3}\right)^{7-k}$. **הפער:** ההצדקה נאמרה בסגנון איבר-איבר ("כי הסתברות ההצלחה $\ge \frac{2}{3}$"), וזה **אינו נכון** איבר-איבר — $p^4(1-p)^3$ אינה עולה ב-p. **ההכרעה:** אי-השוויון עצמו נכון (על הסכום, כלומר על הזנב); נוספה כאן הצדקה מלאה במונוטוניות זנב בינומי בשיטת coupling, ומצוין במפורש שהניסוח איבר-איבר שגוי.

מקור: ההקלטה בלבד, [00:04:15]–[00:04:46]. **הפער:** הדיון מדוע $\mathrm{BPP}\left(\frac{1}{2^{q(n)}},1\right)$ **אינה** ידועה כשווה ל-RP אינו מופיע כלל בסיכום. **ההכרעה:** נכלל כאן כתת-סעיף של משפט 1, עם החשבון שמסביר למה (מספר החזרות הדרוש הוא הופכי לסף).

מקור: ההקלטה בלבד, [00:05:18] ו-[00:48:45]. **הפער:** ההסבר מדוע סף של בדיוק $\frac{1}{2}$ בטעות דו-צדדית חסר תוכן (מטבע הוגן פותר כל שפה), והטריק של "ירידה לסף הקטן" — אינם בסיכום. **ההכרעה:** נכללו, הראשון כ-non-instance בהגדרה 1 והשני כהערה שם.

מקור: ההקלטה בלבד, [00:20:46]. **הפער:** טבלת הבלבול המלאה (false positive / false negative מול yes/no-instance) הוצגה על הלוח והוקדשו לה כחמש דקות; בסיכום אין לה זכר. **ההכרעה:** נכללה כטבלה בהגדרה 2.

מקור: ההקלטה בלבד, [00:30:48]–[00:35:32]. **הפער:** הדיון על אי-תלות מול זרות, ועל תרגום "קיים" ל"או" בקבוצה סופית, הוא כחמש דקות של שיעור ואינו בסיכום כלל (בסיכום מופיעה רק המילה "אי תלות" בכחול מתחת לסימן השוויון). **ההכרעה:** נכלל בהגדרה 3 ובהוכחת משפט 1.

מקור: ההקלטה בלבד, [00:09:39]. **הפער:** ההערה שההעצמה מגדילה את המחרוזת האקראית מ-$p(n)$ ל-$p(n)\cdot q(n)$, ושבשיעור 16 זה הודגם במפורש במודל הדטרמיניסטי, אינה בסיכום. **ההכרעה:** נכללה כהערה בניתוח זמן הריצה ובדוגמה 4.

מקור: ההקלטה בלבד, [00:50:56] ו-[01:08:48]. **הפער:** השם "אי-שוויון צ'רנוף" (בתמלול: "אי שוויון שרנו") וההסבר שהמנגנון הוא ריכוז של משתנה בינומי סביב תוחלתו — אינם בסיכום. **ההכרעה:** נכללו במשפט 2, יחד עם ההצהרה המפורשת שהמשפט אינו מוכח בקורס.

מקור: ההקלטה, [01:10:54]–[01:20:37] מול עמוד 3 בסיכום. **הפער:** עמוד 3 מכיל רק את הגדרת בעיית החתך המינימלי ואת פסאודו-הקוד של אלגוריתם הכיווץ, בעוד שבהקלטה ניתנה גם הדגמה מצוירת של כיווץ, ההנחה שהגרף קשיר, וההערה שהבעיה פתירה בזמן פולינומי דטרמיניסטי אך האלגוריתם מסובך. **ההכרעה:** נכלל בהגדרות 4–5 ובדוגמה 5, בקיצור בכוונה — הניתוח שייך לשיעור 18.

מקור: הנחיות הפרויקט מול המקורות. **הפער:** לא נמצאה בשני המקורות שום התייחסות לשאלה מדוע ל-BPP אין בעיה שלמה ידועה, או מדוע טכניקת ההעצמה אינה חלה על NP. **ההכרעה:** לא הומצא דיון כזה; מצוין ב- `open_questions` .

מקור: מוסכמות הסימון של הפרויקט. **הפער:** הסיכום כותב שמות מחלקות ללא `\mathrm{}` ומכניס עברית לתוך סוגריי ה-Pr. **ההכרעה:** שמות המחלקות והבעיות נכתבו כאן ב- `\mathrm{}` לפי §2a; מאורעות בתוך Pr נכתבו באנגלית (`rejects` / `accepts`) כדי לא לשלב עברית בתוך בלוק מתמטי. אותיות המשתנים (q, $\hat{M}$, x, k, j) נשמרו בדיוק כפי שהן בסיכום.

סיכום ונקודות למבחן

התוצאות שחייבים לזכור בעל פה:

לכל פולינום q: $\mathrm{RP} = \mathrm{BPP}\left(\frac{1}{2},1\right) = \mathrm{BPP}\left(\frac{1}{q(n)},1\right) = \mathrm{BPP}\left(1-\frac{1}{q(n)},1\right)$ (השוויון האחרון משיעור 16).

לכל פולינום q: $\mathrm{BPP} = \mathrm{BPP}\left(\frac{1}{2}+\frac{1}{q(n)},\frac{1}{2}+\frac{1}{q(n)}\right) = \mathrm{BPP}\left(1-\frac{1}{2^{q(n)}},1-\frac{1}{2^{q(n)}}\right)$.

$\mathrm{BPP}\left(\frac{1}{2},\frac{1}{2}\right)$ = כל השפות. חסר תוכן.

אי-השוויון $1+x \le e^x$ ומסקנתו $\left(1-\frac{1}{t}\right)^t \le \frac{1}{e} < \frac{1}{2}$.

המלכודות הסטנדרטיות:

בלבול כיוון ההכלה. דרישת הסתברות **גבוהה יותר** $\Rightarrow$ מחלקה **קטנה יותר**. תמיד בדקו "לאן קשה יותר להיכנס", אל תסמכו על הזיכרון.

בלבול false positive / false negative. ב-RP אין false positives, ולכן accept הוא אמין לחלוטין ו-reject אינו.

החלפת "לפחות פעם אחת" ב"רוב" (או להפך). "לפחות פעם אחת" חוקי **רק** בטעות חד-צדדית. "רוב" נדרש בטעות דו-צדדית, ואז חייבים מספר חזרות אי-זוגי.

שכחת אי-התלות. בלי לומר "בלתי-תלוי" במפורש בהגדרת האלגוריתם, המעבר למכפלה ולנוסחה הבינומית אינו מוצדק ואיבדתם את ההוכחה.

זרים במקום בלתי-תלויים. לפירוק "או" לסכום צריך **זרות**; לפירוק "וגם" למכפלה צריך **אי-תלות**. שני כלים שונים, ובשיעור הזה משתמשים בשניהם — במשפט 1 באי-תלות, במשפט 3 בשניהם.

ניסיון להעצים סף מעריכי. $\frac{1}{2^{q(n)}}$ (בחד-צדדית) או $\frac{1}{2}+\frac{1}{2^{q(n)}}$ (בדו-צדדית) — **אין** לנו העצמה, כי מספר החזרות היה יוצא מעריכי.

שכחת ניתוח זמן הריצה. ההעצמה אינה שלמה בלי להראות שהמכונה החדשה עדיין פולינומית, כולל חישוב $q(|x|)$ עצמו.

צ'ק-ליסט: בסוף השיעור אתם אמורים לדעת

- [ ] לכתוב מהזיכרון את שני משפטי ההעצמה בסימון $\mathrm{BPP}(\alpha,\beta)$.
- [ ] להוכיח במלואו את $\mathrm{RP} \subseteq \mathrm{BPP}\left(\frac{1}{q(n)},1\right)$: אלגוריתם, זמן ריצה, שני מקרי ההסתברות, ואי-השוויון $1+x \le e^x$.
- [ ] להסביר בדיוק היכן נכנסת החד-צדדיות ולמה בלעדיה ההוכחה קורסת.
- [ ] לחשב זנב בינומי כמו $\left(\frac{1}{3}\right)^{7-k}\left(\frac{2}{3}\right)^k\binom{7}{k}$ ולהצדיק את שני המעברים בו (זרות לסכום, מונוטוניות ב-p).
- [ ] לנמק מדוע מספר החזרות חייב להיות אי-זוגי, ומה עולה שימוש במספר זוגי.
- [ ] להסביר במשפט אחד למה סף של בדיוק $\frac{1}{2}$ אינו ניתן להעצמה ולמה פער של $1/\mathrm{poly}$ כן.
- [ ] להשתמש בטענות ההעצמה כ"קופסה שחורה" בתרגיל אחר — זה השימוש הצפוי במבחן.

שאלות שנשארו פתוחות

עמוד 3 בסיכום פותח את בעיית החתך המינימלי ואת אלגוריתם הכיווץ; הניתוח ההסתברותי שייך לשיעור 18 — יש לוודא מול שיעור 18 שאין כפילות ושהאלגוריתם מנוסח שם באותן מילים.

בהקלטה [00:55:19] נאמר 'מספר זוגי של פעמים' אך מיד נבחר 7; מהנימוק (שתמיד יהיה רוב) ברור שהכוונה למספר אי-זוגי, וכך נכתב כאן.

בסיכום עמוד 2, באיבר $k=4$, נכתב $16/31$ במקום $16/81$; תוקן, שאר החישוב בסיכום נכון.

המשפט הכללי על העצמה דו-צדדית נאמר ללא הוכחה (אי-שוויון צ'רנוף אינו נלמד בקורס); ההוכחה כאן היא למקרה הפרטי שהודגם בכיתה בלבד.

לא נמצאה בשני המקורות התייחסות לשאלה מדוע ל-BPP אין בעיה שלמה ידועה או מדוע טכניקת ההעצמה אינה חלה על NP; לא הומצא כאן דיון כזה.

18 בעיית החתך המינימלי: אלגוריתם הכיווץ האקראי, והשיטה ההסתברותית

שיעור בשני חלקים: אלגוריתם אקראי פשוט לבעיית החתך המינימלי — כיווץ קשת אקראית עד שנותרים שני קודקודים — שמחזיר חתך מינימלי ספציפי בהסתברות $\ge 1/\binom{n}{2}$ מעל מטבעות האלגוריתם, ההגברה שלו לחצי ב-$\ln 2\binom{n}{2}$ הרצות, והמסקנה הקומבינטורית שבכל גרף יש לכל היותר $\binom{|V|}{2}$ חתכים מינימליים; ואז השיטה ההסתברותית — הוכחת קיום של חתך בגודל $\ge |E|/2$ ב-MAXCUT בעזרת לינאריות התוחלת ושתי טענות הסתברותיות בסיסיות.

ביטחון: high

בקצרה

בעיית החתך המינימלי (MINCUT): בהינתן גרף $G=(V,E)$, למצוא $\emptyset \subsetneq S \subsetneq V$ שממזערת את מספר הקשתות בין S ל-$\bar{S}$. זו לא בעיה NP-קשה — אבל האלגוריתם שנלמד כאן מעניין בפשטותו ולא ביעילותו.

אלגוריתם הכיווץ: כל עוד יש יותר משני קודקודים, בחר קשת אקראית אחידה וכווץ אותה; בסוף החזר את החתך שנוצר. שורה אחת של קוד, וניתוח שלם.

המשפט המרכזי: לכל גרף קבוע G ולכל חתך מינימלי ספציפי $(S,\bar{S})$, ההסתברות — **מעל מטבעות האלגוריתם בלבד** — שהאלגוריתם מחזיר בדיוק את $(S,\bar{S})$ היא לפחות $1/\binom{n}{2}$.

הכלי שמניע את כל הניתוח הוא חסם אחד: בכל גרף, גודל החתך המינימלי מקיים $K \le \frac{2|E|}{|V|}$, וזה נשמר לאורך כל ריצת האלגוריתם.

הגברה: $\lceil \binom{n}{2}\ln 2 \rceil$ הרצות בלתי תלויות והחזרת החתך הקטן ביותר שהתקבל מעלות את הסתברות ההצלחה מעל $\frac{1}{2}$. הטעות כאן חד-כיוונית, ולכן מחזירים מינימום ולא רוב.

מסקנה קומבינטורית: בכל גרף יש לכל היותר $\binom{|V|}{2}$ חתכים מינימליים — מתוך $2^{|V|-1}-1$ חתכים בסך הכל. טענת ספירה טהורה, שמוכחת בעזרת אלגוריתם אקראי.

החלק השני — השיטה ההסתברותית: בכל גרף קיימת $U \subseteq V$ שהחתך $(U,\bar{U})$ מכיל לפחות $\frac{|E|}{2}$ קשתות. ההוכחה מגרילה את U במטבעות, מחשבת $\mathbb{E}[X]=\frac{|E|}{2}$ בלינאריות התוחלת, ומסיקה קיום מכך ש-$\Pr[X \ge \mathbb{E}[X]] > 0$.

זו הוכחה **שונה** לתוצאה שכבר ראינו פעמיים דטרמיניסטית (ראו שיעור 13 ושיעור 14) — וזה בדיוק העניין: טענה קומבינטורית שאין בה שום אקראיות, שמוכחת בכלים הסתברותיים.

רקע ותלויות

משיעור 17 — ההגדרות והאלגוריתם. בסוף שיעור 17 כבר הוצגו בעיית החתך המינימלי, פעולת הכיווץ של קשת ואלגוריתם הכיווץ עצמו, ואף נעשה מעקב אחרי כיווץ אחד על גרף לדוגמה — אבל **הניתוח נדחה במפורש לשיעור הזה** ([00:00:32]: "הנה האלגוריתם, ראינו אותו בסוף השיעור

שעבר"). לכן החלוקה כאן היא: ההגדרות והאלגוריתם מובאים שוב בקצרה כדי שהקובץ יעמוד בפני עצמו (ראו שיעור 17 להצגה הראשונה ולציור), וכל הניתוח — חסם הדרגה, הסתברות ההצלחה, ההגברה וחסם מספר החתכים המינימליים — נכתב כאן במלואו.

מה-MAXCUT הקודם. בשיעור 10 הוכחנו ש-MAXCUT היא NP-קשה, ברדוקציה $3\mathrm{NAE} \le_p \mathrm{MAXCUT}$ (התזכורת על הכיוון: $A \le_p B$ פירושו ש-B היא הקשה מבין השתיים, כלומר פתרון יעיל ל-B נותן פתרון יעיל ל-A). בשיעור 13 ראינו אלגוריתם **חיפוש מקומי** שנותן יחס קירוב $\frac{1}{2}$ ל-MAXCUT: מזיזים קודקוד מצד לצד כל עוד זה משפר את החתך; בעצירה מתקיים $\mathrm{cut}(v) \ge \mathrm{other}(v)$ לכל v, וספירה כפולה נותנת $|F| \ge \frac{1}{2}|E|$. בשיעור 14 ראינו אלגוריתם **חמדן** במעבר יחיד שמשיג את אותו יחס. שתי התוצאות האלה נותנות בפרט את הטענה הקיומית "בכל גרף יש חתך בגודל $\ge \frac{|E|}{2}$", ובאופן קונסטרוקטיבי. בשיעור הזה נוכיח את אותה טענה קיומית **בדרך שלישית, הסתברותית**, ולכן היא נכתבת כאן במלואה ואינה כפילות: כל העניין הוא בשיטת ההוכחה, לא בתוצאה.

מבלוק האקראיות. בשיעור 15 הוגדר מהו אלגוריתם אקראי והודגש ההסכם שילווה אותנו גם כאן: **הקלט הוא שרירותי וקבוע, וההסתברות נלקחת אך ורק מעל המטבעות הפנימיים של האלגוריתם.** בפרט, כשנכתוב כאן "ההסתברות שהאלגוריתם מחזיר חתך מינימלי", זו הסתברות מעל בחירות הקשתות של האלגוריתם עבור **הגרף הקבוע** G — ולא הסתברות מעל גרפים אקראיים. אין בשיעור הזה שום התפלגות על קלטים. בשיעור 16 (מכונת טיורינג אקראית, RP, coRP, BPP) ראינו את טכניקת ההגברה: הרצות בלתי תלויות מכפילות את הסתברויות הכישלון, ולכן t הרצות מורידות כישלון $p \le$ ל-$p^t \le$. נשתמש בזה כאן כמעט מילה במילה.

כלי אנליטי אחד. נשתמש שוב ושוב באי-השוויון $1 + x \le e^x$ לכל $x \in \mathbb{R}$, ובפרט $1 - a \le e^{-a}$.

מהסתברות. נניח הכרות בסיסית עם תוחלת ולינאריות התוחלת. את ההגדרות הפורמליות של מרחב הסתברות ומשתנה מקרי נחזור ונציב מחדש בסעיף ההגדרות, כי החלק השני של השיעור נשען עליהן בדיוק ולא באינטואיציה.

הגדרות

הגדרה 1: חתך בגרף וגודלו

יהי $G = (V, E)$ גרף פשוט לא מכוון. לכל $S \subseteq V$, ה**חתך** המושרה על ידי S הוא הזוג $(S, \bar{S})$, כאשר $\bar{S} = V \setminus S$. **גודל החתך** הוא מספר הקשתות שקצה אחד שלהן ב-S והשני ב-$\bar{S}$:

$$\left|(S, \bar{S})\right| \;=\; \left|\{\, e = xy \in E \;:\; |e \cap S| = 1 \,\}\right|.$$

אינטואיציה. מחלקים את הקודקודים לשתי קבוצות ומודדים כמה קשתות "נחתכות". שימו לב ש-$(S, \bar{S})$ ו-$(\bar{S}, S)$ הם אותו חתך — הסדר לא משנה.

מופע. בגרף המעגל $1 - 2 - 3 - 4 - 1$ ו-$S = \{1, 2\}$ מתקבל חתך בגודל 2 (הקשתות 23 ו-41).

אי-מופע (מקרה קצה חשוב). $S = \emptyset$ נותנת חתך בגודל 0, וכך גם $S = V$. בבעיית **המינימום** (הגדרה 2) נאסור את שני אלה במפורש, כי אחרת הפתרון טריוויאלי. בטענת **המקסימום** (משפט 10) לא נאסור אותם, כי שם הם ממילא לא מזיקים.

הגדרה 2: בעיית החתך המינימלי

קלט: גרף $G = (V, E)$. **מטרה:** למצוא קבוצה $\emptyset \subsetneq S \subsetneq V$ שעבורה החתך $(S, \bar{S})$ הוא בגודל מינימלי מבין כל החתכים הלא-טריוויאליים.

נסמן את הבעיה MINCUT ואת גודל החתך המינימלי בגרף הנתון ב-K.

אינטואיציה. זו בדיוק "אותה בעיה" כמו MAXCUT אבל עם מינימום במקום מקסימום — ואולם היא **לא** NP-קשה; ידועים לה אלגוריתמים דטרמיניסטיים פולינומיים. הלקח הזה חוזר בקורס: החלפת max ב-min יכולה לשנות את הבעיה מקצה לקצה.

> **הערה:** בהקלטה [00:00:01] הוסבר במפורש מדוע אוסרים את $S = \emptyset$ ואת $S = V$: אחרת "החתך המינימלי" הוא תמיד 0 והשאלה מתרוקנת מתוכן.

אפשר להניח ש-G קשיר. אם G אינו קשיר, נריץ BFS מקודקוד כלשהו בזמן $O(|V| + |E|)$. אם לא הגענו לכל הקודקודים, רכיב הקשירות C שמצאנו מקיים $\emptyset \subsetneq C \subsetneq V$ ואין ממנו אף קשת החוצה, כלומר $(C, V \setminus C)$ הוא חתך בגודל 0 — וזה בוודאי מינימלי. אחרת הגרף קשיר וממשיכים. לכן מכאן ואילך G קשיר, ובפרט $|E| \geq |V| - 1$ ו-$|E| \geq 1$.

הגדרה 3: כיווץ קשת (contraction)

תהי $e = xy \in E$. ה**כיווץ** של e הוא הגרף שמתקבל מ-G על ידי החלפת שני הקודקודים x, y בקודקוד חדש יחיד z, כאשר כל קשת שהייתה מחוברת ל-x או ל-y הופכת לקשת המחוברת ל-z, וכל שאר הקשתות נשמרות. את הקשת e עצמה (וכל קשת מקבילה לה) מוחקים, שכן היא הופכת ללולאה עצמית.

אינטואיציה ועובדה חשובה. התוצאה היא בדרך כלל **מולטי-גרף**: אם ל-x ול-y היה שכן משותף w, הרי שאחרי הכיווץ יש שתי קשתות מקבילות בין z ל-w. זה מכוון, ולא באג: מספר הקשתות המקבילות הוא בדיוק מספר הקשתות המקוריות שיחצו את החתך אם z ו-w יופרדו.

למה מוחקים לולאות. לולאה עצמית לעולם אינה חוצה שום חתך, כי שני קצותיה תמיד באותו צד. מחיקתה אינה משנה אף גודל חתך.

> **הערה:** בהקלטה [00:07:36]–[00:08:08] נשאלה בדיוק השאלה הזו. הובהר שם ששני הדברים לגיטימיים — אפשר גם לשמור את הלולאות — וששמירתן לא הייתה שוברת את הניתוח (היא רק מגדילה את $|E|$ ולכן מקטינה את ההסתברות לבחור קשת חוצה). מוחקים אותן כי כך נקי יותר. כמו כן הודגש שבקורס הזה "גרף" פירושו תמיד גרף פשוט לא מכוון אלא אם נאמר אחרת — הכיווץ הוא היוצא מן הכלל שמייצר מולטי-גרף.

מה באמת קורה מאחורי הקלעים. פורמלית איננו "מוחקים קודקודים": אנחנו מחזיקים חלוקה של V לקבוצות (Union–Find), מתחילים מ-n קבוצות יחידון, וכל איטרציה מאחדת שתי קבוצות. בסוף נשארות בדיוק שתי קבוצות, והן S ו-$\bar{S}$ שהאלגוריתם מחזיר. הציור של "מיזוג קודקודים" נוח יותר להבנה, אבל המימוש הוא איחוד קבוצות ([00:09:13]–[00:10:18]).

הגדרה 4: אלגוריתם הכיווץ האקראי

יהי $G = (V, E)$ גרף (קשיר, לפי ההגדרה 2).

כל עוד יש בגרף יותר משני קודקודים:

בחר באקראי, באופן אחיד ובלתי תלוי בבחירות הקודמות, קשת $e = xy \in E$ מבין כל קשתות הגרף **הנוכחי**;
כווץ את x ו-y.
החזר את החתך המתקבל (שתי קבוצות הקודקודים שנותרו).

> **הערה מינוח:** האלגוריתם הזה מוכר בספרות כאלגוריתם Karger. השם לא נאמר בשיעור ולא נכתב בסיכום; הוא מובא כאן רק כדי שיהיה אפשר לחפש אותו. האלגוריתם עצמו הוצג לראשונה בסוף שיעור 17; כאן הוא חוזר כדי שהניתוח יעמוד בפני עצמו.

אינטואיציה. האלגוריתם לא "מחפש" כלום. הוא רק מדלל את הגרף באקראי, ומקווה שאף פעם לא ימחק בטעות את הגבול הנכון. כל הכובד נמצא בשאלה למה זה בכלל עובד לפעמים.
הערה על הפלט. אפשר להחזיר את החתך עצמו (שתי קבוצות הקודקודים) או רק את גודלו, לפי הגרסה של בעיית האופטימיזציה שמעניינת אותנו (ראו שיעור 13 לטבלת הכרעה/חיפוש/אופטימיזציה).

הגדרה 5: מרחב הסתברות

מרחב הסתברות הוא זוג $(\Omega, \Pr)$ כאשר:
$\Omega \neq \emptyset$ היא קבוצה הנקראת **מרחב המדגם**; כל $\omega \in \Omega$ נקראת **נקודת מדגם**; כל $A \subseteq \Omega$ נקראת **מאורע**.
$\Pr : 2^{\Omega} \to [0,1]$ היא פונקציה המקיימת את שלוש אקסיומות ההסתברות:
$\Pr(\Omega) = 1$;
$\Pr(\emptyset) = 0$;
לכל סדרה $A_1, A_2, \ldots \subseteq \Omega$ של מאורעות **זרים בזוגות**: $\Pr\left(\bigcup_{n=1}^{\infty} A_n\right) = \sum_{n=1}^{\infty} \Pr(A_n)$.

אינטואיציה. הסימון 2^{Ω} הוא **קבוצת** כל תת-הקבוצות של Ω (מה שבתורת הקבוצות סימנתם $P(\Omega)$), לא מספר. ההסתברות מוגדרת על תת-קבוצות של Ω ורק עליהן — זו נקודה שנצטרך אותה מיד.
מופע. הטלת שתי קוביות הוגנות: $\Omega = \{1,\ldots,6\}^2$, $|\Omega| = 36$, וכל נקודת מדגם בהסתברות $\frac{1}{36}$.
אי-מופע. הקבוצה $\{2, 3, \ldots, 12\}$ של הסכומים האפשריים **אינה** מרחב המדגם של הניסוי הזה. מרחב המדגם הוא אוסף התוצאות המלאות של הניסוי; הסכום מגיע רק בשלב הבא, כפונקציה (הגדרה 6). זו הייתה נקודה שחזרה בהקלטה כמה פעמים ([01:32:23], [01:34:30]).

הגדרה 6: משתנה מקרי ומשתנה אינדיקטור

יהי $(\Omega, \Pr)$ מרחב הסתברות. **משתנה מקרי** הוא פונקציה $X : \Omega \to \mathbb{R}$. לכל $A \subseteq \mathbb{R}$ מסמנים $\Pr[X \in A] := \Pr\big(\{\, \omega \in \Omega \,:\, X(\omega) \in A \,\}\big)$.
משתנה אינדיקטור הוא משתנה מקרי שתמונתו מוכלת ב-$\{0,1\}$.
אינטואיציה. "אין שום דבר מקרי במשתנה מקרי" — זו פונקציה, ותו לא. האקראיות יושבת ב-Ω וב-$\Pr$, כלומר בקלט של הפונקציה, לא בפונקציה עצמה. הסימון $\Pr[X \in A]$ הוא קיצור: מאחוריו יש **תמיד** תת-קבוצה של Ω, כי רק לתת-קבוצות של Ω יש הסתברות. אין הסתברות מוגדרת על $\mathbb{R}$.
מופע. בהטלת שתי קוביות, $X(a,b) = a + b$ הוא משתנה מקרי, ו-$\mathbb{E}[X] = 7$.

עובדה שנשתמש בה. לכל משתנה אינדיקטור I: $\mathbb{E}[I] = 0 \cdot \Pr[I=0] + 1 \cdot \Pr[I=1] = \Pr[I=1]$.

הגדרה 7: הסתברות מותנית וכלל השרשרת

לכל שני מאורעות A, B עם $\Pr[B] > 0$: $\Pr[A \cap B] \;=\; \Pr[A \mid B] \cdot \Pr[B]$. בהכללה (באינדוקציה), לכל m מאורעות $E_1, \dots, E_m$ עם $\Pr[E_1 \cap \cdots \cap E_{m-1}] > 0$:

$$\Pr\Big[\bigcap_{j=1}^{m} E_j\Big] \;=\; \Pr[E_1] \cdot \Pr[E_2 \mid E_1] \cdot \Pr[E_3 \mid E_1 \cap E_2] \cdots \Pr[E_m \mid E_1 \cap \cdots \cap E_{m-1}].$$

איך לקרוא את הנוסחה. אל תקראו אותה כ"איך מחשבים הסתברות מותנית". קראו אותה כ**גשר** בין "וגם" לבין מותנה, ולכו בכיוון שנוח לכם. בשיעור הזה נלך מ"וגם" למותנה, כי את המותנות דווקא קל לחשב: ההתניה מספרת לנו בדיוק מה מרחב המדגם הנוכחי, כלומר מתוך אילו קשתות בוחרים ([00:44:20]).

משפטים והוכחות

לאורך כל הסעיף: $G = (V, E)$ **גרף קלט קבוע ושרירותי**, $n = |V|$, ו-K גודל החתך המינימלי בו. כל ההסתברויות והתוחלות הן **מעל המטבעות של האלגוריתם** — כלומר מעל בחירות הקשתות האקראיות — עבור אותו גרף קבוע. אין כאן שום התפלגות על גרפים.

משפט 1: הדרגה המינימלית חוסמת את החתך המינימלי

טענה. לכל $v \in V$ מתקיים $\deg_G(v) \geq K$.

הוכחה. יהי $v \in V$. נניח $n \geq 2$, ואז $\{v\}$ ו-$V \setminus \{v\}$ שתיהן לא ריקות, כלומר $(\{v\}, V \setminus \{v\})$ הוא חתך חוקי. גודלו הוא בדיוק $\deg_G(v)$, שכן כל קשת שנוגעת ב-v חוצה אותו וכל קשת שאינה נוגעת ב-v אינה חוצה אותו. מכיוון ש-K הוא **המינימום** על פני כל החתכים החוקיים, ומינימום של קבוצה קטן־שווה מכל איבר בה, נובע $K \;\leq\; \big|(\{v\}, V \setminus \{v\})\big| \;=\; \deg_G(v)$. ■

מסקנה. $K \leq \dfrac{2|E|}{|V|}$.

הוכחה. לפי למת לחיצת הידיים, $2|E| = \displaystyle\sum_{v \in V} \deg_G(v)$. לפי הטענה כל מחובר בסכום הוא לפחות K, ויש $|V|$ מחוברים, ולכן $2|E| \geq K \cdot |V|$. חלוקה ב-$|V| > 0$ נותנת את הדרוש. ■

> **הערה:** בהקלטה [00:19:32]–[00:21:09] התנהל בדיוק כאן ויכוח, ובצדק: אי-השוויון **אינו** אומר שכל דרגה קטנה מ-K ואינו אומר שכל הדרגות שוות. הוא אומר דבר אחד: לכל קודקוד יש חתך שגודלו בדיוק הדרגה שלו, ולכן המינימום על פני **כל** החתכים קטן־שווה מכל אחת מהדרגות. הכיוון הוא מהחתך אל הדרגה, לא להפך.

משפט 2: ההבחנה נשמרת לאורך הריצה

נסמן ב-$G_0 = G$ את גרף הקלט, וב-G_j את המולטי-גרף שמתקבל אחרי j איטרציות (עם מחיקת לולאות). נסמן V_j, E_j את קבוצות הקודקודים והקשתות של G_j. נקבע מראש חתך מינימלי ספציפי $(S, \bar{S})$ של G, בגודל K.

טענה. נניח שבאיטרציות $1, \dots, j$ **לא** נבחרה אף קשת החוצה את $(S, \bar{S})$. אז:

$|V_j| = n - j$;
החתך $(S, \bar{S})$ "שרד" ב-G_j: כל קבוצת קודקודים מכווצת ב-G_j מוכלת כולה ב-S או כולה ב-$\bar{S}$, והחתך המושרה ב-G_j הוא עדיין בגודל K;
$(S, \bar{S})$ הוא חתך **מינימלי** גם ב-G_j, ולכן $K \le \frac{2|E_j|}{|V_j|} = \frac{2|E_j|}{n-j}$.

הוכחה.
(1) כל איטרציה מאחדת שתי קבוצות לאחת, כלומר מורידה את מספר הקודקודים בדיוק באחד. באינדוקציה, אחרי j איטרציות נותרו $n - j$ קודקודים. (זו גם הסיבה שהלולאה מבצעת בדיוק $n - 2$ איטרציות: היא עוצרת כשנשארו 2.)
(2) באינדוקציה על j. בסיס $j = 0$: כל קבוצה היא יחידון $\{v\}$ ומוכלת בבירור באחד הצדדים. צעד: אם באיטרציה j כווצה קשת $e = xy$ שאינה חוצה את $(S, \bar{S})$, אז x ו-y באותו צד; לפי הנחת האינדוקציה הקבוצות שלהם מוכלות כל אחת בצד שלה, וזה אותו צד, ולכן גם האיחוד שלהן מוכל באותו צד. גודל החתך אינו משתנה: הקשתות שנמחקו הן בדיוק לולאות, שאינן חוצות; כל קשת חוצה של G עדיין קיימת ב-G_j ועדיין חוצה, כי קצותיה נשארו בצדדים שונים.
(3) זה הצעד היחיד שנאמר בהרצאה בקיצור, והנה הפירוט.

> **הערה:** בהרצאה זה נאמר כ"התכונה נשמרת" ([00:23:17], [00:27:37]); הפירוט כאן.

כל חתך של G_j מגדיר חתך של G באותו גודל בדיוק: אם $(T, \bar{T})$ הוא חתך של G_j, נפרוס כל קבוצה מכווצת חזרה לקודקודים המקוריים שלה ונקבל חלוקה של V; קשת של G חוצה את החלוקה הזו אם ורק אם הקשת המתאימה לה ב-G_j (או הלולאה שלה) חוצה את $(T, \bar{T})$, ולולאות אף פעם לא חוצות. לכן אוסף גדלי החתכים של G_j מוכל באוסף גדלי החתכים של G, ומכאן $\min\text{-cut}(G_j) \ge \min\text{-cut}(G) = K$. מצד שני, לפי (2) החתך $(S, \bar{S})$ עצמו קיים ב-G_j ובגודל K, ולכן $\min\text{-cut}(G_j) \le K$. שני האי-שוויונות נותנים $\min\text{-cut}(G_j) = K$. כעת מפעילים את המסקנה של משפט 1 על הגרף G_j — ההוכחה שלה לא השתמשה בכך שהגרף פשוט, אלא רק בכך שלכל קודקוד יש חתך שגודלו דרגתו ובלמת לחיצת הידיים, ושתיהן נכונות גם במולטי-גרף — ומקבלים $K \le \frac{2|E_j|}{|V_j|}$. ■

משפט 3: זמן הריצה

טענה. האלגוריתם רץ בזמן $O(|V| \cdot |E|)$ על גרף קשיר.

הוכחה. מספר האיטרציות הוא בדיוק $n - 2 = O(|V|)$ (משפט 2(1)). כל איטרציה עולה $O(|V| + |E|)$: בחירת קשת אקראית אחידה נחשבת כאן פעולה אטומית, וכיווץ פירושו לעבור על כל הקשתות שנגעו ב-x וב-y ולחבר אותן לקודקוד החדש, ולמחוק לולאות — כל אלה מעבר ליניארי אחד על הייצוג. סך הכל $O(|V| \cdot (|V| + |E|))$. מכיוון שהגרף קשיר, $|E| \ge |V| - 1$, ולכן $|V| + |E| = O(|E|)$ והחסם הוא $O(|V| \cdot |E|)$. ■

משפט 4: קריטריון ההצלחה

טענה. יהי $(S, \bar{S})$ חתך מינימלי של G. האלגוריתם מחזיר בדיוק את $(S, \bar{S})$ **אם ורק אם** באף איטרציה לא נבחרה קשת החוצה את $(S, \bar{S})$.

הוכחה. ($\Rightarrow$, בשלילה) נניח שבאיזושהי איטרציה נבחרה קשת $e = xy$ עם $x \in S$, $y \in \bar{S}$. הכיווץ מאחד את הקבוצה של x עם הקבוצה של y, ומרגע זה ואילך הן לעולם באותה קבוצה, כלומר באותו צד של החתך המוחזר. אבל ב-$(S, \bar{S})$ הם בצדדים שונים, ולכן החתך המוחזר אינו $(S, \bar{S})$.

($\Leftarrow$) נניח שלא נבחרה אף קשת חוצה. לפי משפט 2(2), בסוף הריצה כל אחת משתי הקבוצות שנותרו מוכלת כולה ב-S או כולה ב-$\bar{S}$. שתי הקבוצות זרות ואיחודן V. אילו שתיהן היו מוכלות באותו צד, נניח ב-S, היה מתקבל $V \subseteq S$ בסתירה ל-$\bar{S} \neq \emptyset$. לכן אחת מוכלת ב-S והשנייה ב-$\bar{S}$, ומכיוון שאיחודן $S \cup \bar{S} = V$ והן זרות, בהכרח הראשונה שווה ל-S והשנייה ל-$\bar{S}$. ■

למה זה חשוב. המשפט הזה מתרגם שאלה על **פלט** לשאלה על **מהלך הריצה**, וזו שאלה שאנחנו יודעים לחסום איטרציה אחר איטרציה.

משפט 5: הסתברות ההצלחה

טענה. יהי G גרף קשיר קבוע עם $n = |V| \geq 2$, ויהי $(S, \bar{S})$ חתך מינימלי **ספציפי** שלו. נסמן ב-A את המאורע שהאלגוריתם מחזיר בדיוק את החתך $(S, \bar{S})$. אז, מעל מטבעות האלגוריתם בלבד, $\Pr[A] \geq \frac{1}{\binom{n}{2}} = \frac{2}{n(n-1)}$.

> **למה דווקא חתך ספציפי.** את ההסתברות שהאלגוריתם מחזיר *איזשהו* חתך מינימלי איננו יודעים לחשב. לכן אנחנו חוסמים מלמטה כמות קטנה יותר — ההסתברות להחזיר חתך מינימלי אחד ומסוים — ומכיוון שהמאורע "החזרנו את $(S, \bar{S})$" מוכל במאורע "החזרנו חתך מינימלי כלשהו", החסם עובר ([00:12:57]–[00:13:27]).

הוכחה. לכל $1 \leq j \leq n-2$ נסמן ב-E_j את המאורע שבאיטרציה ה-j לא נבחרה קשת מתוך החתך $(S, \bar{S})$. לפי משפט 4, המאורע A שקול לכך שכל המאורעות E_j התרחשו, ולכן $\Pr[A] = \Pr\left[\bigwedge_{j=1}^{n-2} E_j\right]$.

למה אי אפשר פשוט להכפיל. המאורעות $E_1, \ldots, E_{n-2}$ **אינם** בלתי תלויים. אמנם המטבעות של האלגוריתם בלתי תלויים זה בזה — בכל איטרציה מגרילים מחדש — אבל **מרחב הדגימה** של איטרציה j, כלומר קבוצת הקשתות שמתוכה בוחרים, תלוי לחלוטין במה שכווץ קודם. זו נקודה שקל מאוד לפספס: "בחירה בלתי תלויה" אינה "מאורעות בלתי תלויים" ([00:32:00]). לכן נשתמש בכלל השרשרת (הגדרה 7): $\Pr\left[\bigwedge_{j=1}^{n-2} E_j\right] = \Pr[E_1] \cdot \Pr[E_2 \mid E_1] \cdot \Pr[E_3 \mid E_1 \wedge E_2] \cdots \Pr[E_{n-2} \mid E_1 \wedge \cdots \wedge E_{n-3}]$.

האיבר הראשון. באיטרציה הראשונה בוחרים קשת אחידה מתוך $|E|$ הקשתות, ומתוכן בדיוק K חוצות. לכן $\Pr[E_1] = \frac{|E|-K}{|E|} = 1 - \frac{K}{|E|}$. לפי המסקנה של משפט 1, $K \leq \frac{2|E|}{n}$, ולכן $\frac{K}{|E|} \leq \frac{2|E|/n}{|E|} = \frac{2}{n}$, ומכאן $\Pr[E_1] \geq 1 - \frac{2}{n}$.

האיבר הכללי. יהי $2 \leq j \leq n-2$, ונתון $E_1 \wedge \cdots \wedge E_{j-1}$. תחת ההתניה הזו, הגרף הנוכחי הוא G_{j-1} ולפי משפט 2 הוא מקיים: $|V_{j-1}| = n - (j-1) = n - j + 1$, החתך $(S, \bar{S})$ שרד בו בגודל K, והוא מינימלי בו, ולכן $K \leq \frac{2|E_{j-1}|}{n-j+1}$. באיטרציה j בוחרים קשת אחידה מתוך $|E_{j-1}|$

קשתות, ומתוכן בדיוק K חוצות, ולכן $\Pr[E_j \mid E_1 \wedge \cdots \wedge E_{j-1}] = 1 - \frac{K}{|E_{j-1}|} \geq 1 - \frac{2}{n-j+1}$. שימו לב מדוע ההתניה עוזרת ולא מפריעה: היא בדיוק מה שמבטיח שהחתך עדיין שם ועדיין מינימלי, ולכן שהחסם על K עדיין תקף בגרף הנוכחי ([00:44:20]–[00:45:54]).

המכפלה. נציב: $\Pr\left[\bigwedge_{j=1}^{n-2} E_j\right] \geq \prod_{j=1}^{n-2}\left(1 - \frac{2}{n-j+1}\right) = \left(1-\frac{2}{3}\right)\left(1-\frac{2}{4}\right)\cdots\left(1-\frac{2}{n-1}\right)\left(1-\frac{2}{n}\right)$. נחליף אינדקס: $i = n - j + 1$ רץ מ-n (עבור $j=1$) עד 3 (עבור $j = n-2$), ולכן $\prod_{j=1}^{n-2}\left(1-\frac{2}{n-j+1}\right) = \prod_{i=3}^{n}\frac{i-2}{i} = \frac{1\cdot 2\cdot 3\cdots(n-2)}{3\cdot 4\cdot 5\cdots n} = \frac{(n-2)!}{n!/2} = \frac{2}{n(n-1)} = \frac{1}{\binom{n}{2}}$. הצמצום הטלסקופי גלוי לעין אם כותבים את הגורמים במפורש: $\frac{1}{3}\cdot\frac{2}{4}\cdot\frac{3}{5}\cdots\frac{n-2}{n}$ — כל מונה מצטמצם עם המכנה שני מקומות אחריו, ונשארים המונים $2, 1$ מהסוף והמכנים $n, n-1$ מההתחלה. $\blacksquare$

> **הערה מהשיעור [00:47:28]:** המרצה הדגיש שהוא עצמו לעולם אינו זוכר אם האינדקס העליון הוא $n-2$ או $n-1$, ושהשיטה הנכונה היא לבדוק ערכים קטנים: ב-$n=3$ יש איטרציה אחת, ב-$n=4$ שתיים — ומכאן שהמספר הוא $n-2$. שווה לאמץ את זה למבחן.

משפט 6: הגברה

האלגוריתם המוגבר. הרץ את אלגוריתם הכיווץ $t = \left\lceil \binom{n}{2}\ln 2 \right\rceil$ פעמים, בהרצות בלתי תלויות זו בזו, והחזר את **החתך הקטן ביותר** שהתקבל.

טענה. נסמן ב-B את המאורע שהאלגוריתם המוגבר מחזיר חתך מינימלי. אז $\Pr[B] \geq \frac{1}{2}$.

הוכחה. נקבע חתך מינימלי ספציפי $(S, \bar{S})$, ונסמן ב-C את המאורע שהרצה בודדת מחזירה חתך מינימלי כלשהו, וב-A (כמו במשפט 5) את המאורע שאותה הרצה מחזירה בדיוק את $(S, \bar{S})$. מתקיים $A \subseteq C$, ולכן לפי מונוטוניות ההסתברות (משפט 8(2)) ולפי משפט 5: $\Pr[C] \geq \Pr[A] \geq \frac{1}{\binom{n}{2}}$. לכן הסתברות הכישלון של הרצה בודדת היא $\Pr[\bar{C}] \leq 1 - \frac{1}{\binom{n}{2}}$.

האלגוריתם המוגבר נכשל, כלומר $\bar{B}$ מתרחש, אם ורק אם **כל** t ההרצות נכשלו, וההרצות בלתי תלויות, ולכן ההסתברויות מוכפלות: $\Pr[\bar{B}] \leq \left(1 - \frac{1}{\binom{n}{2}}\right)^{t}$. נשתמש ב-$1 + x \leq e^{x}$ עם $x = -1/\binom{n}{2}$: $\left(1-\frac{1}{\binom{n}{2}}\right)^{t} \leq \left(e^{-1/\binom{n}{2}}\right)^{\binom{n}{2}\ln 2} = e^{-\ln 2} = \frac{1}{2}$. לכן הסתברות ההצלחה היא לפחות $\frac{1}{2}$. $\blacksquare$

למה מחזירים מינימום ולא רוב. הטעות של האלגוריתם היא **חד-כיוונית**: הוא תמיד מחזיר חתך חוקי, וגודלו תמיד $\geq K$. אין מצב שבו הוא מחזיר משהו קטן מדי. לכן ההרצה הטובה ביותר היא פשוט הקטנה ביותר, ואין שום צורך בחציון או ברוב. אילו הטעות הייתה דו-כיוונית — כלומר אילו יכולנו לחזור גם מתחת לערך האמיתי וגם מעליו — היינו נאלצים להסתמך על מדד סטטיסטי כמו חציון, וההגברה הייתה נראית אחרת ([00:54:41]–[00:56:47]). זו בדיוק ההבחנה בין טעות חד-צדדית לדו-צדדית שראינו בשיעורים 15–16.

זמן הריצה של האלגוריתם המוגבר. $O\left(\binom{n}{2}\right) = O(n^2)$ הרצות, כל אחת $O(|V|\,|E|)$, כלומר $O(|V|^3|E|)$ — פולינומי, אבל גרוע יותר מהאלגוריתמים הדטרמיניסטיים הידועים ל-MINCUT. היתרון היחיד, והוא אמיתי, הוא הפשטות ([01:00:57]).

משפט 7: מספר החתכים המינימליים

טענה (קומבינטורית). בכל גרף $G = (V, E)$ יש לכל היותר $\binom{|V|}{2}$ חתכים מינימליים.

מדוע זה מפתיע. מספר החתכים בגרף הוא $2^{|V|-1} - 1$: יש $2^{|V|}$ תת-קבוצות, פוסלים את $\emptyset$ ואת V, וכל חתך נספר פעמיים (פעם כ-S ופעם כ-$\bar{S}$), כלומר $\frac{2^{|V|}-2}{2} = 2^{|V|-1} - 1$. מבין המספר האקספוננציאלי הזה, רק כמות **ריבועית** יכולה להיות מינימלית.

הוכחה. נסמן ב-ℓ את מספר החתכים המינימליים ב-G, ונסדר אותם באופן שרירותי: $C_1, \ldots, C_\ell$. נריץ (בדמיון — זהו כלי הוכחה, לא אלגוריתם שמישהו מריץ) את אלגוריתם הכיווץ הבסיסי פעם אחת, ולכל $1 \le j \le \ell$ נסמן ב-A_j את המאורע שהאלגוריתם החזיר את החתך C_j.

המאורעות זרים בזוגות: הרצה אחת של האלגוריתם מחזירה בדיוק חתך אחד, ולכן לא ייתכן ש-A_i ו-A_j יתרחשו יחד עבור $i \neq j$.

כל אחד מהם כבד מספיק: לפי משפט 5, המופעל על החתך המינימלי C_j (המשפט תקף לכל חתך מינימלי, לא רק לאחד מיוחד), מתקיים $\Pr[A_j] \ge \frac{1}{\binom{|V|}{2}}$.

חיבור: ההסתברות היא לכל היותר 1, ולכן, לפי אדיטיביות סופית (משפט 8(0)) עבור מאורעות זרים בזוגות: $1 \ge \Pr\left[\bigcup_{j=1}^{\ell} A_j\right] = \sum_{j=1}^{\ell} \Pr[A_j] \ge \ell \cdot \frac{1}{\binom{|V|}{2}}$. העברת אגפים נותנת $\ell \le \binom{|V|}{2}$. ■

> **הערה [01:04:46]:** שימו לב מה קרה כאן. הטענה היא טענה קומבינטורית טהורה — ספירה. אין בה אלגוריתם ואין בה הסתברות. ההוכחה, לעומת זאת, היא אלגוריתמית והסתברותית. זה בדיוק הרעיון שנקרא **השיטה ההסתברותית**, והוא הנושא של יתר השיעור.

משפט 8: תכונות בסיסיות של מרחב הסתברות

יהי $(\Omega, \Pr)$ מרחב הסתברות.

(0) אדיטיביות סופית. לכל $A_1, \ldots, A_n \subseteq \Omega$ זרים בזוגות: $\Pr\left(\bigcup_{j=1}^{n} A_j\right) = \sum_{j=1}^{n} \Pr(A_j)$.

הוכחה. אקסיומה 3 מדברת על סדרה **אינסופית**, ובידינו סדרה סופית. נשלים אותה בקבוצות ריקות: נגדיר $B_k = \begin{cases} A_k & 1 \le k \le n \\ \emptyset & \text{otherwise} \end{cases}$ הקבוצות $B_1, B_2, \ldots$ זרות בזוגות (הקבוצה הריקה זרה לכל קבוצה, ובפרט לעצמה), ולכן לפי אקסיומה 3 ואקסיומה 2: $\Pr\left(\bigcup_{k=1}^{n} A_k\right) = \Pr\left(\bigcup_{k=1}^{\infty} B_k\right) = \sum_{k=1}^{\infty} \Pr(B_k) = \sum_{k=1}^{n} \Pr(A_k) + \sum_{k>n} 0 = \sum_{k=1}^{n} \Pr(A_k)$.

השוויון הראשון תקף כי הוספנו לאיחוד רק קבוצות ריקות. ■

(1) משלים. $\Pr(\bar{A}) = 1 - \Pr(A)$. **הוכחה.** A ו-$\bar{A}$ זרות ואיחודן Ω, ולכן לפי (0) ואקסיומה 1: $1 = \Pr(\Omega) = \Pr(A \cup \bar{A}) = \Pr(A) + \Pr(\bar{A})$. ■

(2) מונוטוניות. אם $A \subseteq B$ אז $\Pr(A) \le \Pr(B)$. **הוכחה.** נפרק את B למאורעות זרים: $B = A \cup (B \setminus A)$, ו-$A \cap (B \setminus A) = \emptyset$. לפי (0), $\Pr(B) = \Pr(A) + \Pr(B \setminus A)$. מכיוון ש-$\Pr$ מחזירה ערכים ב-$[0,1]$, בפרט $\Pr(B \setminus A) \ge 0$, ולכן $\Pr(B) \ge \Pr(A)$. שימו לב היכן נדרשה ההנחה $A \subseteq B$: בלעדיה $A \cup (B \setminus A)$ אינו B. ■

(3) חסם האיחוד (union bound). $\Pr(A \cup B) \le \Pr(A) + \Pr(B)$. **הוכחה.** $A \cup B = A \cup (B \setminus A)$, ושתי אלה זרות, ולכן לפי (0): $\Pr(A \cup B) = \Pr(A) + \Pr(B \setminus A)$. אבל $B \setminus A \subseteq B$, ולכן לפי (2) $\Pr(B \setminus A) \le \Pr(B)$, ומכאן $\Pr(A \cup B) \le \Pr(A) + \Pr(B)$. ■

משפט 9: שתי הטענות שמניעות את השיטה ההסתברותית

יהי $(\Omega, \Pr)$ מרחב הסתברות.

(1) יהי A מאורע. אם $\Pr[A] > 0$ אז $A \neq \emptyset$.

הוכחה. בשלילה, אם $A = \emptyset$ אז לפי אקסיומה 2 מתקיים $\Pr[A] = \Pr(\emptyset) = 0$, בסתירה. ■

(2) יהי X משתנה מקרי בעל תוחלת סופית. אז $\Pr[X \ge \mathbb{E}[X]] > 0$.

> **הערה:** בהרצה ([01:58:47]) הטענה הזו נלקחה כנתונה — "קיבלתי אותה מהשמיים" — ולא הוכחה. הנה ההוכחה עבור מרחב מדגם סופי, שהוא המקרה היחיד שנשתמש בו.

הוכחה (ל-Ω סופי). נסמן $\mu = \mathbb{E}[X]$ ונניח בשלילה $\Pr[X \ge \mu] = 0$. אז לפי (1) בכיוון ההפוך — או ישירות מהחישוב שלהלן — לכל $\omega \in \Omega$ עם $\Pr(\{\omega\}) > 0$ מתקיים $X(\omega) < \mu$. נחשב:

$$\mu = \mathbb{E}[X] = \sum_{\omega \in \Omega} \Pr(\{\omega\}) \cdot X(\omega) = \sum_{\omega:\, \Pr(\{\omega\})>0} \Pr(\{\omega\}) \cdot X(\omega) < \sum_{\omega:\, \Pr(\{\omega\})>0} \Pr(\{\omega\}) \cdot \mu = \mu,$$

כאשר האי-שוויון החד תקף מפני שהסכום אינו ריק (סכום ההסתברויות הוא $1 > 0$), והשוויון האחרון כי $\sum_{\omega} \Pr(\{\omega\}) = \Pr(\Omega) = 1$. קיבלנו $\mu < \mu$ — סתירה. ■

איך משתמשים בשתיהן יחד. אם מצליחים לבנות ניסוי אקראי שבו $\mathbb{E}[X] = c$, אז לפי (2) המאורע $\{\omega : X(\omega) \ge c\}$ הוא בעל הסתברות חיובית, ולפי (1) הוא **אינו ריק** — כלומר **קיים** ω שעליו $X(\omega) \ge c$. זהו כל הרעיון: מסיקים קיום מתוחלת.

משפט 10: בכל גרף קיים חתך בגודל $\ge \frac{|E|}{2}$

טענה. יהי $G = (V, E)$ גרף. קיימת קבוצה $U \subseteq V$ כך שהחתך $(U, \bar{U})$ מכיל לפחות $\frac{|E|}{2}$ קשתות.

הערה על ניסוח. כאן לא דורשים $U \neq \emptyset$; הסיכום מציין במפורש שגם $U = \emptyset$ מותרת. זה חף מבעיות: אם $|E| \ge 1$ אז חתך בגודל $\ge \frac{|E|}{2} > 0$ ממילא אינו טריוויאלי.

הניסוי (וזהו למעשה אלגוריתם אקראי). לכל קודקוד $v \in V$, באופן בלתי תלוי בכל שאר הקודקודים, נטיל מטבע הוגן ונכניס את v לקבוצה U בהסתברות $\frac{1}{2}$.

מה בדיוק המרחב. מרחב המדגם הוא $\Omega = 2^V = \{\, U : U \subseteq V \,\}$, כלומר תוצאת הניסוי היא **קבוצת קודקודים**. שוב: ההסתברות היא מעל המטבעות, עבור הגרף הקבוע G; G לא הוגרל.

המשתנים המקריים. נסמן ב-X את גודל החתך: $X : 2^V \to \mathbb{R}, \qquad X(U) = \left|(U, \bar{U})\right|$. ולכל קשת $e \in E$ נסמן ב-I_e את האינדיקטור לכך ש-e חוצה את החתך: $I_e : 2^V \to \mathbb{R}, \qquad I_e(U) = \begin{cases} 1 & |e \cap U| = 1 \\ 0 & \text{otherwise} \end{cases}$ (קשת היא קבוצה בת שני קודקודים, ולכן החיתוך $e \cap U$ מוגדר היטב.)

מהגדרת גודל החתך, כשוויון **בין פונקציות**: $X = \sum_{e \in E} I_e$.

חישוב התוחלת. מלינאריות התוחלת, $\mathbb{E}[X] = \sum_{e \in E} \mathbb{E}[I_e]$. ומכיוון ש-$G$ תהי $e = xy \in E$ (פשוט, $x \neq y$). התוחלת של אינדיקטור היא ההסתברות שהוא 1: $\mathbb{E}[I_e] = \Pr[I_e = 1] = \Pr\big[(x \in U \wedge y \notin U) \ \vee \ (x \notin U \wedge y \in U)\big]$. שני המאורעות **זרים** — לא ייתכן ש-$x \in U$ וגם $x \notin U$ — ולכן לפי אדיטיביות סופית (משפט 8(0)): $= \Pr[x \in U \wedge y \notin U] \ + \ \Pr[x \notin U \wedge y \in U]$. כעת, המאורע "$x \in U$" נקבע על ידי המטבע של x בלבד, והמאורע "$y \in U$" על ידי המטבע של y בלבד, ומטבעות של קודקודים שונים בלתי תלויים — כאן, ורק כאן, נכנסת ההנחה על אי-התלות בין הקודקודים. לכן כל אחד מהמחוברים מתפרק למכפלה: $= \Pr[x \in U] \cdot \Pr[y \notin U] \ + \ \Pr[x \notin U] \cdot \Pr[y \in U] = \frac{1}{2} \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{2}$. ולכן $\Pr[I_e = 1] = \frac{1}{2}$ כלומר U לכל e, ומכאן $\mathbb{E}[I_e] = \frac{1}{2}$. $\mathbb{E}[X] = \sum_{e \in E} \frac{1}{2} = \frac{|E|}{2}$.

מתוחלת לקיום. לפי משפט 9(2) המופעל על X, $\Pr\big[X \geq \mathbb{E}[X]\big] > 0$, כלומר, בכתיב מפורש של הקבוצה שמאחורי הסימון, $\Pr\left(\left\{ U \subseteq V \ : \ X(U) \geq \frac{|E|}{2} \right\}\right) > 0$. שימו לב שהאובייקט שבתוך $\Pr$ הוא באמת תת-קבוצה של $\Omega = 2^V$ — אוסף של קבוצות קודקודים — כפי שההגדרה דורשת. לפי משפט 9(1) הקבוצה הזו **אינה ריקה**, כלומר קיימת $U \subseteq V$ שעבורה $X(U) \geq \frac{|E|}{2}$. מהגדרת X, זהו בדיוק חתך שגודלו לפחות $\frac{|E|}{2}$. ■

> **איפה יושבת האקראיות ([01:53:04], [01:59:21]).** ב-$\Pr[I_e = 1]$ ההסתברות נלקחת על פני U, כי I_e היא פונקציה של U — למרות ש-U לא מופיעה בסימון $\Pr[I_e = 1]$. וכן: $\mathbb{E}[X]$ הוא **מספר קבוע**, אין בו שום אקראיות; האקראיות היא במה שמכניסים ל-X. המרצה ציין שכל ההערות האלה לא נכתבות בשום טקסט הסתברותי, ושדווקא בגלל זה קל כל כך להתבלבל.

היחס לשיעורים 13 ו-14. את **אותה טענה** בדיוק כבר הוכחנו פעמיים באופן דטרמיניסטי וקונסטרוקטיבי — בחיפוש מקומי (שיעור 13) ובאלגוריתם החמדן (שיעור 14). ההוכחה כאן אינה משפרת את התוצאה ואינה מייתרת אותן; היא מדגימה **שיטה**: כדי להוכיח שקיים אובייקט קומבינטורי טוב, מגדירים התפלגות על האובייקטים ומראים שהתוחלת טובה מספיק. אין כאן שום קשר בין הטענה (קומבינטורית) לבין ההסתברות (כלי ההוכחה בלבד).

דוגמאות ותרגילים מהשיעור

דוגמה 1: מעקב מלא אחרי אלגוריתם הכיווץ

נעבוד עם הגרף $G = (V, E)$: $V = \{1, 2, 3, 4, 5\}, \qquad E = \big\{\{1,2\}, \{1,3\}, \{2,3\}, \{3,5\}, \{2,4\}, \{4,5\}\big\}$ (מבנית: משולש $1-2-3$, $|E| = 6$. ומעגל $2 - 4 - 5 - 3 - 2$.)

הדרגות: $\deg(1)=2,\ \deg(2)=3,\ \deg(3)=3,\ \deg(4)=2,\ \deg(5)=2$; סכומן $12=2|E|$ ✓.

מהו החתך המינימלי? הגרף חסין לניתוק בקשת אחת (אין בו גשר), ולכן $K\geq 2$; והחתך $(\{1\},\{2,3,4,5\})$ הוא בגודל 2. לכן $K=2$. בדיקת המסקנה של משפט 1: $K=2\leq \frac{2\cdot 6}{5}=2.4$ ✓.

ריצה לדוגמה. יש $n-2=3$ איטרציות.

איטרציה 1: נניח שנבחרה הקשת $\{1,3\}$ (בהסתברות $\frac{1}{6}$). מכווצים ומקבלים את הקודקוד $a=\{1,3\}$. הגרף החדש: קודקודים $a,2,4,5$; קשתות: $a-2$ **פעמיים** (מ-$\{1,2\}$ ומ-$\{2,3\}$), $a-5$ (מ-$\{3,5\}$), $4-2$, $5-4$. בסך הכל $|E_1|=5$, $|V_1|=4$. הלולאה שנוצרה מ-$\{1,3\}$ נמחקה. בדיקה: $K=2\leq \frac{2\cdot 5}{4}=2.5$ ✓.

איטרציה 2: נניח שנבחרה $\{2,4\}$ (בהסתברות $\frac{1}{5}$). מקבלים $b=\{2,4\}$. קודקודים: $a,b,5$; קשתות: $a-b$ פעמיים, $a-5$, $b-5$. $|E_2|=4$, $|V_2|=3$. בדיקה: $K=2\leq \frac{2\cdot 4}{3}\approx 2.67$ ✓.

איטרציה 3: יש ארבע קשתות. אם נבחרת אחת משתי הקשתות $a-b$ (בהסתברות $\frac{2}{4}=\frac{1}{2}$), מקבלים את שתי הקבוצות $\{1,2,3,4\}$ ו-$\{5\}$, כלומר את החתך $(\{5\},\{1,2,3,4\})$ **בגודל 2 — מינימלי, הצלחה**. אם נבחרת $a-5$ מקבלים $(\{2,4\},\{1,3,5\})$ בגודל 3 — **כישלון**; ואם נבחרת $b-5$ מקבלים $(\{1,3\},\{2,4,5\})$ בגודל 3 — כישלון.

הדוגמה מראה גם את מנגנון ההצלחה וגם את מנגנון הכישלון: החתך המוחזר תמיד חוקי, אבל לא בהכרח מינימלי — וזו בדיוק הטעות החד-כיוונית ממשפט 6.

דוגמה 2: חישוב מדויק של הסתברות ההצלחה, מול החסם

נחשב, על אותו גרף, את ההסתברות המדויקת שהאלגוריתם מחזיר את החתך המינימלי הספציפי $(\{1\},\{2,3,4,5\})$. הקשתות החוצות אותו הן $\{1,2\}$ ו-$\{1,3\}$, כלומר $K=2$.

לפי משפט 4, ההצלחה שקולה לכך שאף אחת משתי הקשתות האלה לא נבחרה. נעקוב אחרי הספירה:

איטרציה 1: 6 קשתות, 2 אסורות $\Rightarrow$ הסתברות $\frac{4}{6}$.

איטרציה 2: בכל אחת מארבע האפשרויות הכשרות של איטרציה 1, הגרף הנוכחי מכיל 5 קשתות ובדיוק 2 מהן עדיין חוצות את $(\{1\},\cdot)$ (משפט 2 מבטיח שהחתך שרד בגודל $K=2$) $\Rightarrow$ הסתברות $\frac{3}{5}$.

איטרציה 3: באותו אופן, 4 קשתות ובדיוק 2 אסורות $\Rightarrow$ הסתברות $\frac{2}{4}$.

לכן, לפי כלל השרשרת, ההסתברות שהאלגוריתם מחזיר בדיוק את החתך $(\{1\},\{2,3,4,5\})$ היא $\frac{4}{6}\cdot\frac{3}{5}\cdot\frac{2}{4}=\frac{24}{120}=\frac{1}{5}=0.2$.

והחסם של משפט 5 נותן $\left(1-\frac{2}{5}\right)\left(1-\frac{2}{4}\right)\left(1-\frac{2}{3}\right)=\frac{3}{5}\cdot\frac{1}{2}\cdot\frac{1}{3}=\frac{1}{10}=\frac{1}{\binom{5}{2}}=0.1$.

$0.2\geq 0.1$ ✓. הפער נובע מכך שבגרף הזה מספר הקשתות יורד מהר מהמקרה הגרוע: החסם התיאורטי מניח $\frac{K}{|E_j|}\leq\frac{2}{|V_j|}$, כלומר $\frac{2}{5},\frac{2}{4},\frac{2}{3}$, ואילו בפועל קיבלנו $\frac{2}{6},\frac{2}{5},\frac{2}{4}$.

דוגמה 3: כמה חתכים מינימליים יש בגרף הזה?

מספר החתכים הכולל: $2^{5-1}-1=15$. נעבור עליהם ונמצא שהחתכים בגודל 2 הם בדיוק ארבעה: $(\{4,5\},\{1,2,3\})$. $(\{5\},\cdot)$, $(\{4\},\cdot)$, $(\{1\},\cdot)$ (לדוגמה, $(\{2\},\cdot)$ הוא בגודל 3, וכך גם $(\{1,2\},\{3,4,5\})$ ו-$(\{1,3\},\{2,4,5\})$.)

החסם של משפט 7: $\binom{5}{2}=10$, ובאמת $4\le 10$ ✓. שימו לב שהחסם רחוק מלהיות הדוק בדוגמה הזו — הוא חסם על המקרה הגרוע.

דוגמה 4: השאלה על הדרגה המינימלית, ולמה התשובה שלילית

השאלה (שאלת סטודנטית בסוף השיעור הקודם, [00:15:09]): אם לכל קודקוד v החתך $(\{v\}, V\setminus\{v\})$ הוא בגודל $\deg(v)$, האם לא מספיק לקחת את הקודקוד בעל הדרגה המינימלית ולהחזיר את החתך שלו?

התשובה: לא. הנה נגד-דוגמה. ניקח שני עותקים של הקליקה K_5 ונחבר ביניהם בקשת אחת: $|V|=10$, $|E|=2\binom{5}{2}+1=21$.

כל קודקוד הוא בדרגה 4, למעט שני קצות הקשת המחברת שדרגתם 5.

החתך המינימלי הוא בגודל 1 — מפרידים בין שתי הקליקות.

אבל כל חתך מהצורה $(\{v\},\cdot)$ הוא בגודל 4 לפחות.

כלומר האסטרטגיה הזו מחזירה 4 במקום 1 — פי ארבעה מהאופטימום. מה **כן** נכון בהבחנה הוא בדיוק משפט 1: הדרגה המינימלית היא **חסם עליון** על K, לא ערכו. ובאמת $K=1\le \frac{2\cdot 21}{10}=4.2$ ✓.

דוגמה 5: ספירת החתכים

תרגיל. כמה חתכים יש בגרף בעל n קודקודים? **פתרון.** כל תת-קבוצה $S\subseteq V$ מגדירה חתך; יש 2^n תת-קבוצות. פוסלים את $S=\emptyset$ ואת $S=V$ (חתכים טריוויאליים): נשארו 2^n-2. כל חתך נספר בדיוק פעמיים, כ-S וכ-$\bar{S}$, ולכן מספר החתכים הוא $\frac{2^n-2}{2}=2^{n-1}-1$. מכאן החוזק של משפט 7: מתוך כמות אקספוננציאלית, רק $O(n^2)$ יכולים להיות מינימליים.

דוגמה 6: משתנה מקרי — הדוגמה עם שתי הקוביות

מטילים שתי קוביות הוגנות בעלות שש פאות, באופן בלתי תלוי, ומסמנים ב-X את סכום ההטלות.

מרחב המדגם: $\Omega=\{1,2,\dots,6\}^2$, כלומר כל הזוגות הסדורים. **לא** $\{2,\dots,12\}$.

המשתנה המקרי: $X:\Omega\to\mathbb{R}$, $X(a,b)=a+b$.

חישוב: $\Pr[X\in\{3,9\}]=\Pr\big(\{(1,2),(2,1),(6,3),(3,6),(5,4),(4,5)\}\big)=\frac{6}{36}=\frac{1}{6}$.

מה שחשוב כאן אינו התוצאה אלא הצורה: $\Pr[X\in A]$ הוא תמיד קיצור להסתברות של תת-קבוצה של Ω — אוסף נקודות המדגם ש-X שולחת אל A. אפשר לכתוב את הקבוצה בהרבה דרכים ($X\ge a$, $X<a$, $X\in A$), אבל בסוף זו תמיד קבוצה, ותמיד בתוך Ω.

הערה קטנה שעלתה בכיתה: הקבוצה A יכולה להכיל גם ערכים בלתי אפשריים (למשל $A=\{3,15\}$) — זה לגיטימי ופשוט לא משנה את ההסתברות, כי אף נקודת מדגם לא נשלחת ל-15.

דוגמה 7: השיטה ההסתברותית על הגרף מדוגמה 1

נחזור לגרף מדוגמה 1, שבו $|E|=6$.

לפי משפט 10, אם נגריל U על ידי מטבע הוגן לכל קודקוד, נקבל $\mathbb{E}[X] = \frac{6}{2} = 3$, ולכן **קיימת** U עם חתך בגודל ≥ 3.

נאמת ידנית ונשפר. ניקח $U = \{2, 5\}$. הקשתות החוצות: $\{1,2\}$ ✓, $\{2,3\}$ ✓, $\{2,4\}$ ✓, $\{3,5\}$ ✓, $\{4,5\}$ ✓; לא חוצה: $\{1,3\}$ (שני קצותיה מחוץ ל-U). כלומר $X(\{2,5\}) = 5 \geq 3$ ✓.

האם אפשר 6? לא. הגרף מכיל את המשולש $3-2-1$, ובכל חלוקה לשתי קבוצות שני קודקודים מהמשולש נופלים באותו צד (עקרון שובך היונים), ולכן לפחות קשת אחת של המשולש אינה חוצה. לכן $\mathrm{MAXCUT}(G) = 5$.

הדוגמה ממחישה את גבולות הטענה: היא **קיומית** ומבטיחה רק $\geq \frac{|E|}{2}$; האופטימום יכול להיות גבוה בהרבה, וכזכור, למצוא אותו זו בעיה NP-קשה (ראו שיעור 10).

הערות מהשיעור

[00:01:04] ההנחה שהגרף קשיר אינה "בלי הגבלת הכלליות" בעל פה — היא נבדקת ב-BFS בזמן ליניארי, ואם הגרף לא קשיר מחזירים רכיב קשירות ומקבלים חתך בגודל 0.

[00:07:36]–[00:08:42] הגרף הופך למולטי-גרף תוך כדי ריצה, גם אם הקלט פשוט. הלולאות נמחקות; אין להן שום השפעה על אף חתך.

[00:09:13]–[00:10:18] "כיווץ" הוא ציור נוח; המימוש האמיתי הוא Union–Find על קבוצות קודקודים, ושתי הקבוצות שנותרות בסוף הן בדיוק S ו-$\bar{S}$.

[00:10:52]–[00:11:53] למה בכלל ללמד אלגוריתם שאיטי מהידוע הטוב ביותר: הוא עומד בבסיס תחום **דילול גרפים** (graph sparsification) — להעיף קשתות מגרף צפוף תוך שמירה מקורבת על תכונות כמו מרחקים או קיבולת.

[00:12:57]–[00:13:27] למה מנתחים חתך מינימלי אחד ספציפי: את "ההסתברות להחזיר איזשהו חתך מינימלי" איננו יודעים לחשב, וזו כמות **גדולה יותר**; לכן חוסמים מלמטה את הקטנה ממנה. שאלת סטודנט חידדה שאלו אכן שתי שאלות שונות, כי ייתכנו כמה חתכים מינימליים.

[00:19:32]–[00:21:09] אזהרת מלכודת: המסקנה $K \leq \frac{2|E|}{|V|}$ **אינה** אומרת ש"כל הדרגות גדולות מ-K" בגלל איזו תכונה של הגרף; היא נובעת מכך שמינימום של קבוצה קטן־שווה מכל איבר בה.

[00:32:00]–[00:32:32] ההערה החשובה ביותר בשיעור לצורך המבחן: המטבעות בלתי תלויים, אבל **מרחב הדגימה תלוי** בעבר, ולכן המאורעות E_j תלויים ואסור להכפיל אותם. זו הסיבה היחידה שנדרש כלל השרשרת.

[00:44:20]–[00:45:54] איך לחשוב על $\Pr[A \wedge B] = \Pr[A \mid B]\Pr[B]$: לא כמתכון לחישוב מותנה, אלא כגשר. כאן "וגם" קשה והמותנה קל, כי ההתניה מספרת בדיוק מה מרחב הדגימה הנוכחי.

[00:47:28] שיטה לזכירת אינדקסים: לבדוק $n = 3$ (איטרציה אחת) ו-$n = 4$ (שתיים), ולהסיק את ה-offset. עדיף מלנסות לזכור.

[00:54:41]–[00:56:47] טעות חד-כיוונית מול דו-כיוונית: כאן מחזירים **מינימום** מבין ההרצות; בבעיה עם טעות דו-כיוונית היינו צריכים חציון או ממוצע. ההגברה מותאמת לסוג הטעות.

[01:00:57]–[01:01:28] למה בכל זאת אלגוריתמים אקראיים: הם לרוב **פשוטים מאוד** ("נבחר משהו באקראי באופן אחיד וזהו"). הפשטות היא היתרון, לא זמן הריצה.

[01:04:08], [01:09:04] הנקודה שהמרצה חזר עליה בהתפעלות: משפט 7 הוא טענה **קומבינטורית** שהוכחתה **אלגוריתמית והסתברותית**. זה בדיוק המעבר לנושא של השיטה ההסתברותית.

[01:30:13] "אין שום דבר מקרי במשתנה מקרי" — משתנה מקרי הוא פונקציה. המרצה ביקש לזכור את המשפט הזה כלשונו.

[01:53:04]–[01:54:38] שאלת הליבה בהוכחת משפט 10: מהיכן צצה פתאום U בתוך $\Pr[I_e = 1] \cdot \frac{1}{2}$? כי I_e היא פונקציה של U, וההסתברות היא תמיד על פני מרחב המדגם. וכן: המעבר למכפלה $\frac{1}{2}$ נשען **אך ורק** על כך שהמטבעות של קודקודים שונים בלתי תלויים.

[01:59:21] $\mathbb{E}[X]$ הוא מספר קבוע. האקראיות אינה ב-X אלא במה שמכניסים לתוכה.

[02:01:27] טיזר לשיעור הבא: אותה טענה בדיוק, עם תיאור אחר של הניסוי — בוחרים U אחידה מתוך 2^V במכה אחת. זו אותה התפלגות, אבל **לא אותו ניסוי**, ולכן הצעד היחיד שישתנה בהוכחה הוא בדיוק המעבר שנשען על אי-תלות; אותו נצטרך לחשב מחדש. משם ממשיכים לדה-רנדומיזציה.

פערים בין הסיכום להקלטה

מקור: עמוד 2 בסיכום. **הפער:** בשורה שמעל תיבת כלל השרשרת נכתב $\Pr\left[\bigwedge_{j=1}^{n} E_j\right]$, בעוד שהתיבה עצמה והשורה שאחריה כותבות $\bigwedge_{j=1}^{n-2}$. **ההכרעה:** זו החלקה בכתיבה; מספר האיטרציות הוא בדיוק $n-2$ (משפט 2(1)), וכך גם בהקלטה [00:30:51]. נכתב $n-2$ בכל מקום.

מקור: עמוד 3 בסיכום ו-[00:53:39]. **הפער:** מספר החזרות בהגברה נרשם $\binom{n}{2}\ln 2$, שאינו מספר שלם. **ההכרעה:** נכתב $\lceil \binom{n}{2}\ln 2 \rceil$; העיגול כלפי מעלה רק משפר את החסם, ולכן חסם הכישלון $\frac{1}{2}$ נשמר.

מקור: עמוד 1 בסיכום. **הפער:** הכותרת הראשית קשה לפענוח מלא. **ההכרעה:** שוחזרה כ"בעיית החתך המינימלי" — גוף העמוד פותח ב"מטרה: למצוא $\emptyset \subsetneq S \subsetneq V$ כך שהחתך $(S, \bar{S})$ מינימלי", וההקלטה [00:00:01] מפורשת בעניין.

מקור: עמודים 1–3 בסיכום. **הפער:** הסיכום קובע ש"האי-שוויונות נשמרים לאורך הריצה" ומשתמש בכך, אך אינו מוכיח שהחתך $(S, \bar{S})$ נשאר **מינימלי** בגרף המכווץ. **ההכרעה:** ההוכחה נכתבה כאן במלואה (משפט 2(3)): כל חתך של הגרף המכווץ הוא חתך של הגרף המקורי באותו גודל, ולכן החתך המינימלי יכול רק לגדול; ומכיוון ש-$(S, \bar{S})$ שרד בגודל K, הוא מינימלי. בהקלטה זה נאמר בקצרה ב-[00:23:17] וב-[00:44:20].

מקור: עמוד 4 בסיכום ו-[01:58:47]. **הפער:** הטענה $\Pr[X \geq \mathbb{E}[X]] > 0$ נרשמת בשני המקורות ללא הוכחה; המרצה אמר במפורש "קיבלתי אותה מהשמיים". **ההכרעה:** ההוכחה נכתבה כאן במלואה עבור מרחב מדגם סופי (משפט 9(2)), עם ההסתייגות המפורשת לגבי המקרה הסופי.

מקור: עמוד 1 בסיכום. **הפער:** תיאור האלגוריתם אינו מזכיר מחיקת לולאות עצמיות. **ההכרעה:** בהקלטה [00:07:36] ו-[00:24:24] נאמר שמוחקים אותן; נכתב כך. נבדק ונמצא שגם שמירת הלולאות לא הייתה שוברת את הניתוח — היא רק מגדילה את $|E_j|$ ולכן מקטינה את ההסתברות לבחור קשת חוצה — ולכן זו החלטת נוחות ולא דרישה.

מקור: ההקלטה [00:00:32]–[00:12:26]. **הפער:** ההקלטה מוסיפה שכבה שלמה שאינה בסיכום — נימוק ה-BFS להנחת הקשירות, הדיון במולטי-גרף, המימוש כ-Union–Find, והמוטיבציה מתחום דילול הגרפים. **ההכרעה:** נכללה כאן, בהגדרות ובהערות מהשיעור.

מקור: ההקלטה [00:15:09]–[00:16:13]. **הפער:** שאלת הסטודנטית על הדרגה המינימלית והנגד-דוגמה של שתי קליקות מחוברות בקשת אינן בסיכום כלל. **ההכרעה:** נכללו כדוגמה 4, עם החישוב המלא שהמרצה לא כתב על הלוח.

מקור: ההקלטה [00:06:30]–[00:07:36]. **הפער:** המרצה צייר גרף בן חמישה קודקודים ועקב אחריו, אך הציור אינו נראה בהקלטה ורשימת הקשתות מתאוששת רק חלקית מהתמלול. **ההכרעה:** נבנתה כאן דוגמה קונקרטית מלאה (דוגמה 1) שעקבית עם התיאור המילולי — כיווץ $\{1,3\}$ מייצר שתי קשתות מקבילות אל 2, קשת אל 5, ולולאה שנמחקת. ייתכן שקשת אחת שונה מהציור המקורי; הדוגמה נכונה בפני עצמה וכל החישובים עליה נבדקו.

מקור: עמוד 6 בסיכום מול שיעורים 13–14. **הפער:** הטענה "קיים חתך בגודל $\geq |E|/2$" הוכחה כבר פעמיים בקורס, דטרמיניסטית. **ההכרעה:** ההוכחה כאן היא **הוכחה שונה מהותית** (השיטה ההסתברותית) ולכן נכתבה במלואה; ההוכחות הדטרמיניסטיות לא שוכפלו אלא הופנו אליהן (שיעור 13, שיעור 14). המרצה עצמו מזכיר את שתיהן ב-[01:43:09].

מקור: ההקלטה מול הסיכום, לאורך כל השיעור. **הפער:** התמלול האוטומטי משבש כמעט כל מונח — "קונטרקט", "מולטיק", "אמפליפיקציה", ובעיקר סימונים ($\binom{n}{2}$ נשמע "n מ-2" ולעיתים "V2"). **ההכרעה:** בכל התנגשות סימונית הסיכום הכריע. שמות המחלקות והבעיות נכתבו לפי מוסכמת הקורס (MINCUT, MAXCUT, NP), ושמות המשתנים והאינדקסים לפי הסיכום ($S, \bar{S}, K, n, E_j, U, X, I_e$).

מקור: שם הקובץ של השיעור. **הפער:** שם הקובץ הוא `lesson-18-max-cut.md` , אך חמישה משש העמודים עוסקים ב-MINCUT ובאלגוריתם הכיווץ, ורק העמוד השישי ב-MAXCUT. **ההכרעה:** שם הקובץ לא שונה, לפי ההנחיה; ה- `slug` בתוך הקובץ תוקן ל-`min-cut--contraction-algorithm`, הכותרת האמיתית ב- `title_he` , והבקשה לשינוי שם הקובץ נרשמה ב- `open_questions` .

מקור: גבול השיעורים 17–18. **הפער:** הגדרת הבעיה, פעולת הכיווץ והאלגוריתם מופיעים גם בעמוד 3 של סיכום שיעור 17 וגם בעמוד 1 של הסיכום הזה. **ההכרעה:** שיעור 17 מחזיק את ההצגה הראשונה ואת המעקב המצויר; כאן הם נכתבים שוב בקצרה כדי שהקובץ יעמוד בפני עצמו, וכל הניתוח — שנדחה שם במפורש — נכתב כאן במלואו. אין כפילות בהוכחות.

סיכום ונקודות למבחן

מה לזכור בעל פה

$K \leq \frac{2|E|}{|V|}$ — גודל החתך המינימלי חסום על ידי הדרגה הממוצעת. זה הצעד שכל הניתוח נשען עליו, והוא נכון גם במולטי-גרף וגם בכל שלב של הריצה.

ההסתברות שאלגוריתם הכיווץ מחזיר חתך מינימלי ספציפי היא לפחות $\frac{1}{\binom{n}{2}}$, וההוכחה: קריטריון "לא כיווצנו קשת חוצה" $\to$ כלל השרשרת $\to 1 - \frac{2}{n-j+1}$ $\to$ מכפלה טלסקופית.

$\lceil \binom{n}{2} \ln 2 \rceil$ הרצות $\Rightarrow$ הצלחה בהסתברות $\geq \frac{1}{2}$, בעזרת $1 - a \leq e^{-a}$.

בכל גרף לכל היותר $\binom{|V|}{2}$ חתכים מינימליים, מתוך $2^{|V|-1} - 1$ חתכים.

בכל גרף קיים חתך בגודל $\geq \frac{|E|}{2}$; ההוכחה: מטבע לכל קודקוד, $\mathbb{E}[I_e] = \frac{1}{2}$, לינאריות, $\mathbb{E}[X] = \frac{|E|}{2}$, ואז $\Pr[X \geq \mathbb{E}[X]] > 0$ הקבוצה לא ריקה.

שתי הטענות של השיטה ההסתברותית: $\Pr[A] > 0 \Rightarrow A \neq \emptyset$, ו-$\Pr[X \geq \mathbb{E}[X]] > 0$.

מלכודות סטנדרטיות

הכפלה במקום שרשרת. המאורעות E_j **תלויים**. "בחירות בלתי תלויות" $\neq$ "מאורעות בלתי תלויים", כי מרחב הדגימה משתנה. מי שכותב $\prod \Pr[E_j]$ טועה.

הסתברות על גרפים. אין דבר כזה בשיעור הזה. ההסתברות היא תמיד על מטבעות האלגוריתם, לגרף קבוע ושרירותי. אמירה כמו "בגרף אקראי" היא טעות מהותית ולא חוסר דיוק.

בלבול בין דרגה מינימלית לחתך מינימלי. הדרגה המינימלית היא חסם עליון על K ולא ערכו (דוגמה 4).

החלפת מינימום ומקסימום בהגברה. בבעיה עם טעות חד-כיוונית מחזירים את הקיצון (כאן: המינימום), ולא רוב או חציון.

שכחת שלמות מרחב המדגם. ב-$\Pr[I_e = 1]$ ההסתברות היא על פני U; ב-$\Pr[X \in A]$ הקבוצה שבתוך $\Pr$ היא תת-קבוצה של Ω ולא של $\mathbb{R}$.

התניה על מאורע בהסתברות אפס. כלל השרשרת דורש $\Pr[E_1 \wedge \cdots \wedge E_{j-1}] > 0$; כאן זה מובטח כי כל הגורמים חיוביים ממש.

המקרה $S = \emptyset$. ב-MINCUT הוא אסור (אחרת התשובה תמיד 0); בטענת MAXCUT הקיומית הוא מותר ואינו מזיק.

מה צריך לדעת לעשות אחרי השיעור

לתאר את אלגוריתם הכיווץ, להריץ אותו על גרף קטן ולעקוב אחרי המולטי-גרף המתקבל בכל שלב.

להוכיח את $K \leq \frac{2|E|}{|V|}$ ולהסביר למה הוא נשמר לאורך הריצה.

לשחזר את ניתוח הסתברות ההצלחה במלואו, כולל הצמצום הטלסקופי, ולהסביר בכל צעד מעל מה נלקחת ההסתברות.

לבצע חישוב הגברה: לגזור כמה חזרות דרושות כדי להגיע לכישלון $\leq \varepsilon$ (כאן: $\binom{n}{2} \ln \frac{1}{\varepsilon}$ חזרות).

להוכיח טענת קיום קומבינטורית בשיטה ההסתברותית: להגדיר ניסוי, להגדיר משתנה מקרי, לפרק לאינדיקטורים, לחשב תוחלת בלינאריות, ולסיים בשתי הטענות של משפט 9.

שאלות שנשארו פתוחות

שם הקובץ שגוי וטעון שינוי: הוא lesson-18-max-cut.md, אך חמישה משמת עמודי הסיכום עוסקים בבעיית החתך המינימלי ובאלגוריתם הכיווץ, ורק העמוד השישי ב-MAXCUT. ה-slug בתוך הקובץ תוקן ל-min-cut-contraction-algorithm והכותרת האמיתית נכתבה ב-title_he; שם הקובץ עצמו לא שונה לפי ההנחיה ודורש שינוי ידני במניפסט.

עמוד 1 בסיכום: הכותרת הראשית קשה לפענוח מלא ברזולוציה הנוכחית; שוחזרה כ'בעיית החתך המינימלי' לפי גוף העמוד ולפי ההקלטה.

עמוד 2 בסיכום: בשורה שלפני התיבה הכחולה נרשם $Pr[\bigwedge_{j=1}^{n} E_j]$ במקום $\bigwedge_{j=1}^{n-2}$; תוקן כאן לפי התיבה עצמה ולפי ההקלטה.

עמוד 3 בסיכום: מספר החזרות בהגברה נרשם $2 \ln \binom{n}{2}$ ואינו שלם; כאן נכתב $\lceil 2 \ln \binom{n}{2} \rceil$, וההערכה $\le \tfrac12$ נשמרת.

הגרף בן חמשת הקודקודים שצוייר בהקלטה ב-[00:06:30] אינו נראה בהקלטה ורשימת הקשתות שלו שוחזרה מהתיאור המילולי; ייתכן שקשת אחת שונה. הדוגמה כאן עקבית בפני עצמה.

השם 'אלגוריתם Karger' אינו מופיע לא בסיכום ולא בהקלטה; הוא נוסף כאן כהערת מינוח בלבד.

19 השיטה ההסתברותית, המשך: ניסוי אחיד ל-MAXCUT, חסם 7/8 ל-3ESAT, ובעיית הקבוצה השלטת

שלוש הפעלות של השיטה ההסתברותית ועוד רדוקציה: הוכחה שנייה לקיום חתך בגודל $\ge|E|/2$ — הפעם בבחירת U אחידה מתוך 2^V ובספירה קומבינטורית במקום מטבע לכל קודקוד; הוכחה שלכל נוסחת 3E-CNF עם m הסגרים קיימת השמה המספקת לפחות $\tfrac78 m$ מהם; הגדרת בעיית הקבוצה השלטת DS והוכחת NP-שלמות שלה דרך $\mathrm{VC}\le_p\mathrm{DS}$; ולבסוף טענת קיום מהכיוון ההפוך — בכל גרף בעל דרגה מינימלית d קיימת קבוצה שלטת בגודל לכל היותר $|V|\frac{\ln(d+1)+1}{d+1}$, כולל הגזירה שממנה הגיע ערך ההסתברות.

ביטחון: high

בקצרה

מוכיחים **מחדש** שבכל גרף $G=(V,E)$ קיים חתך בגודל $\ge \frac{|E|}{2}$, אבל בניסוי אקראי אחר: במקום להטיל מטבע לכל קודקוד, **מגרילים קבוצה** U **באופן אחיד מתוך** 2^V. כל הניתוח זהה חוץ מצעד אחד — חישוב $\Pr[I_e=1]$ — שהופך מחישוב אי-תלות לחישוב **ספירה קומבינטורית**.

מוכיחים שלכל נוסחת 3E-CNF (בדיוק שלושה ליטרלים ממשתנים **שונים** בכל הסגר) עם m הסגרים **קיימת** השמה המספקת לפחות $\frac{7}{8}m$ הסגרים. זהו החסם הטוב ביותר האפשרי מבחינה חישובית: לפי משפט ה-PCP, להבדיל בין $\frac{7}{8}+\varepsilon$ לבין $\frac{7}{8}$ זו בעיה NP-קשה.

מגדירים את **בעיית הקבוצה השלטת** DS ומוכיחים שהיא NP-שלמה, באמצעות הרדוקציה $\mathrm{VC}\le_p\mathrm{DS}$: לכל קשת xy מוסיפים קודקוד חדש v_{xy} ומחברים אותו ל-x ול-y.

מוכיחים טענת קיום מהכיוון **ההפוך**: בכל גרף בעל דרגה מינימלית d קיימת קבוצה שלטת **קטנה** — בגודל לכל היותר $|V|\cdot\frac{\ln(d+1)+1}{d+1}$. כאן משתמשים ב-$\Pr[X\ge\mathbb{E}[X]]>0$ במקום ב-$\Pr[X>0]$.

הניסוי שם הוא **דו-שלבי**: שלב אקראי (כל קודקוד נכנס בהסתברות p בנפרד) ואחריו שלב **דטרמיניסטי מתקן** שדואג שהקבוצה תהיה שלטת **בוודאות**. זהו התבנית "הגרל ואז תקן", ומחירה מתבטא בתוחלת ולא בנכונות.

ערך ההסתברות $p=\frac{\ln(d+1)}{d+1}$ **אינו** קסם: הוא המינימום של הפונקציה $f(p)=p+e^{-p(d+1)}$, ואת הגזירה עושים בשיעור.

מוטיב מרכזי לכל השיעור: **השיטה ההסתברותית היא טיעון ממוצע, לא אלגוריתם.** אין בה שום ניסיון למצוא את האובייקט; היא רק אומרת שמשהו שטוב לפחות כמו הממוצע חייב להתקיים.

רקע ותלויות

מהו חתך (שיעור 10, שיעור 18). בהינתן גרף $G=(V,E)$ וקבוצה $U\subseteq V$, החתך המושרה על ידי U הוא $(U,\bar U)=\{e\in E:\ |e\cap U|=1\}$, כלומר קבוצת הקשתות שקצה אחד שלהן ב-U והקצה השני מחוץ ל-U. גודל החתך הוא $|(U,\bar U)|$. MAXCUT היא בעיית מציאת חתך מקסימלי; היא NP-קשה (שיעור 10, דרך $3\mathrm{NAE}\le_p\mathrm{MAXCUT}$).

כיסוי בקודקודים (שיעור 10). $U \subseteq V$ היא כיסוי בקודקודים אם $\forall e \in E:\ e \cap U \neq \emptyset$. השפה: $\mathrm{VC} = \left\{ \langle G, k \rangle \ :\ G \text{ graph},\ k \in \mathbb{N},\ \exists U \subseteq V \text{ a vertex cover},\ |U| \leq k \right\}$. בשיעור 10 הוכח ש-$\mathrm{VC}$ היא NP-שלמה. זו נקודת המוצא של הרדוקציה כאן.

כיוון הרדוקציה. הסימון $A \leq_p B$ אומר: קיים אלגוריתם פולינומי שממיר קלט של A לקלט של B תוך שימור התשובה. במילים — B **היא הבעיה הקשה יותר**; פתרון ל-B נותן פתרון ל-A. לכן כדי להוכיח ש-DS קשה, נראה $\mathrm{VC} \leq_p \mathrm{DS}$ ולא להפך. (בדיבור מחליפים את הכיוון הזה כל הזמן; שווה לעצור ולוודא.)

שתי הטענות שמניעות את השיטה ההסתברותית (שיעור 18, משפט 9). יהי $(\Omega, \Pr)$ מרחב הסתברות סופי.

אם $A \subseteq \Omega$ מאורע ו-$\Pr[A] > 0$, אז $A \neq \emptyset$.

אם X משתנה מקרי בעל תוחלת, אז $\Pr\left[X \geq \mathbb{E}[X]\right] > 0$.

בשיעור הזה נזדקק גם לגרסה המשלימה של (2), שנוכיח בהמשך (למה 1): $\Pr\left[X \leq \mathbb{E}[X]\right] > 0$.

המשמעות — וזו הנקודה שחוזרת בכל השיעור. הצמד (1)+(2) אומר: אם בניתי ניסוי אקראי על אוסף אובייקטים והראיתי שהתוחלת של מדד האיכות היא c, אז **קיים** אובייקט שאיכותו לפחות c. זהו **טיעון ממוצע**: לא ייתכן שכל האיברים נמצאים מתחת לממוצע. ההוכחה אינה מצביעה על האובייקט, אינה מייצרת אותו, ואינה אלגוריתם — האקראיות היא **כלי הוכחה בלבד**, והטענה שמוכיחים היא טענה קומבינטורית טהורה שאין בה זכר להסתברות.

לינאריות התוחלת (הסתברות, וחזרה בשיעור 18). לכל משתנים מקריים $X_1, \ldots, X_k$ בעלי תוחלת, $\mathbb{E}\left[\sum_{i=1}^{k} X_i\right] = \sum_{i=1}^{k} \mathbb{E}[X_i]$, **בלי שום הנחה על אי-תלות**. זהו הכלי היחיד שנחיל על כל המשתנים ביחד; כל השאר נעשה למשתנה בודד. זו בדיוק הסיבה שנשתמש בתוחלת ולא בשונות — שונות דורשת חישוב קובריאנציות ותקרוס כאן.

אינדיקטור. לכל מאורע A, המשתנה I_A שמקבל 1 אם A קרה ו-0 אחרת מקיים $\mathbb{E}[I_A] = \Pr[A]$.

מ-$3\mathrm{SAT}$ ל"בדיוק שלושה" (שיעור 8). בשיעור 8 ראינו רדוקציה מ-SAT ל-$3\mathrm{SAT}$, ובדרך גם את הטכניקה שממירה הסגר קצר מדי להסגרים באורך בדיוק 3. את זה נניח כאן: אנחנו מתחילים ישירות מנוסחאות שבהן כל הסגר מכיל **בדיוק** שלושה ליטרלים ממשתנים שונים.

הגדרות

הגדרה 1: נוסחת 3E-CNF, והבעיה $\mathrm{MAX\text{-}3ESAT}$

נוסחה בוליאנית φ היא בצורת **3E-CNF** (בהקלטה: "exact SAT 3") אם היא בצורת 3CNF ובנוסף בכל הסגר שלה יש **בדיוק שלושה ליטרלים משלושה משתנים שונים**.

השפה/הבעיה בגרסת האופטימיזציה:

> **קלט:** נוסחה φ בצורת 3E-CNF. **מטרה:** למצוא השמה v המספקת מספר רב ביותר של **הסגרים** ב-φ.

זו גרסת האופטימיזציה של SAT: לא שואלים "כן/לא — האם ניתן לספק את הכול", אלא מבקשים למקסם.

למה נדרשת ההקפדה הזו. שתי הדרישות אינן קישוט. "בדיוק שלושה" (ולא "לכל היותר שלושה") נחוצה כדי שההסתברות שהסגר **אינו** מסופק תהיה בדיוק $\frac{1}{8}$ ולא יותר; "משתנים שונים" נחוצה כדי שנוכל לפרק הסתברות של חיתוך למכפלה. בלי שתיהן החישוב בהמשך פשוט לא עובד. בהקלטה ([00:17:37]) הוסבר שאם אנחנו מדברים על **אלגוריתמים** אפשר לעבור לצורה הזו על ידי רדוקציה, אבל את הקלט עצמו צריך להביא לצורה הזו במפורש.

דוגמה. $\varphi = (x_1 \vee x_2 \vee x_3) \wedge (\neg x_1 \vee x_2 \vee x_4)$ היא 3E-CNF: שני הסגרים, בכל אחד שלושה ליטרלים משלושה משתנים שונים. שימו לב ש-x_1 ו-x_2 **חוזרים** בין הסגרים — זה מותר לגמרי ([00:21:24]).

אי-דוגמה. $(x_1 \vee x_1 \vee x_2)$ אינה חוקית — שני ליטרלים מאותו משתנה בתוך אותו הסגר. גם $(x_1 \vee x_2)$ אינה חוקית — שני ליטרלים בלבד.

הגדרה 2: קבוצה שלטת (Dominating Set)

יהי $G = (V, E)$ גרף. קבוצת קודקודים $U \subseteq V$ תיקרא **קבוצה שלטת** (dominating set) אם $$\forall x \in V : \quad x \in U \ \ \vee \ \ \exists y \in U \text{ such that } xy \in E.$$

במילים: כל קודקוד בגרף הוא או **בתוך** הקבוצה, או **שכן מיידי** של מישהו בקבוצה. שימו לב שמדובר בשכנות ישירה, לא בקיום מסלול ([00:51:24]).

אינטואיציה ומוטיבציה ([00:53:01]). נניח שאני רוצה לשלם למשפיענים ברשת כדי להפיץ מסר. אני רוצה קבוצה שכל אחד ברשת או שילמתי לו, או שהוא מחובר ישירות למישהו ששילמתי לו — וכמה שיותר קטנה, כי משלמים לכל אחד. אותו דבר במיקום רמזורים בצמתים, שלטי פרסומת, או תחנות שירות. זו בדיוק קבוצה שלטת מינימלית.

ההבדל מכיסוי בקודקודים ([01:03:06]). ההגדרות דומות מאוד, אבל מסתכלות מכיוונים שונים: בכיסוי בקודקודים המטרה היא **לגעת בכל קשת**; בקבוצה שלטת המטרה היא **לכסות כל קודקוד**. בקבוצה שלטת אני *לא* חייב לגעת בכל קשת.

דוגמה. במסלול $a - b - c$, הקבוצה $U = \{b\}$ שלטת: $b \in U$, ו-a, c שכנים של b.

אי-דוגמה. באותו גרף, $U' = \{a\}$ **אינה** שלטת: $c \notin U'$ ו-c אינו שכן של a.

הגדרה 3: הבעיה DS

> **קלט:** גרף $G = (V, E)$ ומספר $k \in \mathbb{N}$. **שאלה:** האם קיימת ב-G קבוצה שלטת בגודל **לכל היותר** k?

השפה: $\mathrm{DS} = \left\{ \langle G, k \rangle \ : \ \exists U \subseteq V \text{ dominating in } G,\ |U| \le k \right\}$.

"לכל היותר" מול "בדיוק" ([00:51:57]). כאן ההבחנה אינה משנה: אם U שלטת ו-$U \subseteq U' \subseteq V$, אז U' שלטת גם היא (התנאי הוא קיומי ולא נהרס בהוספה). לכן קיום קבוצה שלטת בגודל $\le k$ שקול לקיום קבוצה שלטת בגודל בדיוק k, כל עוד $k \le |V|$. (לעומת זאת ב-VC, מסיבה דומה, גם שם אין הבדל.)

הגדרה 4: דרגה מינימלית

לגרף $G = (V, E)$ נסמן $d = \min_{v \in V} \deg(v)$, כלומר הדרגה **המינימלית** בגרף. זו הדרגה שתופיע בטענת הקיום של הקבוצה השלטת. שימו לב לכיוון: מכיוון שנרצה לחסום **מלמעלה** ביטוי מהצורה $(1-p)^{\deg(v)+1}$, ומכיוון ש-$0 < 1 - p < 1$, חסם מלמעלה מתקבל מ**חזקה נמוכה יותר**

— כלומר מ-$\deg(v) \geq d$. לכן דווקא הדרגה המינימלית היא הפרמטר הנכון כאן, ולא המקסימלית.

משפטים והוכחות

משפט 1: בכל גרף קיים חתך בגודל $\geq \frac{|E|}{2}$ — הוכחה שנייה, בניסוי אחיד

טענה. יהי $G = (V, E)$ גרף. אז קיימת קבוצה $U \subseteq V$ שהחתך $(U, \bar{U})$ שהיא משרה מכיל לפחות $\frac{|E|}{2}$ קשתות.

מה חדש כאן. את הטענה עצמה כבר הוכחנו בשיעור 18 (משפט 10) בניסוי שבו לכל קודקוד מטילים מטבע הוגן בנפרד ובאופן בלתי תלוי. **הטענה אינה משתנה ואינה משתפרת.** מה שמשתנה הוא הניסוי, ולכן גם צעד אחד בהוכחה. המרצה הציג את זה מפורשות כתרגיל בשיטה ([00:02:45]): "תחשבו על הדבר הטבעי ביותר לעשות — אם אני רוצה להגיד *קיימת קבוצה*, מה האלגוריתם האקראי הכי פשוט שאתם יכולים לדמיין? תבחר קבוצה, באופן אחיד ואקראי." זהו האלגוריתם הקצר ביותר האפשרי; מחירו הוא שהניתוח דורש ספירה.

הניסוי. בהינתן הגרף G (שהוא **קבוע** ואינו מוגרל), נבחר קבוצה $U \subseteq V$ **באופן אחיד ואקראי מתוך כל תת-הקבוצות של** V.

מרחב המדגם. מרחב המדגם הוא $\Omega = 2^V = \{ U : U \subseteq V \}$, כלומר **קבוצת כל תתי-הקבוצות** של V, ו-$|\Omega| = 2^{|V|}$. ההתפלגות היא אחידה: $\Pr[\{U\}] = 2^{-|V|}$ לכל $U \subseteq V$.

> **הערה על סימון ([00:03:50]).** בכיתה נאמר בטעות ש-$|\Omega| = 2$; הובהר מיד ש-Ω עצמו הוא 2^V — **אובייקט**, קבוצת קבוצות — ואילו $2^{|V|}$ הוא **מספר**, גודלו. שני דברים שונים לחלוטין שהסימון הדומה מבלבל ביניהם.

מעל מה ההסתברות. כל ההסתברויות והתוחלות להלן הן מעל בחירת U — כלומר מעל **מטבעות האלגוריתם** — עבור הגרף G **הקבוע**. אין כאן שום הגרלה של גרף.

המשתנים המקריים. נסמן ב-X את גודל החתך, $X : 2^V \to \mathbb{R}, \quad X(U) = \left|(U, \bar{U})\right|$,
ולכל $e \in E$ נסמן ב-I_e את האינדיקטור לכך ש-e בחתך, $I_e : 2^V \to \{0, 1\}, \quad I_e(U) = \begin{cases} 1 & |e \cap U| = 1 \\ 0 & \text{otherwise} \end{cases}$
ואז, כשוויון **בין פונקציות**, $X = \sum_{e \in E} I_e$.

חישוב התוחלת. מלינאריות התוחלת, $\mathbb{E}[X] = \sum_{e \in E} \mathbb{E}[I_e]$. תהי $e = xy \in E$ (ומכיוון שהגרף פשוט, $x \neq y$). אז $\mathbb{E}[I_e] = \Pr[I_e = 1] = \Pr\big[(x \in U \wedge y \notin U) \vee (x \notin U \wedge y \in U)\big]$. שני המאורעות **זרים** (לא ייתכן ש-$x \in U$ וגם $x \notin U$), ולכן מאדיטיביות סופית: $= \Pr[x \in U \wedge y \notin U] + \Pr[x \notin U \wedge y \in U]$.

וכאן — ורק כאן — ההוכחה נפרדת מזו של שיעור 18. אי אפשר לכתוב $\frac{1}{2} \cdot \frac{1}{2}$, כי לא הגדרנו מאורע פר קודקוד ולא הנחנו אי-תלות בין קודקודים; אנחנו מגרילים **קבוצה אחת** ([00:07:49]). מה שכן יש לנו זה שההתפלגות **אחידה**, ובהתפלגות אחידה ההסתברות היא "רצוי חלקי סך הכול":
$\Pr[x \in U \wedge y \notin U] = \frac{\left|\{ U \subseteq V : x \in U \wedge y \notin U \}\right|}{2^{|V|}}$,
ובאותו אופן עבור המחובר השני. נותר לספור את המונה.

הספירה, במלואה. נסמן $\mathcal{A} = \{\, U \subseteq V \;:\; x \in U,\ y \notin U \,\}$, $\mathcal{B} = 2^{V \setminus \{x,y\}}$. נגדיר $\Phi : \mathcal{A} \to \mathcal{B}$ על ידי $\Phi(U) = U \setminus \{x\}$. הפונקציה מוגדרת היטב: אם $U \in \mathcal{A}$ אז $y \notin U$ ולכן $U \setminus \{x\} \subseteq V \setminus \{x,y\}$. היא **חד-חד-ערכית ועל**, כי יש לה הופכית מפורשת $\Psi : \mathcal{B} \to \mathcal{A}$, $\Psi(W) = W \cup \{x\}$ — ואכן $\Psi(W) \in \mathcal{A}$ (מכיל את x, אינו מכיל את y), וכן $\Phi(\Psi(W)) = W$ ו-$\Psi(\Phi(U)) = U$ לכל $U \in \mathcal{A}$ (השוויון האחרון תקף כי $x \in U$). לכן $|\mathcal{A}| = |\mathcal{B}| = 2^{|V|-2}$, שם השוויון האחרון הוא הנוסחה הבסיסית $|2^A| = 2^{|A|}$ עבור $A = V \setminus \{x,y\}$, שגודלה $|V| - 2$ (כי $x \neq y$).

> **הערה:** בהרצאה הצעד הזה נאמר במילה אחת — "זה כמו לבחור תת-קבוצה של $V \setminus \{x,y\}$" — והפירוט הועלה רק אחרי שאלה מהכיתה ([00:09:41]). הפירוט הוא הפונקציה ההפיכה שלמעלה. הטכניקה הכללית ([00:16:12]): כדי לספור קבוצה, מוצאים התאמה חד-חד-ערכית ועל לקבוצה שיש עבורה נוסחה מוכרת.

מסימטריה מלאה (החלפת התפקידים של x ו-y) גם $\left|\{U : x \notin U,\ y \in U\}\right| = 2^{|V|-2}$. לכן $\mathbb{E}[I_e] = \frac{2^{|V|-2}}{2^{|V|}} + \frac{2^{|V|-2}}{2^{|V|}} = \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$, ומכאן $\mathbb{E}[X] = \sum_{e \in E} \frac{1}{2} = \frac{|E|}{2}$.

מתוחלת לקיום. לפי טענה (2) של השיטה ההסתברותית, $\Pr\left[X \geq \frac{|E|}{2}\right] > 0$, כלומר $\Pr\left(\left\{\, U \subseteq V \;:\; X(U) \geq \frac{|E|}{2} \,\right\}\right) > 0$, ולפי טענה (1) הקבוצה הזו אינה ריקה. כלומר **קיימת** $U \subseteq V$ שהחתך שהיא משרה מכיל לפחות $\frac{|E|}{2}$ קשתות. ■

מדוע זה טיעון ממוצע ולא אלגוריתם. מה שהראינו הוא שהערך **הממוצע** של X על פני כל $2^{|V|}$ הקבוצות הוא $\frac{|E|}{2}$. לא ייתכן שכל האיברים בממוצע קטנים ממש מהממוצע, ולכן מישהו לפחות משיג אותו. ההוכחה אינה מצביעה על אף U קונקרטית, ואינה נותנת שיטה למצוא אחת. (למצוא כזו **אפשר** — ראו את החיפוש המקומי בשיעור 13 ואת האלגוריתם החמדן בשיעור 14 — אבל זה סיפור אחר לגמרי.)

> **מלכודת ([00:13:31], [00:14:37]).** שאלה מהכיתה: "למה לא פשוט מכפילים את ההסתברויות?" התשובה: אי-תלות היא משהו שצריך **להוכיח** או **להניח**, לא משהו שנובע מכך שהדגימה אחידה. במקרה הזה זה אמנם נכון — החישוב שביצענו למעשה **מוכיח** ש-$\Pr[x \in U \wedge y \notin U] = \frac{1}{4} = \frac{1}{2} \cdot \frac{1}{2}$ — אבל זה מסקנה של החישוב ולא קלט שלו. שאלה נוספת ערבבה בין "זרים" לבין "בלתי תלויים"; אלה מושגים שונים לחלוטין, ולמעשה **מנוגדים**: שני מאורעות זרים בעלי הסתברות חיובית הם בהכרח **תלויים**.

משפט 2: בכל נוסחת 3E-CNF קיימת השמה המספקת $\geq \frac{7}{8}$ מההסגרים

טענה. תהי φ נוסחה בצורת 3E-CNF עם m הסגרים. אז **קיימת** השמה v המספקת לפחות $\frac{7}{8}m$ מההסגרים של φ.

הניסוי. נסמן את משתני φ ב-$x_1, \ldots, x_n$. נגדיר השמה אקראית v כך: לכל $1 \leq i \leq n$, **באופן בלתי תלוי** בשאר, $\Pr[v(x_i) = 1] = \frac{1}{2}, \qquad \Pr[v(x_i) = 0] = \frac{1}{2}$.

מרחב המדגם ומעל מה ההסתברות. מרחב המדגם הוא קבוצת **כל ההשמות** $\Omega = \{0,1\}^{\{x_1,\ldots,x_n\}}$, $|\Omega| = 2^n$. הנוסחה φ **קבועה** — היא הקלט; היא אינה מוגרלת. כל ההסתברויות והתוחלות הן מעל בחירת ההשמה, כלומר מעל מטבעות האלגוריתם.

המשתנים המקריים. נסמן ב-X את מספר ההסגרים המסופקים: $X : \Omega \to \mathbb{R}, \qquad X(v) = \bigl|\{\, C \text{ a clause of } \varphi \;:\; v \text{ satisfies } C \,\}\bigr|$. לכל הסגר C של φ נסמן ב-I_C את האינדיקטור למאורע "v מספקת את C". שימו לב: I_C היא פונקציה של v בלבד; C אינו קלט שלה אלא חלק מהמבנה שלה ([00:27:32]). אז $X = \sum_{C \in \varphi} I_C$, ולכן מלינאריות התוחלת

$$\mathbb{E}[X] = \sum_{C \in \varphi} \mathbb{E}[I_C].$$

חישוב $\mathbb{E}[I_C]$. יהי C הסגר של φ. לפי ההגדרה קיימים שלושה ליטרלים **ממשתנים שונים** כך ש-$C = \ell_1 \vee \ell_2 \vee \ell_3$. נחשב דווקא את ההסתברות המשלימה, כי היא זו שיש לה תיאור פשוט: $\Pr[I_C = 0] = \Pr\bigl[v \text{ does not satisfy } C\bigr] = \Pr\bigl[v(\ell_1) = 0 \;\wedge\; v(\ell_2) = 0 \;\wedge\; v(\ell_3) = 0\bigr]$, כי דיסיונקציה אינה מסופקת אם ורק אם **כל** הליטרלים שלה מקבלים 0.

כאן נכנסת אי-התלות. שלושת הליטרלים באים משלושה **משתנים שונים**, ולכן שלושת המאורעות $\{v(\ell_j) = 0\}$ נקבעים על ידי שלושה מטבעות שונים ובלתי תלויים, ולכן: $\Pr[v(\ell_1) = 0] \cdot \Pr[v(\ell_2) = 0] \cdot \Pr[v(\ell_3) = 0]$. לכל ליטרל בודד ℓ: אם $\ell = x_i$ אז $\Pr[v(\ell) = 0] = \Pr[v(x_i) = 0] = \frac{1}{2}$; ואם $\ell = \neg x_i$ אז $\Pr[v(\ell) = 0] = \Pr[v(x_i) = 1] = \frac{1}{2}$. בשני המקרים $\Pr[I_C = 0] = \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{8}$, לכן

$$\mathbb{E}[I_C] = \Pr[I_C = 1] = 1 - \tfrac{1}{8} = \tfrac{7}{8}.$$

האינטואיציה מאחורי ה-$\frac{1}{8}$ ([00:20:50]). להסגר עם שלושה ליטרלים ממשתנים שונים יש $2^3 = 8$ דרכים להשים ערכי אמת לליטרלים שלו, ובדיוק **אחת** מהן מכשילה אותו — זו שנותנת 0 לשלושתם. משם ה-8 וגם ה-3: $8 = 2^3$, והמעריך הוא מספר הליטרלים בהסגר.

סיום. נסמן ב-m את מספר ההסגרים ב-φ. אז $\mathbb{E}[X] = \sum_{C \in \varphi} \mathbb{E}[I_C] = \sum_{C \in \varphi} \frac{7}{8} = \frac{7}{8} m$. לפי טענה (2), $\Pr\bigl[X \geq \frac{7}{8} m\bigr] > 0$, ולפי טענה (1) המאורע הזה אינו ריק. כלומר **קיימת** השמה v המספקת לפחות $\frac{7}{8} m$ הסגרים. ■

> **השאלה החשובה של השיעור ([00:34:28]).** סטודנט הצביע על כך שהאינדיקטורים I_C **תלויים זה בזה** — הסגרים שונים חולקים משתנים, ולכן ההסתברות שאחד מסופק בהחלט משפיעה על ההסתברות שהשני מסופק. זו הבחנה נכונה לגמרי, והתשובה היא שזה **לא משנה**: לינאריות התוחלת אינה דורשת דבר מהמשתנים המקריים מלבד קיום התוחלת. ברגע שעברנו מ-$\mathbb{E}\bigl[\sum_C I_C\bigr]$ ל-$\sum_C \mathbb{E}[I_C]$, כל תוחלת מחושבת בנפרד ואין יותר אינטראקציה. אילו היינו רוצים **שונות** — היינו נתקעים, כי היינו צריכים את כל הקובריאנציות. וגם: אילו היינו שואלים "מה ההסתברות שההשמה מספקת בדיוק כך וכך הסגרים", החישוב היה נורא בגלל אותן תלויות. התוחלת היא מדד "חלש" ולכן **מתירני**, וזו בדיוק הסיבה שהיא עובדת פה.

למה 1: $\Pr\bigl[X \leq \mathbb{E}[X]\bigr] > 0$

טענה. יהי $(\Omega, \Pr)$ מרחב הסתברות **סופי** ויהי X משתנה מקרי עליו. אז $\Pr\bigl[X \leq \mathbb{E}[X]\bigr] > 0$.

הוכחה. נסמן $\mu = \mathbb{E}[X]$ ונניח בשלילה $\Pr[X \le \mu] = 0$. אז לכל $\omega \in \Omega$ עם $\Pr[\{\omega\}] > 0$ מתקיים $X(\omega) > \mu$. לכן $\mu = \sum_{\omega \in \Omega} \Pr[\{\omega\}]\, X(\omega) > \sum_{\omega:\, \Pr[\{\omega\}]>0} \Pr[\{\omega\}] \cdot \mu = \mu$, כאשר האי-שוויון חד מפני שהסכום אינו ריק (סכום ההסתברויות הוא $1 > 0$), והשוויון האחרון כי $\sum_{\omega} \Pr[\{\omega\}] = \Pr[\Omega] = 1$. קיבלנו $\mu > \mu$ — סתירה. ■

האינטואיציה ([01:34:49]). תחשבו על ממוצע: לא ייתכן שכל האיברים גדולים ממש מהממוצע, וגם לא ייתכן שכולם קטנים ממנו ממש. מישהו חייב להיות מעליו או שווה לו, ומישהו חייב להיות מתחתיו או שווה לו. זו כל התובנה. בשיעור 18 השתמשנו בכיוון ה-$\ge$ כי רצינו חתך **גדול**; במשפט 5 נשתמש בכיוון ה-$\le$ כי נרצה קבוצה שלטת **קטנה**.

משפט 3: $\mathrm{DS} \in \mathrm{NP}$

טענה. $\mathrm{DS} \in \mathrm{NP}$.

הוכחה (מוודא דטרמיניסטי). נגדיר מוודא M שמקבל קלט $\langle G, k\rangle$ ותעודה $\langle U\rangle$ שהיא קידוד של תת-קבוצה של V. M פועל כך:

בודק ש-$U \subseteq V$ ושו-$|U| \le k$. זמן $O(|V|)$.

לכל $x \in V$ בודק אם $x \in U$; אם לא, עובר על רשימת השכנים של x ובודק אם קיים $y \in U$ עם $xy \in E$. אם עבור איזשהו x שני הבדיקות נכשלו — דוחה.

אם כל הקודקודים עברו — מקבל.

נכונות. לפי הגדרה 2, U שלטת אם ורק אם כל $x \in V$ עובר את הבדיקה בשלב 2. לכן M מקבל את $\langle G, k\rangle, \langle U\rangle$ אם ורק אם U היא קבוצה שלטת בגודל $\le k$; כלומר קיימת תעודה מתקבלת אם ורק אם $\langle G, k\rangle \in \mathrm{DS}$.

חשבון סיבוכיות. אורך התעודה הוא $O(|V|\log|V|)$ ביטים — פולינומי בגודל הקלט. שלב 2 עולה $O(|V|+|E|)$ בייצוג רשימות שכנויות (או $O(|V|^2)$ במטריצת שכנויות). סך הכול פולינומי. ■

> **הערה ([00:54:33]).** ניתן להראות שייכות ל-NP גם על ידי מכונה **אי-דטרמיניסטית** שמנחשת את U ואז בודקת. המרצה העדיף את הניסוח עם המוודא הדטרמיניסטי — "אני מרגיש יותר בשליטה" — ושתי הדרכים תקפות באותה מידה.

משפט 4: $\mathrm{VC} \le_p \mathrm{DS}$, ולכן DS היא NP-שלמה

טענה. $\mathrm{VC} \le_p \mathrm{DS}$. מכיוון ש-$\mathrm{VC}$ היא NP-קשה (שיעור 10), נובע ש-DS NP-קשה; ביחד עם משפט 3, DS היא **NP-שלמה**.

למה דווקא VC ([00:56:07]). כי היא "מריחה דומה" — שתי הבעיות מבקשות קבוצת קודקודים קטנה שמכסה משהו. הדמיון הזה הוא בדיוק מה שמאפשר רדוקציה קצרה, וההבדל ביניהן הוא בדיוק מה שהרדוקציה צריכה לגשר עליו.

הרדוקציה (האלגוריתם R).

קלט: גרף $G = (V, E)$ ומספר $k \in \mathbb{N}$ — כלומר קלט של VC.
לכל קשת $xy \in E$: 1.1. הוסף קודקוד חדש v_{xy} וחבר אותו בקשת ל-x ובקשת ל-y.
הסר מהגרף המתקבל את כל הקודקודים המבודדים, והחזר את הגרף המתקבל $\hat{G} = (\hat{V}, \hat{E})$ יחד עם **אותו** k.

חשבון זמן הריצה ([00:58:56]). הלולאה בשלב 1 רצה $|E|$ פעמים; בכל איטרציה מוסיפים קודקוד אחד ושתי קשתות — פעולה בזמן קבוע (או $O(\log)$ בייצוג סביר). זיהוי הקודקודים המבודדים בשלב 2 הוא מעבר יחיד על רשימות השכנויות, $O(|V| + |E|)$. סך הכול $O(|V| + |E|)$, ובוודאי פולינומי בגודל הקלט. הגרף המוחזר מקיים $|\hat{V}| \le |V| + |E|$ ו-$|\hat{E}| \le 3|E|$, כלומר גם **הפלט** פולינומי — מה שנחוץ, כי אחרת אי אפשר היה לכתוב אותו בזמן פולינומי.
האלגוריתם מחזיר אינסטנס תקין. הקלט הוא זוג $\langle$גרף, מספר$\rangle$ והפלט הוא זוג $\langle$גרף, מספר$\rangle$ — כלומר קלט חוקי של DS.
למה בכלל צריך את שלב 2 ([01:11:49]). קודקוד מבודד ב-G אינו נוגע באף קשת, ולכן **לעולם אינו דרוש** לכיסוי בקודקודים: אם U כיסוי, גם U ללא קודקודים מבודדים הוא כיסוי. לעומת זאת בקבוצה שלטת קודקוד מבודד **חייב** להיכנס לקבוצה — אין לו שכן שיכסה אותו. בלי שלב 2 היינו מחייבים את DS להוסיף קודקודים שאין להם שום מקבילה בצד VC, וזה היה מקלקל את שמירת התשובה. מכיוון שהסרת קודקודים מבודדים אינה משנה את התשובה של VC (הקשתות לא השתנו), מותר לנו להניח מעתה ש-G נטול קודקודים מבודדים.
נסמן מעתה: $G = (V, E)$ הוא הגרף לאחר הסרת הקודקודים המבודדים, $\hat{G} = (\hat{V}, \hat{E})$ הגרף שמחזיר האלגוריתם. שימו לב לתכונה המבנית שנשתמש בה שוב ושוב: **לכל קודקוד חדש** $v_{xy} \in \hat{V} \setminus V$ **יש בדיוק שני שכנים ב-$\hat{G}$, והם x ו-y, ושניהם ב-V.**

כיוון א': אם $\langle G, k\rangle \in \mathrm{VC}$ אז $\langle \hat{G}, k\rangle \in \mathrm{DS}$.
נניח $\langle G, k\rangle \in \mathrm{VC}$. אז קיימת $U \subseteq V$ כך ש-$\forall e \in E:\ e \cap U \neq \emptyset$, וכן $|U| \le k$.
נתבונן ב**אותה** U בדיוק, כתת-קבוצה של $\hat{V}$ (חוקי, כי $V \subseteq \hat{V}$). נראה שהיא שלטת ב-$\hat{G}$. יהי $x \in \hat{V}$; נניח $x \notin U$ (אם $x \in U$ אין מה להוכיח — זו טענת "או", ולהוכחתה מספיק להראות שאם צד אחד לא מתקיים אז השני מתקיים).
מקרה 1: $x \in V$. מכיוון ש-G נטול קודקודים מבודדים, קיים $y \in V$ עם $xy \in E$. U כיסוי בקודקודים, ולכן $xy \cap U \neq \emptyset$, כלומר $x \in U$ או $y \in U$. הנחנו $x \notin U$, ולכן $y \in U$. וכן $xy \in \hat{E}$. אז ל-x יש שכן ב-U.
מקרה 2: $x \notin V$. אז x הוא קודקוד שנוצר בשלב 1, כלומר קיימים $a, b \in V$ עם $ab \in E$ ו-$x = v_{ab}$. U כיסוי בקודקודים, ולכן $a \in U$ או $b \in U$. מהבנייה $ax \in \hat{E}$ וגם $bx \in \hat{E}$. לכן בכל מקרה קיים $y \in \{a, b\} \cap U$, ו-$xy \in \hat{E}$ — כלומר ל-x יש שכן ב-U.
בשני המקרים $x \in U$ או שקיים לו שכן ב-U; לכן U שלטת ב-$\hat{G}$. וגודלה $k \ge |U|$ לא השתנה. לכן $\langle \hat{G}, k\rangle \in \mathrm{DS}$.

כיוון ב': אם $\langle \hat{G}, k\rangle \in \mathrm{DS}$ אז $\langle G, k\rangle \in \mathrm{VC}$.
נניח שקיימת $\hat{U} \subseteq \hat{V}$ שלטת ב-$\hat{G}$ עם $|\hat{U}| \le k$.

כאן אי אפשר לקחת את $\hat{U}$ כמו שהיא ([01:18:11]) — היא אולי מכילה קודקודים חדשים, ולכן אפילו אינה מוכלת ב-V, ולכן ודאי אינה כיסוי בקודקודים של G. נבנה ממנה קבוצה $U \subseteq V$:

> לכל $x \in \hat{U}$:
> אם $x \in V$ — נכניס את x ל-U.
> אם $x \notin V$ — נכניס ל-U **אחד** משכניו (לפי כלל שרירותי קבוע, למשל "הראשון לפי סדר הקידוד"; הבחירה אינה משנה).

U מוכלת ב-V. לכל $x \in \hat{U} \setminus V$ שני שכניו הם קודקודים של V, ולכן הקודקוד שהכנסנו הוא ב-V. ובמקרה הראשון הכנסנו $x \in V$ עצמו.
חשבון הגודל. לכל איבר של $\hat{U}$ הכנסנו ל-U לכל היותר איבר אחד, ולכן $|U| \leq |\hat{U}| \leq k$. (ייתכן שהכנסנו את אותו קודקוד פעמיים — למשל אם v_{ab} ו-v_{ac} שניהם ב-$\hat{U}$ ובשניהם נבחר a — ואז $|U|$ קטן ממש; זה רק לטובתנו, כי אנחנו רוצים חסם עליון.)
U היא כיסוי בקודקודים של G. תהי $xy \in E$ ונניח $x \notin U$; נראה $y \in U$.
ראשית, $x \notin U$ יחד עם $x \in V$ גורר $x \notin \hat{U}$ (אילו היה $x \in \hat{U}$, הרי $x \in V$, והבנייה הייתה מכניסה אותו ל-U).
כעת נתבונן בקודקוד $v_{xy} \in \hat{V}$ — הוא קיים, כי $xy \in E$ ולכן שלב 1 יצר אותו. $\hat{U}$ שלטת ב-$\hat{G}$, ולכן $v_{xy} \in \hat{U}$ או שקיים שכן של v_{xy} ב-$\hat{U}$.
מקרה 1: $v_{xy} \in \hat{U}$. אז בבניית U הכנסנו אחד משכניו — כלומר את x או את y. מכיוון ש-$x \notin U$, בהכרח הכנסנו את y, ולכן $y \in U$.
מקרה 2: קיים שכן של v_{xy} ב-$\hat{U}$. שכניו של v_{xy} הם בדיוק x ו-y, ושניהם ב-V. מכיוון ש-$x \notin \hat{U}$, בהכרח $y \in \hat{U}$; ומכיוון ש-$y \in V$, הבנייה הכניסה את y עצמו ל-U, כלומר $y \in U$.
בשני המקרים $y \in U$, ולכן $xy \cap U \neq \emptyset$. מכיוון ש-xy הייתה קשת שרירותית, U היא כיסוי בקודקודים של G בגודל $\leq k$, ולכן $\langle G, k \rangle \in \mathrm{VC}$.

סיכום. R רץ בזמן פולינומי ומקיים $\langle G, k \rangle \in \mathrm{VC} \iff R(\langle G, k \rangle) \in \mathrm{DS}$. לכן $\mathrm{VC} \leq_p \mathrm{DS}$, ומכיוון ש-$\mathrm{VC}$ NP-קשה גם DS NP-קשה. יחד עם משפט 3, DS היא NP-שלמה. ■

> **מה עושה הקודקוד v_{xy}, בשורה אחת ([01:26:46]).** הוא **כופה** על אחד מבין x, y להיות בפנים. זו כל הרדוקציה: תרגום הדרישה "כל קשת נגועה" לדרישה "כל קודקוד נשלט", על ידי הפיכת כל קשת לקודקוד שדורש שליטה.

> **מלכודת: רדוקציה אינה פותרת ([00:59:59]).** רדוקציה **לעולם** אינה מוצאת פתרון. היא מקבלת אינסטנס ומחזירה אינסטנס. האלגוריתם R אינו יודע מהו U ואינו יודע מהו $\hat{U}$ — אלה מופיעים רק **בהוכחת הנכונות**, שבה מותר לנו להניח שקיים פתרון ולבנות ממנו פתרון לצד השני. אותו דבר בדיוק קרה ברדוקציה $\mathrm{SAT} \leq_p \mathrm{3SAT}$ בשיעור 8: האלגוריתם שיחק רק עם ההסגרים; ההשמות הופיעו רק בהוכחה ([01:29:32]).

משפט 5: בכל גרף בעל דרגה מינימלית d קיימת קבוצה שלטת בגודל $\leq \frac{\ln(d+1)+1}{d+1}|V|$
טענה. יהי $G=(V,E)$ גרף ותהי d הדרגה המינימלית בו. אז קיימת ב-G קבוצה שלטת בגודל לכל היותר $\frac{\ln(d+1)+1}{d+1}\cdot|V|$.
למה זה שונה מקודם. עד עכשיו הוכחנו קיום של אובייקט **גדול** (חתך גדול, הרבה הסגרים מסופקים). כאן אנחנו רוצים אובייקט **קטן**, ולכן נשתמש ב-$\Pr[X\leq\mathbb{E}[X]]>0$ (למה 1) במקום ב-$\Pr[X\geq\mathbb{E}[X]]>0$.
למה לא לבחור קבוצה אחידה ([01:35:52]). אם נגריל U אחידה מתוך 2^V — כמו במשפט 1 — אז כל קודקוד נכנס בהסתברות $\frac{1}{2}$ ולכן $\mathbb{E}[|U|]=\frac{|V|}{2}$, שזה גרוע לחלוטין: אנחנו רוצים קבוצה **קטנה**. לכן נשתמש בהסתברות p **קטנה מ-**$\frac{1}{2}$, ונקבע אותה אחר כך.
הניסוי (אלגוריתם דו-שלבי). נסמן $p=\frac{\ln(d+1)}{d+1}\in(0,1)$, ונתחיל מ-$U=\emptyset$.

> **שלב 1 (אקראי).** לכל קודקוד $v\in V$, **באופן בלתי תלוי** בכל השאר, נכניס את v ל-U בהסתברות p. **שלב 2 (דטרמיניסטי, מתקן).** לכל $x\in V$: אם x **וכל** שכניו אינם ב-U — נכניס את x ל-U.

מרחב המדגם ומעל מה ההסתברות. מרחב המדגם הוא $\Omega=\{0,1\}^V$ — תוצאות $|V|$ המטבעות של שלב 1 — עם ההתפלגות שבה כל קואורדינטה היא 1 בהסתברות p בנפרד ובאופן בלתי תלוי. הגרף G הוא **קבוע**; אין כאן הגרלת גרפים. כל התוחלות מעל מטבעות שלב 1.
נכונות בוודאות. הקבוצה U שמתקבלת בסוף שלב 2 היא **בהכרח** קבוצה שלטת — לא בהסתברות כלשהי, אלא תמיד. הנימוק: יהי $x\in V$ ונניח בסוף התהליך ש-$x\notin U$. אז בפרט x לא הוכנס בשלב 2, כלומר לא התקיים התנאי "x וכל שכניו אינם ב-U" בזמן הבדיקה, כלומר ל-x יש שכן שנכנס ב-U (או ש-x עצמו נכנס — בסתירה להנחה). לכן כל קודקוד הוא ב-U או בעל שכן ב-U ([01:42:52]).
זו התבנית: **הגרל, ואז תקן**. הנכונות מובטחת דטרמיניסטית; מה שנשאר אקראי הוא רק ה**גודל**, וזה בדיוק מה שמנתחים.
פירוק הגודל. נסמן ב-X את מספר הקודקודים שנכנסו ל-U בשלב 1, וב-Y את מספר הקודקודים שנכנסו בשלב 2. שני השלבים מכניסים קודקודים **זרים** (שלב 2 מכניס רק קודקודים שאינם ב-U), ולכן $|U|=X+Y$.

> **למה Y עדיין אקראי, למרות ששלב 2 דטרמיניסטי ([01:44:00]).** שלב 2 אינו מטיל מטבעות, אבל **הקלט שלו** אקראי: אילו קודקודים הוא צריך להוסיף תלוי לחלוטין במה שקרה בשלב 1. זהו מצב שכיח — חלק דטרמיניסטי של אלגוריתם שפועל על קלט אקראי, ולכן פלטו משתנה מקרי.

חישוב $\mathbb{E}[X]$. לכל $v\in V$ נסמן ב-I_v את האינדיקטור למאורע "v הוכנס ל-U בשלב 1". אז $X=\sum_{v\in V}I_v$, ומלינאריות התוחלת $\mathbb{E}[X]=\sum_{v\in V}\mathbb{E}[I_v]=\sum_{v\in V}\Pr[I_v=1]=p|V|=\frac{\ln(d+1)}{d+1}|V|$.
לא השתמשנו באי-תלות כלל — לינאריות התוחלת לא דורשת אותה. אי-התלות תיכנס לראשונה בחישוב $\mathbb{E}[Y]$.)
חישוב $\mathbb{E}[Y]$. לכל $v\in V$ נסמן ב-J_v את האינדיקטור למאורע "v הוכנס ל-U בשלב 2". אז $Y=\sum_{v\in V}J_v$ ומלינאריות התוחלת $\mathbb{E}[Y]=\sum_{v\in V}\mathbb{E}[J_v]$.

יהי $v \in V$. לפי הגדרת שלב 2, $J_v = 1$ אם ורק אם **לא** v **ולא אף אחד משכניו** נכנסו ל-U בשלב 1. אלה $\deg(v)+1$ מטבעות **שונים ובלתי תלויים** (המטבע של v ומטבעות $\deg(v)$ שכניו), וכל אחד מהם צריך להיכשל, כלומר לצאת "לא נכנס", בהסתברות $1-p$ כל אחד. לכן — וכאן, לראשונה, נכנסת אי-התלות בין הקודקודים — $\mathbb{E}[J_v] \;=\; \Pr[J_v = 1] \;=\; (1-p)^{\deg(v)+1}$. כעת נחסום מלמעלה בשלושה צעדים: $(1-p)^{\deg(v)+1} \overset{(a)}{\le} (1-p)^{d+1} \overset{(b)}{\le} \left(e^{-p}\right)^{d+1} = e^{-p(d+1)} \overset{(c)}{=} \frac{1}{d+1}$.

(a) מכיוון ש-d היא הדרגה **המינימלית**, מתקיים $\deg(v) \ge d$ ולכן $\deg(v)+1 \ge d+1$; ומכיוון ש-$1-p < 1$ ו-0, העלאה בחזקה **גדולה יותר** רק מקטינה. (זו בדיוק הסיבה שהפרמטר הוא הדרגה המינימלית ולא המקסימלית.)

(b) מאי-השוויון הסטנדרטי $1 + x \le e^{x}$ לכל $x \in \mathbb{R}$, עם $x = -p$: $1 - p \le e^{-p}$. שני האגפים חיוביים, ולכן מותר להעלות בחזקה חיובית ולשמור על הכיוון.

(c) הצבת $p = \frac{\ln(d+1)}{d+1}$ נותנת $p(d+1) = \ln(d+1)$, ולכן $e^{-p(d+1)} = e^{-\ln(d+1)} = \frac{1}{d+1}$. לכן $\mathbb{E}[Y] \;=\; \sum_{v \in V} \mathbb{E}[J_v] \;\le\; \sum_{v \in V} \frac{1}{d+1} \;=\; \frac{|V|}{d+1}$.

חיבור. מלינאריות התוחלת (גם X ו-Y תלויים זה בזה בצורה חזקה — ושוב, לא אכפת לנו): $\mathbb{E}\big[|U|\big] \;=\; \mathbb{E}[X] + \mathbb{E}[Y] \;\le\; \frac{\ln(d+1)}{d+1}|V| \;+\; \frac{1}{d+1}|V| \;=\; \frac{\ln(d+1)+1}{d+1}\,|V|$.

מתוחלת לקיום. נסמן $c = \frac{\ln(d+1)+1}{d+1}|V|$. לפי למה 1, $\Pr\big[\,|U| \le \mathbb{E}[|U|]\,\big] > 0$, ומכיוון ש-$\mathbb{E}[|U|] \le c$ גם $\Pr\big[\,|U| \le c\,\big] > 0$. לפי טענה (1) המאורע הזה אינו ריק, כלומר **קיימת תוצאה של המטבעות** שעבורה הקבוצה המתקבלת מקיימת $|U| \le c$. ומכיוון שהקבוצה המתקבלת היא **תמיד** שלטת (הראינו לעיל), זוהי קבוצה שלטת בגודל $\le c$. ■

> **הערה עדינה על סדר הטיעונים ([01:48:47]).** סטודנט שאל למה לא לעצור אחרי שלב 1. התשובה: אחרי שלב 1 יש לי קבוצה **קטנה** אבל **אין לי מושג אם היא שלטת**, ולכן לא הוכחתי דבר. אילו הטענה שלי הייתה "לפחות", יכולתי לוותר על התיקון; אבל הטענה היא "לכל היותר", ולכן אני חייב לשלם על הפיכת הקבוצה לשלטת, והתשלום מופיע כתוספת $\mathbb{E}[Y]$.

> **הערה על כיוון החסמים ([01:53:04]).** בחישוב $\mathbb{E}[Y]$ חסמנו **מלמעלה**. בפועל ייתכן ששלב 2 יכניס פחות קודקודים ממה שהחסם מרשה (למשל, ייתכן שקודקוד שנספר "נחסך" כי שכן שלו נכנס). זה בסדר גמור, כי אנחנו מוכיחים "לכל היותר": חסם עליון על התוחלת נותן קיום של אובייקט קטן לפחות כמוהו.

משפט 6: מאיפה הגיע $p = \frac{\ln(d+1)}{d+1}$

טענה. הערך $p = \frac{\ln(d+1)}{d+1}$ הוא **הערך הממזער** של החסם שהניתוח לעיל מייצר, כפונקציה של p.

הגזירה ([01:56:23]–[02:01:08]). נריץ את אותו ניתוח בדיוק עם $p \in (0,1)$ **כללי**, בלי להתחייב לערך. שלב 1 נותן $\mathbb{E}[X] = p|V|$, ושלב 2 נותן, באותם צעדים (a)+(b), $\mathbb{E}[Y] \;\le\; e^{-p(d+1)}|V|$. לכן $\mathbb{E}\big[|U|\big] \;\le\; \left(p + e^{-p(d+1)}\right)\cdot|V|$. הוא קבוע ביחס ל-$p$, ולכן נותר למזער את $f(p) \;=\; p + e^{-p(d+1)}$. נגזור ונשווה לאפס: $f'(p) \;=\; 1 - (d+1)\,e^{-p(d+1)} \;=\; 0 \quad\Longleftrightarrow\quad e^{-p(d+1)} \;=\; \frac{1}{d+1}$. ניקח $\ln$ משני האגפים: $-p(d+1) \;=\; \ln\frac{1}{d+1}$.

$f''(p) = (d+1)^2 e^{-p(d+1)} > 0$ חיובית לכל p (הפונקציה קמורה). הצבת ה-p הזה ב-f נותנת $f(p) = \frac{\ln(d+1)+1}{d+1}$, שזה בדיוק החסם של משפט 5. ■

> **מה כן "הגיע מהשמיים" ([02:00:03]).** לא ה-p — הוא נגזר. מה שהגיע מבחוץ הוא **הסכמה**: הרעיון להכניס כל קודקוד בהסתברות כלשהי ואז לתקן. הסכמה הזו סבירה מאוד ("אנחנו עושים את זה הרבה"), ואחרי שקבעו אותה, ה-p האופטימלי הוא תרגיל חדו"א. שימו לב גם להבחנה שנעשתה בדקה האחרונה: p הוא ה**ארגומנט** האופטימלי, לא הערך האופטימלי; הערך האופטימלי הוא $f(p)$.

דוגמאות ותרגילים מהשיעור

דוגמה 1: מעקב מלא אחרי הניסוי האחיד של משפט 1

יהי G המסלול $V=\{a,b,c\}$, $E=\{ab,\ bc\}$, כלומר $|V|=3$, $|E|=2$. מרחב המדגם הוא $\Omega = 2^V$ ובו $2^3 = 8$ קבוצות. נחשב את $X(U)$ לכל אחת:

U	ab **בחתך?**	bc **בחתך?**	$X(U)$
$\emptyset$	לא	לא	0
$\{a\}$	כן	לא	1
$\{b\}$	כן	כן	2
$\{c\}$	לא	כן	1
$\{a,b\}$	לא	כן	1
$\{a,c\}$	כן	כן	2
$\{b,c\}$	כן	לא	1
$\{a,b,c\}$	לא	לא	0

סכום העמודה הימנית הוא $0+1+2+1+1+2+1+0=8$, ולכן $\mathbb{E}[X] = \frac{8}{8} = 1$ ✓ $= \frac{|E|}{2}$

וגם הספירה הפרטנית עובדת: עבור $e=ab$ ($x=a$, $y=b$), $\{U : a\in U,\ b\notin U\} = \{\{a\},\{a,c\}\}$, $\{U : a\notin U,\ b\in U\} = \{\{b\},\{b,c\}\}$, כלומר 2 קבוצות בכל צד, ואכן $2^{|V|-2} = 2^1 = 2$. לכן $\Pr[I_{ab}=1] = \frac{2}{8}+\frac{2}{8} = \frac{1}{2}$ ✓.

מה זה ממחיש. יש כאן שתי קבוצות ($\{b\}$ ו-$\{a,c\}$) שמשיגות $2 \geq 1$, ויש קבוצות (למשל $\emptyset$) שמשיגות 0. השיטה ההסתברותית **אינה** אומרת שהגרלה תיתן קבוצה טובה — היא אומרת שקבוצה טובה **קיימת**, כי אחרת הממוצע לא היה יכול להיות 1.

דוגמה 2: המספר $\frac{7}{8}$ על נוסחה קונקרטית

תהי $\varphi = (x_1 \vee x_2 \vee x_3) \wedge (\neg x_1 \vee x_2 \vee x_4) \wedge (x_1 \vee \neg x_3 \vee \neg x_4)$, נוסחת 3E-CNF עם $n = 4$ משתנים ו-$m = 3$ הסגרים. המשפט מבטיח קיום השמה המספקת לפחות $\frac{7}{8} \cdot 3 = \frac{21}{8} = 2.625$ הסגרים; ומכיוון שמספר ההסגרים המסופקים הוא **שלם**, המסקנה חזקה יותר: קיימת השמה המספקת לפחות 3 הסגרים, כלומר φ **ספיקה**.

ואכן, $v(x_1) = v(x_2) = v(x_3) = v(x_4) = 1$: ההסגר הראשון מסופק על ידי x_1, השני על ידי x_2, השלישי על ידי x_1. שלושה מתוך שלושה.

אימות ישיר של התוחלת. יש $2^4 = 16$ השמות. כל הסגר בנוי משלושה משתנים שונים, ולכן מספר ההשמות שאינן מספקות אותו הוא $1 \cdot 2^{4-3} = 2$ (קביעה יחידה לשלושת המשתנים שלו, וחופש מלא במשתנה הרביעי). לכן כל הסגר מסופק על ידי $16 - 2 = 14$ השמות. סכום ההסגרים המסופקים על פני כל ההשמות הוא $3 \cdot 14 = 42$, ולכן $\mathbb{E}[X] = \frac{42}{16} = 2.625 = \frac{7}{8} \cdot 3$ ✓

תרגיל מהשיעור 1 ([00:24:11]): להוכיח את משפט 2 בניסוי האחיד

התרגיל שניתן לכיתה. "איזו עוד דרך הייתה לעשות את זה? לבחור באקראי השמה מתוך קבוצת כל ההשמות. זה היה עובד אותו דבר, שווה לנסות בבית."

פתרון מלא. מרחב המדגם הוא $\Omega = \{0,1\}^n$ — כל 2^n ההשמות ל-$x_1, \dots, x_n$ — ונגריל $v \in \Omega$ **באופן אחיד**. שוב $X = \sum_C I_C$ ו-$\mathbb{E}[X] = \sum_C \mathbb{E}[I_C]$ מלינאריות התוחלת. יהי $C = \ell_1 \vee \ell_2 \vee \ell_3$ הסגר על שלושה משתנים שונים $x_{i_1}, x_{i_2}, x_{i_3}$. אז $\Pr[I_C = 0] = \frac{\left|\{\, v \in \Omega : v(\ell_1) = v(\ell_2) = v(\ell_3) = 0 \,\}\right|}{2^n}$. נספור את המונה: התנאי קובע באופן יחיד את הערכים של שלושת המשתנים $x_{i_1}, x_{i_2}, x_{i_3}$ (לכל ליטרל יש בדיוק ערך אחד של המשתנה שלו שמאפס אותו — 0 אם הליטרל חיובי, 1 אם הוא שלילי), ומשאיר את שאר $n - 3$ המשתנים חופשיים לחלוטין. באותו סגנון של משפט 1 אפשר לכתוב פונקציה הפיכה בין הקבוצה הזו לבין $\{0,1\}^{n-3}$ (צמצום ההשמה ל-$n - 3$ המשתנים הנותרים; ההופכית משלימה את שלושת הערכים הכפויים). לכן המונה הוא 2^{n-3} ו-$\Pr[I_C = 0] = \frac{2^{n-3}}{2^n} = \frac{1}{8}$, ומכאן $\mathbb{E}[I_C] = \frac{7}{8}$ ו-$\mathbb{E}[X] = \frac{7}{8}m$ בדיוק כמו קודם. **שימו לב איפה נכנסה הדרישה "שלושה משתנים שונים":** רק בזכותה שלושת התנאים קובעים שלושה משתנים **נפרדים**, ולכן הספירה נותנת 2^{n-3} ולא משהו אחר.

זהו בדיוק אותו יחס שראינו במשפט 1: הניסוי "מטבע לכל אובייקט" מוליך לחישוב אי-תלות, והניסוי "הגרלה אחידה מהמרחב כולו" מוליך לחישוב ספירה. שתי הדרכים נותנות את אותה תוצאה.

דוגמה 3: הרצת הרדוקציה $\mathrm{VC} \le_p \mathrm{DS}$ מקצה לקצה, בשני הכיוונים

יהי G המסלול $V = \{a, b, c\}$, $E = \{ab,\ bc\}$, ו-$k = 1$. אין קודקודים מבודדים.

בניית $\hat{G}$. לכל קשת מוסיפים קודקוד:

עבור ab: קודקוד v_{ab}, קשתות $a\,v_{ab}$ ו-$b\,v_{ab}$.

עבור bc: קודקוד v_{bc}, קשתות $b\,v_{bc}$ ו-$c\,v_{bc}$.

לכן $\hat{E} = \{\, ab,\ bc,\ av_{ab},\ bv_{ab},\ bv_{bc},\ cv_{bc} \,\}$, והפלט הוא $\hat{V} = \{a, b, c, v_{ab}, v_{bc}\}$, $\langle \hat{G}, 1 \rangle$.

כיוון א' (מ-VC ל-DS). $U=\{b\}$ היא כיסוי בקודקודים של G בגודל 1: $ab\cap U=\{b\}$, $bc\cap U=\{b\}$. לכן $\langle G,1\rangle\in\mathrm{VC}$. נבדוק את **אותה** $U=\{b\}$ ב-$\hat{G}$: שכניו של b ב-$\hat{G}$ הם a,c,v_{ab},v_{bc} — כלומר כל שאר הקודקודים. לכן $\{b\}$ שלטת ב-$\hat{G}$, ו-$\langle\hat{G},1\rangle\in\mathrm{DS}$. ✓

כיוון ב' (מ-DS ל-VC), עם בנייה לא טריוויאלית. נשנה ל-$k=2$ כדי לראות את הבנייה עובדת באמת. נניח שקיבלנו את הקבוצה השלטת $|\hat{U}|=2$. בדיקה שהיא אכן $\hat{U}=\{\,v_{ab},\ c\,\}$, שלטת ב-$\hat{G}$: v_{ab} שולט על עצמו, על a ועל b; c שולט על עצמו ועל v_{bc} (ועל b). כל חמשת הקודקודים מכוסים ✓.

הבנייה: $v_{ab}\notin V$ — נכניס את אחד משכניו, ולפי כלל שרירותי קבוע נבחר את הראשון, a. $c\in V$ — נכניס את c עצמו. מתקבל $|U|=2\le k$. בדיקה ש-$U=\{a,c\}$ כיסוי בקודקודים של G: $ab\cap U=\{a\}\neq\emptyset$ ✓, $bc\cap U=\{c\}\neq\emptyset$ ✓. לכן $\langle G,2\rangle\in\mathrm{VC}$ ✓.

שימו לב שהבנייה **החליפה** את v_{ab} בקודקוד ישן — בלי זה הקבוצה לא הייתה אפילו מוכלת ב-V.

דוגמה 4: למה הרדוקציה הזהותית נכשלת ([01:16:03])

נשאל בכיתה: למה לא פשוט להחזיר את G עצמו, בלי להוסיף שום קודקוד? התשובה: **כיוון ב' היה נופל**. ייתכן שיש קבוצה שלטת קטנה בלי שיש כיסוי בקודקודים באותו גודל.

דוגמה נגדית מפורשת. יהי $G=K_4$ — משולש a,b,c ועוד קודקוד מרכזי u המחובר לשלושתם:

$$V=\{a,b,c,u\},\qquad E=\{ab,\ ac,\ bc,\ ua,\ ub,\ uc\},\qquad |E|=6.$$

קבוצה שלטת בגודל 1: $\{u\}$ שולטת — שכן של a, של b ושל c. (למעשה כל קודקוד בודד שולט בגרף הזה.) לכן $\langle G,1\rangle\in\mathrm{DS}$.

אין כיסוי בקודקודים בגודל 1: קודקוד בודד נוגע לכל היותר ב-3 קשתות מתוך 6; למשל $\{u\}$ אינו נוגע ב-ab. לכן $\langle G,1\rangle\notin\mathrm{VC}$. (למעשה כיסוי מינימלי ב-K_4 הוא בגודל 3.)

כלומר הרדוקציה הזהותית הייתה שולחת יֶס-אינסטנס של DS לנוֹ-אינסטנס של VC — בדיוק הכשל שהקודקודים v_{xy} מונעים: הם מכריחים כל קשת "לדרוש" קודקוד משלה.

דוגמה 5: מעקב אחרי האלגוריתם הדו-שלבי של משפט 5

יהי $G=C_4$ המעגל $1-2-3-4-1$. כאן $|V|=4$ וכל הדרגות 2, כלומר $d=2$ ו- $p=\frac{\ln 3}{3}\approx 0.3662,$

והחסם הוא

$$\frac{\ln 3+1}{3}\cdot 4\approx\frac{2.0986}{3}\cdot 4\approx 2.798.$$

מכיוון שהגודל שלם, המסקנה היא שקיימת קבוצה שלטת בגודל ≤ 2 — וזה אכן אופטימלי ל-C_4 (למשל $\{1,3\}$).

ריצה א' (מטבעות: רק הקודקוד 1 נכנס בשלב 1). אחרי שלב 1: $U=\{1\}$, ולכן $X=1$. שלב 2 עובר על הקודקודים:

2: השכן 1 ב-U ⟵ לא מוסיפים.

3: $3\notin U$, שכניו $2,4$ אינם ב-U ⟵ **מוסיפים** את 3.

4: השכן 1 ב-U ⟵ לא מוסיפים.

1: כבר ב-U.

תוצאה: $U=\{1,3\}$, $Y=1$, $|U|=X+Y=2\le 2.798$ ✓ והיא שלטת ✓.

ריצה ב' (מטבעות: אף קודקוד לא נכנס בשלב 1). אז $X = 0$, ושלב 2 מוסיף את **כל** ארבעת הקודקודים: $Y = 4$, $|U| = 4 > 2.798$. הריצה הזו "רעה", וזה בסדר גמור: הטענה היא על ה**תוחלת**, והתוחלת מובטחת רק כממוצע. הריצה הרעה קורית בהסתברות $(1-p)^4 \approx 0.1614$ — קטנה, אבל חיובית.

מה זה ממחיש. גם כאן, השיטה ההסתברותית אינה מבטיחה שהרצה בודדת תיתן משהו טוב; היא מבטיחה שקיימת סדרת מטבעות שתיתן משהו טוב לפחות כמו הממוצע. וגם: **הנכונות** (הקבוצה שלטת) מובטחת בשתי הריצות, כי שלב 2 הוא דטרמיניסטי.

דוגמה 6: כמה טוב החסם $\frac{\ln(d+1)+1}{d+1}$

d	$\frac{\ln(d+1)+1}{d+1}$	**המשמעות**
1	≈ 0.847	קבוצה שלטת על $\leq 84.7\%$ מהקודקודים
3	≈ 0.597	$\leq 59.7\%$
9	≈ 0.330	$\leq 33.0\%$
99	≈ 0.056	$\leq 5.6\%$

מסקנה איכותית ([01:40:05]). ככל שהדרגה המינימלית גדלה, המקדם שואף ל-0 (כי $\frac{\ln x}{x} \to 0$), כלומר בגרפים "צפופים" מובטחת קבוצה שלטת קטנה מאוד יחסית.

דוגמה מספרית: גרף פטרסן. $|V| = 10$, קוביקבי ($d = 3$), ולכן החסם הוא $0.597 \cdot 10 = 5.97$, כלומר קיימת קבוצה שלטת בגודל ≤ 5. (בפועל המינימום הוא 3 — החסם נכון אך לא הדוק.)

מקרה קצה שכדאי לבדוק. אם $d = 0$ (יש קודקוד מבודד) החסם הוא $|V| = |V|$ — נכון טריוויאלית, כי V עצמה תמיד שלטת. החסם אינו יכול להיות טוב יותר במקרה הזה, שהרי קודקוד מבודד **חייב** להיכנס לכל קבוצה שלטת.

הערות מהשיעור

[00:03:50] 2^V הוא אובייקט, $2^{|V|}$ הוא מספר. בלבול בין קבוצת החזקה לבין גודלה חוזר בכל השיעור; שווה לכתוב את מרחב המדגם במפורש כדי לא ליפול בו.

[00:09:41]–[00:16:12] הטכניקה לספירה. כדי לחשב גודל של קבוצה, מוצאים פונקציה חד-חד-ערכית ועל לקבוצה שגודלה ידוע. המרצה הדגיש שברמת קורס בקומבינטוריקה אין צורך לעשות את זה כל כך פורמלית, אבל שהפורמליזציה עוזרת "כשחוקי המשחק לא ברורים".

[00:13:31]–[00:15:10] "זרים" $\neq$ "בלתי תלויים". שאלת סטודנט: אם אמרנו שהמאורעות זרים, איך הם יכולים גם להיות תלויים? התשובה: זרות ואי-תלות הן תכונות שונות לגמרי. בהוכחה השתמשנו בזרות (כדי לחבר הסתברויות של איחוד) — לא באי-תלות. אי-תלות היא משהו שצריך להוכיח, ולא נובעת מכך שהדגימה אחידה.

[00:21:24] משתנים בין הסגרים. בתוך הסגר — שלושה משתנים **שונים**. בין הסגרים — משתנים חוזרים על עצמם בחופשיות. זה מקור התלות שנדונה מיד אחר כך.

[00:34:28]–[00:39:12] שאלת עומר. האינדיקטורים I_C תלויים; לינאריות התוחלת עדיין תקפה, כי היא מתקיימת לכל אוסף משתנים מקריים בעלי תוחלת. אילו היינו מחשבים שונות היינו נתקעים. "התוחלת היא מדד מאוד חלש, ולכן הוא מתירני."

[00:39:45]–[00:49:49] אסייד: משפט ה-PCP — הוצהר מפורשות כמחוץ לחומר ולא למבחן. הקשר לשיעור: ראינו שתמיד קיימת השמה המספקת $\frac{7}{8}$. הבעיה של להכריע, בהינתן $\varepsilon > 0$ ונוסחת 3E-CNF, האם המקסימום הוא לכל היותר $\frac{7}{8}m$ או לפחות $(\frac{7}{8}+\varepsilon)m$ — היא **NP-קשה** לכל $\varepsilon > 0$ קבוע. כלומר להבחין בין מה שתמיד מובטח לבין "קצת יותר" זה כבר קשה. הניסוח השני של אותו משפט: PCP = probabilistically checkable proofs — לכל בעיה ב-NP קיים מוודא הסתברותי שקורא רק **מספר קבוע** של ביטים מהתעודה, באופן אחיד ואקראי; אם הקלט בשפה קיימת תעודה שתשכנע אותו בהסתברות טובה, ואם אינו בשפה שום תעודה לא תשכנע אותו. אותה אי-סימטריה חד-צדדית שראינו ב-NP ובאלגוריתמים אקראיים עם טעות חד-צדדית (שיעור 15, שיעור 17), ולכן אפשר להגביר. המרצה ציין שההוכחה ארוכה מאוד ומוקדשים לה קורסים שלמים, ושהיא מסוף המאה הקודמת — חדשה יחסית לשאר החומר.

[00:52:28]–[00:53:31] מוטיבציה ל-DS. משפיענים ברשת, רמזורים בצמתים, שלטי פרסומת. ואמירה חצי-רצינית: "אם זה מעניין וזה כריע — זה NP-קשה". מיד גם הובהר שאין משפט כזה, זו רק תחושת ניסיון.

[00:59:59]–[01:00:29] רדוקציה אינה מוצאת פתרון. "רדוקציה אף פעם לא תמצא לי פתרון... אני מקבל אינסטנס של בעיה אחת ומחזיר אינסטנס של בעיה אחרת." אילו הרדוקציה הייתה פותרת, היינו מוכיחים $\mathrm{P} = \mathrm{NP}$.

[01:04:43]–[01:05:14] הקודקודים המבודדים. הצורך בהם עלה תוך כדי ההוכחה, בעקבות הערה מהכיתה. זו הערה מהותית ולא טכנית: בלעדיה הרדוקציה שגויה. שווה לזכור אותה כמלכודת מבחן.

[01:29:32]–[01:31:38] על מה מותר להסתמך בהוכחת נכונות. בבניית U מתוך $\hat{U}$ **מותר** להסתמך על מבנה הגרף שהאלגוריתם בנה (למשל: לקודקוד חדש יש בדיוק שני שכנים) — כי זה חלק מהפלט. **אסור** להניח שהאלגוריתם יודע מהי $\hat{U}$ — היא "התקבלה מהשמיים" בתוך ההוכחה בלבד.

[01:34:18] הכיוון החדש של השיטה. "הפעם, בניגוד לפעמים קודמות, זה **לכל היותר**." לכן משתמשים ב-$\Pr[X \le \mathbb{E}[X]] > 0$.

[01:42:18] הטריידאוף בין שני השלבים. אחרי שלב 1 יש גודל טוב ואין תכונה; אחרי שלב 2 יש תכונה בוודאות והגודל כבר לא ידוע במדויק — רק בתוחלת. זה מבנה שחוזר בהמון אלגוריתמים אקראיים.

[01:56:23] "ישבתי בחושך וחישבתי." התשובה לשאלה מאיפה הגיע p, ומשם הגזירה של משפט 6.

פערים בין הסיכום להקלטה

מקור: שם הקובץ והמשימה. **הפער:** שם הקובץ הוא `lesson-19-cut-algorithms.md` , אך רק עמוד 1 מתוך 5 עוסק בחתכים; העמודים 2–5 עוסקים ב-$\mathrm{3ESAT}$, בקבוצה שלטת וברדוקציה $\mathrm{VC} \le_p \mathrm{DS}$. **ההכרעה:** שם הקובץ נשמר לפי ההנחיה, ה- `slug` בקובץ תוקן

ל- probabilistic-method-and-dominating-set , והכותרת האמיתית נכתבה ב- title_he . נרשם ב- open_questions .

מקור: הבריף למשימה. **הפער:** הבריף תיאר את השיעור כעוסק בדה-רנדומיזציה בשיטת התוחלות המותנות. הנושא אכן מוזכר בפתיחת ההקלטה ([00:00:00]–[00:00:33]) כיעד אפשרי ליום ההוא, אך נדחה במפורש ("יכול להיות שנשאיר את זה ליום חמישי") ולא נלמד; הוא אינו מופיע באף עמוד מהסיכום. **ההכרעה:** נכתב מה שבסיכום ובהקלטה בפועל. הדה-רנדומיזציה שייכת לשיעור 20.

מקור: ההקלטה, [00:39:45]–[00:49:49]. **הפער:** אסייד ארוך על משפט ה-PCP (שתי הגרסאות שלו) שאינו מופיע בסיכום כלל. **ההכרעה:** נכלל ב- הערות מהשיעור ## בלבד, עם ציון מפורש שהמרצה הגדיר אותו כמחוץ לחומר ולא למבחן.

מקור: ההקלטה, [01:56:23]–[02:01:08]. **הפער:** הגזירה שממנה מגיע $p = \frac{\ln(d+1)}{d+1}$ (מזעור $f(p) = p + e^{-p(d+1)}$, נגזרת ראשונה ושנייה) אינה מופיעה בעמוד 5 בסיכום — שם p פשוט מוגדר. **ההכרעה:** נכתבה במלואה כמשפט 6, כי בלעדיה הערך נראה שרירותי.

מקור: ההקלטה, [01:04:43]–[01:05:14] ועמוד 3 בסיכום. **הפער:** הצורך להסיר קודקודים מבודדים התגלה בהרצאה תוך כדי ההוכחה; בסיכום הוא כבר משולב בשלב 2 של האלגוריתם. **ההכרעה:** נכתב כחלק מהאלגוריתם, עם פסקה נפרדת שמסבירה למה הוא הכרחי ולמה הסרתם אינה משנה את התשובה של VC.

מקור: עמוד 3 בסיכום. **הפער:** בהגדרת VC בכיוון הראשון של הרדוקציה נרשם $|U| = k$, בעוד שהגדרת VC (שיעור 10) היא $|U| \le k$. **ההכרעה:** נכתב $|U| \le k$; ההבדל אינו מהותי (אפשר תמיד להשלים כיסוי לגודל בדיוק k), והוסבר בגוף הטקסט. אותה הערה תקפה גם ל-DS ([00:51:57]).

מקור: ההקלטה, [00:18:44]. **הפער:** התמלול האוטומטי אומר "למצוא השמה המספקת מספר רב ביותר של **ליטרלים**". זו שגיאת תמלול; המטרה היא למקסם את מספר ה**הסגרים** המסופקים, כפי שנאמר מיד אחר כך וכפי שכתוב בסיכום. **ההכרעה:** נכתב "הסגרים".

מקור: ההקלטה, [00:03:50]. **הפער:** בכיתה נאמר שגודל מרחב המדגם הוא "שתיים"; המרצה תיקן מיד ל-$2^{|V|}$ והבחין בין 2^V (אובייקט) לבין $2^{|V|}$ (מספר). **ההכרעה:** נכתב הניסוח המתוקן, וההבחנה נשמרה כהערה.

מקור: עמוד 5 בסיכום. **הפער:** המילה המתארת את d ("הדרגה ה___ ב-G") אינה חדה לחלוטין בסריקה. **ההכרעה:** פוענחה כ"מינימלית". שלוש אמירות מפורשות בהקלטה ([01:33:14], [01:50:25], [01:51:26]) מאשרות זאת, וגם הצעד $(1-p)^{\deg(v)+1} \le (1-p)^{d+1}$ תקף אך ורק עבור הדרגה המינימלית. נרשם ב- open_questions .

מקור: התמלול לאורך כל ההקלטה. **הפער:** התמלול מרנדר "קבוצה שלטת" לסירוגין כ"שולט", "דומיננטית", "דומיניטינג". **ההכרעה:** לאורך כל הקובץ נעשה שימוש במונח "קבוצה שלטת" (dominating set), כפי שכתוב בסיכום. המונח "קבוצה דומיננטית" אינו התרגום המקובל וההקלטה עצמה מתקנת אותו ב-[00:55:04].

מקור: קונבנציות הכתיבה. **הפער:** הסיכום כותב את ההסתברות באות P גדולה ואת מספר ההסגרים ב-m. **ההכרעה:** נשמרו שמות המשתנים והאינדקסים של הסיכום ($U, \hat{U}, X, Y, I_v, J_v, p, d, m, k$), ואילו שמות המחלקות והבעיות נכתבו לפי הקונבנציה של

הפרויקט (NP, VC, DS, MAXCUT) — כולל עטיפה ב- `\mathrm{}` .

סיכום ונקודות למבחן

התוצאות שכדאי לזכור בעל פה.

בכל גרף קיים חתך בגודל $\geq \frac{|E|}{2}$. יש לזה **שתי** הוכחות הסתברותיות (מטבע לכל קודקוד — שיעור 18; הגרלה אחידה מ-2^V — כאן) ושתי הוכחות קונסטרוקטיביות (חיפוש מקומי — שיעור 13; חמדן — שיעור 14).

בכל נוסחת 3E-CNF עם m הסגרים קיימת השמה המספקת $\geq \frac{7}{8}m$ הסגרים.

DS היא NP-שלמה. הרדוקציה: $\mathrm{VC} \leq_p \mathrm{DS}$, על ידי הוספת v_{xy} לכל קשת xy והסרת קודקודים מבודדים.

בכל גרף בעל דרגה מינימלית d קיימת קבוצה שלטת בגודל $\leq \frac{\ln(d+1)+1}{d+1}|V|$, עם $p = \frac{\ln(d+1)}{d+1}$.

המלכודות הסטנדרטיות.

לכתוב "ההסתברות מעל הגרפים". ההסתברות היא **תמיד** מעל מטבעות האלגוריתם, לגרף **קבוע** נתון. שום גרף לא מוגרל באף אחת מההוכחות כאן.

להסיק אי-תלות מאחידות. בהגרלה אחידה של קבוצה אין מאורע פר קודקוד; מי שרוצה להכפיל הסתברויות חייב להוכיח אי-תלות. בפועל, החישוב הקומבינטורי הוא זה שמוכיח אותה.

לבלבל בין "זרים" ל"בלתי תלויים". זרים $\Longrightarrow$ מחברים הסתברויות. בלתי תלויים $\Longleftarrow$ מכפילים. מאורעות זרים בעלי הסתברות חיובית הם דווקא **תלויים**.

לחשוש מתלות בין אינדיקטורים. לינאריות התוחלת לא אכפת לה. אילו הייתם צריכים שונות או הסתברות מדויקת — היה אכפת מאוד.

לשכוח את הקודקודים המבודדים ברדוקציה. בלי הסרתם, כיוון ב' פשוט לא נכון.

לנסות את הרדוקציה הזהותית מ-VC ל-DS. K_4 הוא דוגמה נגדית של ארבעה קודקודים.

לחשוב שהשיטה ההסתברותית נותנת אלגוריתם. היא נותנת **קיום** בלבד; זהו טיעון ממוצע.

לבלבל בין הדרגה המינימלית למקסימלית במשפט 5. הכיוון של האי-שוויון $(1-p)^{\deg(v)+1} \leq (1-p)^{d+1}$ מחייב $d = \min \deg$.

צ'ק-ליסט — מה סטודנט צריך לדעת לעשות אחרי השיעור.

לתאר ניסוי אקראי במפורש: מהו Ω, מהי ההתפלגות, מהו המשתנה המקרי ומה הוא מקבל.

לפרק משתנה מקרי לסכום אינדיקטורים ולהפעיל לינאריות תוחלת, תוך ציון מפורש היכן (אם בכלל) נדרשת אי-תלות.

לחשב הסתברות בהתפלגות אחידה על ידי ספירה, כולל הצדקת הספירה בפונקציה הפיכה.

להסיק קיום מתוחלת בשני הכיוונים ($\geq$ ו-$\leq$), ולנמק למה הצעד הזה חוקי.

לנסח את DS, להוכיח שהיא ב-NP, ולכתוב את הרדוקציה $\mathrm{VC} \leq_p \mathrm{DS}$ עם שני כיווני הנכונות, כולל טיפול בקודקודים מבודדים.

לנתח אלגוריתם דו-שלבי מסוג "הגרל ואז תקן": להראות נכונות דטרמיניסטית ולחסום את הגודל בתוחלת.

לבצע את האופטימיזציה של פרמטר ההסתברות: לכתוב את החסם כפונקציה של p, לגזור, ולאמת שזו נקודת מינימום.

שאלות שנשארו פתוחות

שם הקובץ lesson-19-cut-algorithms.md אינו תואם את התוכן: רק עמוד 1 מתוך 5 עוסק בחתכים, והשאר ב-3ESAT ובקבוצה שלטת. ה-slug בקובץ תוקן ל-probabilistic-method-and-dominating-set והכותרת האמיתית נכתבה ב-title_he; שם הקובץ לא שונה לפי ההנחיה ודורש תיקון ידני במניפסט.

הבריף למשימה זו ציין שהשיעור עוסק בדה-רנדומיזציה בשיטת התוחלות המותנות. הנושא הזה אכן הוזכר בפתיחת ההקלטה כיעד ליום ההוא, אך נדחה במפורש ([00:00:33]) ולא נלמד; הוא אינו מופיע באף אחד מחמשת עמודי הסיכום. הוא ככל הנראה חומר של שיעור 20.

עמוד 5 בסיכום: המילה המתארת את d פוענחה כ'הדרגה המינימלית'. הקריאה אושרה שלוש פעמים בהקלטה ([01:33:14], [01:50:25], [01:51:26]) והיא גם הכרחית מתמטית, אך ברזולוציה הנוכחית של הסריקה המילה עצמה אינה חדה לחלוטין.

20 אלגוריתמים אקראיים לספיקות: אי־שוויון מרקוב, הגברה ודה־רנדומיזציה

כיצד הופכים את התוחלת $7m/8$ של מספר הפסוקיות המסופקות בנוסחת 3ECNF לערובה בהסתברות גבוהה — באמצעות אי־שוויון מרקוב והגברה — ואז מסלקים את האקראיות לגמרי בשיטת התוחלות המותנות.

ביטחון: high

בקצרה

בשיעור הקודם הראינו שהשמה אקראית אחידה מספקת **בתוחלת** $\frac{7}{8}$ מהפסוקיות של נוסחת $3\mathrm{ECNF}$. תוחלת היא מדד חלש: היא אינה אומרת דבר על ההסתברות שריצה בודדת באמת תשיג את המספר הזה.

אי־שוויון מרקוב הוא הגשר: הוא מתרגם ידיעה על תוחלת לחסם על הסתברות. הוא חד־כיווני — חוסם מלמעלה את ההסתברות שמשתנה אי־שלילי גדול, ולכן מפעילים אותו על $Y = m - X$ (מספר הפסוקיות ה**לא** מסופקות) ולא על X עצמו.

התוצאה: לכל נוסחת $3\mathrm{ECNF}$ קבועה, ההסתברות (מעל מטבעות האלגוריתם) שריצה בודדת תספק לפחות $\frac{7m}{8}$ פסוקיות היא לפחות $\Theta(1/m)$ — הסתברות קטנה, אבל **הסתברות אמיתית** ולא רק תוחלת.

מכיוון שהטעות כאן **חד־צדדית** (לוקחים את המקסימום מבין הריצות), **הגברה** פשוטה בעלות $t = \Theta(m)$ חזרות מביאה את הצלחה ל־99%, ובעלות $t = \Theta(m \log m)$ אף ל־$1 - 1/m$.

לבסוף מסלקים את האקראיות לגמרי: **שיטת התוחלות המותנות** בונה השמה משתנה־אחר־משתנה, שומרת על השמורה $\mathbb{E}[X \mid \rho] \geq \frac{7m}{8}$ כאשר ρ היא ההשמה החלקית שנקבעה עד כה, ומחזירה **בוודאות** השמה שמספקת לפחות $\frac{7m}{8}$ פסוקיות בזמן $O(|\varphi|^2)$.

הדרישה ל**בדיוק** שלושה ליטרלים מעל שלושה משתנים שונים דרושה **רק לתנאי ההתחלה** של האינדוקציה. לאחר הצבה ראשונה הנוסחה כבר אינה $3\mathrm{ECNF}$ — וזה בסדר, כי מכאן והלאה החסם $\frac{7m}{8}$ עובר בירושה מהאיטרציה הקודמת ולא מחושב מחדש.

רקע ותלויות

מודל האקראיות ומוסכמת ההסתברות

מכונות ומחלקות אקראיות (BPP, coRP, RP) הוגדרו בשיעור 16, והגברת הסתברות הצלחה נדונה שם ובשיעור 17. כאן איננו זקוקים למחלקות עצמן — רק לתמונת המכונה: אלגוריתם אקראי מקבל קלט **קבוע** ובנוסף אליו מחרוזת ביטים אקראיים ("מטבעות").

> **מוסכמה שתלווה את כל הקובץ.** כל הסתברות וכל תוחלת שנכתוב הן **מעל מטבעות האלגוריתם בלבד, עבור נוסחה φ קבועה שנתונה כקלט**. אין כאן שום התפלגות על נוסחאות. בהרצאה זה נאמר במפורש ברגע שהוצג הסימון: "עד פה שום דבר אקראי — קיבלתי נוסחה ואני מסמן את מספר הפסוקיות שלה" [00:11:24].

הצורה $\mathrm{3ECNF}$ ומדוע היא לא $\mathrm{3CNF}$

בשיעור 8 (הרדוקציה $\mathrm{SAT} \le_p \mathrm{3SAT}$) הוגדרה נוסחת $\mathrm{3CNF}$ כקוניונקציה של פסוקיות שבכל אחת מהן **לכל היותר** שלושה ליטרלים. ההגדרה הגמישה הזו נוחה לרדוקציות, אך היא הורסת את החישוב שאנחנו עומדים לעשות. לכן עובדים כאן עם צורה קשיחה יותר, שהסיכום מסמן $\mathrm{3ECNF}$ (בהרצאה: "exact CNF 3"): **בכל פסוקית בדיוק שלושה ליטרלים, מעל שלושה משתנים שונים** [00:13:40].

התוצאה משיעור 19, במלואה

זו התוצאה שכל השיעור הזה נשען עליה, ולכן היא מובאת כאן במלואה ולא בהפניה בלבד (ההוכחה עצמה שייכת לשיעור 19; ראו שם, וכן את השיטה ההסתברותית ל־MAXCUT בשיעור 18).

האלגוריתם האקראי הבסיסי. בהינתן φ בצורת $\mathrm{3ECNF}$ מעל $x_1, \dots, x_n$: לכל משתנה, **באופן אחיד ובלתי תלוי באחרים**, קבע את ערכו ל־1 בהסתברות $\frac{1}{2}$ ול־0 בהסתברות $\frac{1}{2}$. החזר את ההשמה v שהתקבלה.

התוצאה. אם m הוא מספר הפסוקיות ב־φ ו־X הוא מספר הפסוקיות ש־v מספקת, אז $\mathbb{E}[X] = \frac{7m}{8}$.

ההוכחה חוזרת כאן במלואה כמשפט 1, גם מפני שהיא נדרשת שוב מילולית בחלק הדה־רנדומיזציה.

כלי ההגברה של טעות חד־צדדית

בשיעור 18, בניתוח אלגוריתם החתך המינימלי, ראינו את התבנית: אם ריצה בודדת מצליחה בהסתברות p והטעות חד־צדדית (כלומר החזרת ה"טובה ביותר" מבין הריצות אינה יכולה להזיק), אז t ריצות בלתי תלויות נכשלות כולן בהסתברות $\le (1-p)^t$. המרצה הדגיש שזו בדיוק אותה תבנית: "החזרתיות הזו — חשוב שתראו אותה, זה תמיד אותו פרינציפ" [00:57:32].

הגדרות

הגדרה 1: נוסחת $\mathrm{3ECNF}$

נוסחה φ היא בצורת $\mathrm{3ECNF}$ אם $\varphi = C_1 \wedge C_2 \wedge \cdots \wedge C_m$, וכל פסוקית היא דיסיונקציה $C_i = (\ell_{i,1} \vee \ell_{i,2} \vee \ell_{i,3})$ של **בדיוק** שלושה ליטרלים, כאשר שלושת הליטרלים הם מעל שלושה **משתנים שונים**.

אינטואיציה. זו דרישה מבנית טהורה על אופן הכתיבה של הנוסחה, לא על ספיקותה. שתי המילים החשובות הן "בדיוק" ו"שונים". "בדיוק שלושה" מונע פסוקיות קצרות שקל מאוד להפר; "משתנים שונים" מבטיח ששלושת הליטרלים הם משתנים מקריים **בלתי תלויים** תחת השמה אקראית, וזה מה שמאפשר לכפול הסתברויות.

דוגמה. $(\bar{x}_1 \vee x_2 \vee \bar{x}_3) \wedge (x_1 \vee \bar{x}_4 \vee x_3) \wedge (\bar{x}_1 \vee \bar{x}_2 \vee x_3)$ — שלוש פסוקיות, כל אחת בדיוק שלושה ליטרלים מעל שלושה משתנים שונים.

אי־דוגמה 1 (הגבול החשוב). $(x_1 \vee x_2) \wedge (x_3)$ היא $\mathrm{3CNF}$ תקינה לפי הגדרת שיעור 8, אך **אינה** $\mathrm{3ECNF}$. הפסוקית (x_3) אינה מסופקת בהסתברות $\frac{1}{2}$ ולא $\frac{1}{8}$ — וזה בדיוק מה שהורס את החסם.

אי־דוגמה 2. $(x_1 \vee x_1 \vee x_2)$ — שלושה ליטרלים, אך שני משתנים בלבד. כאן ההסתברות שהפסוקית אינה מסופקת היא $\Pr[x_1 = 0 \wedge x_2 = 0] = \frac{1}{4}$ ולא $\frac{1}{8}$.

הגדרה 2: המשתנים המקריים X ו־Y
תהי φ נוסחת $3\mathrm{ECNF}$ קבועה עם m פסוקיות, ותהי v ההשמה שדוגם האלגוריתם האקראי הבסיסי. נגדיר: X הוא מספר הפסוקיות של φ שההשמה v מספקת, ו־$Y = m - X$.
אינטואיציה. X הוא הרווח ו־Y הוא ההפסד. שניהם פונקציות של המטבעות בלבד (כי φ קבועה), שניהם מקבלים **ערכים שלמים** בין 0 ל־m, ובפרט שניהם **אי־שליליים**. שתי התכונות האלה — אי־שליליות ושלמות — הן בדיוק שתי התכונות שנצטרך בהמשך, ולא במקרה.
מופע. עבור φ מהדוגמה שבהגדרה 1 ו־$v = (x_1, x_2, x_3, x_4) = (1, 0, 1, 0)$ מתקבל $X = 2$ (הפסוקית הראשונה מופרת) ו־$Y = 1$.
הגדרה 3: בעיית האופטימיזציה שברקע
בהינתן נוסחת $3\mathrm{ECNF}$, המטרה היא למצוא השמה המספקת **כמה שיותר** פסוקיות. בספרות הבעיה נקראת $\mathrm{MAX\text{-}E3SAT}$; בהרצאה היא לא זכתה לשם, ודובר עליה ישירות כ"לספק כמה שיותר פסוקיות". שימו לב שזו אינה בעיית הכרעה: איננו שואלים אם φ ספיקה, אלא כמה מפסוקיותיה ניתן לספק בו־זמנית. בפרט התוצאה שלנו תקפה גם לנוסחאות **לא ספיקות**.
הגדרה 4: השמה חלקית והנוסחה השיורית
תהי ρ השמה חלקית שקובעת ערכים לתת־קבוצה של המשתנים. הנוסחה השיורית $\varphi|_\rho$ מתקבלת מ־φ על ידי הצבת הערכים והפשטה: ליטרל שקיבל 1 הופך את פסוקיתו לאמת, וליטרל שקיבל 0 נמחק מהפסוקית.
אינטואיציה והערה קריטית. לאחר הצבה אחת בלבד הנוסחה כבר **אינה** $3\mathrm{ECNF}$ — יש בה פסוקיות באורך 2 ופסוקיות שהן קבוע האמת. המרצה חזר לנקודה הזו פעמיים, כי היא נראית כמו קריסה של כל הבנייה, והיא לא [01:26:10] ו־[הקלטה 26, 00:23:17].

משפטים והוכחות
משפט 1: התוחלת של מספר הפסוקיות המסופקות (תזכורת משיעור 19)
תוצאה זו הוכחה בשיעור 19 והיא בבעלותו; היא מובאת כאן במלואה משום ששלוש התוצאות המרכזיות של השיעור הזה (משפט 4, משפט 5 ובסיס האינדוקציה של משפט 7) נשענות עליה ישירות, ומשום שאותו חישוב־פסוקית עצמו חוזר ומשמש בשלב א של משפט 7.
טענה. תהי φ נוסחת $3\mathrm{ECNF}$ קבועה עם m פסוקיות. אז, מעל מטבעות האלגוריתם האקראי הבסיסי, $\mathbb{E}[X] = \frac{7m}{8}$.
הוכחה. לכל $1 \le i \le m$ נגדיר משתנה מציין (אינדיקטור) שערכו $X_i = 1$ אם הפסוקית C_i מסופקת על ידי v, ו־$X_i = 0$ אחרת, ואז $X = \sum_{i=1}^{m} X_i$ (סכימת אינדיקטורים היא בדיוק ספירה).
חישוב לפסוקית בודדת. תהי $C_i = (\ell_{i,1} \vee \ell_{i,2} \vee \ell_{i,3})$. פסוקית זו **אינה** מסופקת אם ורק אם **שלושת** הליטרלים מקבלים 0. ליטרל בודד ℓ מעל משתנה x מקבל 0 בהסתברות $\frac{1}{2}$ בדיוק: אם $\ell = x$ זה קורה כאשר $v(x) = 0$, ואם $\ell = \bar{x}$ זה קורה כאשר $v(x) = 1$ — בשני המקרים הסתברות $\frac{1}{2}$, כי $v(x)$ אחיד. כאן נכנסת לפעולה הדרישה ששלושת הליטרלים הם מעל שלושה **משתנים שונים**: שלושת המאורעות "$\ell_{i,j} = 0$" נקבעים על ידי שלושה משתנים שונים, שהאלגוריתם הגריל **בלתי תלוי**

זה בזה, ולכן הם בלתי תלויים ומותר לכפול. לכן ההסתברות ש־C_i אינה מסופקת היא $\left(\frac{1}{2}\right)^3 = \frac{1}{8}$. כלומר: מבין 8 תבניות האמת האפשריות של שלושת המשתנים, בדיוק **אחת** מפילה את הפסוקית — זו שמאפסת את כל שלושת הליטרלים. לכן $\mathbb{E}[X_i] = \Pr[X_i = 1] = 1 - \frac{1}{8} = \frac{7}{8}$.

סכימה. מליניאריות התוחלת, $\mathbb{E}[X] = \mathbb{E}[\sum_{i=1}^{m} X_i] = \sum_{i=1}^{m} \mathbb{E}[X_i] = m \cdot \frac{7}{8} = \frac{7m}{8}$. ■

הערה: ליניאריות התוחלת **אינה** דורשת אי־תלות בין ה־X_i. וזה חיוני: פסוקיות שונות חולקות משתנים, ולכן ה־X_i תלויים זה בזה מאוד. המרצה הדגיש שזה בדיוק ה"טרייד־אוף" של התוחלת — "התוחלת מאפשרת לי את הליניאריות, אבל היא גם מדד מאוד חלש" [00:02:07]. אי־התלות שכן שימשה אותנו היא רק *בתוך* פסוקית בודדת, בין שלושת הליטרלים שלה.

מסקנה 1א: הטענה הקיומית (השיטה ההסתברותית)

טענה (בבעלות שיעור 19 — ראו שם להוכחה המלאה בהקשר השיטה ההסתברותית). לכל נוסחת $3\mathrm{ECNF}$ עם m פסוקיות **קיימת** השמה v^* המספקת לפחות $\frac{7m}{8}$ פסוקיות; מכיוון שמספר פסוקיות הוא שלם, קיימת השמה המספקת לפחות $\lceil 7m/8 \rceil$ פסוקיות.

שרטוט הטיעון, כי הוא נדרש להבנת ההמשך. ההשמה נדגמת אחידה מבין כל 2^n ההשמות, ולכן $\mathbb{E}[X]$ הוא בדיוק **הממוצע** של X על פני כל ההשמות: $\frac{7m}{8} = \mathbb{E}[X] = \frac{1}{2^n}\sum_{v \in \{0,1\}^n} X(v)$. אילו לכל השמה v היה מתקיים $X(v) < \frac{7m}{8}$, היה הסכום קטן ממש מ־$2^n \cdot \frac{7m}{8}$ והממוצע קטן ממש מ־$\frac{7m}{8}$ — בסתירה לשוויון לעיל. לכן קיימת v^* עם $X(v^*) \geq \frac{7m}{8}$. ■

אזהרה מרכזית, וזו נקודת הפתיחה של כל השיעור. "קיימת השמה טובה" ו"האלגוריתם מוצא השמה טובה בסבירות סבירה" הם שני דברים שונים לחלוטין. מסקנה 1א היא טענת **קיום** בלבד: היא אינה נותנת אלגוריתם ואינה מבטיחה שדגימה אחת תפגע. באופן עקרוני ייתכן היה שהתוחלת $\frac{7m}{8}$ מושגת על ידי מיעוט זעיר של השמות מצוינות ורוב עצום של השמות בינוניות. המרצה ניסח את זה כך: "אולי לקבל השמה שמספקת שבע שמיניות — יש לי הסתברות מאוד קטנה. איך בדיוק התוחלת מתפרקת אני לא יודע, כי לא חישבתי את ההתפלגות, ואני גם לא רוצה — יש שם המון תלויות" [00:03:43]. כל מה שנעשה מכאן הוא לסגור את הפער הזה בלי לחשב את ההתפלגות.

משפט 2: אי־שוויון מרקוב

טענה. יהי X משתנה מקרי **אי־שלילי** בעל תוחלת סופית. אז לכל $a > 0$: $\Pr\left(X \geq a\,\mathbb{E}[X]\right) \leq \frac{1}{a}$.

הוכחה. נניח $\mathbb{E}[X] > 0$ (אחרת, אם $\mathbb{E}[X] = 0$ ו־X אי־שלילי, אז $X = 0$ כמעט תמיד והטענה טריוויאלית). נסמן $t = a\,\mathbb{E}[X] > 0$ ונגדיר את האינדיקטור $I = \mathbf{1}[X \geq t]$. מכיוון ש־$X \geq 0$, מתקיים לכל ערך אפשרי של X אי־השוויון הנקודתי $X \geq t \cdot I$. אכן: אם $X \geq t$ אז $I = 1$ והאגף הימני הוא $t \leq X$; ואם $X < t$ אז $I = 0$ והאגף הימני הוא $0 \leq X$ מאי־שליליות. כעת ניקח תוחלת משני האגפים (מונוטוניות התוחלת): $\mathbb{E}[X] \geq t \cdot \mathbb{E}[I] = t \cdot \Pr(X \geq t) = a\,\mathbb{E}[X] \cdot \Pr\left(X \geq a\mathbb{E}[X]\right)$, וחלוקה ב־$a\,\mathbb{E}[X] > 0$ נותנת את הטענה. ■

הערה: בהרצאה אי־השוויון הוצג בלי הוכחה, כתוצאה מקורס הסתברות ("בעיקרון לומדים את זה בהסתברות; אני מבין שאתם לא למדתם את זה" [00:06:27]). ההוכחה הובאה כאן במלואה כי היא קצרה, וכי היא מסבירה מיד **למה** דרושה אי־שליליות: בלעדיה אי־השוויון הנקודתי $X \geq t \cdot I$ קורס במקרה $X < 0$.

אינטואיציה ומופע מספרי (מההרצאה, [00:14:12]). מרקוב אומר: משתנה אי־שלילי לא יכול להיות הרבה יותר גדול מהתוחלת שלו לעיתים קרובות. אם $\mathbb{E}[X] = 3$, אז $\Pr(X \geq 6) \leq \frac{1}{2}$ — כי $6 = 2\mathbb{E}[X]$, כלומר $a = 2$. שימו לב ש־a **אינו** סף מוחלט אלא "פי כמה מהתוחלת".

מה מרקוב לא נותן. מרקוב חוסם **מלמעלה** את ההסתברות שהמשתנה **גדול**. הוא לא אומר כלום על ההסתברות שהמשתנה **קטן**. זו נקודת המפתח של השיעור, ואליה נחזור מיד. עוד שימו לב שעבור $a \leq 1$ החסם הוא $1 \geq$ ולכן חסר תוכן; מרקוב מתחיל להיות שימושי רק כאשר $a > 1$ [00:36:29].

משפט 3: אי־שוויון צ'בישב (העשרה — לא בחומר)

טענה. יהי X משתנה מקרי בעל תוחלת ושונות סופיות. אז לכל $a > 0$: $\Pr\left(\left|X - \mathbb{E}[X]\right| > a\sqrt{V(X)}\right) \leq \frac{1}{a^2}$.

הוכחה. נגדיר $Z = (X - \mathbb{E}[X])^2$. זהו משתנה מקרי אי־שלילי, ו־$\mathbb{E}[Z] = V(X)$ לפי הגדרת השונות. המאורע $|X - \mathbb{E}[X]| > a\sqrt{V(X)}$ שקול בדיוק למאורע $Z > a^2 V(X) = a^2\,\mathbb{E}[Z]$. הפעלת מרקוב (משפט 2) על Z עם המקדם a^2 נותנת $\Pr(Z \geq a^2\mathbb{E}[Z]) \leq 1/a^2$, ומכיוון שהמאורע עם $>$ מוכל במאורע עם $\geq$, נובעת הטענה. ■

למה הוא טוב יותר, ומה המחיר. צ'בישב חוסם דו־כיוונית (מרחק מהתוחלת בשני הכיוונים) ושואף לאפס מהר יותר — $1/a^2$ במקום $1/a$ [00:09:07]. אבל הוא **דורש יותר**: קיום שונות וידיעת ערכה. בשיעור נאמר במפורש: "אי־שוויון מרקוב אנחנו נשתמש בו, יש לכם אותו גם במטלה. את צ'בישב אני רק מראה לכם — אתם לא צריכים לדעת אותו בקורס הזה, אבל אתם כן צריכים לדעת שהוא קיים" [00:09:40]. במקרה שלנו חישוב $V(X)$ קשה בגלל התלויות בין הפסוקיות, ולכן ממילא לא היינו רוצים ללכת בדרך הזו.

משפט 4: חסם הסתברותי לריצה בודדת

טענה. תהי φ נוסחת $3\mathrm{ECNF}$ עם m פסוקיות, ונניח $8 \mid m$. אז, מעל מטבעות האלגוריתם האקראי הבסיסי, $\Pr\left(X \geq \frac{7m}{8}\right) \geq \frac{4}{m+4}$.

מדוע לא מפעילים את מרקוב על X ישירות — הניסיון שנכשל. מה שאנחנו רוצים הוא ש־X יהיה **גדול**, כלומר חסם **מלמטה** על $\Pr(X \geq \cdot)$. מרקוב נותן בדיוק את ההפך: חסם **מלמעלה** על ההסתברות ש־X גדול. המרצה עצר על כך זמן רב, כי זה בדיוק המקום שבו נופלים: "אני הייתי רוצה את האי־שוויון ההפוך, אבל אין לי את האי־שוויון ההפוך; מרקוב נותן לי כיוון אחד" [00:17:52].

הפתרון: לעבור למשלים **הכמותי** ולא הלוגי — לא $\Pr$ המשלימה, אלא המשתנה המשלים $Y = m - X$. מכיוון ש־"Y קטן" שקול ל־"X גדול", חסם מלמעלה על ההסתברות ש־Y גדול הוא בדיוק החסם מלמטה שרצינו [00:18:54].

הוכחה.

שלב 1 — תנאי מרקוב. $Y = m - X$, ומכיוון ש־$0 \le X \le m$ תמיד, Y אי־שלילי. מליניאריות התוחלת ומשפט 1, $\mathbb{E}[Y] = m - \mathbb{E}[X] = m - \frac{7m}{8} = \frac{m}{8}$. לכן Y הוא מועמד חוקי למרקוב, ולכל $a > 0$: $\Pr\left(Y > a \cdot \frac{m}{8}\right) \le \frac{1}{a}$ (השאלה אם לכתוב $>$ או $\ge$ אינה מהותית: $\Pr(Y > t) \le \Pr(Y \ge t)$, ומרקוב חוסם כבר את הגדול מביניהם. כך נאמר גם בהרצאה [00:20:00].)

שלב 2 — בחירת a, וזה הלב. מה שאנחנו רוצים באמת הוא $Y \le \frac{m}{8}$ (שקול ל־$X \ge \frac{7m}{8}$). אבל הצבת $a = 1$ במרקוב נותנת את החסם הריק $\Pr(Y > \frac{m}{8}) \le 1$. לכן מגדילים את הסף **טיפה**, ומנצלים ש־Y מקבל **ערכים שלמים**: תחת ההנחה $8 \mid m$ המספר $\frac{m}{8}$ הוא שלם, ולכן לכל Y שלם $Y \le \frac{m}{8} + \frac{1}{2} \iff Y \le \frac{m}{8}$. (אם ידוע שמספר שלם קטן־שווה מ־3.5, ידוע שהוא קטן־שווה מ־3 [00:59:13].) הגדלת הסף בחצי היחידה "עולה" לנו בהסתברות, אך **לא** מוסיפה ולו פסוקית אחת לא־מסופקת. נחשב את ה־a המתאים: $a \cdot \frac{m}{8} = \frac{m}{8} + \frac{1}{2} = \frac{m+4}{8} \implies a = \frac{m+4}{m}$.

שלב 3 — הצבה. $\Pr\left(Y > \frac{m}{8} + \frac{1}{2}\right) = \Pr\left(Y > \frac{m+4}{m} \cdot \frac{m}{8}\right) \le \frac{1}{\frac{m+4}{m}} = \frac{m}{m+4}$.

שלב 4 — משלים לוגי. מעבר למאורע המשלים הופך $>$ ל־$\le$ ומחליף כיוון:

$$\Pr\left(Y \le \tfrac{m}{8} + \tfrac{1}{2}\right) \ge 1 - \frac{m}{m+4} = \frac{m+4-m}{m+4} = \frac{4}{m+4}.$$

שלב 5 — שלמות ותרגום חזרה. לפי שלב 2, המאורע $Y \le \frac{m}{8} + \frac{1}{2}$ הוא בדיוק המאורע $Y \le \frac{m}{8}$, ולכן $\Pr\left(Y \le \frac{m}{8}\right) \ge \frac{4}{m+4}$. לבסוף, $Y = m - X$ ולכן $Y \le \frac{m}{8} \iff m - X \le m - \frac{m}{8} = \frac{7m}{8}$, $\iff X \ge \frac{7m}{8}$ ומכאן $\Pr\left(X \ge \frac{7m}{8}\right) \ge \frac{4}{m+4}$. ■

> **הערה:** בשלבים 4 ו־5 מתרחשים שני מעברים שונים שקל לבלבל ביניהם, והמרצה הפריד ביניהם במפורש [00:38:39]. שלב 4 הוא **משלים לוגי** של מאורע — ולכן $>$ הופך ל־$\le$ וכיוון אי־השוויון בין ההסתברויות מתהפך. שלב 5 הוא **אלגברה** בתוך המאורע — סידור מחדש של $Y = m - X$, שאינו נוגע בהסתברויות כלל.

הכללה ל־m שרירותי (הרחבה של מה שנרמז בהרצאה). ההנחה $8 \mid m$ נאמרה בהרצאה במפורש [00:34:17] אך אינה רשומה בסיכום, והיא **הכרחית** לשלב 2. במקרה הכללי $\frac{m}{8}$ אינו שלם, ותוספת של $\frac{1}{2}$ עלולה לחצות את השלם הבא. התיקון שהוצע בהרצאה הוא להשתמש בתוספת קטנה יותר, $\frac{1}{16}$ [00:39:43]: מכיוון ש־$\frac{m}{8}$ הוא כפולה של $\frac{1}{8}$, כל תוספת קטנה מ־$\frac{1}{8}$ אינה מגיעה לשלם הבא, ולכן $Y \le \left\lfloor \frac{m}{8} \right\rfloor + \frac{1}{16} \iff Y \le \frac{m}{8}$. עם $a \cdot \frac{m}{8} = \frac{2m+1}{16}$, כלומר $a = \frac{2m+1}{2m}$, מתקבל $\Pr\left(X \ge \frac{7m}{8}\right) \ge 1 - \frac{2m}{2m+1} = \frac{1}{2m+1}$. ניסוח נקי ותקף לכל m (מקבלים אותו בבחירת הסף $1 + \lfloor m/8 \rfloor$ ישירות): $\Pr\left(X \ge \frac{7m}{8}\right) \ge \frac{1}{m+1}$. בכל אחת מהגרסאות החסם הוא $\Theta(1/m)$, וזה כל מה שנדרש בהמשך. המרצה אמר בדיוק את זה: "הייתי מקבל קבועים קצת יותר מגעילים, אבל העיקרון היה נשאר אותו עיקרון... סדר הגודל הוא $\Theta(1/m)$" [00:43:26].

> **הערה:** המרצה כינה את התעלול של שלב 2 "קצת רמאות" [00:42:56], ולשאלת סטודנטית "למה דווקא חצי, אפשר היה כל מספר?" ענה שאין לחצי שום חשיבות מיוחדת — הוא נבחר רק כדי שהמספרים יצאו נוחים תחת ההנחה $8 \mid m$.

משפט 5: האלגוריתם המשודרג — הגברה

האלגוריתם. בהינתן נוסחה φ בצורת $\mathrm{3ECNF}$:

חזור t פעמים, **באופן בלתי תלוי**, על דגימת ההשמה של האלגוריתם הבסיסי.

החזר את ההשמה שסיפקה מספר **מקסימלי** של פסוקיות.

טענה. נניח $8 \mid m$ ונבחר $t \geq \frac{m+4}{4} \ln 100$. אז $\Pr\left(X \geq \frac{7m}{8}\right) \geq 1 - \frac{1}{100}$, כאשר X הוא מספר הפסוקיות שמספקת ההשמה **שהאלגוריתם מחזיר**. זמן הריצה הוא $O(t \cdot |\varphi|) = O(m \cdot |\varphi|)$, כלומר פולינומי.

הוכחה.

סימונים. לכל $j = 1, 2, \ldots, t$ נסמן ב־X_j את מספר הפסוקיות שמספקת ההשמה שנדגמה בריצה j, וב־X את מספר הפסוקיות שמספקת ההשמה המוחזרת. מהגדרת האלגוריתם, $X = \max\{X_1, X_2, \ldots, X_t\}$.

מדוע "לכל" ולא "קיים". המאורע $X \geq \frac{7m}{8}$ הוא "קיים j שעבורו $X_j \geq \frac{7m}{8}$", ואיתו קשה לעבוד: המאורעות $\{X_j \geq \frac{7m}{8}\}$ **אינם זרים**, ולכן אי אפשר לחבר את הסתברויותיהם; וכימות "קיים" מתורגם ל־$\vee$, בעוד שאי־תלות מתורגמת למכפלה ולכן משרתת רק את $\wedge$ [00:51:08]. לכן עוברים למאורע המשלים, שבו המקסימום הופך ל"כולם": $\max_j X_j < \frac{7m}{8} \iff \forall j : \; X_j < \frac{7m}{8}$.

חישוב. $\Pr\left(X < \frac{7m}{8}\right) = \Pr\left(\bigwedge_{j=1}^{t} \left(X_j < \frac{7m}{8}\right)\right) \overset{(*)}{=} \prod_{j=1}^{t} \Pr\left(X_j < \frac{7m}{8}\right) \leq \left(1 - \frac{4}{m+4}\right)^t$, כאשר $(*)$ היא **אי־תלות בין הריצות** — כל ריצה משתמשת במטבעות טריים משלה — והאי־שוויון האחרון הוא משפט 4 המופעל על כל ריצה בנפרד (לכל j: $\Pr(X_j < \frac{7m}{8}) = 1 - \Pr(X_j \geq \frac{7m}{8}) \leq 1 - \frac{4}{m+4}$).

כעת נשתמש באי־השוויון האלמנטרי $1 - z \leq e^{-z}$ התקף לכל $z \in \mathbb{R}$: $\left(1 - \frac{4}{m+4}\right)^t \leq \left(e^{-\frac{4}{m+4}}\right)^t = e^{-\frac{4t}{m+4}}$.

בחירת t. נדרוש $e^{-4t/(m+4)} \leq \frac{1}{100}$. לקיחת לוגריתם טבעי (פונקציה מונוטונית עולה) נותנת $-\frac{4t}{m+4} \leq -\ln 100 \iff \frac{4t}{m+4} \geq \ln 100 \iff t \geq \frac{m+4}{4} \ln 100$. (שימו לב לכפל ב־$(-1)$ שהפך את כיוון אי־השוויון — המרצה עצר על כך במפורש [00:55:59].) לכן לכל t כזה, $\Pr\left(X < \frac{7m}{8}\right) \leq \frac{1}{100}$, ובמעבר למשלים מתקבלת הטענה.

חשבון זמן ריצה. ריצה בודדת עולה $O(|\varphi|)$: דגימת ההשמה דורשת ביט אקראי אחד לכל משתנה, ומספר המשתנים אינו עולה על $|\varphi|$; וספירת הפסוקיות המסופקות היא מעבר אחד על הנוסחה. סך הכול $O(t \cdot |\varphi|)$, ועם $t = \Theta(m)$ ו־$m \leq |\varphi|$ זהו $O(|\varphi|^2)$ לכל היותר — בוודאי פולינומי [00:48:28]. ■

> **הערה — למה טעות חד־צדדית היא מה שמציל אותנו כאן.** האלגוריתם מחזיר את המקסימום, ולכן הוא **לא יכול** לטעות כלפי מעלה: אי אפשר שהמקסימום יהיה גדול ממה שבאמת הושג. הטעות היחידה האפשרית היא להשיג פחות מהיעד. המרצה קישר זאת ישירות לבחירת הכלי: "לכן גם מרקוב היה כלי טוב, כי הוא חוסם לי רק כיוון אחד" [01:01:21]. לשם השוואה, אילו היינו רוצים **בדיוק** $\frac{7m}{8}$ פסוקיות ולא "לפחות", היינו יכולים לטעות לשני הכיוונים, וההגברה על ידי מקסימום לא הייתה עובדת [01:01:51].

וריאציה. אם רוצים הסתברות כישלון $\frac{1}{m}$ במקום $\frac{1}{100}$, מחליפים $\ln 100$ ב־$\ln m$ ומקבלים $t = \Theta(m \log m)$ — עדיין פולינומי [00:56:29].

משפט 6: נוסחת התוחלת השלמה, והמסקנה על הממוצע

טענה (תוחלת שלמה, המקרה הבינארי). יהי X משתנה מקרי בעל תוחלת ויהי A מאורע עם $0 < \Pr(A) < 1$. אז במקרה שלנו $A = \{v(x_1) = 1\}$ ו־$\mathbb{E}[X] = \mathbb{E}[X \mid A] \cdot \Pr(A) + \mathbb{E}[X \mid \bar{A}] \cdot \Pr(\bar{A})$. ולכן $\Pr(A) = \Pr(\bar{A}) = \frac{1}{2}$, $\mathbb{E}[X] = \frac{\mathbb{E}[X \mid v(x_1)=1] + \mathbb{E}[X \mid v(x_1)=0]}{2}$.

מסקנה 6א. אם $\mathbb{E}[X] = \frac{7m}{8}$ אז $\mathbb{E}[X \mid v(x_1) = 1] \;\geq\; \frac{7m}{8}$ או $\mathbb{E}[X \mid v(x_1) = 0] \;\geq\; \frac{7m}{8}$.

הוכחה של המסקנה. זו טענה על ממוצעים בלבד. נסמן $a = \mathbb{E}[X \mid v(x_1) = 1]$, $b = \mathbb{E}[X \mid v(x_1) = 0]$ ו־$c = \frac{7m}{8}$, כך ש־$c = \frac{a+b}{2}$. נניח בשלילה $a < c$ וגם $b < c$. אז $c = \frac{a+b}{2} < \frac{c+c}{2} = c$, סתירה. לכן $a \geq c$ או $b \geq c$ [הקלטה 26, 00:17:21]. ■

> **הערה:** בהרצאה זה נאמר בקיצור ("אם ממוצע של שני מספרים שווה למשהו, אחד מהם חייב להיות לפחות המשהו הזה"); הפירוט כאן. שימו לב שהמסקנה נותנת $\geq$ ולא $>$: ייתכן ששני האגפים שווים בדיוק ל־$\frac{7m}{8}$.

משפט 7: דה־רנדומיזציה בשיטת התוחלות המותנות

זהו החלק שבו "מוציאים את האקראיות". השיטה — בניית פתרון משתנה־אחר־משתנה תוך שמירה על ערכה של תוחלת מותנית — מוצגת כאן לראשונה בקורס, ולכן היא נכתבת במלואה. הרקע שהיא נשענת עליו הוא הטענה הקיומית ההסתברותית (מסקנה 1א, בבעלות שיעור 19, ובמקבילה ל־MAXCUT — שיעורים 18–19): אנחנו כבר יודעים שהשמה טובה **קיימת**, והשאלה היחידה היא איך למצוא אותה בלי הגרלות ובלי לסרוק את כל 2^n ההשמות.

> **הערה על מיקום החומר:** בפתיחת המפגש הקודם הוכרזה הדה־רנדומיזציה כיעד היום ואז נדחתה במפורש ("יכול להיות שנשאיר את זה ליום חמישי"), ולכן היא נלמדה בפועל כאן ואינה מופיעה בסיכום של שיעור 19.

האלגוריתם (דטרמיניסטי). בהינתן φ בצורת $3\mathrm{ECNF}$ מעל $x_1, \dots, x_n$, עם m פסוקיות:

לכל $i = 1, \dots, n$:

חשב $E_1 = \mathbb{E}\big[X \mid v(x_1), \dots, v(x_{i-1}),\ v(x_i) = 1\big]$, כאשר $v(x_1), \dots, v(x_{i-1})$ הם הערכים שכבר נקבעו.

אם $E_1 \geq \frac{7m}{8}$ — קבע $v(x_i) = 1$ והצב 1 במקום x_i בנוסחה.

אחרת — קבע $v(x_i) = 0$ והצב 0 במקום x_i.

בסוף החזר את v.

כאן X הוא, כמו תמיד, מספר הפסוקיות של **הנוסחה המקורית** φ שמסופקות על ידי ההשמה שמתקבלת מהשלמת המשתנים שטרם נקבעו בהגרלה אחידה בלתי תלויה.

טענה. האלגוריתם דטרמיניסטי לחלוטין, רץ בזמן $O(|\varphi|^2)$, ומחזיר **בוודאות** השמה v המספקת לפחות $\frac{7m}{8}$ מפסוקיות φ.

הוכחה.

שלב א — חישוב התוחלת המותנית הוא דטרמיניסטי, ולינארי. זו הנקודה שהמרצה חזר עליה יותר מכל אחרת [01:13:14], [הקלטה 26, 00:04:17]: כדי **לחשב** תוחלת אין צורך להגריל דבר. תהי ρ ההשמה החלקית הנוכחית. לכל פסוקית C_i של φ נגדיר את תרומתה:

אם ρ כבר קבעה ליטרל של C_i ל־1 — הפסוקית מסופקת בוודאות, תרומתה 1.

אם ρ אפסה את **כל** שלושת הליטרלים — תרומתה 0.

אחרת, אם נותרו $k \in \{1,2,3\}$ ליטרלים לא־מוכרעים (מעל משתנים שונים, כי כך היה כבר בנוסחה המקורית וההצבה רק מוחקת ליטרלים) — התרומה היא $1 - \left(\frac{1}{2}\right)^k$.

לפי ליניאריות התוחלת (בדיוק כמו במשפט 1), $\mathbb{E}[X \mid \rho]$ הוא **סכום** התרומות. חישוב זה הוא מעבר בודד על הנוסחה: $O(|\varphi|)$, ואינו צורך אף ביט אקראי [הקלטה 26, 00:00:34]. לכן האלגוריתם דטרמיניסטי, למרות שבניסוחו מופיעים משתנה מקרי ותוחלת — אלה תיאורים על הנייר של ניסוי שלעולם אינו מבוצע.

שלב ב — השמורה, באינדוקציה. נסמן ב־ρ_i את ההשמה החלקית שנקבעה אחרי i איטרציות. נוכיח באינדוקציה על i: $\mathbb{E}[X \mid \rho_i] \geq \frac{7m}{8}$.

בסיס $i = 0$: ρ_0 ריקה, ולכן $\mathbb{E}[X \mid \rho_0] = \mathbb{E}[X] = \frac{7m}{8}$ לפי משפט 1. **זהו — וזה בלבד — המקום שבו נדרשת ההנחה ש־φ היא $3\mathrm{CNF}$.**

צעד: נניח $\mathbb{E}[X \mid \rho_{i-1}] \geq \frac{7m}{8}$. לפי משפט 6 המופעל על המשתנה x_i (בהינתן ρ_{i-1}), $\mathbb{E}[X \mid \rho_{i-1}] = \frac{\mathbb{E}[X \mid \rho_{i-1}, v(x_i)=1] + \mathbb{E}[X \mid \rho_{i-1}, v(x_i)=0]}{2}$, ולכן לפי מסקנה 6א לפחות אחד משני הענפים הוא לפחות $\mathbb{E}[X \mid \rho_{i-1}] \geq \frac{7m}{8}$. האלגוריתם בודק את הענף $v(x_i) = 1$; אם הוא עומד בסף — הוא נבחר, ואז $\mathbb{E}[X \mid \rho_i] = E_1 \geq \frac{7m}{8}$. אם אינו עומד בסף, אז בהכרח הענף השני עומד בו, והאלגוריתם בוחר בו. בשני המקרים $\mathbb{E}[X \mid \rho_i] \geq \frac{7m}{8}$.

שלב ג — סיום. אחרי n איטרציות ρ_n קובעת ערך לכל משתנה. בהינתן ρ_n אין יותר אקראיות: X הוא **משתנה מקרי מנוון**, כלומר פונקציה קבועה [הקלטה 26, 00:27:06]. תוחלת של קבוע היא הקבוע עצמו, ולכן $\mathbb{E}[X \mid \rho_n] \geq \frac{7m}{8}$, כלומר ההשמה v שהוחזרה מספקת לפחות $\frac{7m}{8}$ פסוקיות — **בוודאות**, בלי הסתברות כלל.

שלב ד — חשבון זמן ריצה. יש n איטרציות; בכל איטרציה מחשבים לכל היותר שתי תוחלות מותנות, כל אחת ב־$O(|\varphi|)$, ומבצעים הצבה שגם היא $O(|\varphi|)$. מכיוון ש־$n \leq |\varphi|$, סך הכול $O(n \cdot |\varphi|) = O(|\varphi|^2)$ — ריבועי [01:22:59]. $\blacksquare$

> **הערה — מדוע זה לא מעבר על עץ ההשמות.** לשאלה טבעית מהכיתה ("אבל אתה מחשב שני ענפים כל פעם, אז זה 2^n?") התשובה היא: בכל צומת מחשבים שני ערכים אך **יורדים רק בענף אחד**. סך החישובים הוא $2n$ ולא 2^n [01:24:35]. זו בדיוק הנקודה שבה הוכחת הקיום ההסתברותית "משלמת" — היא מבטיחה שהענף שנבחר לעולם אינו מבוי סתום.

הערה — מדוע מותר שהנוסחה השיורית אינה $3\mathrm{ECNF}$. זו הייתה שאלת המחשבה שהמרצה השאיר לכיתה בסוף השיעור [01:25:37], והתשובה ניתנה בפתיחת המפגש הבא: את התכונה "בדיוק שלושה ליטרלים מעל משתנים שונים" צריכים **רק לתנאי ההתחלה** — כדי לקבל $\mathbb{E}[X]=\frac{7m}{8}$ באיטרציה ה־0. מהאיטרציה הראשונה והלאה, החסם $\frac{7m}{8}$ אינו מחושב מחדש מהמבנה של הנוסחה השיורית אלא **עובר בירושה מהאיטרציה הקודמת** דרך מסקנה 6א. "מאיפה הגיע השבע שמיניות על הנוסחה החדשה? מהתוחלת הקודמת. את השלוש־אקזקט הייתי צריך רק בשביל תנאי ההתחלה" [הקלטה 26, 00:23:17]. שימו לב גם ש־m בביטוי $\frac{7m}{8}$ הוא תמיד מספר הפסוקיות ב־φ **המקורית**, ופסוקית שההצבה הפכה לאמת ממשיכה להיספר כמסופקת.

דוגמאות ותרגילים מהשיעור

דוגמה 1: מרקוב במספרים

X אי־שלילי עם $\mathbb{E}[X]=3$. מהו חסם על $\Pr(X\geq 6)$?

פתרון. $6=2\cdot\mathbb{E}[X]$, כלומר $a=2$, ולכן $\Pr(X\geq 6)\leq\frac{1}{2}$. שימו לב ש־$a$ נמדד **ביחידות של תוחלת** ולא בערך מוחלט; לו היינו שואלים על $\Pr(X\geq 3)$ היינו מקבלים $a=1$ והחסם הריק ≤ 1.

דוגמה 2: הגרסה ה"עצלה" של משפט 4

בהרצאה הודגם קודם חסם חלש יותר, כחימום [00:30:03]. ניקח $a=2$ במרקוב על Y: $\Pr\left(Y>\frac{m}{4}\right)\leq\frac{1}{2}$. ומכיוון ש־$Y=m-X$, לכן $\Pr\left(Y\leq\frac{m}{4}\right)\geq\frac{1}{2}$ כלומר: בהסתברות לפחות חצי, ריצה בודדת מספקת לפחות $\frac{3}{4}$ מהפסוקיות. עם הגברה על ידי t חזרות ולקיחת המקסימום, ההצלחה עולה ל־$1-\left(\frac{1}{2}\right)^t$ — שלוש ריצות כבר נותנות $\frac{7}{8}$ **הסתברות** להשיג $\frac{3}{4}$ **מהפסוקיות** [00:17:21]. אל תתבלבלו בין שני ה־$\frac{7}{8}$ האלה: האחד הוא הסתברות והשני הוא שבר מהפסוקיות.

דוגמה 3: מעקב מלא אחרי נוסחה קונקרטית

זו הנוסחה שבסיכום (עמוד 3) ובהרצאה [01:14:34]: $\varphi=(\bar{x}_1\vee x_2\vee\bar{x}_3)\wedge(x_1\vee\bar{x}_4\vee x_3)\wedge(\bar{x}_1\vee\bar{x}_2\vee x_3)$, $m=3,\ n=4$.

(א) התוחלת. כל פסוקית היא בדיוק שלושה ליטרלים מעל שלושה משתנים שונים, ולכן $\mathbb{E}[X_i]=\frac{7}{8}$ לכל i, ומליניאריות $\mathbb{E}[X]=3\cdot\frac{7}{8}=\frac{21}{8}=2.625$.

(ב) ההתפלגות המלאה, כבדיקת שפיות. נבדוק מתי כל פסוקית **נכשלת**:

C_1 נכשלת אך ורק כאשר $x_1=1,\ x_2=0,\ x_3=1$.

C_2 נכשלת אך ורק כאשר $x_1=0,\ x_4=1,\ x_3=0$.

C_3 נכשלת אך ורק כאשר $x_1=1,\ x_2=1,\ x_3=0$.

שלושת מאורעות הכישלון **זרים בזוגות**: C_1 ו־C_3 דורשות $x_1=1$ בעוד C_2 דורשת $x_1=0$; ו־C_1 דורשת $x_3=1$ בעוד C_3 דורשת $x_3=0$. מבין $2^4=16$ ההשמות, כל מאורע כישלון מתקיים ב־2 השמות (המשתנה הרביעי חופשי), ולכן ב־6 השמות בדיוק פסוקית אחת נכשלת ($X=2$), וב־10

השמות אף פסוקית לא נכשלת ($X=3$). בדיקה: $\mathbb{E}[X]=\frac{10\cdot 3+6\cdot 2}{16}=\frac{42}{16}=\frac{21}{8}$ ✓ מכאן גם $\Pr\left(X\ge \frac{7m}{8}\right)=\Pr(X\ge 2.625)=\Pr(X=3)=\frac{10}{16}=0.625$ — לעומת החסם הכללי $\frac{1}{m+1}=\frac{1}{4}$ שנתן משפט 4. מרקוב אכן רופף מאוד; זו המחיר של כלי שאינו מניח דבר על ההתפלגות.

(ג) קיום מול הסתברות. התוחלת $\frac{21}{8}$ מבטיחה לפי מסקנה 1א שקיימת השמה עם $X\ge\frac{21}{8}$, ומכיוון ש־X שלם — עם $X\ge 3$. ואכן $v=(0,1,1,1)$ מספקת את שלוש הפסוקיות.

(ד) איטרציה ראשונה של הדה־רנדומיזציה. נחשב את שתי התוחלות המותנות (זהו החישוב שבסיכום, עמוד 3):

עבור $v(x_1)=1$ הנוסחה הופכת ל־$(0\vee x_2\vee \bar{x}_3)\wedge(1\vee \bar{x}_4\vee x_3)\wedge(0\vee \bar{x}_2\vee x_3)$, כלומר לפסוקיות $(x_2\vee\bar{x}_3)$, אמת, $(\bar{x}_2\vee x_3)$. התרומות: $1-\frac{1}{4}=\frac{3}{4}$, ואז 1, ואז $\frac{3}{4}$. סך הכול $\mathbb{E}[X\mid v(x_1)=1]=\frac{3}{4}+1+\frac{3}{4}=2\frac{1}{2}=\frac{20}{8}$.

עבור $v(x_1)=0$ הנוסחה הופכת ל־$(1\vee x_2\vee \bar{x}_3)\wedge(0\vee \bar{x}_4\vee x_3)\wedge(1\vee \bar{x}_2\vee x_3)$, כלומר אמת, $(\bar{x}_4\vee x_3)$, אמת. התרומות: 1, $\frac{3}{4}$, 1. סך הכול $\mathbb{E}[X\mid v(x_1)=0]=1+\frac{3}{4}+1=2\frac{3}{4}=\frac{22}{8}$.

בדיקת עקביות עם משפט 6: $\frac{1}{2}\left(\frac{20}{8}+\frac{22}{8}\right)=\frac{42}{16}=\frac{21}{8}=\mathbb{E}[X]$ ✓. אכן אחת התוחלות $\ge\frac{21}{8}$ והשנייה $\le\frac{21}{8}$, כפי שהעיר הסיכום בשוליים. האלגוריתם בודק תחילה את $v(x_1)=1$, מוצא $\frac{20}{8}<\frac{21}{8}$, ולכן קובע $\boxed{v(x_1)=0}$.

(ה) המשך המעקב עד הסוף (הרחבה — בהרצאה נעצרו אחרי המשתנה הראשון). אחרי ההצבה נותרנו עם שתי פסוקיות מסופקות בוודאות ועם הפסוקית $(\bar{x}_4\vee x_3)$; הסף שיש לשמור עליו הוא תמיד $\frac{7m}{8}=\frac{21}{8}=2.625$.

x_2: אינו מופיע יותר. שני הענפים נותנים $2+\frac{3}{4}=2.75\ge 2.625$; האלגוריתם בודק תחילה את 1 ומקבל אותו: $v(x_2)=1$.

x_3: עבור $v(x_3)=1$ הפסוקית הופכת לאמת והתוחלת היא $2+1=3\ge 2.625$ — נקבע $v(x_3)=1$. (עבור $v(x_3)=0$ היינו מקבלים $2+\frac{1}{2}=2.5<2.625$, כלומר הענף הזה היה נופל מהסף — בדיוק ההתנהגות שהמרצה תיאר בתשובה לשאלה מהכיתה [01:24:03].)

x_4: הפסוקית כבר מסופקת, שני הענפים נותנים 3; נקבע $v(x_4)=1$.

התוצאה: $v=(0,1,1,1)$, ובבדיקה ידנית — $C_1=\bar{0}\vee 1\vee\bar{1}=1$, $C_2=0\vee\bar{1}\vee 1=1$, $C_3=\bar{0}\vee\bar{1}\vee 1=1$. כל שלוש הפסוקיות מסופקות, ובוודאי $3\ge\frac{21}{8}$. ✓

תרגיל 1 (שאלת המרצה בסוף השיעור): למה דווקא $3\mathrm{ECNF}$?

השאלה [01:25:37]. למה היינו חייבים "בדיוק שלושה ליטרלים מעל משתנים שונים"? מה היה קורה עם ההגדרה הרגילה של $3\mathrm{CNF}$ ("לכל היותר שלושה")?

פתרון מלא. החסם $\frac{7}{8}$ מגיע כולו מהחישוב שההסתברות שפסוקית אינה מסופקת היא 2^{-3}. תחת "לכל היותר שלושה":

פסוקית עם ליטרל אחד, (x), אינה מסופקת בהסתברות $\frac{1}{2}$, כלומר מסופקת בהסתברות $\frac{1}{2}$ בלבד.

פסוקית עם שני ליטרלים מסופקת בהסתברות $\frac{3}{4}$.

פסוקית עם שלושה ליטרלים אך שני משתנים, כגון $(x\vee x\vee y)$, מסופקת בהסתברות $\frac{3}{4}$ ולא $\frac{7}{8}$.

בהינתן נוסחת $3\mathrm{CNF}$ כללית, החסם התחתון הטוב ביותר שאפשר לתת אחיד על כל הפסוקיות הוא $\frac{1}{2}$, ולכן היינו מקבלים $\mathbb{E}[X] \geq \frac{m}{2}$ בלבד — תוצאה חלשה בהרבה. זו בדיוק תשובת המרצה: "אם זה היה לכל היותר שלושה ליטרלים — מה החסם הכי טוב שהייתי יכול לתת? חצי" [01:26:10]. (הערה: אילו כל הפסוקיות היו בדיוק באורך k מעל משתנים שונים, אותו חישוב היה נותן $\mathbb{E}[X] = (1 - 2^{-k})m$.)

תרגיל 2 (שאלת המחשבה לשיעור הבא)

השאלה. אחרי איטרציה אחת של הדה־רנדומיזציה הנוסחה כבר אינה $3\mathrm{ECNF}$. למה האלגוריתם עדיין נכון?

פתרון. ראו ההערה בסוף משפט 7: הדרישה $3\mathrm{ECNF}$ נחוצה **רק** לבסיס האינדוקציה. שלב האינדוקציה משתמש אך ורק בנוסחת התוחלת השלמה (משפט 6), שתקפה לכל נוסחת CNF שהיא, ובעובדה שהתוחלת המותנית ניתנת לחישוב מדויק בזמן לינארי גם כשאורכי הפסוקיות מעורבים ($1 - 2^{-k}$ עבור פסוקית עם k ליטרלים חיים). לכן הערך $\frac{7m}{8}$ נשמר לאורך כל הריצה כירושה, ולא כתוצאה של מבנה הנוסחה השיורית.

תרגיל 3: איפה ההנחה $8 \mid m$ באמת נחוצה

השאלה. הראו שבלי ההנחה $8 \mid m$, הטענה $\Pr\left(X \geq \frac{7m}{8}\right) > \frac{4}{m+4}$ אינה נכונה.

פתרון. ניקח $m = 5$ ושלושה משתנים x_1, x_2, x_3. יש בדיוק 8 פסוקיות אפשריות של שלושה ליטרלים מעל שלושת המשתנים, וכל אחת מהן נכשלת בהשמה **אחת** ויחידה, ולכולן השמות כישלון שונות. נבחר 5 מהן; נסמן את φ כקוניונקציה שלהן. אז Y (מספר הפסוקיות הלא מסופקות) מקבל ערך 1 בדיוק כאשר ההשמה נופלת על אחת מ־5 נקודות הכישלון, ו־0 אחרת. לכן $\Pr\left(X \geq \frac{7\cdot 5}{8}\right) = \Pr(Y = 0) = \frac{8-5}{8} = \frac{3}{8} = 0.375$. אבל $0.375 > 0.444 \approx \frac{4}{9} = \frac{4}{m+4}$. הנוסחה $\frac{4}{m+4}$ נכשלת כאן. לעומת זאת החסם הכללי ממשפט 4 עומד יפה: $\frac{1}{m+1} = \frac{1}{6} \approx 0.167 \leq 0.375$ ✓.

הערות מהשיעור

[00:01:34] תוחלת היא מדד חלש — זו הנקודה שממנה יוצא כל השיעור. "כבר אמרתי לכם שתוחלת זה מדד מאוד חלש... ההולי גרייל זה הסתברות גבוהה." מתודולוגיה שהוצעה בפירוש: כשמנתחים אלגוריתם אקראי, בודקים **קודם** את התוחלת, כי אם היא לא מסתדרת כנראה שהכיוון שגוי; אבל לא עוצרים שם.

[00:04:44] הבהרה חשובה על מדדים סטטיסטיים. שונות וסטיית תקן הן מדדי פיזור — הן **לא** נותנות הסתברויות. הכלי שמתרגם תוחלת (ולפעמים שונות) להסתברות הוא אי־שוויון: מרקוב, צ'בישב.

[00:09:40] מה נדרש למבחן. מרקוב — כן, ואף מופיע במטלה. צ'בישב — לא בחומר; מספיק לדעת שהוא קיים ומה הוא נותן.

[00:20:30] "טיוטה" מול "הוכחה". המרצה כתב את הבחירה של a בתור טיוטה על הלוח והדגיש: בהוכחה כתובה מציגים את $a = \frac{m+4}{m}$ **מוכן מראש**, בלי לחשוף את חיפוש הערך. "אנחנו לא מצטטים טענות לקורא" — סדר ההצגה בהוכחה אינו סדר הגילוי.

[00:42:56] "זה קצת רמאות". התוספת של $\frac{1}{2}$ לסף היא תחבולה מודעת: מרקוב בסף $\frac{m}{8}$ בדיוק נותן את החסם הריק 1, אז מגדילים את הסף ב"קצת" — מספיק כדי שמרקוב יהיה לא־טריוויאלי, ולא מספיק כדי לאבד ולו פסוקית אחת. אין לחצי משמעות מיוחדת; כל תוספת שאינה מגיעה לשלם הבא מתאימה.

[00:45:37] מה נחשב "הסתברות גבוהה". שאלה מהכיתה: מה מספיק — 0.9? 0.99? התשובה: **כל** הסתברות שהיא $1/\mathrm{poly}$ מספיקה כשהטעות חד־צדדית, כי ההגברה תעלה אותה לכל רמה שנרצה במחיר פולינומי. "אם הגעתי לעשירית אני home free; אפילו אם הייתי מגיע ל־$1/m$ בעשירית — אני home free" [01:00:16].

[00:51:08] טעות נפוצה: "קיים" מול "לכל". המאורע "אחת הריצות הצליחה" הוא כימות קיום ומתרגם ל־$\vee$; אי־תלות מתרגמת למכפלה ולכן שימושית רק ל־$\wedge$. לכן **תמיד** עוברים למאורע המשלים "כל הריצות נכשלו" לפני שכופלים הסתברויות. בנוסף, מאורעות ההצלחה של ריצות שונות אינם זרים ולכן אסור לחבר את הסתברויותיהם.

[01:01:21] למה מרקוב הוא הכלי הנכון דווקא כאן. הבעיה שלנו היא "לפחות $\frac{7m}{8}$", כלומר טעות חד־צדדית; מרקוב הוא חסם חד־כיווני. ההתאמה אינה מקרית. אילו הייתה נדרשת תוצאה מדויקת ("בדיוק $\frac{7m}{8}$"), היינו יכולים לטעות לשני הכיוונים וכל המבנה — כולל ההגברה על ידי מקסימום — היה קורס.

[01:03:58] מה קונים בדה־רנדומיזציה ומה משלמים. אותה ערובה, אותו סדר גודל של זמן ריצה, אבל **בוודאות** במקום בהסתברות. המחיר: האלגוריתם מסובך יותר למימוש. לעומת זאת [הקלטה 26, 00:10:06] היתרון הקלאסי של האלגוריתם האקראי הוא הפשטות הקיצונית שלו: "דוגם משהו באקראי, בודק אם זה עבד, זהו".

[הקלטה 26, 00:04:17] הנקודה שחוזרת במבחנים. בניסוח האלגוריתם הדטרמיניסטי מופיעים "משתנה מקרי" ו"תוחלת", ובכל זאת האלגוריתם דטרמיניסטי. הסיבה: כדי **לחשב** תוחלת לא צריך ביטים אקראיים. "כל מה שעשינו בשיעור, גם כשכתבנו על הלוח אלגוריתמים אקראיים — החישובים עצמם היו דטרמיניסטיים."

הקשר חיצוני (לא נאמר בהרצאה, מובא כאוריינטציה בלבד). החסם $\frac{7}{8}$ אינו מקרי: ידוע שקירוב טוב יותר מ־$\frac{7}{8}+\varepsilon$ ל־$\mathrm{MAX\text{-}E3SAT}$ הוא NP־קשה. כלומר האלגוריתם הנאיבי ביותר שאפשר להעלות על הדעת הוא כבר אופטימלי מבחינת יחס הקירוב. אין להסתמך על משפט זה בבחינה בקורס הזה.

פערים בין הסיכום להקלטה

מקור: עמוד 1–2 בסיכום, המשפט על $\Pr(Y > \frac{m}{8} + \frac{1}{2})$. **הפער:** הסיכום מבצע את המעבר "Y שלם, ולכן $Y \le \frac{m}{8} + \frac{1}{2}$ אם ורק אם $Y \le \frac{m}{8}$" **בלי לרשום את ההנחה** $8 \mid m$. בהקלטה ההנחה נאמרה במפורש פעמיים [00:34:17], [00:39:43]. בלעדיה הטענה שגויה: עבור $m \equiv 5 \pmod 8$ קיימת נוסחת $3\mathrm{ECNF}$ (תרגיל 3) שבה $\Pr\left(X \ge \frac{7m}{8}\right) = \frac{3}{8} < \frac{4}{9} = \frac{4}{m+4}$. **ההכרעה:** משפט 4 נוסח כאן עם ההנחה $8 \mid m$ מפורשת, ובנוסף הובאה הכללה תקפה לכל m (התוספת $\frac{1}{16}$ שהוצעה בהקלטה, והניסוח הנקי $\Pr \ge \frac{1}{m+1}$), ותרגיל 3 מדגים את הצורך בהנחה.

מקור: עמוד 1 בסיכום מול ההקלטה. **הפער:** הסיכום פותח ב"מהשיעור הקודם" ומצטט את התוצאה $\frac{7}{8}$ בשורה אחת בלבד, בלי החישוב שההסתברות שפסוקית נכשלת היא $\frac{1}{8}$ ובלי ליניאריות התוחלת. **ההכרעה:** ההוכחה המלאה שוחזרה כאן כמשפט 1 (על בסיס ההקלטה ושיעור 19), כי כל השיעור נשען עליה ומשפט 7 משתמש בה שוב.

מקור: ההקלטה. **הפער:** בהקלטה מופיעה גרסת חימום שלמה של החסם $\Pr(X \geq a = 2$ — $1 - (\frac{1}{2})^t \geq \frac{1}{2}$ ($\frac{3m}{4}$, כולל דיון בהגברה — שאינה בסיכום כלל. **ההכרעה:** נכללה כדוגמה 2, כי היא מבהירה את מנגנון הבחירה של a לפני שנכנסים לחשבון המדויק.

מקור: ההקלטה. **הפער:** ההסבר מדוע יש להשתמש ב"לכל j" ולא ב"קיים j" (המאורעות אינם זרים; אי־תלות משרתת רק $\wedge$) קיים בהקלטה [00:51:08] ואינו בסיכום, שבו מופיע רק המעבר הסופי. **ההכרעה:** נכלל בגוף ההוכחה של משפט 5.

מקור: ההקלטה מול הסיכום. **הפער:** הסיכום מסתיים בעמוד 3 בחישוב האיטרציה הראשונה של הדה־רנדומיזציה בלבד; הניסוח הפורמלי של האלגוריתם, הוכחת הנכונות באינדוקציה, טיעון ה"משתנה המקרי המנוון" באיטרציה האחרונה וחשבון הזמן הריבועי הושלמו רק בפתיחת המפגש הבא. **ההכרעה:** הושלמו כאן ממנת ההקלטה השנייה (עד [הקלטה 26, 00:27:30]), ומסומנים בציטוט מפורש כ"הקלטה 26". מ־[00:27:36] ואילך ההקלטה עוברת למשפט $\mathrm{NP} \subseteq \mathrm{BPP} \Rightarrow \mathrm{NP} = \mathrm{P}$, שהוא חומר שיעור 21.

מקור: ההקלטה. **הפער:** בסיום השיעור נשאלה שאלת מחשבה (למה מותר שהנוסחה השיורית אינה $3\mathrm{ECNF}$) שאין לה זכר בסיכום. **ההכרעה:** נכללה כתרגיל 2, עם התשובה שניתנה בפועל במפגש הבא.

מקור: עמוד 1 בסיכום, ההערות בכחול בשולי אי־שוויון מרקוב. **הפער:** כתב היד בהערות השוליים הקצרות ליד הנוסחה קטן ולא פוענח במלואו; לפי ההקשר ולפי ההקלטה הן מוסרות את האינטואיציה ("חסם גס שאינו מניח דבר על ההתפלגות" ו"ההסתברות ש־X גדול פי a מהתוחלת שלו"). **ההכרעה:** האינטואיציה נכתבה כאן מתוך ההקלטה, שבה היא נאמרה במפורש, ולא מתוך שחזור של השוליים.

מקור: מוסכמות הסימון. **הפער:** הסיכום וההרצאה כותבים את הצורה כ־$3\mathrm{ECNF}$ ("exact CNF 3"), בעוד שבספרות רווח הסימון $\mathrm{E3CNF}$; כמו כן בעיית האופטימיזציה אינה מקבלת שם בשני המקורות. **ההכרעה:** נשמר סימון המקור $3\mathrm{ECNF}$, ושם הבעיה $\mathrm{MAX\text{-}E3SAT}$ הובא פעם אחת ומסומן כמינוח ספרותי חיצוני.

מקור: הסיכום וההקלטה. **הפער:** אין ביניהם שום סתירה מתמטית מהותית מעבר לפער ההנחה $8 \mid m$ שתואר בסעיף הראשון; כל המספרים ($\frac{m+4}{m}$, $\frac{m}{m+4}$, $\frac{4}{m+4}$, $t = \frac{m+4}{4}\ln 100$, $\frac{20}{8}$, $\frac{22}{8}$, $\frac{21}{8}$) תואמים בשני המקורות ואומתו בחישוב עצמאי. **ההכרעה:** `confidence: high` .

סיכום ונקודות למבחן

התוצאות שכדאי לזכור בעל פה.

טענה	נוסח
תוחלת	$\mathbb{E}[X] = \frac{7m}{8}$ עבור $3\mathrm{ECNF}$, מליניאריות

טענה	נוסח
קיום	קיימת השמה המספקת $\geq \lceil \frac{7m}{8} \rceil$ פסוקיות
מרקוב	$X \geq 0 \;\Rightarrow\; \Pr(X \geq a\mathbb{E}[X]) \leq \frac{1}{a}$
ריצה בודדת	$\Pr\left(X \geq \frac{7m}{8}\right) \geq \frac{4}{m+4} \geq \frac{1}{m+1}$ (כאשר $8 \mid m$); בכלליות
הגברה	$t \geq \frac{m+4}{4}\ln 100$ ריצות $\Rightarrow$ הצלחה ≥ 0.99; זמן $O(t\|\varphi\|)$
דה־רנדומיזציה	אלגוריתם דטרמיניסטי, $O(\|\varphi\|^2)$, מבטיח $\geq \frac{7m}{8}$ **בוודאות**

מלכודות סטנדרטיות.

"התוחלת היא $\frac{7m}{8}$, אז בהסתברות גבוהה נקבל $\frac{7m}{8}$" — לא. זו בדיוק הטעות שכל השיעור נועד למנוע. תוחלת אינה חסם הסתברותי; צריך את מרקוב כדי לגשר.

הפעלת מרקוב על X במקום על $Y = m - X$ — מרקוב חוסם רק את הזנב **העליון**. מי שרוצה חסם מלמטה על $\Pr(X$ גדול$)$ חייב לעבור למשתנה המשלים.

שכחת השלמות — בלי הטיעון "Y שלם" מרקוב בסף $\frac{m}{8}$ נותן חסם ריק. ובכיוון השני: המעבר הזה דורש שהתוספת לסף לא תחצה לשלם הבא, ולכן ההנחה $8 \mid m$ (או תוספת $< \frac{1}{8}$).

חיבור הסתברויות של ריצות — מאורעות ההצלחה אינם זרים. עוברים למשלים ומכפילים.

בלבול בין המשלים הלוגי לאלגברה — המעבר $\Pr(A) \geq \alpha \Rightarrow \Pr(\bar{A}) \leq 1 - \alpha$ הופך כיוון; הסידור $Y = m - X$ אינו.

"האלגוריתם הדטרמיניסטי משתמש בתוחלת, אז הוא אקראי" — לא. חישוב תוחלת אינו צורך ביטים אקראיים.

דרישת $3\mathrm{ECNF}$ בכל איטרציה — נדרשת רק בבסיס. הנוסחה השיורית אינה $3\mathrm{ECNF}$ וזה תקין.

בלבול בין שני ה־$\frac{7}{8}$ — $\frac{7}{8}$ מהפסוקיות (יחס קירוב) לעומת הסתברות הצלחה של $\frac{7}{8}$ (שמופיעה במקרה אחרי שלוש הגברות בדוגמה 2).

מה סטודנט אמור לדעת לעשות אחרי השיעור.

לחשב את תוחלת מספר הפסוקיות המסופקות עבור נוסחה נתונה, גם כשאורכי הפסוקיות מעורבים ($1 - 2^{-k}$ לפסוקית עם k ליטרלים מעל משתנים שונים).

לנסח ולהפעיל את אי־שוויון מרקוב, כולל בחירה מכוונת של a כך שהסף ייצא במקום שרוצים.

לבצע את המהלך המלא תוחלת $\to$ מרקוב על המשלים $\to$ שלמות $\to$ חסם הסתברותי $\to$ הגברה, ולנמק כל מעבר.

לחשב את מספר החזרות t הדרוש להסתברות כישלון נתונה, באמצעות $1 - z \leq e^{-z}$.

להריץ את שיטת התוחלות המותנות על נוסחה קטנה, משתנה־אחר־משתנה, ולנמק מדוע התוצאה מובטחת ולא הסתברותית.

להסביר בדיוק היכן נדרשת הדרישה "בדיוק שלושה ליטרלים מעל שלושה משתנים שונים", ומה קורה בלעדיה.

הסיכום בכתב יד שעליו מבוסס הקובץ הוא של גיא סופר.

שאלות שנשארו פתוחות

עמוד 1 בסיכום: הכותרת הירוקה בראש העמוד קשה לפענוח; הכותרת שנבחרה לקובץ נגזרה מהתוכן ומההקלטה ולא מקריאה ודאית של הדיו.

עמוד 1 בסיכום: ליד הכותרת של אי־שוויון צ'בישב מופיעה הערה בסוגריים שנקראה כ'(לא בחומר)'; בהקלטה נאמר במפורש שצ'בישב אינו בחומר, ולכן כך הובאה.

רשימת prereq_lessons נמסרה על ידי הרכז ככוללת את שיעור 15; תוכנו של שיעור 15 לא נבדק כאן ולכן לא נעשתה אליו הפניה בגוף הטקסט. בפועל התלות ההדוקה ביותר היא בשיעור 19, שבו הוכחה התוחלת $7m/8$.

השם $\mathrm{MAX\text{-}E3SAT}$ לא נאמר בהרצאה ולא נכתב בסיכום; הוא נוסף כאן כמינוח מקובל בספרות בלבד.

הסיכום אינו רושם את ההנחה $m \mid 8$ שנאמרה בהרצאה ושבלעדיה שלב השלמות בהוכחה אינו תקף; ראו סעיף הפערים.

ה-slug randomized-satisfiability תקף — כל השיעור עוסק באלגוריתמים אקראיים לספיקות — אך אינו מדויק: מרכז הכובד הוא אי־שוויון מרקוב, הגברה ודה־רנדומיזציה. slug מדויק יותר היה markov-amplification-derandomization. שם הקובץ נשמר כפי שהוקצה.

התוצאה $\mathbb{E}[X]=7m/8$ והמסקנה הקיומית הנגזרת ממנה הן בבעלות שיעור 19; כאן הן מובאות כתזכורת מפורשת בלבד, כי כל תוצאות השיעור נשענות עליהן. הדה־רנדומיזציה בשיטת התוחלות המותנות אינה מופיעה בסיכום 19 ונלמדה בפועל בשיעור הזה.

21 יחס הקירוב 7/8 ל-MAX-3ECNF, רדוקציה עצמית של SAT, ו-coNP

השיעור סוגר את פרק האקראיות: אורז את האלגוריתם הדטרמיניסטי ל-3ECNF כקירוב ביחס 7/8, משתמש ברדוקציה העצמית של SAT כדי להוכיח שאם SAT ב-BPP אז NP מוכלת ב-RP, ופותח את הפרקון על coNP.

ביטחון: high

בקצרה

הפתיחה **אורזת** את האלגוריתם הדטרמיניסטי מהשיעור הקודם כאלגוריתם **קירוב**: יחס $\alpha = \frac{7}{8}$ במוסכמת המקסימיזציה של שיעור 13, $\mathrm{ALG} \geq \alpha \cdot \mathrm{OPT}$ עם $0 < \alpha \leq 1$. הצעד שאסור לדלג עליו הוא החסם $\mathrm{OPT} \leq m$.

האלגוריתם עצמו — שיטת התוחלות המותנות ל-3ECNF — והוכחת נכונותו נלמדו ונכתבו ב**שיעור 20**, ותוצאת הקיום $\geq \frac{7}{8}m$ שעליה הכול נשען הוכחה ב**שיעור 19**. כאן הם משמשים כקופסה שחורה, בניסוח מדויק.

מוכיחים שה-SAT היא **self-reducible**: אלגוריתם פולינומי לבעיית ההכרעה גורר אלגוריתם פולינומי לבעיית החיפוש. זהו חימום דטרמיניסטי, אבל אותה בנייה בדיוק היא לב ההוכחה הבאה.

המשפט המרכזי: אם $\mathrm{SAT} \in \mathrm{BPP}$ אז $\mathrm{NP} \subseteq \mathrm{RP}$ — כלומר טעות דו-צדדית לכל בעיה ב-NP גוררת טעות חד-צדדית לכל בעיה ב-NP. ההוכחה משלבת את הרדוקציה העצמית עם אמפליפיקציה וחסם האיחוד.

הטריק שגורם לטעות להיות חד-צדדית: השלב האחרון של האלגוריתם הוא **בדיקה דטרמיניסטית** של ההשמה שנבנתה. "כן" נאמר רק כשההשמה מספקת בפועל.

הפרקון האחרון מגדיר את coNP ומוכיח: $\mathrm{coP} = \mathrm{P}$, $\mathrm{P} \subseteq \mathrm{NP} \cap \mathrm{coNP}$, ש-$\mathrm{NP} = \mathrm{coNP}$ שקול ל-$\mathrm{NP} \subseteq \mathrm{coNP}$ וגם שקול ל-$\mathrm{SAT} \in \mathrm{coNP}$, ושבעיה A היא coNP-קשה אם ורק אם $\bar{A}$ היא NP-קשה.

רקע ותלויות

מבעיות אופטימיזציה ויחס קירוב (שיעור 13). בעיית אופטימיזציה של מקסימיזציה מתאימה לכל קלט x אוסף פתרונות אפשריים ולכל פתרון ערך; $\mathrm{OPT}(x)$ הוא הערך המקסימלי. אלגוריתם ALG הוא **קירוב ביחס** α (עם $0 < \alpha \leq 1$) אם לכל קלט x הוא מחזיר פתרון **חוקי** שערכו מקיים $\mathrm{ALG}(x) \geq \alpha \cdot \mathrm{OPT}(x)$. זו המוסכמת של בעיות מקסימום; בבעיות מינימום המוסכמת ההפוכה, $\mathrm{ALG}(x) \leq \alpha \cdot \mathrm{OPT}(x)$ עם $\alpha \geq 1$ (כמו הקירוב 2 ל-VC שם). בכל טענת קירוב כאן נדרשות שתי הוכחות נפרדות: שהפלט חוקי, ושהוא עומד בחסם מול OPT.

חסם ה-$\frac{7}{8}$ (שיעור 19). תהא φ נוסחה בצורת 3ECNF — כלומר בכל הסגר בדיוק שלושה ליטרלים מעל **שלושה משתנים שונים** — עם m הסגרים. נדגום השמה v במידה אחידה מתוך 2^n ההשמות, ונסמן ב-X את מספר ההסגרים המסופקים. לכל הסגר C, ההסתברות שהוא **אינו** מסופק היא $\left(\frac{1}{2}\right)^3 = \frac{1}{8}$, כי שלושת הליטרלים הם מעל משתנים שונים ולכן ערכיהם בלתי תלויים, ויש בדיוק

השמה אחת לשלושת המשתנים האלה שמפילה את ההסגר. מלינאריות התוחלת מעל ההסגרים, $\mathbb{E}[X] = \sum_{C \in \varphi} \Pr[C \text{ satisfied}] = m \cdot \frac{7}{8}$. מכאן, בשיטה ההסתברותית, **קיימת** השמה המספקת לפחות $\frac{7}{8}m$ הסגרים.

למה דווקא 3ECNF ולא 3CNF. בקורס הזה 3CNF מוגדרת כ"לכל היותר שלושה ליטרלים בהסגר" (ראו שיעור 8, שם הרדוקציה $\mathrm{SAT} \le_p 3\mathrm{SAT}$ מייצרת הסגרים כאלה). החישוב למעלה נשען על כך שבכל הסגר יש **בדיוק** שלושה ליטרלים מעל שלושה משתנים **שונים**: הסגר באורך 1 נכשל בהסתברות $\frac{1}{2}$, ולכן נוסחה של הסגרי יחידה בלבד מקיימת $\mathbb{E}[X] = \frac{1}{2}m$ ולא $\frac{7}{8}m$; והסגר שבו אותו משתנה מופיע פעמיים ($x \vee x \vee y$) נכשל בהסתברות $\frac{1}{4}$. לכן MAX-3ECNF ולא MAX-3SAT.

הדרנדומיזציה (שיעור 20). שיטת התוחלות המותנות (שהופיעה לראשונה בשיעור 19 על MAXCUT) הופכת את הקיום לבנייה: משתנה מקרי X שתוחלתו ידועה, ורצף החלטות בינאריות; בכל צעד קובעים משתנה אחד לפי הענף שבו התוחלת המותנית אינה יורדת מתחת לסף, ובסוף התוחלת המותנית היא ערך קונקרטי. **שיעור 20 מבצע את השיטה במלואה עבור 3ECNF ומוכיח את נכונותה**; כאן מנוסחת התוצאה שלו כמשפט 1 ומשמשת כקופסה שחורה, וההוכחה החדשה שנוספת עליה היא רק אריזת התוצאה כיחס קירוב מול OPT.

מחלקות אקראיות (שיעורים 16–17). נזכיר: $L \in \mathrm{BPP}$ אם קיימת מכונה אקראית פולינומית M כך שלכל x, $\Pr[M(x) = [x \in L]] \ge \frac{2}{3}$ — טעות **דו-צדדית**. $L \in \mathrm{RP}$ אם קיימת מכונה אקראית פולינומית M כך שאם $x \in L$ אז $\Pr[M \text{ accepts } x] \ge \frac{1}{2}$, ואם $x \notin L$ אז $\Pr[M \text{ accepts } x] = 0$ — טעות **חד-צדדית**, רק false negatives. שתי המחלקות סגורות לרדוקציות זמן פולינומי. **אמפליפיקציה:** לכל פולינום q, כל שפה ב-BPP מוכרעת בזמן פולינומי בהסתברות שגיאה $\le 1/q(|x|)$ (חזרות בלתי תלויות והכרעת רוב, עם חסם צ'רנוף).

רדוקציות. $A \le_p B$ פירושו: קיימת פונקציה f הניתנת לחישוב בזמן פולינומי כך ש- $x \in A \iff f(x) \in B$. הכיוון חשוב — B היא ה**קשה** מבין השתיים. SAT היא NP-שלמה (שיעור 9), כלומר $\mathrm{SAT} \in \mathrm{NP}$ וגם NP-קשה.

הגדרות

הגדרה 1: MAX-3ECNF

הקלט: נוסחה φ בצורת 3ECNF מעל המשתנים $x_1, \ldots, x_n$, עם m הסגרים. **הפתרונות החוקיים:** כל ההשמות המלאות $v : \{x_1, \ldots, x_n\} \to \{0,1\}$. **הערך:** מספר ההסגרים של φ שההשמה v מספקת. **המטרה:** מקסימום. נסמן $\mathrm{OPT}(\varphi) = \max_v \#\{C \in \varphi : v \models C\}$.

אינטואיציה. בניגוד ל-SAT אין כאן שאלת "כן/לא" אלא דרישה להפיק כמה שיותר. מפני שכל השמה מלאה היא פתרון חוקי, בעיית החוקיות טריוויאלית — הקושי כולו בערך. זו נקודה שכדאי לשים לב אליה: בבעיות אופטימיזציה אחרות (למשל VC) עצם החוקיות של הפלט היא חלק מההוכחה.

דוגמה. $\varphi = (x_1 \vee x_2 \vee x_3) \wedge (\neg x_1 \vee \neg x_2 \vee \neg x_3)$: כאן $m = 2$, $\mathrm{OPT} = 2$ (למשל $v = (1,0,0)$).

דוגמה נגדית (מה איננו קלט חוקי). $(x_1 \vee x_2) \wedge (x_1 \vee \neg x_1 \vee x_2)$ אינה 3ECNF: ההסגר הראשון באורך 2, ובשני מופיע x_1 פעמיים. שתי החריגות שוברות את חישוב ה-$\frac{1}{8}$.

הגדרה 2: השמה חלקית והשלמה

השמה חלקית v היא פונקציה חלקית מקבוצת המשתנים ל-$\{0,1\}$ — כלומר, ייתכן שאינה מוגדרת על חלק מהמשתנים. **השלמה** של v היא השמה מלאה $\hat{v}$ המוגדרת על כל המשתנים, כך שבכל מקום שבו v מוגדרת מתקיים $\hat{v}(x) = v(x)$; על המשתנים שבהם v אינה מוגדרת אין ל-$\hat{v}$ שום מחויבות.

אינטואיציה. האלגוריתמים בשיעור בונים את ההשמה משתנה-משתנה. בכל רגע ביד יש השמה חלקית, והאינווריאנטה שנשמור עליה תמיד תהיה מהצורה "קיימת השלמה של v בעלת תכונה טובה". כשההשמה נעשית מלאה, ההשלמה היחידה שלה היא היא עצמה — ולכן התכונה הטובה עוברת אליה. זה כל מנגנון ההוכחה בשני האלגוריתמים הבאים.

הגדרה 3: התוחלת המותנית של מספר ההסגרים המסופקים (מובאת משיעור 20 לצורך ציטוט)

יהי φ קבוע עם m הסגרים, ותהא ρ השמה חלקית. נסמן $\mathbb{E}[X \mid \rho] = \mathbb{E}\big[\#\{C \in \varphi : v \models C\} \;\big|\; v \text{ extends } \rho\big]$, כאשר ההשמה v נדגמת אחידה מבין כל ההשמות המלאות המרחיבות את ρ — כלומר, כל משתנה שאינו בתחום של ρ מקבל 0 או 1 בהסתברות $\tfrac{1}{2}$ באופן בלתי תלוי.

אינטואיציה ואופן החישוב. למרות שהביטוי הזה מדבר על אקראיות, יש לו נוסחה סגורה שמחושבת **דטרמיניסטית** במעבר אחד על הנוסחה. עוברים הסגר-הסגר; אם בהסגר יש ליטרל ש-ρ כבר קבעה ל-TRUE, תרומתו 1; אם ρ הפילה את כל ליטרליו, תרומתו 0; אחרת, אם נותרו בו $k \geq 1$ ליטרלים חופשיים (מעל משתנים שונים), תרומתו $1 - 2^{-k}$. סוכמים. **אין כאן שום הטלת מטבע.** זו נקודה שהמרצה עמד עליה ארוכות: כל השיעורים על אלגוריתמים אקראיים דיברו על אקראיות באופן דטרמיניסטי לגמרי — הניתוח על הנייר הוא חישוב, לא ניסוי.

מקרה קצה חשוב. אם ρ היא השמה **מלאה**, אין משתנים חופשיים, המשתנה המקרי הוא קבוע, ולכן $\mathbb{E}[X \mid \rho]$ שווה בדיוק למספר ההסגרים שהשמה ρ מספקת. זהו הצעד שסוגר את הוכחת הנכונות בשיעור 20.

הגדרה 4: גרסת ההכרעה מול גרסת החיפוש של SAT

גרסת ההכרעה (SAT): הקלט הוא נוסחת CNF φ, והפלט הוא "כן" אם קיימת ל-φ השמה מספקת ו"לא" אחרת. **גרסת החיפוש**: הקלט הוא נוסחת CNF φ, והפלט הוא השמה מספקת ל-φ אם קיימת כזו, ו"אין השמה מספקת" אחרת.

אינטואיציה. ההכרעה מחזירה ביט; החיפוש מחזיר עד. ברור שהחיפוש לא קל יותר: מי שפותר את החיפוש בזמן פולינומי פותר גם את ההכרעה (מריצים ומסתכלים בפלט). הכיוון ההפוך — שלפתור את ההכרעה מספיק כדי לפתור את החיפוש — הוא **לא** טריוויאלי, וזה בדיוק משפט 2.

הגדרה 5: coNP

$$\mathrm{coNP} = \{\, \bar{A} \;\mid\; A \in \mathrm{NP} \,\}.$$

אינטואיציה ואזהרה. coNP היא **אוסף המשלימים** של שפות ב-NP, ולא *המשלים* של האוסף NP. שפה שאינה ב-NP אינה בהכרח ב-coNP, ושפה ב-coNP יכולה בהחלט להיות גם ב-NP (כל שפה ב-P, למשל). זה בדיוק כמו R ו-coR בחישוביות — שם $\mathrm{coR} = \mathrm{R}$, ולא "המשלים של R". מקור אי-הסימטריה: ההגדרה של NP אינה סימטרית. עבור yes-instance נדרש **קיום** (קיים עד קצר, או קיימת ריצה מקבלת של מכונה לא-דטרמיניסטית), ועבור no-instance נדרש **לכל** (כל עד נדחה). היפוך התשובה של מכונה לא-דטרמיניסטית אינו מחליף בין "קיים" ל"לכל", ולכן הטריק שעובד ב-P אינו עובד כאן.

מופע. $\overline{\mathrm{SAT}}$ — קבוצת נוסחאות ה-CNF שאין להן השמה מספקת — היא ב-coNP לפי ההגדרה, כי $\mathrm{SAT} \in \mathrm{NP}$. **אי-מופע.** אין לנו הצדקה לטעון ש-$\overline{\mathrm{SAT}} \in \mathrm{NP}$: אין עד קצר ידוע לאי-ספיקות. השאלה אם $\mathrm{NP} = \mathrm{coNP}$ **פתוחה**.

משפטים והוכחות

משפט 1: יחס הקירוב 7/8 ל-MAX-3ECNF

> **גבול בעלות:** האלגוריתם שלהלן והוכחת נכונותו (האינווריאנטה, האינדוקציה, סיום המשתנה המנוון וחשבון זמן הריצה) שייכים **לשיעור 20** ונכתבו שם במלואם. כאן הם מובאים בניסוח מדויק בלבד, כדי שאפשר יהיה לצטט אותם; מה שמוכח כאן במלואו הוא **ארזית התוצאה כיחס קירוב** — חוקיות הפלט והשוואה ל-OPT.

האלגוריתם A (משיעור 20). קלט: נוסחה φ בצורת 3ECNF. נסמן ב-$x_1, \dots, x_n$ את משתני הנוסחה, וב-m את מספר ההסגרים. הערך m **נקבע פעם אחת בתחילת הריצה ואינו משתנה**.

לכל $1 \le i \le n$:

אם $\mathbb{E}[X \mid v(x_i) = 1] \;\ge\; \frac{7}{8}m$ — קבע $v(x_i) = 1$ והצב 1 במקום x_i ב-φ.

אחרת — קבע $v(x_i) = 0$ והצב 0 במקום x_i ב-φ.

החזר את v.

(התוחלת בשלב 1 מחושבת ביחס להשמה החלקית שנבנתה עד כה, כלומר $\mathbb{E}[X \mid v(x_1), \dots, v(x_{i-1}), v(x_i) = 1]$ בסימוני הגדרה 3; זו בדיוק התוחלת על הנוסחה הנוכחית לאחר ההצבות, בתוספת ההסגרים שכבר סופקו.)

מה הוכח בשיעור 20 (מצוטט כאן). האלגוריתם A הוא **דטרמיניסטי** (אין בו ביט אקראי אחד — $\mathbb{E}[X \mid \cdot]$ הוא מספר שמחושב בנוסחה סגורה לפי הגדרה 3), רץ בזמן $O(|\varphi|^2)$, ולכל נוסחה φ בצורת 3ECNF עם m הסגרים הוא מחזיר השמה מלאה v המקיימת $\#\{C \in \varphi : \; v \models C\} \;\ge\; \frac{7}{8}m$. ההוכחה שם היא אינדוקציה על האינווריאנטה $\mathbb{E}[X \mid \rho_i] \ge \frac{7}{8}m$, המשלבת את משפט התוחלת השלמה עם טיעון "ממוצע של שניים $\Longrightarrow$ אחד מהם לפחות הממוצע", ומסתיימת בכך שכשההשמה מלאה המשתנה המקרי מנוון ולכן תוחלתו היא ערכו. **ראו שיעור 20 לפרטים המלאים**, ושיעור 19 לתנאי ההתחלה $\mathbb{E}[X] = \frac{7}{8}m$ שממנו האינדוקציה יוצאת.

המשפט (החלק החדש כאן). האלגוריתם A הוא אלגוריתם **קירוב ביחס** $\alpha = \frac{7}{8}$ ל-$\mathrm{MAX\text{-}3ECNF}$ במוסכמת המקסימיזציה של שיעור 13: לכל נוסחה φ בצורת 3ECNF הוא מחזיר פתרון חוקי המקיים $\mathrm{ALG}(\varphi) \ge \frac{7}{8} \cdot \mathrm{OPT}(\varphi)$.

הוכחה — חוקיות הפלט. האלגוריתם קובע ערך לכל x_i, $1 \le i \le n$, בדיוק פעם אחת. לכן הפלט הוא השמה מלאה על כל המשתנים, וכל השמה מלאה היא פתרון חוקי של $\mathrm{MAX\text{-}3ECNF}$ (הגדרה 1). אין כאן מה להוכיח מעבר לכך, אבל חשוב לומר זאת במפורש: בהוכחת יחס קירוב תמיד יש שני חלקים, וזה הראשון.

הוכחה — חסימת OPT מלמעלה. זהו הצעד המהותי, והוא זה שאסור להשאיר משתמע. הערבות של האלגוריתם היא **מוחלטת** — "לפחות $\frac{7}{8}m$ הסגרים" — ואילו יחס קירוב מוגדר תמיד **יחסית ל-**OPT, שערכו לא ידוע לנו. המעבר בין השניים דורש לחסום את OPT מלמעלה בגודל

שהאלגוריתם שולט בו. כאן החסם מיידי: לנוסחה יש בסך הכול m הסגרים, ולכן שום השמה — ובכללן ההשמה האופטימלית — אינה יכולה לספק יותר מ-m מהם: $\mathrm{OPT}(\varphi) \le m.$
הוכחה — יחס הקירוב. נשלב את שני החסמים: $\mathrm{ALG}(\varphi) \ge \frac{7}{8}m \ge \frac{7}{8}\cdot\mathrm{OPT}(\varphi),$ כאשר אי-השוויון הראשון הוא הערבות של שיעור 20 והשני הוא $\mathrm{OPT} \le m$ מוכפל ב-$\frac{7}{8} > 0$. כלומר $\mathrm{ALG} \ge \alpha\cdot\mathrm{OPT}$ עם $\alpha = \frac{7}{8} \in (0,1]$ — בדיוק מוסכמת המקסימיזציה של שיעור 13. ■
שתי הערות על היחס.
הערבות $\mathrm{ALG} \ge \frac{7}{8}m$ **חזקה** מיחס הקירוב $\frac{7}{8}$: כל אימת ש-$\mathrm{OPT} < m$ (כלומר, כשהנוסחה אינה ספיקה) היחס בפועל טוב מ-$\frac{7}{8}$. ראו דוגמה 2, שבה $\mathrm{OPT} = 7$, $m = 8$, והיחס בפועל הוא 1.
הכיוון של אי-השוויון תלוי במוסכמה. במוסכמת המינימיזציה של שיעור 13 היינו כותבים $\mathrm{ALG} \le \alpha\cdot\mathrm{OPT}$ עם $\alpha \ge 1$; לכתוב כאן $\alpha = \frac{8}{7}$ יהיה שגוי במוסכמה שנקבעה בקורס. תמיד לציין את המוסכמה במפורש.
איפה נגמרת הבעלות של שיעור 20 ומתחילה זו של השיעור הזה. כל מה שקדם לחסם $\mathrm{OPT} \le m$ — האלגוריתם, האינווריאנטה, האינדוקציה, וההסבר מדוע תכונת ה-3ECNF נחוצה אך ורק לתנאי ההתחלה — נלמד בהקלטה לפני [00:27:36] ונכתב בשיעור 20. החומר של השיעור הזה מתחיל ב-[00:27:36], עם הטענה המרכזית על BPP ו-RP (משפט 4).
משפט 2: SAT היא self-reducible
המשפט. אם קיים אלגוריתם זמן ריצה פולינומי עבור SAT (גרסת ההכרעה), אז קיים אלגוריתם זמן ריצה פולינומי עבור גרסת החיפוש של SAT.
הערה על השם. זו **אינה** רדוקציית מיפוי: רדוקציות מיפוי הוגדרו בין בעיות **הכרעה**, וגרסת החיפוש אינה בעיית הכרעה. במובן של קורס אלגוריתמים זו בהחלט רדוקציה (שימוש באלגוריתם אחד כתת-שגרה בתוך אחר), אך לא רדוקציה במובן של חישוביות/סיבוכיות. התכונה נקראת **self-reducibility**, ולא כל בעיה NP-שלמה ידועה ככזו — עבור חלק מהן זו שאלה פתוחה. זו אחת הדוגמאות לכך שבעיות NP-שלמות **אינן** נראות אותו הדבר ברזולוציה עדינה יותר מ-NP-קושי; הבדל אחר הוא קירוביות — ל-VC יש קירוב 2 (שיעור 13), ואילו ל-TSP הכללי קירוב כלשהו כבר גורר $\mathrm{P} = \mathrm{NP}$ (שם).
הוכחה. נניח שקיים אלגוריתם M המכריע את SAT בזמן פולינומי. נתבונן באלגוריתם $\hat{M}$ הבא:
קלט: נוסחה φ בצורת CNF. נסמן $x_1, \dots, x_n$ את משתני הנוסחה.
אם M דוחה את φ — החזר "אין השמה מספקת".
לכל $1 \le i \le n$:
אם M מקבלת את $\varphi \wedge x_i$ — קבע $v(x_i) = 1$ והצב $\varphi \leftarrow \varphi \wedge x_i$.
אחרת — קבע $v(x_i) = 0$ והצב $\varphi \leftarrow \varphi \wedge \neg x_i$.
החזר את v.
החלטת התכנון החשובה. במשפט 1 קבענו משתנה על ידי **הצבה**, וכך המשתנה נעלם מהנוסחה. כאן, במקום להציב, אנחנו **מוסיפים הסגר יחידה** (x_i) או $(\neg x_i)$. האפקט זהה — כל השמה מספקת של הנוסחה החדשה חייבת לתת ל-x_i את הערך שקבענו — אבל מספר המשתנים ואורך

הנוסחה נשמרים בערך. במשפט 2 עצמו אין לכך צורך; הסיבה תתגלה במשפט 4, שם הסתברות השגיאה תלויה ב-n ולכן חשוב ש-n לא יקטן. (בנוסף, דידקטית זו דרך שנייה ושימושית לקבע ערך של משתנה.) הנוסחה שנשארת היא עדיין נוסחת CNF תקינה.

ניתוח זמן ריצה. קיים $c > 0$ כך שלכל נוסחה ψ מתקיים $\mathrm{time}_M(\psi) \le O(|\psi|^c)$. האלגוריתם $\hat{M}$ מריץ את M לכל היותר $n + 1 \le |\varphi| + 1$ פעמים. לגבי אורך הקלטים: בכל איטרציה מתווסף הסגר יחידה בודד, ומשתנה זה כבר הופיע ב-φ; לכן לאחר n איטרציות האורך גדל לכל היותר פי שניים, $|\psi| \le 2|\varphi|$. מכאן, $\mathrm{time}_{\hat{M}}(\varphi) \le (|\varphi|+1)\cdot O\big((2|\varphi|)^c\big) = O\big(|\varphi|^{c+1}\big)$, פולינומי באורך הקלט.

ניתוח סמנטי. תהא φ נוסחת CNF.

אם $\varphi \notin \mathrm{SAT}$: M מכריעה נכון, לכן היא דוחה בשלב 1 ו-$\hat{M}$ מחזירה "אין השמה מספקת" — נכון.

אם $\varphi \in \mathrm{SAT}$: נסמן ב-φ_i את הנוסחה שבידי האלגוריתם בסוף איטרציה i (ו-$\varphi_0 = \varphi$), וב-v_i את ההשמה החלקית שנבנתה עד אז. נוכיח באינדוקציה על i את האינווריאנטה:

$\varphi_i \in \mathrm{SAT}$, כלומר קיימת השמה מספקת של φ המשלימה את v_i.

(שתי הניסוחים שקולים כאן: $\varphi_i = \varphi \wedge \bigwedge_{j \le i}(\text{literal for } v_i(x_j))$, ולכן השמה מספקת את φ_i אם ורק אם היא מספקת את φ ומסכימה עם v_i.)

בסיס $i = 0$: $\varphi_0 = \varphi \in \mathrm{SAT}$ לפי ההנחה, ו-v_0 ריקה.

צעד: נניח $\varphi_{i-1} \in \mathrm{SAT}$. — אם M מקבלת את x_i: מכיוון ש-M מכריעה את SAT נכון, $\varphi_{i-1} \wedge x_i$ אכן ספיקה. — אם M דוחה את x_i: אז $\varphi_{i-1} \wedge x_i$ אינה ספיקה, כלומר **אין** השמה המספקת את φ_{i-1} ונותנת ל-x_i את הערך 1. אבל φ_{i-1} כן ספיקה לפי הנחת האינדוקציה, ולכל השמה יש ערך יחיד עבור x_i; לכן כל השמה מספקת של φ_{i-1} נותנת ל-x_i את הערך 0, ובפרט קיימת כזו. מכאן $\varphi_i = \varphi_{i-1} \wedge \neg x_i$ ספיקה.

> **הערה:** בהרצאה ובסיכום הצעד הזה נאמר בקיצור — "באינדוקציה"; הפירוט למעלה הוא מה שהאינדוקציה עומדת עליו. הנקודה היחידה שאינה אוטומטית היא שדחייה של הענף $x_i = 1$ **בשילוב** עם ספיקות φ_{i-1} מכריחה את קיומה של השמה מספקת עם $x_i = 0$.

סיום: בתום האיטרציה ה-n ההשמה v_n מוגדרת על כל המשתנים, כלומר מלאה. לפי האינווריאנטה קיימת השמה מספקת של φ המשלימה את v_n; אבל ההשלמה היחידה של השמה מלאה היא היא עצמה, ולכן v_n עצמה מספקת את φ. ■

משפט 3: $\mathrm{NP} \subseteq \mathrm{BPP}$ אם ורק אם $\mathrm{SAT} \in \mathrm{BPP}$ (וכנ"ל עבור RP)

המשפט. $\mathrm{NP} \subseteq \mathrm{BPP}$ אם ורק אם $\mathrm{SAT} \in \mathrm{BPP}$.

הוכחה. ($\Rightarrow$) $\mathrm{SAT} \in \mathrm{NP}$, ולכן מהכלה $\mathrm{SAT} \in \mathrm{BPP}$. זהו טיעון תורת-קבוצות בלבד — ובכל זאת יש לכתוב אותו; דילוג על מה שנראה מובן מאליו הוא מקור נפוץ לטעויות.

($\Leftarrow$) נניח $\mathrm{SAT} \in \mathrm{BPP}$, ותהא $L \in \mathrm{NP}$. מכיוון ש-SAT היא NP-קשה, קיימת רדוקציה $L \le_p \mathrm{SAT}$. מכיוון ש-BPP סגורה לרדוקציות זמן פולינומי, נובע $L \in \mathrm{BPP}$. לכן $\mathrm{NP} \subseteq \mathrm{BPP}$. ■

איזו תכונה שימשה בכל כיוון. לכיוון ($\Leftarrow$) נדרשה רק NP**-קושי** של SAT (שיש רדוקציה אליה מכל בעיה ב-NP) וסגירות המחלקה לרדוקציות. לכיוון ($\Rightarrow$) נדרשה דווקא **השייכות** $\mathrm{SAT} \in \mathrm{NP}$. שני התנאים יחד הם בדיוק NP-שלמות. אותו טיעון בדיוק תקף עם RP במקום BPP, כי גם RP סגורה

לרדוקציות זמן פולינומי.

משפט 4: אם $\mathrm{SAT} \in \mathrm{BPP}$ אז $\mathrm{NP} \subseteq \mathrm{RP}$

מה המשפט אומר. זוהי טענת הכלה, ולכן היא מתחילה ב"לכל": אם לכל בעיה ב-NP יש אלגוריתם אקראי פולינומי עם טעות **דו-צדדית**, אז לכל בעיה ב-NP יש אלגוריתם אקראי פולינומי עם טעות **חד-צדדית**. ההבדל בין BPP ל-RP אינו הקבועים $\frac{2}{3}$ ו-$\frac{1}{2}$ (ראינו באמפליפיקציה שהם ניתנים לשינוי כמעט כרצוננו) אלא צדדיות הטעות: ב-RP אין false positives כלל.

הערת ניסוח. ניסחנו את התנאי כ-$\mathrm{SAT} \in \mathrm{BPP}$ (החלש ביותר) ואת המסקנה כ-$\mathrm{NP} \subseteq \mathrm{RP}$ (החזקה ביותר), למרות שלפי משפט 3 שתי הצורות שקולות. זה עניין של נראות: תמיד עדיף לנסח משפט עם הנחה חלשה ככל האפשר ומסקנה חזקה ככל האפשר.

הוכחה. נניח $\mathrm{SAT} \in \mathrm{BPP}$. נעבור ממכונה אקראית למכונה אקראית — אין סיבה לעבור דרך מכונה דטרמיניסטית, כי היעד RP הוא ממילא אקראי.

שלב א' — אמפליפיקציה. מהנחת $\mathrm{SAT} \in \mathrm{BPP}$ ומשפט האמפליפיקציה (שיעור 17) קיימת מכונה אקראית M הרצה בזמן פולינומי כך שלכל נוסחת CNF ψ:

$$\psi\notin\mathrm{SAT}\;\Rightarrow\;\Pr[M \text{ rejects } \psi]\ \ge\ 1-\frac{1}{2(n+1)}$$

כאשר n הוא מספר המשתנים בנוסחת הקלט φ שבה נעסוק. > **הערה:** בהרצאה ובסיכום הפרמטר נכתב ישירות כ-n; הפירוט כאן. האמפליפיקציה מנוסחת ביחס ל**אורך הקלט**: לכל פולינום q אפשר לקבל שגיאה $\le 1/q(|\psi|)$. ניקח $q(\ell)=2(\ell+1)$. מכיוון שכל משתנה חייב להופיע בקידוד, $n\le|\psi|$, ולכן $\frac{1}{2(n+1)}\le\frac{1}{2(|\psi|+1)}$ והחסם הדרוש מתקיים. חשוב לוודא שזה נכון גם עבור הנוסחאות **העזר** $\psi=\varphi_i\wedge x_i$ שנשאל עליהן: מכיוון שהאלגוריתם למטה **אינו מעלים משתנים**, לכולן אותה קבוצת משתנים בגודל n, וגם עבורן $n\le|\psi|$. זו בדיוק הסיבה שבחרנו במשפט 2 להוסיף הסגרי יחידה ולא להציב. הבחירה $\frac{1}{2(n+1)}$ אינה מקרית — היא נקבעה לאחור, מתוך ידיעה שנכפול ב-$n+1$ ונרצה לקבל $\frac12$. **שלב ב' — האלגוריתם $\hat M$.** קלט: נוסחה φ בצורת CNF, עם משתנים $x_1,\dots,x_n$. אם M דוחה את φ — דחה. 2. לכל $1 \le i \le n$: אם M מקבלת את $\varphi\wedge x_i$ — קבע $v(x_i)=1$ והצב $\varphi\leftarrow\varphi\wedge x_i$. 2. אחרת — קבע $v(x_i)=0$ והצב $\varphi\leftarrow\varphi\wedge\neg x_i$. 3. אם v מספקת את φ — קבל; אחרת — דחה. **ההבדל מהאלגוריתם של משפט 2** אינו בתחביר אלא בהקשר. הטקסט כמעט זהה, מלבד שלב 3 שמחזיר "קבל/דחה" ולא השמה. ההבדל האמיתי: שם M הייתה **דטרמיניסטית** ולכן כל האלגוריתם היה דטרמיניסטי; כאן M היא מכונה **אקראית** ולכן כל האלגוריתם אקראי ויכול לטעות. **ניתוח זמן ריצה.** זהה מילה במילה לניתוח של משפט 2 — החסם על זמן הריצה של M הוא דטרמיניסטי (מתקיים בכל הרצה), ולכן $\mathrm{time}_{\hat M}(\varphi)=O(|\varphi|^{c+1})$. **ניתוח סמנטי, מקרה $\varphi\notin\mathrm{SAT}$** — אין false positives.** נטען: $\Pr[\hat M \text{ rejects } \varphi]=1$, כלומר הסתברות הקבלה היא 0 בדיוק. התבוננו ברמה התחבירית: **המקום היחיד באלגוריתם שבו מופיעה המילה "קבל" הוא שלב 3**, ותנאי הכניסה אליו הוא ש-v מספקת את φ. שלב 3 הוא דטרמיניסטי לחלוטין — יש ביד השמה מלאה, ובודקים אותה מול הנוסחה. נתק אותו לרגע מכל השאר: נניח שמישהו נותן לך נוסחה φ והשמה v שהגיעה מהשמיים,

ואתה מקבל אם ורק אם $v\models\varphi$. אם ל-φ אין השמה מספקת כלל, אז **שום השמה — ולא משנה איך התקבלה, כמה טעויות נעשו בדרך, ומה היו תוצאות ההטלות — לא תספק אותה, ולכן לעולם לא תקבל. לכן $\Pr[\hat M \text{ accepts } \varphi]=0$. (בפרט שלב 1 אינו נחוץ לנכונות; הוא נשמר כדי לשמור על הדמיון לאלגוריתם הקודם.) **ניתוח סמנטי, מקרה $\varphi\in\mathrm{SAT}$.** ההסתברויות כאן הן **מעל המטבעות של $\hat M$ עבור הנוסחה הקבועה φ** — לא מעל נוסחאות אקראיות. נגדיר שני מאורעות: - A — "המאורע $\hat M$ מקבלת את B - φ". - B — "המאורע M **צודקת בכל אחת** מההרצות שלה במהלך הריצה של $\hat M$". **טענת ההכלה $B\subseteq A$.** אם M צודקת בכל הרצותיה, אז כל תשובה שקיבל $\hat M$ מ-M זהה לתשובה שהייתה מקבלת מהמכריע המדויק, ולכן $\hat M$ מתנהג בדיוק כמו האלגוריתם הדטרמיניסטי של משפט 2. לפי משפט 2, אותו אלגוריתם בונה השמה v **המספקת** את φ; אז שלב 3 מקבל. לכן כל תוצאת מטבעות ב-B שייכת גם ל-A, ומכאן $\Pr(B)\le\Pr(A)$. < **הערה:** ההכלה היא בכיוון אחד בלבד, וזה בסדר גמור. ייתכן ש-$\hat M$ תקבל למרות ש-M טעתה בדרך — טעות, תיקון, טעות, תיקון, ובסוף במקרה נבנתה השמה מספקת. אנחנו רק חוסמים מלמטה, ולכן די בכיוון הזה. שימו לב גם ש-B הוא תנאי **חזק** — הוא דורש צדקות בכל ההרצות, גם כשיש הרבה השמות מספקות ולכן "מותר" ל-M לטעות ולהצליח בכל זאת. **חסימת $\Pr(B)$ מלמטה.** בהסתברות יש הרבה יותר כלים לחסום מלמעלה מאשר מלמטה (למשל אי-שוויון מרקוב, שיעור 20), ולכן נחסום מלמעלה את המשלים. נסמן: - B_0 — המאורע "M צדקה בשלב 1". - לכל $1 \le i \le n$: B_i — המאורע "M צדקה בקריאה שבאיטרציה ה-i". אז $B=\bigcap_{i=0}^{n}B_i$, ולכן לפי דה-מורגן $\bar B=\bigcup_{i=0}^{n}\bar B_i$. המאורעות $\bar B_i$ אינם זרים ואינם בלתי תלויים, ולכן אי אפשר לחשב את הסתברות האיחוד; אבל **חסם האיחוד** אינו דורש דבר מאלה: $$\Pr(\bar B) \le \sum_{i=0}^{n}\Pr(\bar B_i) \le (n+1)\cdot\frac{1}{2(n+1)} = \frac12 .$$ < **הערה:** בהרצאה החסם $\frac{1}{2(n+1)}$ נלקח ישירות מהאמפליפיקציה; הפירוט כאן. הנוסחה שעליה M נקראת באיטרציה i תלויה בתשובות הקודמות, ולכן $\bar B_i$ אינו "כישלון על קלט קבוע". אבל כל קריאה משתמשת במטבעות **טריים**, ולכן לכל היסטוריה h של הקריאות הקודמות מתקיים $\Pr[\bar B_i\mid h]\le\frac{1}{2(n+1)}$ — כי בהינתן h הנוסחה הנשאלת קבועה, וכל נוסחה כזו היא קלט לגיטימי ל-M עם אותה קבוצת n משתנים. מנוסחת ההסתברות השלמה, $\Pr(\bar B_i)=\sum_h \Pr(h)\Pr[\bar B_i\mid h]\le\frac{1}{2(n+1)}$. לכן $\Pr(B)=1-\Pr(\bar B)\ge\tfrac12$, ומההכלה $B\subseteq A$ נובע $$\Pr[\hat M \text{ accepts } \varphi] = \Pr(A) \ge \tfrac12 .$$ **מסקנת ביניים.** $\hat M$ היא מכונה אקראית פולינומית שמקבלת נוסחה ספיקה בהסתברות $\ge\tfrac12$ ואינה מקבלת נוסחה בלתי ספיקה לעולם. לכן $\mathrm{SAT}\in\mathrm{RP}$. **סיום.** תהא $L\in\mathrm{NP}$. מכיוון ש-SAT היא NP-קשה מתקיים $L\le_p\mathrm{SAT}$, ומכיוון ש-RP סגורה לרדוקציות זמן פולינומי נובע $L\in\mathrm{RP}$. לכן $\mathrm{NP}\subseteq\mathrm{RP}$. ### משפט 5: $\mathrm{coP}=\mathrm{P}$ נגדיר $\mathrm{coP}=\{\bar A\mid A\in\mathrm{P}\}$. **טענה:** $\mathrm{coP}=\mathrm{P}$. **הוכחה.** תהא A שפה כלשהי. נטען $A\in\mathrm{P}\iff\bar A\in\mathrm{P}$ (סגירות P למשלים): אם M $$\blacksquare$$

מכריעה את A בזמן פולינומי, המכונה שמריצה את M והופכת את התשובה (מקבלת כאשר M דוחה ולהפך) מכריעה את $\bar A$ באותו זמן ריצה; זה חוקי כי M **דטרמיניסטית ועוצרת תמיד**. הכיוון השני זהה. כעת: אם $B\in\mathrm{coP}$ אז $B=\bar A$ עבור $A\in\mathrm{P}$, ולכן $B\in\mathrm{P}$; ואם $B\in\mathrm{P}$ אז $\bar B\in\mathrm{P}$ ולכן $B=\overline{\bar B}\in\mathrm{coP}$. $\blacksquare$

למה זה נכשל ב-NP. הטריק "הפוך את התשובה" דורש שהמכונה תהיה דטרמיניסטית. ב-NP ההגדרה אינה סימטרית: $x\in L$ פירושו ש**קיימת** ריצה מקבלת (או **קיים** עד קצר), ו-$x\notin L$ פירושו ש**לכל** ריצה/עד התשובה שלילית. היפוך התשובה של כל ריצה בנפרד אינו מחליף בין הכמתים. לכן $\mathrm{NP}\overset{?}{=}\mathrm{coNP}$ היא **בעיה פתוחה**.

משפט 6: $\mathrm{P}\subseteq\mathrm{NP}\cap\mathrm{coNP}$

הוכחה. ראינו $\mathrm{P}\subseteq\mathrm{NP}$ (שיעור 6). נותר להראות $\mathrm{P}\subseteq\mathrm{coNP}$. תהא $A\in\mathrm{P}$. לפי משפט 5, $\bar A\in\mathrm{P}$, ולכן $\bar A\in\mathrm{NP}$. לפי הגדרת coNP, המשלים של שפה ב-NP הוא ב-coNP; והמשלים של $\bar A$ הוא A. מכאן $A\in\mathrm{coNP}$. לכן $\mathrm{P}\subseteq\mathrm{NP}\cap\mathrm{coNP}$. $\blacksquare$

משפט 7: $\mathrm{NP}=\mathrm{coNP}$ אם ורק אם $\mathrm{NP}\subseteq\mathrm{coNP}$

הוכחה. ($\Rightarrow$) מהגדרת שוויון קבוצות, שוויון גורר הכלה. ($\Leftarrow$) נניח $\mathrm{NP}\subseteq\mathrm{coNP}$. נותר להראות $\mathrm{coNP}\subseteq\mathrm{NP}$. תהא $A\in\mathrm{coNP}$. מהגדרת coNP קיימת $C\in\mathrm{NP}$ עם $A=\bar C$, ולכן $\bar A=C\in\mathrm{NP}$. מההנחה, $\bar A\in\mathrm{coNP}$; שוב מההגדרה, $\overline{\bar A}=A\in\mathrm{NP}$. לכן $\mathrm{NP}=\mathrm{coNP}$, ויחד עם ההנחה $\mathrm{coNP}\subseteq\mathrm{NP}$. $\blacksquare$

שימו לב שאין בהוכחה הזו שום סיבוכיות — היא כולה תורת קבוצות על אופרטור המשלים.

משפט 8: $\mathrm{SAT}\in\mathrm{coNP}$ אם ורק אם $\mathrm{NP}=\mathrm{coNP}$

הוכחה. ($\Rightarrow$) ומהשוויון ($\Leftarrow$) $\mathrm{SAT}\in\mathrm{NP}$, $\mathrm{SAT}\in\mathrm{coNP}$. נניח $\mathrm{SAT}\in\mathrm{coNP}$, ותהא $A\in\mathrm{NP}$. מ-NP-קושי של SAT קיימת רדוקציה $A\le_p\mathrm{SAT}$. מסגירות coNP לרדוקציות זמן פולינומי (ראו תרגיל 3 בסעיף הדוגמאות) נובע $A\in\mathrm{coNP}$. לכן $\mathrm{NP}\subseteq\mathrm{coNP}$, ולפי משפט 7 $\mathrm{NP}=\mathrm{coNP}$. $\blacksquare$

משפט 9: A היא coNP-קשה אם ורק אם $\bar A$ היא NP-קשה

תהא A בעיית הכרעה. **הוכחה.** ($\Rightarrow$) נניח ש-A היא coNP-קשה, כלומר לכל $D\in\mathrm{coNP}$ מתקיים $D\le_p A$. תהא $B\in\mathrm{NP}$. אז $\bar B\in\mathrm{coNP}$ (coNP מהגדרת), ולכן $\bar B\le_p A$; תהא f הרדוקציה, כלומר $x\in\bar B\iff f(x)\in A$ לכל x. **אותה f בדיוק** היא רדוקציה מ-B ל-$\bar A$: $$x\in B\iff x\notin\bar B\iff f(x)\notin A\iff f(x)\in\bar A .$$ עדיין ניתנת לחישוב בזמן פולינומי — לא נגענו בה כלל. לכן $B\le_p\bar A$ לכל $B\in\mathrm{NP}$, כלומר $\bar A$ היא

NP-קשה. ($\Leftarrow$) בדומה, בהחלפת התפקידים. נניח ש-A היא NP-קשה, ותהא $D\in\mathrm{coNP}$. אז $\bar D\in\mathrm{NP}$, ולכן $\bar A\le_p D$ באמצעות g כלשהי; ואותה g נותנת $D\le_p A$, שכן $x\in D\iff x\notin\bar A\iff g(x)\in A$. לכן A היא coNP-קשה. $\blacksquare$

הערה: בהרצאה [02:01:20] המרצה פתח בטעות מהכיוון ההפוך, סטודנט העיר על כך, והוא תיקן והמשיך מהכיוון הנכון [02:02:26]. הגרסה כאן היא הגרסה של הסיכום, שהיא הנכונה. **הנקודה המפתיעה שהודגשה בכיתה.** רדוקציית מיפוי "יודעת" להתהפך בשני הצדדים בו-זמנית — אין צורך "להפוך את התוצאה" של f (רדוקציה אינה מחזירה כן/לא, היא מחזירה מופע!). אותה פונקציה בדיוק משמשת גם בכיוון המשלים. זה נראה כבר בחישוביות, וכאן הוא מופיע שוב. --- ## דוגמאות ותרגילים מהשיעור ### דוגמה 1: הרצה מלאה של אלגוריתם הקירוב על נוסחה קונקרטית *(הרצת האלגוריתם עצמו היא חומר של שיעור 20; היא מובאת כאן כדי שיהיה אפשר לסגור את חשבון הקירוב מקצה לקצה על מספרים ממשיים.)* $$\varphi=\underbrace{(x_1\vee x_2\vee x_3)}_{C_1}\wedge\underbrace{(x_1\vee\neg x_2\vee\neg x_4)}_{C_2}\wedge\underbrace{(\neg x_1\vee x_3\vee\neg x_4)}_{C_3}\wedge\underbrace{(\neg x_2\vee\neg x_3)}_{C_4}$$ נוסחה זו היא 3ECNF: בכל הסגר בדיוק שלושה ליטרלים מעל שלושה משתנים שונים. $n=4$, $m=4$, והסף הוא $\tfrac{7}{8}\cdot 4=3.5$. תנאי ההתחלה: $\mathbb{E}[X]=4\cdot\tfrac{7}{8}=3.5$. **איטרציה 1 ($x_1$).** נציב $x_1=1$: C_1,C_2,C_3 מסופקים (תרומה 1 כל אחד); C_4 מצטמצם ל-$(\neg x_2\vee\neg x_3)$, שני ליטרלים חופשיים, תרומה $2^{-2}=\tfrac{1}{4}$. $$\mathbb{E}[X\mid x_1=1]=1+1+1+\tfrac{3}{4}=3.75$$. בדיקה (לצורך ההמחשה בלבד — האלגוריתם לא מחשב אותה): $x_1=0$ נותן $C_1\to(x_2\vee x_3)$: $\tfrac{3}{4}$; $C_2\to(\neg x_2\vee x_4)$: $\tfrac{3}{4}$; $C_3\to(x_3\vee\neg x_4)$: $\tfrac{3}{4}$; C_4 מסופק: 1. סה"כ 3.25. ואכן $\mathbb{E}[X]=\frac{3.75+3.25}{2}=3.5$, כמתחייב ממשפט התוחלת השלמה. $3.75\ge 3.5$, לכן $v(x_1)=1$. הנוסחה הנוכחית: שלושה הסגרים מסופקים לצמיתות $+\ (\neg x_2\vee\neg x_3)$. **איטרציה 2 ($x_2$).** $\Pr[v(x_2)=1]=3+\Pr[\neg v(x_1)=1,v(x_2)=1]=3+\mathbb{E}[X\mid v(x_1)=1,v(x_2)=1]=3+\tfrac{1}{2}=3.5\ \ge\ 3.5$. לכן $v(x_2)=1$. נותר ההסגר $(\neg x_3)$. **איטרציה 3 (x_3).** $\mathbb{E}[X\mid \dots,v(x_3)=1]=3+0=3\ <\ 3.5$. לכן $v(x_3)=0$, ואז $\mathbb{E}[X\mid\dots,v(x_3)=0]=3+1=4\ge 3.5$ — האינווריאנטה נשמרה, כמובטח מטיעון הממוצע. **איטרציה 4 (x_4).** כבר אינו מופיע בשום הסגר לא-מסופק, ולכן $\mathbb{E}[X\mid\dots,v(x_4)=1]=4\ge 3.5$; האלגוריתם קובע $v(x_4)=1$. **פלט:** $v=(1,1,0,1)$. בדיקה: C_1 ✓ (מ-x_1), C_4 ✓, C_3 ✓, C_2 ✓ (מ-$\neg x_3$). $\mathrm{ALG}=4\ge 3.5$. כאן במקרה $\mathrm{ALG}=4=\mathrm{OPT}$, ויחס הקירוב בפועל הוא $1\le\frac{7}{8}$. ### דוגמה 2: המקרה ההדוק — כשהחסם $m\le\mathrm{OPT}$ אינו חד ניקח את הנוסחה שכל שמונת ההסגרים מעל x_1,x_2,x_3 מופיעים בה: $$\varphi^*=\bigwedge_{(a,b,c)\in\{0,1\}^3}\big(x_1^{a}\vee x_2^{b}\vee x_3^{c}\big),\qquad x^{1}:=x,\ x^{0}:=\neg x$$. כאן $m=8$, $n=3$, וזו 3ECNF תקינה. כל השמה מלאה (u_1,u_2,u_3) מפילה **בדיוק הסגר אחד** — זה שכל ליטרליו מנוגדים לה. לכן

$\mathrm{OPT}(\varphi^*)=7<8=m$, והנוסחה אינה ספיקה. הרצת האלגוריתם: הסף הוא $\tfrac78\cdot8=7$. - $\mathbb{E}[X\mid v(x_1)=1]$: ארבעת ההסגרים המכילים x_1 מסופקים (4); ארבעת ההסגרים המכילים $\neg x_1$ מצטמצמים להסגרים באורך 2, כל אחד תורם $\tfrac34$, סה"כ 3. יחד $7 \ge 7$ $\Longrightarrow$ $v(x_1)=1$. - $\mathbb{E}[X\mid v(x_1)=1,v(x_2)=1]=4+\big(1+1+\tfrac12+\tfrac12\big)=7\ge7$ $\Longrightarrow$ $v(x_2)=1$. - $\mathbb{E}[X\mid\dots,v(x_3)=1]=4+1+1+0=7\ge7$ $\Longrightarrow$ $v(x_3)=1$. פלט $v=(1,1,1)$, המספק 7 הסגרים — **בדיוק** $\tfrac78\,m$. שתי מסקנות על יחס הקירוב: 1. הערבות $\mathrm{ALG}\ge\tfrac78\,m$ **הדוקה**: יש נוסחה שעליה האלגוריתם משיג בדיוק את החסם ולא יותר. 2. החסם $\mathrm{OPT}\le m$ **אינו** הדוק כאן ($\mathrm{OPT}=7<8=m$), ולכן היחס בפועל מול OPT הוא $7/7=1$ — טוב מ-$\tfrac78$. זה בדיוק המחיר של המעבר מערבות מוחלטת ליחס קירוב: אנחנו מוותרים על חדות כדי לקבל טענה שמנוסחת מול OPT, שאותו איננו יודעים לחשב. ### דוגמה 3: הרצת הרדוקציה העצמית (משפט 2) על נוסחה קונקרטית $\varphi=(x_1\vee x_2)\wedge(\neg x_1\vee x_3)\wedge(\neg x_2\vee\neg x_3)$. - **שלב 1:** φ ספיקה (למשל $(0,1,0)$), ולכן M מקבלת ואנחנו ממשיכים. - **$i=1$:** האם $\varphi\wedge(x_1)$ ספיקה? $x_1=1$ מכריח $x_3=1$ (מההסגר השני), ואז ההסגר השלישי מכריח $x_2=0$; ההשמה $(1,0,1)$ מספקת. M מקבלת $\Longrightarrow$ $v(x_1)=1$, $\varphi\leftarrow\varphi\wedge(x_1)$. - **$i=2$:** האם $\varphi\wedge(x_1)\wedge(x_2)$ ספיקה? $x_1=1$ מכריח $x_3=1$, ו-$x_2=1$ יחד עם $x_3=1$ מפילים את ההסגר השלישי. אין השמה מספקת. M דוחה $\Longrightarrow$ $v(x_2)=0$, $\varphi\leftarrow\varphi\wedge(x_1)\wedge(\neg x_2)$. - **$i=3$:** האם $\varphi\wedge(x_1)\wedge(\neg x_2)\wedge(x_3)$ ספיקה? ההשמה $(1,0,1)$ מספקת. M מקבלת $\Longrightarrow$ $v(x_3)=1$. - **פלט:** $v=(1,0,1)$. בדיקה: $(x_1\vee x_2)$ ✓, $(\neg x_1\vee x_3)$ ✓, $(\neg x_2\vee\neg x_3)=1\vee0=1$ ✓. שימו לב לאורך: התחלנו עם 3 הסגרים והוספנו 3 הסגרי יחידה — לכל היותר הכפלה, כמו שנטען בניתוח. ### דוגמה 4: איפה בדיוק נכנסת הטעות באלגוריתם האקראי, ולמה היא חד-צדדית ניקח את אותה φ מדוגמה 3, ונדמיין ש-M (האקראית) **טועה** באיטרציה $i=1$ ודוחה את $\varphi\wedge(x_1)$ למרות שהיא ספיקה. אז $\hat M$ קובעת $v(x_1)=0$ ומוסיפה $(\neg x_1)$. הנוסחה עדיין ספיקה ($(0,1,0)$), ולכן ייתכן שנתאושש: אם M תצדק בהמשך נקבל $v=(0,1,0)$, שמספקת. אבל אם M תטעה שוב ותקבל את $\varphi\wedge(\neg x_1)\wedge(x_2)\wedge(x_3)$ — שאינה ספיקה — נסיים עם $v=(0,1,1)$, שמפילה את ההסגר השלישי. אז שלב 3 בודק, מגלה ש-v אינה מספקת, ו**דוחה**. זו טעות מסוג false negative: נוסחה ספיקה נדחתה. false positive לעולם אינו אפשרי, כי כדי לקבל צריך להחזיק ביד השמה מספקת — וכזו לא קיימת לנוסחה בלתי ספיקה. זו בדיוק ההבחנה בין BPP (שתי הטעויות אפשריות) ל-RP (רק false negatives), ובשפת מטריצת הבלבול: ב-RP אין false positives. ### תרגיל 1 (מהשיעור): מדוע $\Pr(B)\le\Pr(A)$ ולא להפך? **השאלה בכיתה:** אינטואיטיבית נדמה ש"להיות צודקת בכל ההרצות" קורה יותר מ"$\hat M$ מקבלת", ולכן ההסתברות שלו גדולה יותר. **התשובה:** ההפך. "צודקת בכל ההרצות" היא דרישה **חזקה יותר** מ"$\hat M$ מקבלת" — כל

תוצאת מטבעות שמקיימת אותה גורמת לקבלה, אבל יש תוצאות שגורמות לקבלה בלי שהיא מתקיימת (M טעתה ובכל זאת נבנתה השמה מספקת). לכן $B\subseteq A$ כקבוצות של תוצאות, ומכאן $\Pr(B)\le\Pr(A)$. חוסמים מלמטה את $\Pr(A)$ דרך $\Pr(B)$ — וזה מותר, כי אנחנו רק צריכים חסם תחתון. ### תרגיל 2 (מהשיעור): למה לא לחסום את $\Pr(\bar B)$ במכפלה $\big(\tfrac{1}{2(n+1)}\big)^{n+1}$? **התשובה:** מכפלה כזו הייתה נכונה רק אם המאורעות $\bar B_i$ היו בלתי תלויים. הם אינם: הנוסחה שנשאלת באיטרציה i תלויה בתשובות הקודמות. אפשר תמיד לכתוב את הסתברות החיתוך כמכפלת הסתברויות **מותנות** (כמו בניתוח אלגוריתם החתך המינימלי, שיעור 18), אבל אלה אינן ההסתברויות הבלתי מותנות, וההשוואה בין המכפלה לביטוי המקורי אינה קבועה בכיוונה. חסם האיחוד, לעומת זאת, תקף תמיד ללא שום הנחת תלות — וזו בדיוק הסיבה שבחרנו בו. ### תרגיל 3 (שהמרצה השאיר לבית): coNP סגורה לרדוקציות זמן פולינומי **הטענה.** אם $A\in\mathrm{coNP}$ ו-$B\le_p A$, אז $B\in\mathrm{coNP}$. **פתרון מלא.** תהא f הרדוקציה הפולינומית, $x\in B\iff f(x)\in A$. מהגדרת coNP, $\bar A\in\mathrm{NP}$. אותה f היא רדוקציה מ-$\bar B$ ל-$\bar A$: $x\in\bar B\iff x\notin B\iff f(x)\notin A\iff f(x)\in\bar A$. לכן $\bar B\le_p\bar A$. מכיוון ש-NP סגורה לרדוקציות זמן פולינומי (ראו שיעור 7), $\bar B\in\mathrm{NP}$, ולכן לפי ההגדרה $B=\overline{\bar B}\in\mathrm{coNP}$. $\blacksquare$ זה בדיוק מה שהמרצה ביקש: להשתמש בסגירות של NP במקום לרדת לרמת המכונה. ### תרגיל 4: $\overline{\mathrm{SAT}}$ היא coNP-קשה **פתרון.** SAT היא NP-קשה. נפעיל את משפט 9 עם $A=\overline{\mathrm{SAT}}$: אז $\bar A=\mathrm{SAT}$ היא NP-קשה, ולכן $\overline{\mathrm{SAT}}$ היא coNP-קשה. יחד עם $\overline{\mathrm{SAT}}\in\mathrm{coNP}$ (מהגדרה, כי $\mathrm{SAT}\in\mathrm{NP}$), $\overline{\mathrm{SAT}}$ היא coNP-שלמה. --- ## הערות מהשיעור - *(האסופה של הערות המרצה על הדרנדומיזציה עצמה — "משתנה מקרי הוא פונקציה, לא מספר" [00:04:17], היתרון בפשטות של אלגוריתמים אקראיים [00:09:35], מדוע ה-$\tfrac78$ שורד גם כשהנוסחה חדלה להיות 3ECNF [00:22:14], והמשתנה המנוון באיטרציה האחרונה [00:26:33] — שייכת לשיעור 20; ראו שם.)* - **שגיאת תמלול שכדאי להכיר.** התמלול האוטומטי כותב "אם NP מוכל בBPP אז NP מוכל בP". זה שגוי: הסיכום כותב $\mathrm{NP}\subseteq\mathrm{RP}$, וכל הדיון שבא מיד אחריו [00:31:21]–[00:33:57] עוסק בהבדל בין טעות דו-צדדית לחד-צדדית, כלומר בין BPP ל-RP — ולא ב-P. - **[00:30:20] טענת הכלה מתחילה ב"לכל".** המרצה עצר את הכיתה על ניסוח: *"ברגע שתצייתו לתבנית, הסיכוי שלכם לטעות יורד משמעותית."* ההוכחה של $\mathrm{NP}\subseteq\mathrm{RP}$ חייבת להתחיל ב"תהא $L\in\mathrm{NP}$", לא ב"קיים". - **[00:33:27] "התחילו מההבדל התחבירי."** לפני שמחפשים אינטואיציה, משווים את הסימנים: BPP מול RP נבדלות בשתי אותיות, והקבועים $\tfrac12,\tfrac23$ אינם המהות (אמפליפיקציה משנה אותם). מה שנשאר הוא **צדדיות הטעות**. *"הפורמליזם הוא כאן כדי לשמור עלינו מטעויות."* - **[00:40:17] איזו תכונה נדרשת בכל כיוון.** בשקילות $\mathrm{NP}\subseteq\mathrm{BPP}\iff\mathrm{SAT}\in\mathrm{BPP}$ — כיוון אחד

משתמש ב-NP-**קושי** בלבד, השני בשייכות $\mathrm{SAT}\in\mathrm{NP}$. המרצה ביקש במפורש: אל תזרקו "כי SAT היא NP-שלמה" בלי לומר איזו חצי-תכונה נחוצה איפה. *"אני יודע מתי סתם זורקים דברים; זה ניכר."* - **[00:46:09] לא כל הבעיות ה-NP-שלמות נראות אותו הדבר.** ברזולוציה של NP-קושי הן זהות, אבל self-reducibility אינה ידועה לכולן, ובקירוביות יש ביניהן פערים עצומים (VC עם קירוב 2, מול TSP שקירוב כלשהו שלה גורר $\mathrm{P}=\mathrm{NP}$; ראו שיעור 13). - **[01:06:37] ניסוח מיטבי של משפט.** *"כשאני מנסח statement, אני אדאג שהתנאי יהיה כמה שיותר חלש והתוצאה כמה שיותר חזקה."* לכן נכתב "אם $\mathrm{SAT}\in\mathrm{BPP}$ אז $\mathrm{NP}\subseteq\mathrm{RP}$" ולא "אם $\mathrm{NP}\subseteq\mathrm{BPP}$ אז $\mathrm{SAT}\in\mathrm{RP}$", למרות ששתיהן שקולות. - **[01:26:19] "it all boils down" — הרגע היפה של השיעור.** כשסטודנט התקשה, המרצה מחק את הלוח: *"שכח מהאלגוריתם. אני נותן לך נוסחה והשמה. אם ההשמה מספקת, אתה מקבל; אחרת אתה דוחה. אם הנוסחה לא הייתה ספיקה, האם יש מצב שתקבל?"* — ה-one-sidedness כולה יושבת על שלב 3 הדטרמיניסטי, ולא על שום דבר בבנייה שלפניו. - **[01:31:30] למה חוסמים את המשלים.** *"בהסתברות יש לי הרבה יותר כלים לחסום דברים מלמעלה"* (מרקוב, צ'רנוף, חסם האיחוד). לכן כדי לחסום $\Pr(B)$ מלמטה חוסמים את $\Pr(\bar B)$ מלמעלה. - **[01:40:27] הסיבה שלא העלמנו משתנים.** *"אם הסתברות ההצלחה תלויה במספר המשתנים, אני לא רוצה להקטין את מספר המשתנים, כי אני לא רוצה לשנות את ההסתברות."* זו התשובה לחידה שהושארה פתוחה שעה שלמה קודם. - **[01:39:23] שאלה שנשאלה ותשובתה.** אם הסתברות ההצלחה הייתה $\tfrac12$ בדיוק (בלי "bounded away") לא היה אפשר לעשות דבר — זהו תרגיל בית. - **[01:47:35] אזהרת בלבול.** coNP הוא **אוסף המשלימים** ולא **המשלים של האוסף**. *"בדיוק כמו R ו-coR: coR זה לא המשלים של R." - **[02:04:33] גישת ה-high-level.** *"הוכחתי מספיק דברים בחיינו כדי שלא אצטרך לרדת לרמת המכונה. אם ה-high-level לא עובד, אני אפתח את מכסה המנוע."* כל הוכחות ה-coNP-קשה בשיעור נעשות ברמת סגירויות ורדוקציות, בלי מכונות. - **[02:05:37] הכנה לשיעור הבא.** המרצה ביקש לחזור על הרדוקציות מ-SAT ל-IS ול-MAXIS מתרגיל הבית, כי השיעור הבא יראה ש-MAXIS היא גם NP-קשה וגם coNP-קשה — יישום ישיר של משפט 9. --- ## פערים בין הסיכום להקלטה - **מקור:** עמודים 1–2 בסיכום מול גבול הבעלות בין השיעורים. **הפער:** שני העמודים הראשונים של הסיכום של שיעור 21 מכילים את אלגוריתם הדרנדומיזציה ל-3ECNF ואת הוכחת נכונותו במלואם, אך בהקלטה החומר הזה נלמד לפני [00:27:36] ונכתב בשיעור 20. **ההכרעה:** האלגוריתם והתוצאה מנוסחים כאן במדויק ומצוטטים בהפניה לשיעור 20; מה שמוכח כאן במלואו הוא רק אריזתם כיחס קירוב ($\mathrm{OPT}\le m$, חוקיות הפלט, המוסכמה). מתועד גם ב-`open_questions`. - **מקור:** ההקלטה [00:29:48] מול הסיכום עמוד 2. **הפער:** התמלול האוטומטי כותב "אם NP מוכל בBPP אז NP מוכל בP", בעוד שהסיכום כותב $\mathrm{NP}\subseteq\mathrm{RP}$. **ההכרעה:** הסיכום. ההקשר בהקלטה מכריע חד-משמעית לטובתו: מיד אחר כך [00:31:21]–[00:33:57] מנוהל דיון שכולו על ההבדל בין טעות דו-צדדית לחד-צדדית ועל כך ש"ההבדל בין

BPP ל-RP הוא שתי אותיות" — טיעון חסר משמעות אילו המסקנה הייתה P. - **מקור:** ההקלטה [00:53:18] ו-[01:40:27]. **הפער:** הסיכום מציג את הוספת הסגרי היחידה (במקום הצבה) בלי נימוק. **ההכרעה:** הנימוק — שמירת מספר המשתנים בגלל שגיאה התלויה ב-n — נכתב בגוף בשני המקומות, כפי שהמרצה חשף אותו רק בהמשך. - **מקור:** הסיכום, עמודים 4–5. **הפער:** האות A משמשת גם למאורע "$\hat M$ מקבלת את φ" וגם לשפה $A\in\mathrm{NP}$ בשורות הסיום — התנגשות סימונים ממש בתוך אותה הוכחה. **ההכרעה:** נשמרו A,B למאורעות (כמו בסיכום ובהקלטה), והשפה סומנה L. מתועד גם ב-`open_questions`. - **מקור:** הסיכום, עמוד 4. **הפער:** הסתברות השגיאה נכתבת כ-$1-\frac{1}{2(n+1)}$ עם n = מספר המשתנים, בעוד שמשפט האמפליפיקציה מנוסח לפי אורך הקלט. **ההכרעה:** הושלם בגוף (הערה בתוך הוכחת משפט 4): בוחרים $q(\ell)=2(\ell+1)$, ומכיוון ש-$|n\le|\psi|$ החסם הדרוש נובע — כולל עבור נוסחאות העזר, שלהן אותם n משתנים. - **מקור:** הסיכום, עמוד 5. **הפער:** נכתב $Pr(\bar B_i)\le\frac{1}{2(n+1)}$ בלי לטפל בכך שהנוסחה הנשאלת באיטרציה i תלויה בתשובות הקודמות. **ההכרעה:** הושלם בגוף בהערה — התניה על ההיסטוריה + נוסחת ההסתברות השלמה, תוך שימוש בכך שכל קריאה משתמשת במטבעות טריים. - **מקור:** הסיכום, עמוד 3. **הפער:** האינדוקציה "קיימת השמה מספקת המשלימה את v" נרשמת במילה "אינדוקציה" בלבד. **ההכרעה:** נכתבה במלואה, כולל הצעד הלא-אוטומטי שדחייה של הענף $x_i=1$ יחד עם ספיקות הנוסחה מכריחה קיום השמה מספקת עם $x_i=0$. - **מקור:** ההקלטה [02:01:20]–[02:02:26]. **הפער:** המרצה פתח את הוכחת משפט 9 מהכיוון ההפוך מזה שרצה, ותיקן לאחר שאלת סטודנט. **ההכרעה:** הגוף עוקב אחרי הניסוח והכיוון של הסיכום, שהם הנכונים; התקלה מתועדת כהערה מתחת למשפט 9. - **מקור:** הסיכום, עמוד 6. **הפער:** ליד השימוש בסגירות coNP לרדוקציות מסומן "צ" (צריך להוכיח) והמרצה השאיר זאת כתרגיל בית [01:59:43]; אין הוכחה בשום מקור. **ההכרעה:** ההוכחה נכתבה במלואה כתרגיל 3 בסעיף הדוגמאות. - **מקור:** הסיכום, עמוד 6. **הפער:** כיוון ($\Leftarrow$) של משפט 9 נכתב "בדומה" בלבד. **ההכרעה:** נכתב במלואו. - **מקור:** ההקלטה, כותרת הקובץ. **הפער:** תמלול 26 מתויג "שיעור 20" בעוד שתוכנו הוא שיעור 21 לפי מספור הסיכומים. **ההכרעה:** התיוג מתועלם, וההצמדה נעשתה לפי התוכן; מתועד ב-`sources`. - **מקור:** התמלול השני (27). **הפער:** אינו מכסה חומר של שיעור זה כלל — הוא של שיעור 22 (MAXIS). **ההכרעה:** נרשם עם `coverage: none` והערה; ממנו נלקחה רק ההצבעה על כך שטענות ה-coNP כאן משמשות מיד בשיעור הבא. - לא הופיע בסיכום ולא בהקלטה: תוצאת אי-קרִיבוּת מתאימה (חסם תחתון של $\tfrac78+\varepsilon$). **ההכרעה:** לא נכתבה כאן, כדי לא להכניס חומר שאינו מהמקורות. --- ## סיכום ונקודות למבחן **מה לזכור בעל פה.** 1. **$\mathrm{MAX\text{-}3ECNF}$:** האלגוריתם הדטרמיניסטי של שיעור 20 מחזיר השמה המספקת m הסגרים; בצירוף $\mathrm{OPT}\le m$ זה קירוב ביחס $\alpha=\tfrac78$ במוסכמת המקסימיזציה $\mathrm{ALG}\ge\alpha\cdot\mathrm{OPT}$. הצעד $\mathrm{OPT}\le m$ הוא כל ההבדל בין ערבות מוחלטת ליחס קירוב. 2. **SAT היא self-reducible:** אלגוריתם פולינומי להכרעה $\Longrightarrow$ אלגוריתם פולינומי לחיפוש. אינה רדוקציית מיפוי. 4. **אם $\mathrm{SAT}\in\mathrm{BPP}$ אז

$\mathrm{NP}\subseteq\mathrm{RP}$.** ההוכחה: אמפליפיקציה לשגיאה $\frac{1}{2(n+1)}$ + אותה בנייה כמו ברדוקציה העצמית + חסם איחוד על $n+1$ קריאות + בדיקה דטרמיניסטית בסוף. 5. **$\mathrm{coP}=\mathrm{P}$, $\mathrm{coNP}=\{\bar A\mid A\in\mathrm{NP}\}$**, $\mathrm{P}\subseteq\mathrm{NP}\cap\mathrm{coNP}$, $\mathrm{NP}=\mathrm{coNP}\iff\mathrm{NP}\subseteq\mathrm{coNP}\iff\mathrm{SAT}\in\mathrm{coNP}$ ו-A היא coNP-קשה $\bar A$ iff היא NP-קשה. **מלכודות סטנדרטיות.** - לכתוב את יחס הקירוב במוסכמה ההפוכה ($\alpha=\frac87$). בבעיית מקסימום המוסכמה היא $\mathrm{ALG}\ge\alpha\cdot\mathrm{OPT}$ עם $0<\alpha\le1$. - לבלבל בין coNP ל"המשלים של NP". - לומר "SAT היא NP-שלמה" בלי לציין אם השתמשתם בNP-**קושי** או בשייכות ל-NP — במשפט 3 כל כיוון משתמש בחצי אחרת. - לנסות לחסום $\Pr(\bar B)$ במכפלה. המאורעות אינם בלתי תלויים; חסם האיחוד הוא הכלי. - לשכוח את הצעד $\mathrm{OPT}\le m$ ולהסיק ישירות "$\mathrm{ALG}\ge\frac78 m$ ולכן קירוב $\frac78$". - להתחיל הוכחת הכלה ב"קיים" במקום ב"לכל". **צ'ק-ליסט — מה סטודנט אמור לדעת לעשות אחרי השיעור.** - להוכיח את יחס הקירוב $\frac78$ בשני החלקים: חוקיות הפלט, וההשוואה ל-OPT דרך $\mathrm{OPT}\le m$ — בהינתן הערבות $\mathrm{ALG}\ge\frac78 m$ משיעור 20. - לרשום את אלגוריתם הרדוקציה העצמית ולהוכיח את האינווריאנטה באינדוקציה — כולל הצעד של הענף השלילי. - לשחזר את ההוכחה ש-$\mathrm{SAT}\in\mathrm{RP}$: לזהות איפה נכנסת האמפליפיקציה, למה n נשמר, מהם A ו-B, למה $B\subseteq A$, ואיפה בדיוק מובטח שאין false positives. - להוכיח את כל טענות ה-coNP ברמת סגירויות ורדוקציות, בלי לרדת לרמת המכונה, כולל "אותה רדוקציה בדיוק עובדת גם למשלימים". > **הערה שלא נאמרה בהרצאה:** מכיוון שידוע גם $\mathrm{NP}\subseteq\mathrm{RP}$, המסקנה של משפט 4 שקולה למעשה ל-$\mathrm{NP}=\mathrm{RP}$. זה לא נאמר בשיעור ולא נכתב בסיכום, ולכן אינו חלק מהחומר הנדרש. --- *הסיכום הכתוב שעליו מבוסס קובץ זה נכתב על ידי גיא סופר.*

שאלות שנשארו פתוחות

ה-slug approximation-max-3ecnf מתאר רק את הפתיחה; עיקר השיעור (SAT ∈ BPP ⟹ NP ⊆ RP, ו-coNP) אינו קירוב כלל.

עמודים 1–2 בסיכום של שיעור 21 מכילים את אלגוריתם הדרנדומיזציה ל-3ECNF ואת הוכחת נכונותו במלואם, אך אלה נלמדו בהקלטה לפני [00:27:36] ונכתבו בשיעור 20; כאן הם מוצגים כהפניה, ורק אריזתם כיחס קירוב מוכחת בגוף.

בעמוד 4–5 בסיכום האות A משמשת גם למאורע 'M̂ מקבלת את φ' וגם לשפה A ∈ NP בשורות הסיום; כאן השפה סומנה L כדי למנוע התנגשות.

הסיכום מנסח את הגברת ההסתברות כ-(1−1/2(n+1)) לפי מספר המשתנים n; פורמלית האמפליפיקציה נותנת חסם לפי אורך הקלט, וההשלמה מופיעה בגוף (|φ| ≤ n).

MaxIS 22 — הקבוצה הבלתי תלויה המקסימלית: NP-קשה וגם coNP-קשה

הבעיה MaxIS שואלת האם הגודל המקסימלי של קבוצה בלתי תלויה בגרף הוא בדיוק k; מפני שזו טענת "קיים וגם לכל" היא יוצאת גם NP-קשה (רדוקציה מ-SAT) וגם coNP-קשה (רדוקציה מ-$\overline{\mathrm{IS}}$), ומכאן ש-$\mathrm{MaxIS}\in\mathrm{NP}\cup\mathrm{coNP}$ אם ורק אם $\mathrm{NP}=\mathrm{coNP}$.

ביטחון: high

בקצרה

מגדירים את MaxIS: בהינתן גרף G ומספר k, האם **הגודל המקסימלי** של קבוצה בלתי תלויה ב-G הוא k. זו איננה בעיית IS הרגילה — היא מחביאה בתוכה טענת **קיום** וטענת **לכל** גם יחד.
מוכיחים $\mathrm{SAT}\le_p\mathrm{MaxIS}$ ולכן MaxIS היא **NP-קשה**. זו אותה רדוקציה מוכרת של SAT ל-IS (קודקוד לכל ליטרל, קליקה בתוך פסוקית, קשת בין ליטרל לשלילתו), אבל הפעם צריך להוכיח גם את **חסם המקסימליות** $\alpha(G_\varphi)\le m$.
מוכיחים $\overline{\mathrm{IS}}\le_p\mathrm{MaxIS}$ ולכן MaxIS היא גם **coNP-קשה**. הרדוקציה: מוסיפים $k-1$ קודקודים חדשים ומחברים כל אחד מהם לכל קודקוד ישן, ומחזירים $\langle\hat{G},k-1\rangle$.
המסקנה החריפה: $\mathrm{MaxIS}\in\mathrm{NP}\cup\mathrm{coNP}$ **אם ורק אם** $\mathrm{NP}=\mathrm{coNP}$. כלומר עצם ההוכחה ש-$\mathrm{MaxIS}$ בעלת אימות קצר (או שמשלימתה כזו) תפתור בעיה פתוחה. בפרט **אסור** לקרוא ל-MaxIS "NP-שלמה" — אין לנו מושג אם היא ב-NP.
לעומת זאת $\mathrm{IS}\in\mathrm{P}\Rightarrow\mathrm{MaxIS}\in\mathrm{P}$ בקלות (סריקה על k), כך שהקושי כאן הוא קושי של **מבנה הטענה**, לא של כמות החישוב.
לאורך כל השיעור המרצה מלמד סגנון: טענת "לכל" מתחילה תמיד ב"תהא/יהי"; להוכחה יש גישה להשמה ולקבוצה — לאלגוריתם אין; והוכחת קיום אינה חייבת להיות אלגוריתמית.

רקע ותלויות

השיעור הזה כמעט ולא מוסיף מכניזם חדש — הוא מרכיב יחד ארבעה דברים שכבר ראינו. כדי שלא תצטרכו לקפוץ, הנה כולם במלואם.
משיעור 7 — קבוצה בלתי תלויה, IS, ורדוקציות. בגרף $G=(V,E)$, קבוצה $U\subseteq V$ נקראת **בלתי תלויה** (independent set) אם לכל $x,y\in U$ מתקיים $xy\notin E$. השפה IS מכילה את כל הזוגות $\langle G,k\rangle$ שבהם G גרף, $k\in\mathbb{N}$, וקיימת ב-G קבוצה בלתי תלויה בגודל לפחות k. נסמן $\alpha(G)$ את הגודל המקסימלי של קבוצה בלתי תלויה ב-G (הסימון α לא הופיע בסיכום; הוא מקוצר כאן לנוחות). כלומר $\langle G,k\rangle\in\mathrm{IS}\iff\alpha(G)\ge k$.
רדוקציית זמן פולינומי: $A\le_p B$ אם קיימת f הניתנת לחישוב בזמן פולינומי כך שלכל x מתקיים $x\in A\iff f(x)\in B$. **כיוון החץ במילים:** $A\le_p B$ אומר ש-B היא **הקשה יותר** — כל מי שיודע לפתור את B יודע לפתור את A. בהקלטות ובעל פה הכיוון הזה מתהפך כל הזמן, ולכן בכל

פעם שנכתוב רדוקציה נאמר במפורש ממי למי.
L היא **NP-קשה** אם לכל $A \in \mathrm{NP}$ מתקיים $A \le_p L$, והיא **NP-שלמה** אם בנוסף $L \in \mathrm{NP}$. באופן סימטרי, L היא **coNP-קשה** אם לכל $A \in \mathrm{coNP}$ מתקיים $A \le_p L$.
סגירות: אם $A \le_p B$ ו-$B \in \mathrm{NP}$ אז $A \in \mathrm{NP}$; אותו דבר עבור P. וכן $\le_p$ **טרנזיטיבית**: $A \le_p B \le_p C \Rightarrow A \le_p C$. משתי אלה נובע הכלל שנשתמש בו שוב ושוב: כדי להראות ש-L היא NP-קשה מספיק להראות $B \le_p L$ עבור B אחת שכבר ידועה כ-NP-קשה.
משיעור 9 — קוק–לוין. SAT היא NP-שלמה. בפרט היא NP-קשה, ולכן רדוקציה **מ-SAT אל** בעיה כלשהי מוכיחה שהבעיה ההיא NP-קשה. כמו כן ראינו את השרשרת $\mathrm{SAT} \le_p 3\mathrm{SAT} \le_p \mathrm{IS}$, ולכן IS היא NP-שלמה.
משיעור 10 — "לפחות k" מול "בדיוק k". קבוצה בלתי תלויה היא תכונה **תורשתית**: כל תת-קבוצה של קבוצה בלתי תלויה היא בלתי תלויה. לכן אם יש ב-G קבוצה בלתי תלויה בגודל $\ge k$, אפשר להוריד ממנה קודקודים עד לגודל k בדיוק. מכאן:
קיימת ב-G קבוצה בלתי תלויה בגודל לפחות k אם ורק אם קיימת ב-G קבוצה בלתי תלויה בגודל בדיוק k.
בשיעור הזה נשתמש בשוויון הזה בלי הודעה מוקדמת, בשני הכיוונים.
משיעור 21 — מחלקות משלימות. $\mathrm{coNP} = \{L \mid \overline{L} \in \mathrm{NP}\}$. שלוש עובדות משם, שכולן ישוחזרו כאן במלואן במקום שבו הן משמשות:
למת המשלימים: f היא רדוקציה מ-A ל-B אם ורק אם אותה f עצמה היא רדוקציה מ-$\overline{A}$ ל-$\overline{B}$ (הוכחה בלמה 3.1 להלן).
סגורה תחת $\le_p$ coNP: אם $B \in \mathrm{coNP}$ ו-$A \le_p B$ אז $A \in \mathrm{coNP}$.
אם קיימת שפה שהיא **גם** NP-קשה **וגם** שייכת ל-coNP (או סימטרית: גם coNP-קשה וגם ב-NP), אז $\mathrm{NP} = \mathrm{coNP}$.
הערת רקע על ההקלטה. ההקלטה הרלוונטית ([27], video_id: `AGUI69L7aDA`) נפתחת מיד בחומר של השיעור הזה — אין בה קטע חזרה. בסוף ההקלטה הקודמת המרצה אף מודיע במפורש: "השיעור הבא יעסוק ב-MaxIS, נראה שהיא coNP-קשה גם".

הגדרות
הגדרה 1: הבעיה MaxIS
קלט: גרף $G = (V, E)$ ומספר $k \in \mathbb{N}$.
שאלה: האם הגודל המקסימלי של קבוצה בלתי תלויה ב-G הוא k?
כשפה: $\mathrm{MaxIS} = \{\langle G, k\rangle \mid \alpha(G) = k\}$.
הפירוק שבסיכום (שתי ההערות המודגשות בעמוד 1). הדרישה "$\alpha(G) = k$" נראית תמימה, אבל היא **מחביאה בתוכה שתי טענות מסוגים שונים**, והסיכום מסמן אותן בשני חצים:
טענת קיום: קיימת ב-G קבוצה בלתי תלויה בגודל k;
וגם טענת "לכל": כל קבוצה בלתי תלויה ב-G היא בגודל לכל היותר k.

זו הנקודה שכל השיעור נשען עליה. המרצה מתעכב עליה [00:01:36]–[00:03:43]: "מקסימום זה לא משהו שאני רוצה לעבוד איתו — אני רוצה לפרק את זה לפרימיטיבים". שימו לב גם לסדר: **קודם** אומרים שהקבוצה קיימת, ורק **אחר כך** מדברים עליה. סטודנט התחיל את הניסוח ב"קבוצה אחרת קטנה ממנה", והמרצה עצר: "מי זה 'ממנה'? אין פה קבוצה עדיין" [00:01:36].

דוגמה. $G = K_3$ (משולש על a, b, c). כל שני קודקודים מחוברים, ולכן קבוצה בלתי תלויה מכילה קודקוד אחד לכל היותר, ו-$\{a\}$ אכן בלתי תלויה. לכן $\alpha(K_3) = 1$, כלומר $\langle K_3, 1\rangle \in \mathrm{MaxIS}$.

אי-דוגמה (וזה בדיוק ההבדל מ-IS). $\langle K_3, 0\rangle \notin \mathrm{MaxIS}$ כי $\alpha(K_3) = 1 \neq 0$, וגם $\langle K_3, 2\rangle \notin \mathrm{MaxIS}$ כי $1 \neq 2$. לעומת זאת $\langle K_3, 0\rangle \in \mathrm{IS}$ (הקבוצה הריקה בלתי תלויה) וגם $\langle K_3, 1\rangle \in \mathrm{IS}$.

כלומר IS "סובלנית כלפי מטה" ו-MaxIS לא — ולכן, שלא כמו ב-IS, הטיעון התורשתי משיעור 10 **אינו** מאפשר להחליף כאן "$=k$" ב-"$\geq k$".

הגדרה 2: הפירוק של MaxIS לחיתוך שתי שפות

הפירוק שלמעלה הוא בדיוק חיתוך של שתי שפות (עמוד 5 בסיכום): $\mathrm{MaxIS} = \mathrm{IS} \cap \mathrm{IS}^{\leq}$, כאשר IS היא אוסף הזוגות $\langle G, k\rangle$ שבהם קיימת ב-G קבוצה בלתי תלויה בגודל k, ו-$\mathrm{IS}^{\leq}$ היא אוסף הזוגות $\langle G, k\rangle$ שבהם כל קבוצה בלתי תלויה ב-G היא בגודל $\leq k$.

השוויון של הגורם השמאלי ל-IS הוא בדיוק הלמה התורשתית משיעור 10 ("בגודל k" $\equiv$ "בגודל לפחות k"). הגורם הימני, $\mathrm{IS}^{\leq}$, הוא "כמעט $\overline{\mathrm{IS}}$": המרצה מנסח זאת [01:26:30] כ"עד כדי קוסמטיקה", כי $\overline{\mathrm{IS}^{\leq}} = \{\langle G, k\rangle \mid \alpha(G) \geq k+1\}$ וזו בדיוק IS עם $k+1$ במקום k. בפרט $\mathrm{IS}^{\leq} \in \mathrm{coNP}$ — ראו את הוכחת משפט 4.

למה זה חשוב. MaxIS היא חיתוך של שפה ב-NP עם שפה ב-coNP. חיתוך כזה, במצב הידע הנוכחי, אינו יושב באף אחת מהמחלקות. כל השיעור הוא בעצם פירוט של ההערה הזאת.

הגדרה 3: הגרף G_φ — הבנייה של הרדוקציה מ-SAT

תהא φ נוסחה בצורת CNF עם m פסוקיות. נגדיר גרף $G_\varphi = (V, E)$:

קודקודים. לכל פסוקית ב-φ, ולכל ליטרל בפסוקית, ניצור **קודקוד**. נסמן ב-V את קבוצת הקודקודים.

שימו לב [00:08:58]: ליטרל שמופיע בכמה פסוקיות מקבל **כמה קודקודים**, אחד לכל מופע. הקודקוד מייצג *מופע*, לא משתנה.

קשתות אדומות (בתוך פסוקית). לכל פסוקית ב-φ, נחבר בקשת כל שני קודקודים שנוצרו מאותה פסוקית. כלומר כל פסוקית הופכת ל**קליקה**.

קשתות שחורות (בין ליטרל לשלילתו). לכל ליטרל ב-φ, נחבר בקשת את הקודקודים המתאימים לו עם הקודקודים המתאימים לשלילתו.

הפלט של הרדוקציה הוא $\langle G_\varphi, m\rangle$.

האינטואיציה מאחורי כל צבע [00:13:53]:

הקשתות **האדומות** מבטיחות שקבוצה בלתי תלויה תיקח **לכל היותר קודקוד אחד מכל פסוקית**. זה מה שיחסום את המקסימום מלמעלה ב-m.

הקשתות **השחורות** מבטיחות שקבוצה בלתי תלויה לא תיקח בו-זמנית ליטרל ואת שלילתו — כלומר שהבחירה שלה **עקבית** ומתורגמת להשמה חוקית.

הערה: בסיכום, הקשתות "בין ליטרל לשלילתו" מצוירות בעיפרון **כחול** בציור שבעמוד 1, אך בטקסט ההוכחה (עמודים 2–3) הן נקראות "קשתות שחורות" — כמו בהרצאה. כאן שימרנו את המינוח **אדומות/שחורות** לכל אורך הקובץ.

משפטים והוכחות

משפט 1: אם $\mathrm{IS} \in \mathrm{P}$ אז $\mathrm{MaxIS} \in \mathrm{P}$

זו לא טענה עמוקה, והמרצה פותח בה [00:04:14] כדי לנקות את השאלה "האם MaxIS קשה יותר בגלל שיש בה יותר חישוב". התשובה: לא, ההבדל הוא במבנה הלוגי בלבד.

טענה. אם קיים אלגוריתם דטרמיניסטי A המכריע את IS בזמן $t(n)$, אז קיים אלגוריתם המכריע את MaxIS בזמן $O(|V| \cdot t(n) + n)$. בפרט אם t פולינומי אז גם זמן הריצה של השני פולינומי.

הוכחה. בהינתן $\langle G, k \rangle$ עם $G = (V, E)$:

לכל $j = 0, 1, 2, \ldots, |V|$, נריץ את A על $\langle G, j \rangle$.

נסמן ב-j^{*} את ה-j הגדול ביותר שעבורו A ענתה "כן".

נחזיר "כן" אם ורק אם $j^{*} = k$.

נאותות. לפי ההגדרה A עונה "כן" על $\langle G, j \rangle$ אם ורק אם $\alpha(G) \geq j$. לכן קבוצת ה-j-ים שעבורם התשובה "כן" היא בדיוק $\{0, 1, \ldots, \alpha(G)\}$ — קטע רצוף שמתחיל ב-0 (הקבוצה הריקה תמיד בלתי תלויה) ונגמר ב-$\alpha(G)$. מכאן ש-j^{*} מוגדר היטב ו-$j^{*} = \alpha(G)$. לכן האלגוריתם עונה "כן" אם ורק אם $\alpha(G) = k$, כלומר אם ורק אם $\langle G, k \rangle \in \mathrm{MaxIS}$.

זמן ריצה. $|V| + 1$ קריאות ל-A, כל אחת על קלט שאורכו $O(n)$, ועוד עבודה לינארית לניהול הלולאה. סך הכול $O(|V| \cdot t(n) + n)$. $\blacksquare$

הערה: בהרצאה הניסוח היה "אני עובר על כל ה-k מאחד עד n ורואה מתי הפעם הראשונה שאני מקבל 'לא'" [00:04:48]. זו בדיוק אותה סריקה, רק מלמטה למעלה. הפירוט של המונוטוניות — שקבוצת התשובות "כן" היא קטע רצוף — נאמר בהרצאה במשפט אחד, וכאן הוא כתוב מפורשות, כי בלעדיו אין הצדקה ל"הפעם הראשונה שקיבלתי 'לא'".

משפט 2: $\mathrm{SAT} \leq_p \mathrm{MaxIS}$, ולכן MaxIS היא NP-קשה

הכיוון במילים. מבצעים רדוקציה **מ**-SAT (הבעיה שכבר ידוע שהיא NP-קשה, משיעור 9) **אל** MaxIS. התוצאה: MaxIS קשה לפחות כמו SAT.

הרדוקציה. בהינתן נוסחה φ בצורת CNF עם m פסוקיות, נחזיר את $\langle G_\varphi, m \rangle$ כפי שהוגדר בהגדרה 3.

שימו לב שהקלט הוא **CNF כללי** — לא $3\mathrm{CNF}$. פסוקית יכולה להיות מכל גודל, והמרצה בחר בכוונה דוגמה שבה פסוקית אחת היא בגודל 2 "כדי שלא יבלבל אתכם שזה חייב להיות שלוש" [00:12:16].

2א. ניתוח זמן ריצה

שלב 1 (יצירת הקודקודים) דורש $O(|\varphi|)$ צעדים: עוברים פעם אחת על הנוסחה ומייצרים קודקוד לכל מופע ליטרל. בפרט מתקיים $|V| \leq |\varphi|$ — מספר הקודקודים חסום באורך הנוסחה, כי כל קודקוד נולד ממופע ליטרל אחד.

שלבים 2 ו-3 (הקשתות) דורשים $O\left(\binom{|V|}{2}\right)$ צעדים: עוברים על כל **הזוגות** של קודקודים ומחליטים לכל זוג אם להוסיף קשת (אדומה אם באו מאותה פסוקית, שחורה אם הם ליטרל ושלילתו). לכל זוג ההחלטה היא בדיקה מקומית בזמן קבוע. ומכיוון ש-$\binom{|V|}{2} = \frac{|V|(|V|-1)}{2} = O(|V|^2)$, ובפרט $|V| \le |\varphi|$, זה $O(|\varphi|^2)$.

סך הכול: $O(|\varphi|^2)$, כלומר הרדוקציה **פולינומית באורך הקלט**.

> **הערה:** בהרצאה נשאלה שאלה [00:17:40] "למה $\binom{V}{2}$ הופך ל-V בריבוע?" והתשובה: $\binom{n}{2} = \frac{n(n-1)}{2}$. באופן כללי $\binom{n}{k} \le n^k$, ולכל k קבוע זה פולינומי.

2ב. ניתוח נאותות — כיוון $\Longrightarrow$

תהא φ נוסחה בצורת CNF, ונסמן ב-$\langle G_\varphi, m\rangle$ את פלט הרדוקציה. **נניח $\varphi \in \mathrm{SAT}$.**

אזי קיימת השמה $\mathcal{V}$ המספקת את φ. לפי ההגדרה של סיפוק CNF:

לכל פסוקית ב-φ **קיים** לפחות ליטרל אחד ש-$\mathcal{V}$ נותנת לו את הערך 1.

> **הערה — סדר הכמתים** [00:19:52]. המרצה עצר כאן במפורש: הניסוח הוא "**לכל** פסוקית **קיים** ליטרל", ולא "**קיים** ליטרל **לכל** פסוקית". ההיפוך היה טענה חזקה בהרבה (ליטרל אחד שמספק את כל הנוסחה) ופשוט לא נכונה.

נסמן ב-U קבוצה המורכבת מקודקוד אחד כזה מכל פסוקית: מכל פסוקית בוחרים ליטרל אחד שהשמתו 1, ולוקחים את הקודקוד המתאים לו. מכיוון שיש m פסוקיות ובחרנו קודקוד אחד מכל אחת, ומכיוון שקודקודים של פסוקיות שונות שונים זה מזה (כל קודקוד נוצר ממופע יחיד), $|U| = m$.

טענה: U בלתי תלויה. יהיו $x, y \in U$ שונים. צריך להראות שאין ביניהם קשת. יש שני סוגי קשתות בלבד:

קשת אדומה? ב-U יש בדיוק קודקוד אחד המשויך לכל פסוקית, ולכן x ו-y נוצרו **מפסוקיות שונות**. קשת אדומה מחברת רק קודקודים מאותה פסוקית, ולכן אין ביניהם קשת אדומה.

קשת שחורה? לפי בחירת U, ההשמה $\mathcal{V}$ נותנת **לשני** הליטרלים המתאימים ל-x ול-y את הערך 1. אבל ליטרל ושלילתו לעולם לא מקבלים שניהם 1 תחת אותה השמה. לכן לא ייתכן ש-x ו-y הם ליטרל ושלילתו, ולכן אין ביניהם קשת שחורה.

מכאן ש-U בלתי תלויה, וקיבלנו קבוצה בלתי תלויה בגודל m ב-G_φ.

עדיין לא סיימנו [00:25:12]. עד כאן הוכחנו רק את חצי הטענה — את חלק ה"קיים". זה בדיוק הנקודה שבה תרגיל הבית על $\mathrm{SAT} \le_p \mathrm{IS}$ מסתיים; כאן צריך גם את חלק ה"לכל".

טענה 2.1 (חסם המקסימליות): כל קבוצה בלתי תלויה ב-G_φ היא בגודל לכל היותר m.

הוכחה (הגרסה הישירה, [00:29:26]). תהא $\hat{U}$ קבוצה בלתי תלויה ב-G_φ. כל שני קודקודים המשויכים לאותה פסוקית מחוברים בקשת אדומה, ומכיוון ש-$\hat{U}$ בלתי תלויה, אין ב-$\hat{U}$ שני קודקודים מאותה פסוקית. לכן $\hat{U}$ מכילה לכל היותר קודקוד אחד מכל פסוקית, ויש m פסוקיות, ולכן $|\hat{U}| \le m$.

הוכחה (הגרסה בשלילה, כפי שנרשמה בסיכום). נניח בשלילה $|\hat{U}| > m$. לפי **עקרון שובך היונים**, מכיוון שיש m פסוקיות ו-$|\hat{U}| > m$ קודקודים, קיימת פסוקית שעבורה קיימים שני ליטרלים ממנה שהקודקודים המתאימים להם שייכים ל-$\hat{U}$. אבל שניהם מאותה פסוקית, ולכן יש ביניהם קשת אדומה — בסתירה לכך ש-$\hat{U}$ בלתי תלויה. $\square$

הערה מתודית חשובה [00:26:14]–[00:29:56]. סטודנטית הציעה לפתוח את ההוכחה ב"נניח בשלילה שיש קבוצה גדולה יותר", והמרצה עצר: הטענה שרוצים להוכיח היא **טענת "לכל"** ("לכל קבוצה בלתי תלויה..."), ולכן ההוכחה **חייבת** להתחיל ב"תהא $\hat{U}$ קבוצה בלתי תלויה". רק אחרי שהמשתנה הוצג אפשר להניח בשלילה. "אם הטענה מתחילה ב'לכל', לעולם ההוכחה תתחיל ב'יהי/תהא'... זה מה שמציג לי את המשתנה שאני אעבוד איתו אחר כך."

שילוב שתי הטענות: קיימת קבוצה בלתי תלויה בגודל m, וכל קבוצה בלתי תלויה היא בגודל $\leq m$.
לכן $\alpha(G_\varphi) = m$, כלומר $\langle G_\varphi, m\rangle \in \mathrm{MaxIS}$.

הערה: שימו לב שטענה 2.1 נכונה **לכל** φ, גם לא ספיקה. היא תלויה אך ורק בקשתות האדומות. נשתמש בה שוב בכיוון ההפוך.

2ג. ניתוח נאותות — כיוון $\Longleftarrow$
נניח $\langle G_\varphi, m\rangle \in \mathrm{MaxIS}$, כלומר $\alpha(G_\varphi) = m$. אזי קיימת U בלתי תלויה ב-G_φ כך ש- $|U| = m$.
U בלתי תלויה, ולכן בין כל שני קודקודים ב-U **אין קשת אדומה**. מכאן ש-U מכילה **לכל היותר** קודקוד אחד מכל פסוקית.
מכיוון ש-$|U| = m$ ויש בדיוק m פסוקיות, ולכל פסוקית לכל היותר קודקוד אחד — לפי שובך יונים (הפעם בכיוון הצפוף) U מכילה **בדיוק** קודקוד אחד מכל פסוקית.

הערה [00:31:51]–[00:32:54]. אלה **שני** טיעונים נפרדים, לא אחד: הראשון (אין שניים) מגיע מאי-התלות, השני (יש בדיוק אחד) מגיע מספירה. המרצה עמד על ההפרדה: "כמה שאני יותר אפרק את הטיעון שלי, אני פחות פרון לעשות טעויות".

U בלתי תלויה, ולכן לכל $x, y \in U$ אין ביניהם **קשת שחורה**. לכן אין ב-U שני קודקודים המתאימים לליטרל ולשלילתו.
אוסף הליטרלים המתאימים לקודקודי U הוא אפוא אוסף **עקבי**: אין בו משתנה שמופיע גם חיובי וגם שלילי. לכן **קיימת** השמה $\mathcal{V}$ המספקת את כל הליטרלים המתאימים לקודקודים ב-U (למשל: לכל משתנה שמופיע באוסף נותנים את הערך שמספק את המופע שלו; לשאר המשתנים נותנים ערך שרירותי, נניח 0).
לפי סעיף 2, ב-U יש קודקוד מכל פסוקית, ולכן $\mathcal{V}$ מספקת לפחות ליטרל אחד בכל פסוקית של φ, כלומר $\mathcal{V}$ מספקת את φ.
מכאן $\varphi \in \mathrm{SAT}$.

הערה — "קיימת" ולא "ניתן לקבוע" [00:34:31]–[00:35:37]. סטודנט הציע לומר "אפשר לקבוע את ההשמה", והמרצה סירב: הניסוח הזה רומז ל**יחידות**, ואין כאן יחידות. בדוגמה הקונקרטית שלמטה יש **שתי** השמות שמספקות את הליטרלים של U, כי המשתנה x_4 אינו מופיע ב-U כלל וערכו חופשי. הניסוח הנכון הוא **"קיימת השמה"**.

הערה — הוכחת קיום מול הוכחה אלגוריתמית [00:36:38]–[00:37:39]. בסעיף 4 ההוכחה **מפסיקה להיות אלגוריתמית**: לא הראינו איך בוחרים את $\mathcal{V}$, רק שהיא קיימת. וזה מספיק — הרדוקציה מחייבת אותנו להוכיח **קיום גורר קיום**, וטיעון אלגוריתמי הוא רק *דרך אחת* להוכיח קיום. המרצה הביא בהשוואה את המשפט "בכל עץ יש עלה", שההוכחה שלו (סכימת דרגות) אינה אלגוריתמית כלל.

2ד. סיכום המשפט

הראינו: הרדוקציה מוגדרת היטב, פולינומית, ולכל φ מתקיים $\varphi \in \mathrm{SAT} \iff \langle G_\varphi, m\rangle \in \mathrm{MaxIS}$. לכן $\mathrm{SAT} \le_p \mathrm{MaxIS}$. מכיוון ש-$\mathrm{SAT}$ היא NP-קשה ו-$\le_p$ טרנזיטיבית — לכל $A \in \mathrm{NP}$ מתקיים $A \le_p \mathrm{SAT} \le_p \mathrm{MaxIS}$ ולכן $A \le_p \mathrm{MaxIS}$ — מכאן ש-MaxIS **היא NP-קשה**. ■

הערה טכנית (השלמה שלנו, לא במקורות). אם ב-φ יש פסוקית **ריקה**, אין לה קודקודים כלל, ואז $\alpha(G_\varphi) \le m-1 < m$ ולכן $\langle G_\varphi, m\rangle \notin \mathrm{MaxIS}$ — וזה נכון, כי נוסחה עם פסוקית ריקה איננה ספיקה. אם פסוקית מכילה ליטרל ואת שלילתו, הזוג המתאים מחובר גם בקשת אדומה וגם בקשת שחורה; זו אותה קשת בגרף פשוט וההוכחה אינה משתנה.

משפט 3: $\overline{\mathrm{IS}} \le_p \mathrm{MaxIS}$, ולכן MaxIS היא coNP-קשה

3א. למת המשלימים, ולמה בכלל מתחילים מ-$\overline{\mathrm{IS}}$

למה 3.1 (הקופסה הכחולה בעמוד 3; משיעור 21). תהא f פונקציה הניתנת לחישוב בזמן פולינומי. אז

f היא רדוקציה מ-A ל-B אם ורק אם f היא רדוקציה מ-$\overline{A}$ ל-$\overline{B}$.

הוכחה. f רדוקציה מ-A ל-B פירושו: לכל x, מתקיים $x \in A \iff f(x) \in B$. שקילות לוגית שקולה לשקילות של שני השלילות: $x \notin A \iff f(x) \notin B$, כלומר $x \in \overline{A} \iff f(x) \in \overline{B}$ — וזה בדיוק "f רדוקציה מ-$\overline{A}$ ל-$\overline{B}$". החישוביות בזמן פולינומי היא תכונה של f בלבד ואינה מושפעת. □

בניסוח של ההרצאה [00:46:13]: "כל מה שב-A הולך ל-B, וכל מה שלא ב-A הולך ללא-B. עכשיו תסתכל על זה מהזווית ההפוכה — זו אותה רדוקציה בדיוק."

מסקנה 3.2. מכיוון ש-IS היא NP-שלמה, $\overline{\mathrm{IS}}$ היא **coNP-שלמה**. אכן, יהא $A \in \mathrm{coNP}$. אז $\overline{A} \in \mathrm{NP}$, ולכן קיימת רדוקציה f מ-$\overline{A}$ ל-IS. לפי למה 3.1 אותה f היא רדוקציה מ-A ל-$\overline{\mathrm{IS}}$. לכן לכל $A \in \mathrm{coNP}$ מתקיים $A \le_p \overline{\mathrm{IS}}$.

מסקנה 3.3. לכן, אם נוכיח $\overline{\mathrm{IS}} \le_p \mathrm{MaxIS}$, נקבל מטרנזיטיביות שלכל $A \in \mathrm{coNP}$ מתקיים $A \le_p \overline{\mathrm{IS}} \le_p \mathrm{MaxIS}$, ומכאן ש-$\mathrm{MaxIS}$ היא coNP-קשה.

למה דווקא $\overline{\mathrm{IS}} \le_p \mathrm{MaxIS}$ ולא $\mathrm{IS} \le_p \overline{\mathrm{MaxIS}}$? [00:46:44]–[00:49:22]. לפי למה 3.1 אלה **אותה רדוקציה בדיוק**, אז זו שאלה של נוחות כתיבה — והמרצה מסביר את הבחירה, וזה אחד הרגעים הכי מלמדים בשיעור. שייכות ל-MaxIS היא **טענת "וגם"** ("קיים... וגם לכל..."). השלילה של טענת "וגם" היא **טענת "או"**, ואת אלה לא נעים להוכיח. אם נכתוב $\overline{\mathrm{IS}} \le_p \mathrm{MaxIS}$, אז בכיוון אחד נצטרך **להוכיח** שייכות ל-MaxIS (טענת "וגם" — מוכיחים שני חלקים, כל אחד לחוד), ובכיוון השני **להשתמש** בשייכות ל-MaxIS (שוב "וגם" — מקבלים שני דברים). לעומת זאת $\mathrm{IS} \le_p \overline{\mathrm{MaxIS}}$ היה מחייב אותנו להתעסק עם טענות "או". האנלוגיה של המרצה: טענת "וגם" היא כמו **תרגיל כפל** שכל אחד מהכופלים בו הוא תרגיל חיבור — שני חלקים מוכרים; טענת "או" היא חיה אחרת.

3ב. הרדוקציה

קלט: גרף $G = (V, E)$ ומספר $k \in \mathbb{N}$.

נוסיף ל-G עוד $k - 1$ קודקודים חדשים. נסמן ב-$\hat{V}$ את קבוצת הקודקודים החדשה (כלומר $\hat{V}$ הוא V יחד עם הקודקודים החדשים, ו-$\hat{V} \setminus V$ הם החדשים בלבד, $|\hat{V} \setminus V| = k - 1$).

נוסיף קשתות מכל קודקוד חדש אל **כל אחד** מהקודקודים ב-V. נסמן ב-$\hat{E}$ את קבוצת הקשתות המתקבלת. שימו לב: בין הקודקודים החדשים לבין עצמם **אין** קשתות, ובין קודקודי V לבין עצמם לא הוספנו ולא הסרנו כלום.

נחזיר את $\langle \hat{G}, k-1 \rangle$ כאשר $\hat{G} = (\hat{V}, \hat{E})$.

האינטואיציה [00:51:47]–[00:53:21]. אנחנו רוצים ש-$\langle G, k \rangle \in \overline{\mathrm{IS}}$ (כלומר: אין ב-G קבוצה בלתי תלויה בגודל k) יתורגם לשאלת מקסימום. אם אין ב-G קבוצה בלתי תלויה בגודל k, אז המקסימום ב-G הוא **לכל היותר** $k-1$ — אבל אין לנו ערובה שהוא *בדיוק* $k-1$. לכן "שותלים" קבוצה בלתי תלויה בגודל $k-1$ בדיוק. סטודנט הציע להוסיף $k-1$ קודקודים **מבודדים**, והמרצה: "זה כמעט נכון" — קודקודים מבודדים היו **מצטרפים** לקבוצות הישנות ומגדילים את המקסימום. לכן מחברים כל קודקוד חדש לכל הקודקודים הישנים: כך הקבוצה החדשה קיימת אך אינה מתערבבת.

טיפול ב-$k = 0$ (השלמה שלנו — אינו מופיע באף אחד מהמקורות). לכל גרף מתקיים $\langle G, 0 \rangle \in \mathrm{IS}$ (הקבוצה הריקה בלתי תלויה ו-$|\emptyset| = 0 \ge 0$), ולכן $\langle G, 0 \rangle \notin \overline{\mathrm{IS}}$. נגדיר אפוא שעל קלט עם $k = 0$ הרדוקציה מחזירה מחרוזת קבועה שאיננה ב-MaxIS, למשל $\langle K_1, 0 \rangle$ (גרף בעל קודקוד יחיד, ו-$\alpha(K_1) = 1 \ne 0$). מכאן ואילך נניח $k \ge 1$, ואז $k - 1 \ge 0$ והבנייה חוקית.

3ג. ניתוח זמן ריצה

הוספת הקודקודים: $O(|V|)$. כאן נדרשת הבחנה עדינה [00:59:54]–[01:00:24]: בגודל הייצוג של הקלט, המספר k תופס רק $\log k$ ביטים, ולכן **אסור** לחסום שום דבר "באמצעות k". אבל מותר להניח בלי הגבלת הכלליות $k \le |V|$: אם $k > |V|$ אז בוודאי אין ב-G קבוצה בלתי תלויה בגודל k, כי אין בו בכלל k קודקודים, והרדוקציה יכולה להחזיר במקרה זה מחרוזת קבועה ששייכת ל-MaxIS (למשל $\langle K_1, 1 \rangle$). לכן $k - 1 < |V|$ והוספת הקודקודים היא $O(|V|)$.

הוספת הקשתות: לכל אחד מ-$k-1$ הקודקודים החדשים מוסיפים $|V|$ קשתות (אחת לכל קודקוד ישן), כלומר $(k-1) \cdot |V| = O(|V|^2)$ קשתות. זה גם מסדר גודל $O(|V|^2)$ צעדים.

סך הכול: $O\big(|\langle G, k \rangle|^2\big)$, כלומר **פולינומי בגודל הקלט**.

הערה [00:56:09]. סטודנט חשב שכל קודקוד חדש מקבל k קשתות; המרצה הבהיר: כל קודקוד **חדש** מקבל קשת לכל קודקוד **ישן**, כלומר $|V|$ קשתות, ובסך הכול $(k-1)\cdot|V|$.

3ד. ניתוח נאותות — כיוון $\Longrightarrow$

יהי $G=(V,E)$ ו-$k\in\mathbb{N}$, ונניח $\langle G,k\rangle\in\overline{\text{IS}}$ — כלומר **אין** ב-G קבוצה בלתי תלויה בגודל k. צריך להוכיח $\langle\hat{G},k-1\rangle\in\text{MaxIS}$, כלומר את שני חלקי ה"וגם".

(א) חלק הקיום. הקבוצה $\hat{V}\setminus V$ (הקודקודים החדשים) היא קבוצה בלתי תלויה ב-$\hat{G}$: הרדוקציה לא הוסיפה שום קשת בין שני קודקודים חדשים. גודלה בדיוק $k-1$. לכן קיימת ב-$\hat{G}$ קבוצה בלתי תלויה בגודל $k-1$. ✓

(ב) חלק ה"לכל". תהא $U\subseteq\hat{V}$ קבוצה בלתי תלויה ב-$\hat{G}$.

ב-$\hat{G}$ יש קשת בין **כל** קודקוד ב-$\hat{V}\setminus V$ ובין **כל** קודקוד ב-V — כך בנינו. לכן U אינה יכולה להכיל בו-זמנית קודקוד חדש וקודקוד ישן, ומכאן שמתקיים אחד משניים: $U\subseteq\hat{V}\setminus V$

או

$$U\subseteq V.$$

אם $U\subseteq\hat{V}\setminus V$: אז $|U|\le|\hat{V}\setminus V|=k-1$.

אחרת $U\subseteq V$: מכיוון שהרדוקציה **לא הסירה ולא הוסיפה** קשתות בין קודקודי V, קבוצה שהיא בלתי תלויה ב-$\hat{G}$ ומוכלת ב-V היא בלתי תלויה גם ב-G. ומכיוון ש-$\langle G,k\rangle\in\overline{\text{IS}}$, אין ב-$G$ קבוצה בלתי תלויה בגודל k, ולפי הלמה התורשתית משיעור 10 גם אין בו קבוצה בלתי תלויה בגודל **גדול** מ-k (אם הייתה, היינו מורידים ממנה קודקודים ומקבלים אחת בגודל k בדיוק). לכן $|U|\le k-1$.

בשני המקרים $|U|\le k-1$. ✓

משני החלקים: המקסימום ב-$\hat{G}$ הוא בדיוק $k-1$, כלומר $\langle\hat{G},k-1\rangle\in\text{MaxIS}$.

הערה — שאלת סטודנט (עומר), [01:09:51]–[01:11:54]. למה מ"אין קבוצה בגודל k" נובע "אין קבוצה בגודל $k>$"? התשובה: **הרדוקציה בכלל לא נוגעת בקבוצות הבלתי תלויות** — היא מטפלת בגרף בלבד. הטיעון על התורשתיות הוא טיעון של **ההוכחה**, לא של האלגוריתם: ברמת ההוכחה אני לוקח קבוצה בלתי תלויה בגודל $k+1$, מוריד ממנה קודקוד אחד, ומקבל קבוצה בלתי תלויה בגודל k. המרצה חזר על ההבחנה הזו פעמיים: "האלגוריתם לא נוגע בפתרון לבעיה, הוא רק מטפל בגרף".

3ה. ניתוח נאותות — כיוון $\Longleftarrow$

נניח $\langle\hat{G},k-1\rangle\in\text{MaxIS}$. צריך להוכיח $\langle G,k\rangle\in\overline{\text{IS}}$, כלומר: **לכל** קבוצה בלתי תלויה U ב-G מתקיים $|U|\neq k$. זו טענת "לכל", ולכן — כמו שהמרצה עמד על כך שוב [01:04:54] — נתחיל ב"תהא".

תהא $U\subseteq V$ קבוצה בלתי תלויה ב-G.

הרדוקציה לא הוסיפה שום קשת **בין קודקודי** V (הקשתות היחידות שהוספנו יוצאות מהקודקודים החדשים). לכן U, כתת-קבוצה של $\hat{V}$, היא גם קבוצה בלתי תלויה ב-$\hat{G}$.

מהנחתנו $\alpha(\hat{G})=k-1$, ולכן **כל** קבוצה בלתי תלויה ב-$\hat{G}$ היא בגודל $\le k-1$. בפרט $|U|\le k-1$.

מכאן בפרט $|U| \neq k$.

מכיוון שזה נכון לכל בלתי תלויה ב-U, אין ב-G קבוצה בלתי תלויה בגודל k, כלומר $\langle G, k\rangle \in \overline{\text{IS}}$.

3ו. סיכום המשפט

הרדוקציה מוגדרת היטב, פולינומית, ולכל קלט $\langle G, k\rangle$ מתקיים $\langle G, k\rangle \in \overline{\text{IS}} \iff \langle \hat{G}, k - 1\rangle \in \text{MaxIS}$. לכן $\overline{\text{IS}} \leq_p \text{MaxIS}$, ולפי מסקנות 3.2–3.3 — MaxIS **היא coNP-קשה**. ■

מסקנה מיידית. MaxIS היא גם NP-קשה וגם coNP-קשה. שתי התכונות האלה יחד הן שיוצרות את המצב המוזר של המשפט הבא.

משפט 4: $\text{MaxIS} \in \text{NP} \cup \text{coNP}$ אם ורק אם $\text{NP} = \text{coNP}$

זהו התרגיל שהמרצה נתן בכיתה [01:12:44] וגם פתר. שימו לב לצורת השאלה: מבקשים להראות ש**טענה על מחלקות סיבוכיות שקולה לבעיה פתוחה**. המרצה מדגיש [01:13:17]: הצעד הראשון בתרגיל כזה הוא **לבחור את הבעיה הפתוחה הנכונה**. כאן המועמדת הטבעית היא $\text{NP} = \text{coNP}$ ולא $\text{P} = \text{NP}$, "כי P לא מוזכרת פה בכלל".

4א. כיוון $\Longrightarrow$: אם $\text{MaxIS} \in \text{NP} \cup \text{coNP}$ אז $\text{NP} = \text{coNP}$

נשתמש פעמיים בלמת עזר:

למה 4.1. coNP סגורה תחת $\leq_p$: אם $A \leq_p B$ ו-$B \in \text{coNP}$ אז $A \in \text{coNP}$. *הוכחה.* תהא f הרדוקציה מ-A ל-B. לפי למה 3.1, f היא גם רדוקציה מ-$\overline{A}$ ל-$\overline{B}$. מכיוון ש-$B \in \text{coNP}$, מתקיים $\overline{B} \in \text{NP}$, ומכיוון ש-NP סגורה תחת $\leq_p$ (שיעור 7) נקבל $\overline{A} \in \text{NP}$, כלומר $A \in \text{coNP}$. □

למה 4.2. אם $\text{coNP} \subseteq \text{NP}$ אז $\text{NP} = \text{coNP}$, וכן להפך. *הוכחה.* נניח $\text{coNP} \subseteq \text{NP}$, ותהא $L \in \text{NP}$. אז $\overline{L} \in \text{coNP} \subseteq \text{NP}$, ולכן $\overline{L} \in \text{NP}$, ולכן לפי ההגדרה $L \in \text{coNP}$. קיבלנו $\text{NP} \subseteq \text{coNP}$, ויחד עם ההנחה — שוויון. הכיוון השני סימטרי לחלוטין. □

כעת נניח $\text{MaxIS} \in \text{NP} \cup \text{coNP}$, ונחלק לשני מקרים.

מקרה 1: $\text{MaxIS} \in \text{NP}$. לפי משפט 3, MaxIS היא coNP-קשה, כלומר לכל $A \in \text{coNP}$ מתקיים $A \leq_p \text{MaxIS}$. מכיוון ש-NP סגורה תחת $\leq_p$ ו-$\text{MaxIS} \in \text{NP}$, נקבל $A \in \text{NP}$ לכל $A \in \text{coNP}$, כלומר $\text{coNP} \subseteq \text{NP}$. לפי למה 4.2, $\text{NP} = \text{coNP}$.

מקרה 2: $\text{MaxIS} \in \text{coNP}$. לפי משפט 2, MaxIS היא NP-קשה, כלומר לכל $A \in \text{NP}$ מתקיים $A \leq_p \text{MaxIS}$. לפי למה 4.1, $A \in \text{coNP}$. לכן $\text{NP} \subseteq \text{coNP}$, ולפי למה 4.2 שוב $\text{NP} = \text{coNP}$.

בשני המקרים $\text{NP} = \text{coNP}$. ✓

> **הערה** [01:19:33]–[01:22:15]. סטודנט שאל למה מקרה 2 עובד. התשובה של המרצה: זה "משחק משלימים" — אם $\text{MaxIS} \in \text{coNP}$ אז $\overline{\text{MaxIS}} \in \text{NP}$, והיא coNP-קשה, וחוזרים למקרה 1. שתי הדרכים נכונות; כאן הובאה הגרסה הישירה עם למה 4.1.

4ב. כיוון $\Longleftarrow$: אם $\text{NP} = \text{coNP}$ אז $\text{MaxIS} \in \text{NP} \cup \text{coNP}$

תחילה הבחנה [01:22:49]: אם $\text{NP} = \text{coNP}$ אז $\text{NP} \cup \text{coNP} = \text{NP}$, ולכן די להוכיח $\text{MaxIS} \in \text{NP}$.

נשתמש בפירוק מהגדרה 2: $\text{MaxIS} = \text{IS} \cap \text{IS}^{\leq}$,

כאשר $\text{IS}^{\leq}$ היא אוסף הזוגות $\langle G, k\rangle$ שבהם כל קבוצה בלתי תלויה ב-G היא בגודל $\leq k$.

(א) $\mathrm{IS} \in \mathrm{NP}$ — משיעור 7 (העד הוא קבוצת הקודקודים; האימות בודק שגודלה $\geq k$ ושאין בין אבריה קשת, בזמן פולינומי).

(ב) $\mathrm{IS}^{\leq} \in \mathrm{coNP}$. נראה ש-$\overline{\mathrm{IS}^{\leq}} \in \mathrm{NP}$. לפי ההגדרה, $\overline{\mathrm{IS}^{\leq}}$ היא אוסף הזוגות $\langle G, k \rangle$ שבהם קיימת ב-G קבוצה בלתי תלויה בגודל לפחות $k+1$. זו בדיוק IS עם $k+1$ במקום k. אפשר לומר זאת בשתי דרכים, ושתיהן הוזכרו בהרצאה [01:28:04]:

באמצעות רדוקציה: הפונקציה $\langle G, k \rangle \mapsto \langle G, k+1 \rangle$ ניתנת לחישוב בזמן פולינומי (הוספת 1 למספר בייצוג בינארי), והיא רדוקציה מ-$\overline{\mathrm{IS}^{\leq}}$ ל-IS. מכיוון ש-$\mathrm{IS} \in \mathrm{NP}$ ו-NP סגורה תחת $\leq_p$, נקבל $\overline{\mathrm{IS}^{\leq}} \in \mathrm{NP}$.

באמצעות מאמת ישיר: העד הוא קבוצת קודקודים U; המאמת בודק ש-$|U| \geq k+1$ ושלכל $x, y \in U$ מתקיים $xy \notin E$. אורך העד $O(|V| \log |V|)$ פולינומי, וזמן האימות $O(|U|^2)$ פולינומי.

לכן $\mathrm{IS}^{\leq} \in \mathrm{coNP}$.

(ג) הפעלת ההנחה. מההנחה $\mathrm{NP} = \mathrm{coNP}$ נובע $\mathrm{IS}^{\leq} \in \mathrm{NP}$.

(ד) סגירות לחיתוך. NP סגורה תחת חיתוך. בפירוט: אם $L_1, L_2 \in \mathrm{NP}$ עם מאמתים M_1, M_2 ואורכי עדים $p_1(n), p_2(n)$, נגדיר מאמת ל-$L_1 \cap L_2$ שמקבל עד $w = \langle w_1, w_2 \rangle$ באורך $p_1(n) + p_2(n) + O(\log n)$, מפצל אותו, ומריץ את M_1 על $\langle x, w_1 \rangle$ ואת M_2 על $\langle x, w_2 \rangle$, ומקבל אם ורק אם שניהם קיבלו. הזמן והאורך פולינומיים, ו-$x \in L_1 \cap L_2$ אם ורק אם קיימים שני עדים כאלה.

לכן $\mathrm{MaxIS} = \mathrm{IS} \cap \mathrm{IS}^{\leq} \in \mathrm{NP} \subseteq \mathrm{NP} \cup \mathrm{coNP}$. ■

4ג. מה זה אומר בפועל

מסקנה 4.3. אילו ידענו ש-$\mathrm{MaxIS} \in \mathrm{NP}$, היינו מקבלים מיד $\mathrm{NP} = \mathrm{coNP}$ — בעיה פתוחה. לכן:

אסור לומר ש-MaxIS היא NP-שלמה. NP-שלמות דורשת שייכות ל-NP, וזו בדיוק הנקודה שאנחנו לא יודעים. המרצה נשאל על כך ישירות [00:42:27] וענה "אני באמת לא יודע — זו שאלה פתוחה".

מסקנה 4.4. אם $\mathrm{MaxIS} \in \mathrm{P}$ אז $\mathrm{P} = \mathrm{NP}$. אכן, P סגורה תחת $\leq_p$, ו-MaxIS היא NP-קשה, ולכן כל $A \in \mathrm{NP}$ מקיימת $A \leq_p \mathrm{MaxIS} \in \mathrm{P}$ ולכן $A \in \mathrm{P}$. (יחד עם משפט 1 זה נותן: אם $\mathrm{IS} \in \mathrm{P}$ אז $\mathrm{MaxIS} \in \mathrm{P}$ ואז $\mathrm{P} = \mathrm{NP}$ — עקבי עם NP-שלמותה של IS.)

התמונה הכללית של הבעיות הפתוחות [01:14:19]–[01:15:52]. המרצה שרטט את מה שידוע ומה שלא: $\mathrm{P} \subseteq \mathrm{NP} \cap \mathrm{coNP} \subseteq \mathrm{NP}$, $\mathrm{P} \subseteq \mathrm{NP} \cap \mathrm{coNP} \subseteq \mathrm{coNP}$. שלוש שאלות פתוחות בו-זמנית: האם $\mathrm{P} = \mathrm{NP}$? האם $\mathrm{NP} = \mathrm{coNP}$? והאם $\mathrm{NP} \cap \mathrm{coNP} = \mathrm{P}$? "תיאורטית יכול להיות שיש בעיה שהיא גם ב-NP וגם ב-coNP והיא לא ב-P. המצב פה הרבה יותר מורכב ממה שהיה בחישוביות, שם $\mathrm{R} = \mathrm{RE} \cap \mathrm{coRE}$ בדיוק."

דוגמאות ותרגילים מהשיעור

דוגמה 1: הרצת הרדוקציה $\mathrm{SAT} \le_p \mathrm{MaxIS}$ מקצה לקצה

זו הדוגמה שעל הלוח ובעמוד 1 בסיכום. הנוסחה: $\varphi = (\overline{x_1} \vee x_2 \vee \overline{x_3}) \wedge (x_1 \vee \overline{x_2} \vee x_4) \wedge (x_3 \vee x_4 \vee x_2) \wedge (x_1 \vee x_3)$. כאן $m = 4$. הפסוקית הרביעית היא בגודל 2 בכוונה, כדי להזכיר שהרדוקציה עובדת ל-CNF כללי.

שלב 1 — קודקודים. מופע ליטרל $\to$ קודקוד. 11 קודקודים, מסודרים בשורות לפי פסוקית:

פסוקית	קודקודים
C_1	$u_1 = \overline{x_1},\ u_2 = x_2,\ u_3 = \overline{x_3}$
C_2	$u_4 = x_1,\ u_5 = \overline{x_2},\ u_6 = x_4$
C_3	$u_7 = x_3,\ u_8 = x_4,\ u_9 = x_2$
C_4	$u_{10} = x_1,\ u_{11} = x_3$

שלב 2 — קשתות אדומות (קליקה בכל שורה), 10 קשתות:

$$u_1u_2,\ u_1u_3,\ u_2u_3; \quad u_4u_5,\ u_4u_6,\ u_5u_6; \quad u_7u_8,\ u_7u_9,\ u_8u_9; \quad u_{10}u_{11}.$$

שלב 3 — קשתות שחורות (ליטרל $\leftrightarrow$ שלילתו), 6 קשתות:

משתנה	מופעים חיוביים	מופעים שליליים	קשתות
x_1	u_4, u_{10}	u_1	$u_1u_4,\ u_1u_{10}$
x_2	u_2, u_9	u_5	$u_2u_5,\ u_5u_9$
x_3	u_7, u_{11}	u_3	$u_3u_7,\ u_3u_{11}$
x_4	u_6, u_8	—	אין

סך הכול $|V| = 11$, $|E| = 16$. הפלט: $\langle G_\varphi, 4 \rangle$.

כיוון $\Longrightarrow$ (מהשמה לקבוצה). ההשמה שנבחרה בכיתה [00:22:31]: $\mathcal{V}(x_1) = 1, \quad \mathcal{V}(x_2) = 1, \quad \mathcal{V}(x_3) = 1, \quad \mathcal{V}(x_4) = 0$. נבדוק שהיא מספקת: ✓ $x_2 = 1 \to C_1$; ✓ $x_1 = 1 \to C_2$; ✓ $x_3 = 1 \to C_3$; ✓ $x_1 = 1 \to C_4$.

נבחר מכל פסוקית ליטרל מסופק אחד: $U = \{\, u_2,\ u_4,\ u_7,\ u_{10} \,\}, \qquad |U| = 4 = m$,

כאשר u_2 הוא x_2 ב-C_1, u_4 הוא x_1 ב-C_2, u_7 הוא x_3 ב-C_3, ו-u_{10} הוא x_1 ב-C_4.

נבדוק ידנית שכל ששת הזוגות אינם קשתות:

זוג	אותה פסוקית?	ליטרל ושלילתו?	קשת?
u_2, u_4	לא (C_1, C_2)	x_2 מול x_1 — לא	אין
u_2, u_7	לא (C_1, C_3)	x_2 מול x_3 — לא	אין
u_2, u_{10}	לא (C_1, C_4)	x_2 מול x_1 — לא	אין
u_4, u_7	לא (C_2, C_3)	x_1 מול x_3 — לא	אין

זוג	אותה פסוקית?	ליטרל ושלילתו?	קשת?
u_4, u_{10}	לא (C_2, C_4)	x_1 מול x_1 — **אותו ליטרל**, לא שלילתו	אין
u_7, u_{10}	לא (C_3, C_4)	x_3 מול x_1 — לא	אין

השורה החמישית היא הנקודה הכי חשובה בטבלה: קשת שחורה מחברת ליטרל ל**שלילתו**, ולא שני מופעים של אותו ליטרל. אחרת הרדוקציה לא הייתה עובדת כלל.

לפי טענה 2.1 כל קבוצה בלתי תלויה כאן היא בגודל ≤ 4, ומצאנו אחת בגודל 4; לכן $\alpha(G_\varphi) = 4$ ו-$\langle G_\varphi, 4\rangle \in \text{MaxIS}$. ✓

כיוון $\Longleftarrow$ (מהקבוצה להשמה). נניח שקיבלנו את U הזו כ"קופסה שחורה". הליטרלים המתאימים הם x_2, x_1, x_3, x_1 — אין בהם משתנה שמופיע גם חיובי וגם שלילי. לכן קיימת השמה שמספקת את כולם: $\mathcal{V}(x_1) = \mathcal{V}(x_2) = \mathcal{V}(x_3) = 1$. **המשתנה x_4 נשאר חופשי**, ולכן יש כאן **שתי** השמות מספקות — זו עם $\mathcal{V}(x_4) = 0$ וזו עם $\mathcal{V}(x_4) = 1$ [00:35:02]. וזו בדיוק הסיבה שבניסוח ההוכחה כותבים "**קיימת** השמה" ולא "ניתן לקבוע את ההשמה". ומכיוון שב-U יש קודקוד מכל פסוקית, כל פסוקית מסופקת, כלומר $\varphi \in \text{SAT}$. ✓

בחירה חלופית. בפסוקית C_4 יכולנו לבחור את $u_{11} = x_3$ במקום $u_{10} = x_1$ [00:23:04]; נקבל $U' = \{u_2, u_4, u_7, u_{11}\}$, שגם היא בלתי תלויה בגודל 4. אין יחידות — ולא נדרשת.

דוגמה 2: מופע לא ספיק, מקצה לקצה

$$\psi = (x_1) \wedge (\overline{x_1}), \qquad m = 2.$$

קודקודים: $v_1 = x_1$ (מ-C_1), $v_2 = \overline{x_1}$ (מ-C_2). $|V| = 2$.

קשתות אדומות: אין — כל פסוקית מכילה ליטרל אחד בלבד, ואין בה זוגות.

קשתות שחורות: $v_1 v_2$ (ליטרל ושלילתו).

הפלט: $\langle G_\psi, 2\rangle$.

$\alpha(G_\psi) = 1$ (הגרף הוא קשת אחת), ולכן $\alpha(G_\psi) = 1 \neq 2$ ו-$\langle G_\psi, 2\rangle \notin \text{MaxIS}$. ואכן $\psi \notin \text{SAT}$. ✓ שימו לב שכאן דווקא הקשת **השחורה** היא זו שמונעת את הקבוצה בגודל 2 — בדיוק כפי שצריך, כי חוסר הסיפוק נובע מהתנגשות בין ליטרל לשלילתו.

דוגמה 3: הרצת הרדוקציה $\overline{\text{IS}} \leq_p \text{MaxIS}$

מופע "כן". $G = K_3$ על $\{a, b, c\}$, $k = 2$. מתקיים $\alpha(K_3) = 1 < 2$, ולכן $\langle K_3, 2\rangle \in \overline{\text{IS}}$. הרדוקציה מוסיפה $k - 1 = 1$ קודקוד חדש w ומחברת אותו ל-a, b, c. מתקבל $\hat{G} = K_4$, ו-$\langle K_4, 1\rangle$ הוא הפלט. אכן $\alpha(K_4) = 1 = k - 1$, ולכן $\langle K_4, 1\rangle \in \text{MaxIS}$. ✓

מופע "כן" שבו הגרף המקורי הוא זה שקובע. $G = P_3$ (מסלול $a - b - c$), $k = 3$. מתקיים $\alpha(P_3) = 2$ (הקבוצה $\{a, c\}$), ולכן אין קבוצה בגודל 3 ו-$\langle P_3, 3\rangle \in \overline{\text{IS}}$. מוסיפים $k - 1 = 2$ קודקודים w_1, w_2, כל אחד מחובר ל-a, b, c אך **לא** זה לזה. עכשיו:

$\{w_1, w_2\}$ בלתי תלויה בגודל 2;

$\{a, c\}$ בלתי תלויה בגודל 2;

אין קבוצה בגודל 3: קבוצה בלתי תלויה חייבת להיות כולה בצד החדש (ואז ≤ 2) או כולה בצד הישן (ואז $\leq \alpha(P_3) = 2$).

לכן $\alpha(\hat{G}) = 2 = k - 1$ ו-$\langle \hat{G}, 2 \rangle \in \text{MaxIS}$. ✓ שימו לב ששני המקרים בהוכחה נתנו כאן בדיוק את אותו החסם — זה מותר לגמרי, ההוכחה דורשת רק $\leq k - 1$.

מופע "לא". $G = P_3$, $k = 2$. מתקיים $\alpha(P_3) = 2 \geq 2$, ולכן $\langle P_3, 2 \rangle \notin \overline{\text{IS}}$. הרדוקציה מוסיפה קודקוד w המחובר ל-a, b, c, ומחזירה $\langle \hat{G}, 1 \rangle$. אבל $\{a, c\}$ נשארה בלתי תלויה ב-$\hat{G}$ (לא הסרנו קשתות ולא הוספנו בין a ל-c), ולכן $\alpha(\hat{G}) = 2 \neq 1$ ו-$\langle \hat{G}, 1 \rangle \notin \text{MaxIS}$. ✓ שני הצדדים ענו "לא" — כנדרש.

תרגיל 1 (מהשיעור): הראו כי $\text{MaxIS} \in \text{NP} \cup \text{coNP}$ אם ורק אם $\text{NP} = \text{coNP}$

זהו בדיוק משפט 4, והפתרון המלא בסעיף המשפטים. הדגשים שהמרצה נתן לתרגילים מהסוג הזה [01:13:17]:

קודם כול — **לזהות את הבעיה הפתוחה** שאליה שואפים. כאן: $\text{NP} = \text{coNP}$, כי P אינה מופיעה בטענה.

בכיוון "אם השפה במחלקה" — לחלק למקרים לפי איזה איבר של האיחוד מתקיים, ובכל מקרה להשתמש ב**קשיות** מהצד השני.

בכיוון "אם המחלקות שוות" — לפרק את השפה ל**חיתוך** של רכיב ב-NP ורכיב ב-coNP, ואז ההנחה מאחדת אותם.

תרגיל 2 (השלמה מתבקשת): מדוע לא הראינו $\text{SAT} \leq_p \overline{\text{MaxIS}}$?

פתרון. אפשר, וזו למעשה **אותה רדוקציה** — לפי למה 3.1, כל רדוקציה מ-$\overline{\text{IS}}$ ל-MaxIS היא רדוקציה מ-IS ל-$\overline{\text{MaxIS}}$ ולהפך. הסיבה שבחרנו את הניסוח שכן בחרנו היא **נוחות הוכחה**: שייכות ל-MaxIS היא טענת "וגם", ולכן נוח גם להוכיח אותה (מוכיחים שני חלקים) וגם להשתמש בה (מקבלים שני חלקים). שייכות ל-$\overline{\text{MaxIS}}$ היא טענת "או", ואיתה פחות נעים לעבוד — צריך לפצל למקרים בלי לדעת מראש איזה מהם מתקיים [00:47:16].

הערות מהשיעור

[00:00:34]–[00:03:43] — "פרקו את המקסימום לפרימיטיבים". ההערה המרכזית של השיעור. "מקסימום זה לא משהו שאני רוצה לעבוד איתו." הפירוק ל"קיים **וגם** לכל" הוא מה שמייצר את כל התוצאות הבאות.

[00:01:36] — אל תדברו על אובייקט לפני שהצהרתם על קיומו. תיקון לניסוח של סטודנט. "אתה מדבר על אובייקט שמבחינתי עוד אין לו משמעות."

[00:07:55] — הרדוקציה לא פותרת כלום. לשאלה "מה הרדוקציה מחזירה?" סטודנט ענה "קבוצת קודקודים". המרצה: "הוא לא יכול להחזיר קבוצת קודקודים. הרדוקציה לא פותרת שום דבר." הפלט הוא **מופע** של הבעיה השנייה — כאן גרף ומספר.

[00:08:58] — קודקוד למופע, לא למשתנה. ליטרל שחוזר בכמה פסוקיות מקבל כמה קודקודים.

[00:15:28] — "תריצו לעצמכם, תלושו את זה בידיים." ההמלצה החוזרת של המרצה לפני ניתוח נאותות.

[00:19:52] — סדר הכמתים. "לכל פסוקית קיים ליטרל", לא "קיים ליטרל לכל פסוקית".

[00:20:55]–[00:21:59] — להוכחה יש גישה, לאלגוריתם אין. נקודה שהמרצה הדגיש כ"תמיד ככה, בכל הרדוקציות שעשינו": בהוכחת הנאותות מותר לנו להשתמש בהשמה המספקת ובקבוצה הבלתי תלויה, למרות שהאלגוריתם עצמו אינו רואה אותן. ההוכחה חיה **מעל** האלגוריתם.

[00:26:14]–[00:29:56] — טענת "לכל" מתחילה ב"תהא". גם אם בסוף רוצים להניח בשלילה. "זה מה שמציג לי את המשתנה." המרצה חזר על התיקון הזה שוב בכיוון השני של הרדוקציה השנייה [01:04:54].

[00:32:54] — לפרק את הטיעון. "כמה שאני יותר אפרק את הטיעון שלי, אני פחות פרון לעשות טעויות." גם כשהתשובה נכונה, דרך הגעה מקוצרת היא הרגל שיפיל אתכם במקום אחר.

[00:34:31]–[00:35:37] — "קיימת" ולא "ניתן לקבוע". "ניתן לקבוע" מרמז על יחידות שאיננה קיימת. בדוגמה יש שתי השמות.

[00:36:38]–[00:37:39] — הוכחת קיום אינה חייבת להיות אלגוריתמית. "במדעי המחשב הרבה פעמים נוח לי לעשות הוכחת קיום אלגוריתמית כי זו השפה שאני מדבר, אבל היא לא חייבת." הדוגמה הנגדית: "בכל עץ יש עלה" — הוכחה בסכימת דרגות, לא אלגוריתמית.

[00:40:49]–[00:41:51] — עד כמה לנמק במבחן? שאלת סטודנט. התשובה הכנה: "אין לי תשובה נוסחתית. צריך לנמק מספיק כדי שאני אדע שאתה יודע על מה אתה מדבר. ברגע שהשתכנעתי — you can get away with a lot." אבל **המבנה חייב להיות מבנה** — זה מה שמשדר שאתם יודעים מה הסדר הטבעי של הדברים.

[00:41:51] — הקשר לתרגיל הבית. הרדוקציה מ-SAT הופיעה כבר בתרגיל בית 2, שם עבור IS; ההבדל היחיד כאן הוא הוספת חלק המקסימליות.

[00:42:27]–[00:44:32] — "אני באמת לא יודע." לשאלה אם $\mathrm{MaxIS} \in \mathrm{NP}$ המרצה ענה שזו שאלה פתוחה, ובמפורש: אילו ידענו זאת, היינו מקבלים $\mathrm{NP} = \mathrm{coNP}$.

[00:46:44]–[00:49:22] — למה בוחרים לנסח רדוקציה בכיוון מסוים. "הבחירות שאני עושה לא שרירותיות. לפעמים הן שרירותיות ואז אני אומר שזה שרירותי לגמרי — אבל תבינו שיש חשיבה מאחורי הבחירה." והאנלוגיה: טענת "וגם" היא תרגיל כפל שכל כופל בו הוא תרגיל חיבור.

[00:52:50] — "קודקודים מבודדים? כמעט נכון." ההצעה של סטודנט הייתה כמעט הבנייה הנכונה; החיבור לכל הקודקודים הישנים הוא מה שמונע מהקבוצה החדשה להתערבב בישנה.

[00:59:54]–[01:00:24] — היזהרו מגודל ייצוג של מספר. "הגודל של k בייצוג הוא $\log k$, אז אני לא יכול באמת לחסום דרכו שום דבר." הפתרון: להניח בלי הגבלת הכלליות $k \le |V|$, כי אחרת התשובה טריוויאלית.

[01:09:51]–[01:11:54] — שאלת סטודנט (עומר). "האלגוריתם לא נוגע בקבוצות הבלתי תלויות, הוא רק מטפל בגרף." הטיעון "מורידים קודקוד מקבוצה בלתי תלויה ומקבלים קבוצה בלתי תלויה קטנה יותר" הוא טיעון של ההוכחה, ברמת ההגדרה — לא פעולה שהאלגוריתם מבצע. המרצה סימן זאת כ"ממש ממש חשוב".

[01:14:19]–[01:15:52] — מפת הבעיות הפתוחות. P מוכלת ב-$\mathrm{NP} \cap \mathrm{coNP}$, אבל לא ידוע אם בשוויון; לא ידוע אם $\mathrm{NP} = \mathrm{coNP}$; ולא ידוע אם קיימת שפה ב-$\mathrm{NP} \cap \mathrm{coNP}$ שאינה ב-P. "בחישוביות היה R, RE, והחיתוך היה בדיוק R — פה זה לא המצב."

[01:29:07] — אנקדוטה לסיום. המרצה סיפר על נואם ידוע שבשולי הנאום שלו נמצאה הערה לעצמו ליד טיעון חלש. המסר בהקשר של המבחן: תדעו על מה אתם מדברים ותכתבו בביטחון — אבל שהביטחון יהיה מכוסה בתוכן. (התמלול האוטומטי משבש את הנוסח המדויק של ההערה.)

פערים בין הסיכום להקלטה

מקור: ההקלטה [00:04:14]–[00:05:51]. **הפער:** הטיעון "אם $\mathrm{IS} \in \mathrm{P}$ אז $\mathrm{MaxIS} \in \mathrm{P}$" (סריקה על k עם פקטור $|V|$ נוסף) נאמר בהרצאה ואינו מופיע בסיכום כלל. **ההכרעה:** נכלל כמשפט 1, כי בלעדיו לא ברור מה בדיוק המקור לקושי של MaxIS.

מקור: ההקלטה [00:12:16] מול הסיכום, עמוד 1. **הפער:** בתמלול הפסוקית הרביעית נשמעת כ-$(x_1 \vee x_3 \vee x_4)$, אך בסיכום — ובכוונה המפורשת שהמרצה הצהיר עליה שנייה קודם ("בואו נעשה אחד שהוא בגודל שתיים") — היא $(x_1 \vee x_3)$. **ההכרעה:** נלקחה גרסת הסיכום. באופן דומה, התמלול [00:14:56] מזכיר קשת בין $\overline{x_4}$ ל-x_4, אך ב-φ אין מופע של $\overline{x_4}$ ואין קשת כזו.

מקור: הסיכום, עמוד 1 מול עמודים 2–3. **הפער:** הקשתות "ליטרל–שלילתו" מצוירות בציור בעיפרון כחול אך נקראות "קשתות שחורות" בטקסט ההוכחה ובהרצאה. **ההכרעה:** אומץ המינוח **אדומות/שחורות** בכל הקובץ, כדי שהטקסט וההוכחות יהיו עקביים.

מקור: הסיכום, עמוד 1 מול ההקלטה. **הפער:** הסיכום משתמש באות V פעמיים — גם לקבוצת הקודקודים וגם להשמה המספקת ("$V(x_1) = 1$"). **ההכרעה:** ההשמה סומנה כאן $\mathcal{V}$; קבוצת הקודקודים נשארה V, כדרישת הסימון של הסיכום.

מקור: הסיכום, עמוד 2. **הפער:** חסם המקסימליות $|\hat{U}| \le m$ מובא שם בשלילה בלבד (שובך יונים). בהרצאה [00:29:26] המרצה הוסיף מפורשות את הגרסה הישירה ואמר שהיא עדיפה מבחינת מבנה. **ההכרעה:** שתי הגרסאות מובאות, הישירה ראשונה.

מקור: הסיכום, עמוד 3 (הקופסה הכחולה). **הפער:** למת המשלימים רשומה שם ללא הוכחה וללא הצמדה למקום השימוש. **ההכרעה:** הוכחה במלואה (למה 3.1) והוצמדה לשתי הנקודות שבהן היא משמשת — מסקנה 3.2 ולמה 4.1.

מקור: שני המקורות. **הפער:** המקרה $k = 0$ ברדוקציה השנייה יוצר פלט $\langle \hat{G}, -1 \rangle$ שאינו מופע חוקי. **ההכרעה:** הושלם בגוף השיעור — עבור $k = 0$ הרדוקציה מחזירה מחרוזת קבועה שאיננה ב-MaxIS. באופן דומה, ההנחה $k \le |V|$ (שנאמרה בהרצאה [01:00:24] רק לצורך זמן הריצה) נוסחה כאן כטיפול מפורש במקרה $k > |V|$.

מקור: תוספת שלנו. **הפער:** אף אחד מהמקורות אינו דן בפסוקית ריקה או בפסוקית המכילה ליטרל ואת שלילתו. **ההכרעה:** נוספה הערה טכנית קצרה אחרי משפט 2 — שני המקרים אינם פוגמים בנאותות.

מקור: ההקלטה [01:28:04]. **הפער:** המרצה השאיר את ההצדקה ש-$\mathrm{IS}^{\le} \in \mathrm{coNP}$ ברמת "בשלוש מילים אתה מסביר למה זה ב-NP". **ההכרעה:** נכתבו שתי ההצדקות במלואן (רדוקציה $k \mapsto k+1$, ומאמת ישיר), וכן פורטה הוכחת הסגירות של NP לחיתוך, שנאמרה בהרצאה במילה אחת.

מקור: הנחיית הרכז מול המקורות. **הפער:** הרכז צפה שיעור על **קירוב** ל-Max Independent Set (חסם מסוג Turán, שיטה הסתברותית) והנחה `prereq_lessons: [7, 10, 13, 18]`. **ההכרעה:** בשיעור אין קירוב, אין הסתברות ואין אקראיות; הוא כולו רדוקציות ומחלקות משלימות.

נרשמו `[7, 9, 10, 21]` , והפער נרשם גם ב- `open_questions` .

סיכום ונקודות למבחן

הדברים שכדאי לזכור בעל פה

$\text{MaxIS} = \{\langle G, k\rangle \mid \alpha(G) = k\}$, ומיד לפרק: **קיימת** קבוצה בלתי תלויה בגודל k, **וגם** כל קבוצה בלתי תלויה היא בגודל $\leq k$.

$\text{SAT} \leq_p \text{MaxIS}$: קודקוד לכל מופע ליטרל, **קליקה אדומה** בכל פסוקית, **קשת שחורה** בין ליטרל לשלילתו, והמספר הוא m = מספר הפסוקיות.

$\overline{\text{IS}} \leq_p \text{MaxIS}$: מוסיפים $k-1$ קודקודים, מחברים כל אחד מהם לכל הקודקודים **הישנים** ולא זה לזה, ומחזירים $\langle \hat{G}, k-1\rangle$.

MaxIS היא **NP-קשה וגם coNP-קשה**, ולכן $\text{MaxIS} \in \text{NP} \cup \text{coNP} \iff \text{NP} = \text{coNP}$.

אין לומר "MaxIS NP-שלמה" — שייכותה ל-NP שקולה לבעיה פתוחה.

המלכודות הסטנדרטיות

לשכוח את חצי המקסימליות. ההוכחה ש-$\text{SAT} \leq_p \text{IS}$ מסתיימת אחרי בניית U בגודל m; ההוכחה ש-$\text{SAT} \leq_p \text{MaxIS}$ **לא** — חייבים גם את $\alpha(G_\varphi) \leq m$.

לפתוח טענת "לכל" בהנחה בשלילה. תמיד קודם "תהא U קבוצה בלתי תלויה", ורק אחר כך, אם רוצים, "נניח בשלילה".

לכתוב "ניתן לקבוע את ההשמה". הניסוח הנכון הוא "קיימת השמה"; אין יחידות.

להפוך את כיוון הרדוקציה. $A \leq_p B$ פירושו ש-B קשה יותר. כדי להוכיח קושי של L מפחיתים **אל** L.

לחשוב שקשת שחורה מחברת שני מופעים של אותו ליטרל. לא — רק ליטרל ושלילתו. בלי זה הקבוצה $\{u_4, u_{10}\}$ בדוגמה לא הייתה חוקית.

לחסום זמן ריצה באמצעות k. בייצוג הקלט k תופס $\log k$ ביטים. חוסמים באמצעות $|V|$.

לשכוח שהרדוקציה השנייה לא מחברת את הקודקודים החדשים זה לזה. אם נחבר גם ביניהם, הקבוצה החדשה לא תהיה בלתי תלויה וההוכחה תיפול.

צ'ק-ליסט: מה סטודנט צריך לדעת לעשות אחרי השיעור

לפרק בעיית "מקסימום/מינימום" לטענת קיום וטענת "לכל", ולזהות שזו טענת "וגם".

לבנות את G_φ עבור CNF נתון, לספור קודקודים וקשתות, ולהריץ את שני כיווני הנאותות על מופע קונקרטי.

להוכיח את **שני** חלקי השייכות ל-MaxIS, כל אחד בנפרד.

להשתמש בלמת המשלימים כדי להפוך רדוקציה בין שפות לרדוקציה בין משלימותיהן, ולהסיק coNP-קשיות מ-NP-שלמות של IS.

להוכיח טענות מהצורה "$L \in \mathcal{C}$ אם ורק אם [בעיה פתוחה]": לבחור את הבעיה הפתוחה, לחלק למקרים לפי איבר האיחוד, ולפרק את L לחיתוך של רכיב ב-NP ורכיב ב-coNP.

לנמק זמן ריצה של רדוקציה במונחי $|V|$ ולא במונחי k.

שאלות שנשארו פתוחות

הרכז הנחה prereq_lessons=[7,10,13,18] מתוך הנחה שהשיעור עוסק בקירוב ל-Max Independent Set; בפועל אין בשיעור אף מילה על יחסי קירוב או על הסתברות, ולכן נרשמו [7,9,10,21]. יש להכריע ברמת המניפסט.

ה-slug 'max-independent-set' מדויק בשמו אך עלול להיקרא כאילו מדובר באלגוריתם קירוב; מדובר בבעיית ההכרעה 'האם המקסימום הוא בדיוק k'.

עמוד 1 בסיכום: הסיכום משתמש באות V גם לקבוצת הקודקודים וגם להשמה המספקת; כאן ההשמה סומנה $\mathcal{V}$ כדי למנוע התנגשות.

עמוד 3 בסיכום: המסגרת הכחולה (למת המשלימים) נכתבה ללא הוכחה ובלי להצמיד אותה למקום שבו היא משמשת; השיבוץ כאן הוא שחזור לפי ההקלטה [00:45:38].

המקרה $$k=0$$ ברדוקציה $\le_p\mathrm{MaxIS}$ אינו מטופל בשני המקורות (הפלט היה $$k-1=-1$$); הושלם כאן בגוף השיעור.

בהקלטה [01:29:07] מסופרת אנקדוטה על הערת שוליים בנאום; התמלול האוטומטי משבש את הניסוח והובא כאן רק הרעיון.

23 חזרה למבחן א׳: פתרון מטלה 1 ושאלה 1 ממבחן 2

שיעור חזרה שכולו פתרון תרגילים: סידור שבע מחלקות סיבוכיות לפי הכלה, המחלקה TISP, שתי ההוכחות ש-NP מוכלת ב-EXP וב-PSPACE, וארבע טענות רדוקציה ממבחן — שלוש מהן עם אלגוריתם שגוי שיש להפריך.

ביטחון: low | ללא הקלטה

בקצרה

זהו הראשון מארבעה שיעורי חזרה. אין בו תיאוריה חדשה: הוא פתרון מלא של **מטלה 1** (שאלות 3, 4, 8) ושל **שאלה 1 ממבחן 2** (סעיפים א, ד, ה, ו).

סידור שבע מחלקות סיבוכיות לפי הכלה, וקביעה לגבי כל הכלה האם היא שוויון או הכלה ממש. התוצאה: שלוש מהמחלקות "המפחידות" מתמוטטות ל-P או ל-EXP, ושלוש ההכלות שנשארות הן ממש — כולן דרך משפט ההיררכיה בזמן.

המחלקה $\mathrm{TISP}(f,g)$ (חסם זמן וחסם מקום בו-זמנית): מוכיחים ש-$\mathrm{TISP}(f,f)=\mathrm{DTime}(f)$, ומסיקים שהטענה $\bigcup_c \mathrm{TISP}(n^c,n^c)=\mathrm{PSPACE}$ שקולה לשאלה הפתוחה $\mathrm{P}=\mathrm{PSPACE}$.

שתי הוכחות שונות לחסם עליון על NP: $\mathrm{NP}\subseteq\mathrm{EXP}$ דרך סריקת עץ הריצות של מכונה אי-דטרמיניסטית, ו-$\mathrm{NP}\subseteq\mathrm{PSPACE}$ דרך מעבר על כל העדים. הנקודה שהמרצה הדגיש: **אותה מכונה בדיוק** משמשת לשתי ההוכחות — היא צנועה במקום ובזבזנית בזמן.

שלוש טענות רדוקציה שהאלגוריתם המוצע להן שגוי, וזה עיקר השיעור: פלט שאינו קלט חוקי של בעיית היעד; פונקציית הזהות שאינה שומרת על כיוון ההכרעה; ואלגוריתם שבונה מספר אקספוננציאלי של קודקודים. בשלושתן **הטענה עצמה נכונה** — רק ההוכחה קרסה.

הסעיף האחרון של שאלת המבחן נגמר בשאלה מושגית: $\text{MAX-IS}\le_p \text{IS}$ מתקיים תמיד, ואילו $\text{IS}\le_p \text{MAX-IS}$ מתקיים **אם ורק אם** $\mathrm{NP}=\mathrm{coNP}$.

מי שקורא רק את הסעיף הזה יכול לדלג — אבל לא כדאי: קובץ זה הוא בדיוק סוג העבודה שהמבחן דורש.

רקע ותלויות

שיעור חזרה נשען על כל מה שקדם לו. אלה התוצאות שהתרגילים כאן משתמשים בהן בפועל, ואת כולן נחזור ונצטט במלואן בסעיף הבא כדי שלא תצטרכו לקפוץ:

המחלקות העדינות והגסות — $\mathrm{DTime}(f)$, $\mathrm{DSpace}(f)$, ומעליהן $\mathrm{P}=\bigcup_{c\ge1}\mathrm{DTime}(n^c)$, $\mathrm{EXP}=\bigcup_{c\ge1}\mathrm{DTime}(2^{n^c})$, $\mathrm{PSPACE}=\bigcup_{c\ge1}\mathrm{DSpace}(n^c)$ (ראו שיעור 2). שייכות למחלקה גסה היא **טענת קיום** — קודם "מקלפים" את הקיים ורק אז מגיעים למכונה.

מונוטוניות — אם $f=O(g)$ אז $\mathrm{DTime}(f)\subseteq\mathrm{DTime}(g)$ (שיעור 2, משפט 4). זהו סוס העבודה של תרגיל 1: כמעט כל הכלה שם היא הערכת סדר גודל אחת ואז ציטוט המשפט.

הקשר בין מקום לזמן — $\mathrm{space}_M(x)\le\mathrm{time}_M(x)$ (שיעור 2, משפט 2; ובמודל האי-דטרמיניסטי שיעור 4, משפט 3). זהו כל תרגיל 2 סעיף (א).

משפט ההיררכיה בזמן (שיעור 3, משפט 4) — היחיד שיודע להוכיח **הכלה ממש**. בלעדיו אין לתרגיל 1 סעיף שני.
מכונות אי-דטרמיניסטיות ועץ הריצות (שיעור 4) — הגדרת ההכרעה האי-דטרמיניסטית, וספירת הקונפיגורציות.
שתי ההגדרות של NP — עם מכונת הכרעה אי-דטרמיניסטית (שיעור 4) ועם מוודא דטרמיניסטי ועד (שיעור 6). התרגיל דורש במפורש הוכחה **לכל הגדרה בנפרד**.
$\mathrm{NP} \subseteq \mathrm{PSPACE}$ (שיעור 8, משפט 1) ו**סגירות** $\mathrm{P}, \mathrm{NP}, \mathrm{PSPACE}$ **כלפי מטה תחת** $\leq_p$ (שיעור 7 ושיעור 8).
רדוקציות, NP-קשיות ו-NP-שלמות (שיעור 7), והשפות IS ו-SAT (שיעורים 5, 7).
$\mathrm{MAX\text{-}IS}$**, קשיותה משני הצדדים, והקשר ל-**$\mathrm{NP} = \mathrm{coNP}$ (שיעור 22).
תזכורת על כיוון הרדוקציה, כי בעל פה מבלבלים בזה תמיד: $A \leq_p B$ פירושו שקיימת פונקציה f הניתנת לחישוב בזמן פולינומי כך שלכל x מתקיים $x \in A \iff f(x) \in B$. כלומר B **היא הקשה מבין השתיים**: מי שיודע לפתור את B יודע לפתור גם את A.

הגדרות

הסעיף הזה קצר בכוונה — נזכיר רק את מה שהתרגילים כאן באמת משתמשים בו.

הגדרה 1: $\mathrm{TISP}(f, g)$

תהיינה $f, g : \mathbb{N} \to \mathbb{N}$. המחלקה $\mathrm{TISP}(f, g)$ היא מחלקת השפות $A \subseteq \Sigma^*$ שעבורן **קיימת** מכונת טיורינג M עם אלפבית קלט Σ ו**קיימים** קבועים $c, d > 0$ כך ש-M מכריעה את A, **וגם** לכל $x \in \Sigma^*$ מתקיים

$$\mathrm{time}_M(x) \leq c \cdot f(|x|) \qquad \text{and} \qquad \mathrm{space}_M(x) \leq d \cdot g(|x|).$$

אינטואיציה. השם הוא ראשי תיבות של TIme–SPace: זו מחלקה שדורשת משאב אחד **בו-זמנית** בשני החסמים — לא "יש מכונה מהירה ויש מכונה חסכונית", אלא "יש מכונה **אחת** שהיא גם מהירה וגם חסכונית". הסדר של הכמתים הוא הרגיל: קודם המכונה והקבועים, ואחר כך כל הקלטים.

מופע. $\mathrm{PAL} \in \mathrm{TISP}(n^2, n)$: האלגוריתם הנאיבי לפלינדרומים רץ בזמן $O(n^2)$ ואינו כותב מחוץ לאזור הקלט.

אי-מופע שמחדד את הגבול. המכונה שעוברת על כל העדים בהוכחת $\mathrm{NP} \subseteq \mathrm{PSPACE}$ (תרגיל 3(ב) להלן) מעידה על שייכות ל-$\mathrm{DSpace}(n^k)$, אבל **לא** על שייכות ל-$\mathrm{TISP}(n^k, n^k)$: זמן הריצה שלה אקספוננציאלי. שני החסמים חייבים להיתפס על ידי אותה מכונה.

הגדרה 2: ספיקות מסוג NAE ובעיית $4\mathrm{NAE}$

השמה V **מספקת נוסחה באופן** **NAE** (Not-All-Equal) אם בכל הסגר יש לפחות ליטרל אחד שערכו True **וגם** לפחות ליטרל אחד שערכו False — כלומר, ערכי הליטרלים בהסגר אינם כולם שווים.

$4\mathrm{NAE}$ היא שפת נוסחאות ה-4CNF שקיימת עבורן השמה המספקת אותן באופן NAE.

אינטואיציה. ספיקות רגילה דורשת "לפחות אחד אמת"; NAE דורשת בנוסף "לפחות אחד שקר". זו דרישה **סימטרית** בין אמת לשקר, ומכאן נובעת התכונה המרכזית שמשמשת בתרגיל 4 (ראו משפט 5).

מופע. $(x_1 \vee x_2)$ עם $V(x_1) = \mathrm{True}, V(x_2) = \mathrm{False}$ — מסופקת באופן NAE.

אי-מופע. ההשמה $V(x_1) = V(x_2) = \text{True}$ מספקת את $(x_1 \vee x_2)$ במובן הרגיל אך **לא** באופן NAE.

הגדרה 3: IS ו-MAX-IS

$$\text{IS} = \{\langle G, k\rangle \mid \text{there is an independent set of size } k \text{ in } G\},\ \text{MAX-IS} = \{\langle G, k\rangle \mid \text{the maximum size of an independent set in } G \text{ equals } k\}.$$

אינטואיציה, וזו הנקודה שכל תרגילים 5–6 יושבים עליה. IS היא טענת **קיום** בלבד. MAX-IS היא טענת **וגם**: קיימת קבוצה בגודל k, **וגם** כל קבוצה בלתי תלויה היא בגודל לכל היותר k. החלק הראשון ב-NP, החלק השני ב-coNP — ולכן שתי השפות מתנהגות אחרת לגמרי (ראו שיעור 22).

מופע. G = שני קודקודים ללא קשת, $k = 2$: $\langle G, 2\rangle \in \text{MAX-IS}$ וגם $\langle G, 2\rangle \in \text{IS}$.

אי-מופע שמפריד בין השתיים. אותו G עם $k = 1$: $\langle G, 1\rangle \in \text{IS}$ (קודקוד בודד הוא קבוצה בלתי תלויה בגודל 1), אבל $\langle G, 1\rangle \notin \text{MAX-IS}$ (המקסימום הוא 2). זהו בדיוק הזוג שמפריך את שני האלגוריתמים בתרגילים 5–6.

משפטים והוכחות

בשיעור חזרה, סעיף זה אינו המקום להוכיח מחדש את מה ששיעור קודם כבר הוכיח. להלן התוצאות שהתרגילים נשענים עליהן, כל אחת בניסוח מדויק, עם הפניה מפורשת לשיעור שמחזיק את ההוכחה — ועם הוכחה מלאה רק היכן שאף שיעור קודם אינו מחזיק אותה.

משפט 1: מונוטוניות ביחס לסדר גודל

> תהיינה $f, g : \mathbb{N} \to \mathbb{N}$. אם $f = O(g)$ אז $\text{DTime}(f) \subseteq \text{DTime}(g)$, ובאותו אופן $\text{DSpace}(f) \subseteq \text{DSpace}(g)$.

ההוכחה — שיעור 2, משפט 4. בשורה אחת: אם M ו-c מעידים על $A \in \text{DTime}(f)$ ו- $f \le c_0 \cdot$ g, אז **אותה מכונה** עם הקבוע $c \cdot c_0$ מעידה על $A \in \text{DTime}(g)$. אין בנייה, רק החלפת קבוע.

למה זה כל כך חשוב כאן. כל אחת מההכלות (להבדיל מההכלות-ממש) בתרגיל 1 היא בדיוק שימוש אחד במשפט הזה, ולכן כל העבודה בתרגיל 1 היא **חשבון סדרי גודל**, לא בניית מכונות.

משפט 2: משפט ההיררכיה בזמן

> תהיינה $f, g : \mathbb{N} \to \mathbb{N}$. נניח כי (1) $g = o(f)$; (2) f ישימה בזמן; (3) f סופר-לינארית. אז $\text{DTime}(g) \subsetneq \text{DTime}\big(f^2\big)$.

ההוכחה — שיעור 3, משפט 4 (ושם גם ההסבר מאיפה צומח הריבוע: המעבר ממכונה רב-סרטית למכונה חד-סרטית עולה ריבוע בזמן, בעוד שבמקום הוא עולה רק קבוע).

איך משתמשים בו נכון — וזו הטעות הנפוצה. המשפט אינו אומר "יש שפה קשה"; הוא אומר שקיימת שפה ב-$\text{DTime}(f^2)$ שאינה ב-$\text{DTime}(g)$. כדי להוכיח $\mathcal{C}_1 \subsetneq \mathcal{C}_2$ בין שתי מחלקות **גסות** צריך תמיד את אותו ריקוד בן שלושה צעדים:

לחסום את המחלקה הקטנה בתוך מחלקה **עדינה** אחת: $\mathcal{C}_1 \subseteq \text{DTime}(g)$.

לבחור f ישימה בזמן וסופר-לינארית כך ש-$g = o(f)$ **וגם** $\text{DTime}(f^2) \subseteq \mathcal{C}_2$.

להסיק $\mathcal{C}_1 \subseteq \text{DTime}(g) \subsetneq \text{DTime}(f^2) \subseteq \mathcal{C}_2$.

צעד 1 הוא היחיד שדורש מחשבה, והוא אפשרי רק מפני שהאיחוד הוא של פונקציות שכולן נבלעות בפונקציה אחת גדולה יותר.

הערה: הסיכום מציין עבור $2^{n^6/2}$ רק שהיא "סופר-לינארית". תנאי הישימות בזמן נדרש גם הוא, והוא אכן מתקיים לכל הפונקציות מהצורה $2^{p(n)}$ עבור פולינום p בעל מקדמים טבעיים; השלמתי אותו בגוף הפתרון.

משפט 3: מקום חסום בזמן

לכל מכונה M ולכל קלט x שעליו M עוצרת: $\mathrm{space}_M(x) \le \mathrm{time}_M(x)$.

ההוכחה — שיעור 2, משפט 2 (ובמודל האי-דטרמיניסטי: שיעור 4, משפט 3). הטיעון בשורה אחת: בכל צעד הראש זז לכל היותר תא אחד, ולכן מספר התאים השונים שבהם ביקרה המכונה אינו עולה על מספר הצעדים שביצעה.

זהו כל תרגיל 2 סעיף (א) — הכיוון הלא-טריוויאלי שם הוא ציטוט אחד של המשפט הזה.

משפט 4: $\mathrm{NP} \subseteq \mathrm{PSPACE}$ (בהגדרת המוודא)

כל שפה ב-NP ניתנת להכרעה במקום פולינומי.

ההוכחה במלואה — שיעור 8, משפט 1. המכונה M_A מקבלת x, מחשבת את $q(|x|)$, ועוברת בסדר לקסיקוגרפי על כל $w \in \{0,1\}^{q(|x|)}$; לכל w היא מריצה את המוודא M על (x, w) ומקבלת אם M קיבלה; בסוף הלולאה היא דוחה. **הנקודה שהכול תלוי בה:** לפני כל איטרציה מוחקים את סרט העבודה, ולכן המקום אינו מצטבר, אף שמספר האיטרציות אקספוננציאלי.

מה שהסיכום מוסיף כאן ואינו בשיעור 8 (ההערה הכחולה בעמוד 5): **אותה מכונה בדיוק**, אם מסתכלים עליה במשקפי זמן ולא במשקפי מקום, רצה בזמן $2^{q(|x|)} \cdot \mathrm{poly}(|x|)$ — אקספוננציאלי — ולכן היא מוכיחה בו-זמנית גם $\mathrm{NP} \subseteq \mathrm{EXP}$. זה הופך אותה לפתרון חלופי מלא לסעיף (א) של תרגיל 3, בלי לגעת בעץ הריצות.

משפט 5: עץ הריצות של מכונה אי-דטרמיניסטית

זהו החישוב שסעיף (א) של תרגיל 3 בנוי עליו, ולכן הוא כתוב כאן במלואו.

תהא M מכונת טיורינג אי-דטרמיניסטית ויהי x קלט. נתבונן בעץ **כל הריצות האפשריות** של M על x: הקודקודים הם הקונפיגורציות המופיעות בריצות, והקשתות הן צעדי δ. אז:

מספר הבנים של כל צומת חסום ב-$\alpha = |Q| \cdot |\Gamma| \cdot 2$;

אם $\mathrm{time}_M(x) \le T$ אז עומק העץ חסום ב-T;

מספר הצמתים בעץ חסום ב-$\displaystyle\sum_{i=0}^{T} \alpha^i = O\!\left(\alpha^{T+1}\right) = O\!\left(2^{(\lg \alpha)(T+1)}\right)$.

הוכחה. (1) צעד יחיד של M מקונפיגורציה נתונה נקבע כולו על ידי שלישייה: המצב שאליו עוברים ($|Q|$ אפשרויות), האות הנכתבת ($|\Gamma|$ אפשרויות), וכיוון תזוזת הראש (שתי אפשרויות). לכן δ יכולה להציע לכל היותר $|Q| \cdot |\Gamma| \cdot 2$ המשכים שונים, וזה מספר הבנים.

(2) מסלול מהשורש לעלה הוא בדיוק ריצה אפשרית אחת, ואורכו הוא מספר הצעדים באותה ריצה. לפי הגדרת $\mathrm{time}_M(x)$ כמקסימום על פני כל הריצות האפשריות, אורך כל מסלול חסום ב-T.
(3) עץ שבו לכל צומת לכל היותר α בנים ושעומקו לכל היותר T מכיל לכל היותר α^i צמתים ברמה i, ולכן לכל היותר $1 + \alpha + \alpha^2 + \cdots + \alpha^T$ צמתים בסך הכול. זהו סכום סדרה הנדסית, וכשהמנה קבועה וגדולה מ-1 הוא מסדר גודל האיבר האחרון: $O(\alpha^{T+1})$. הכתיבה מחדש בבסיס 2 היא זהות: $\alpha^{T+1} = 2^{(\lg \alpha)(T+1)}$. ■

> **הערה:** בסיכום החזקה נכתבה פעמיים $|x|^2$ ופעם אחת $|x|^c$ באותו חישוב עצמו. מכיוון שהחסם על זמן הריצה שממנו הכול נגזר הוא $d \cdot |x|^c$, המעריך הנכון בכל שלושת המקומות הוא c; כך כתוב כאן.

משפט 6: התכונה הסימטרית של ספיקות NAE

> תהא φ נוסחת CNF ותהא V השמה למשתני φ המספקת אותה באופן NAE. תהא $\widehat{V}$ ההשמה המשלימה, כלומר $\widehat{V}(y) = \neg V(y)$ לכל משתנה y. אז גם $\widehat{V}$ מספקת את φ באופן NAE.

הוכחה. יהי C הסגר של φ. לפי ההנחה קיימים ב-C ליטרל ℓ_1 שערכו תחת V הוא True וליטרל ℓ_2 שערכו תחת V הוא False. היפוך ערכו של כל משתנה הופך את ערכו של כל ליטרל, ולכן תחת $\widehat{V}$ ערכו של ℓ_1 הוא False וערכו של ℓ_2 הוא True. שוב יש ב-C ליטרל אמת וליטרל שקר, כלומר C מסופק באופן NAE. הטענה נכונה לכל הסגר, ולכן $\widehat{V}$ מספקת את φ באופן NAE. ■

למה זה בדיוק המנוע של תרגיל 4. התכונה הזו היא שמאפשרת "להניח בלי הגבלת הכלליות" שהמשתנה החדש קיבל False — וזה כל מה שהאלגוריתם שבשאלה ניסה להשיג בכוח, על ידי צירוף השמה לפלט.

משפט 7: מתי $\text{MAX-IS} \le_p \text{IS}$

> $\text{MAX-IS} \le_p \text{IS}$ אם ורק אם $\text{NP} = \text{coNP}$.

ההוכחה — שיעור 22, שבו הוכח ש-MAX-IS היא גם NP-קשה וגם coNP-קשה, וש-$\text{MAX-IS} \in \text{NP} \cup \text{coNP}$ שקולה ל-$\text{NP} = \text{coNP}$. שתי הרוחות של הטיעון, בקצרה, כדי שהמסקנה בתרגיל 6 לא תיפול מהשמיים:

($\Rightarrow$) נניח $\text{MAX-IS} \le_p \text{IS}$. מכיוון ש-$\text{IS} \in \text{NP}$ ו-NP סגורה כלפי מטה תחת $\le_p$ (שיעור 7), נובע $\text{MAX-IS} \in \text{NP}$. אבל MAX-IS היא coNP-קשה, ושפה coNP-קשה שנמצאת ב-NP גוררת $\text{coNP} \subseteq \text{NP}$ ומכאן $\text{NP} = \text{coNP}$.

($\Leftarrow$) נניח $\text{NP} = \text{coNP}$. השייכות $\langle G, k\rangle \in \text{MAX-IS}$ היא חיתוך של שתי טענות: "קיימת קבוצה בלתי תלויה בגודל k" (ב-NP) ו"כל קבוצה בלתי תלויה היא בגודל לכל היותר k" (ב-coNP). תחת ההנחה שתיהן ב-NP, ו-NP סגורה לחיתוך, ולכן $\text{MAX-IS} \in \text{NP}$. מכיוון ש-IS היא NP-שלמה, קיימת רדוקציה $\text{MAX-IS} \le_p \text{IS}$.

דוגמאות ותרגילים מהשיעור

זהו לב הקובץ. שלושת התרגילים הראשונים הם מ**מטלה 1** (שאלות 4, 3, 8 בהתאמה — הסיכום פותר אותן בסדר הזה), וארבעת האחרונים הם סעיפים משאלה 1 של **מבחן 2**.

תרגיל 1 (מטלה 1, שאלה 4): סידור שבע מחלקות סיבוכיות

הנוסח. נתונות שבע מחלקות סיבוכיות:

$$\bigcup_{c\geq 1}\mathrm{DTime}\left(n^{(2^c)}\right),\quad \bigcup_{c\geq 1}\mathrm{DTime}(c^{cn}),\quad \bigcup_{c\geq 1}\mathrm{DTime}\left(c^{n^c}\right),\quad \bigcup_{c\geq 1}\mathrm{DTime}\left(n^{n^c}\right).$$

סדרו את המחלקות בשורה כך שכל מחלקה מכילה את קודמתה. לגבי כל אחת מההכלות המתקבלות, קבעו האם מדובר בשוויון או בהכלה ממש.

התשובה.

$$\bigcup_{c\geq 1}\mathrm{DTime}\left(n^{2^c}\right)=\mathrm{P}\subsetneq\bigcup_{c\geq 1}\mathrm{DTime}(c^{cn})\subsetneq\mathrm{DTime}\left(2^{n^6}\right)\subsetneq\mathrm{EXP}=\bigcup_{c\geq 1}\mathrm{DTime}\left(c^{n^c}\right)=\bigcup_{c\geq 1}\mathrm{DTime}\left(n^{n^c}\right).$$

כלומר: שלוש מהמחלקות מתמוטטות למחלקות מוכרות, ושלוש ההכלות שנשארות הן ממש.

שלב א: $\mathrm{P}=\bigcup_{c\geq 1}\mathrm{DTime}(n^{2^c})$

כיוון ראשון. תהא $A\in\mathrm{P}$. לפי הגדרת P קיים $c\geq 1$ כך ש-$A\in\mathrm{DTime}(n^c)$. לכל $n\geq 1$ מתקיים $c\leq 2^c$, ולכן לכל $n\geq 1$ מתקיים $n^c\leq n^{2^c}$, כלומר $n^c=O(n^{2^c})$. לפי משפט 1 נובע $A\in\mathrm{DTime}(n^{2^c})$, ובפרט $A\in\bigcup_{c\geq 1}\mathrm{DTime}(n^{2^c})$.

כיוון שני. תהא $A\in\bigcup_{c\geq 1}\mathrm{DTime}(n^{2^c})$. לפי הגדרת האיחוד קיים $c\geq 1$ כך ש-$A\in\mathrm{DTime}(n^{2^c})$. נסמן $d=2^c$; זהו מספר טבעי המקיים $d\geq 1$, ולכן $A\in\mathrm{DTime}(n^d)\subseteq\bigcup_{d\geq 1}\mathrm{DTime}(n^d)=\mathrm{P}$. ■

> **הערה:** בסיכום נכתב בשורה האחרונה $\bigcup_{d\geq 1}\mathrm{DTime}(2^d)=\mathrm{P}$. זו פליטת קולמוס: המחלקה $\mathrm{DTime}(2^d)$ עבור d קבוע היא זמן **קבוע**, וההגדרה של P היא $\bigcup_{d\geq 1}\mathrm{DTime}(n^d)$. תוקן כאן.

מה הרעיון מאחורי התוצאה. 2^c נראה מפחיד, אבל הוא **חזקה קבועה** — כשמאחדים על כל c, "החזקה הקבועה הגדולה" מתגלה כסתם עוד חזקה קבועה. זה בדיוק מה שהמרצה חזר עליו בשיעור העוקב: "לא כל מה שיש לו צורה מעריכית הוא מעריכי; מה שמעניין הוא אם זה מעריכי **כפונקציה של אורך הקלט**" ([00:59:55], הקלטת שיעור 24).

שלב ב: $\mathrm{EXP}=\bigcup_{c\geq 1}\mathrm{DTime}(n^{n^c})$

כיוון ראשון. תהא $A\in\mathrm{EXP}$, כלומר קיים $c\geq 1$ עם $A\in\mathrm{DTime}(2^{n^c})$. לכל $n\geq 2$ מתקיים $n\leq 2^{n^c}$ ולכן $2^{n^c}\leq n^{n^c}$, כלומר $2^{n^c}=O(n^{n^c})$. לפי משפט 1, $A\in\mathrm{DTime}(n^{n^c})$, ובפרט באיחוד.

כיוון שני. תהא $A\in\bigcup_{c\geq 1}\mathrm{DTime}(n^{n^c})$, ויהי $c\geq 1$ עם $A\in\mathrm{DTime}(n^{n^c})$. נכתוב $n^{n^c}=2^{n^c\cdot\lg n}$.

מכיוון ש-$\lg n\leq n$ לכל $n\geq 1$, מתקיים $n^c\cdot\lg n\leq n^{c+1}$, ולכן $n^{n^c}\leq 2^{n^{c+1}}$, כלומר $A\in\mathrm{DTime}\left(2^{n^{c+1}}\right)\subseteq\mathrm{EXP}$ לפי משפט 1, $O\left(2^{n^{c+1}}\right)$. ■

שלב ג: $\mathrm{EXP} = \bigcup_{c \geq 1} \mathrm{DTime}(c^{n^c})$
הסיכום אינו מטפל במחלקה הזו; היא נסגרת באותה טכניקה בדיוק ולכן היא כתובה כאן במלואה.
כיוון ראשון ($\subseteq$). יהי $c \geq 1$. אז $c^{n^c} = 2^{(\lg c) \cdot n^c}$. הגודל $\lg c$ הוא **קבוע** שאינו תלוי ב-n, ולכן לכל n גדול מספיק $(\lg c) \cdot n^c \leq n^{c+1}$, כלומר $c^{n^c} = O\left(2^{n^{c+1}}\right)$. לפי משפט 1, $\mathrm{DTime}(c^{n^c}) \subseteq \mathrm{DTime}\left(2^{n^{c+1}}\right) \subseteq \mathrm{EXP}$, ומכאן שגם האיחוד מוכל ב-EXP.
כיוון שני ($\supseteq$). תהא $A \in \mathrm{EXP}$ עם $A \in \mathrm{DTime}(2^{n^c})$. נבחר $c' = \max\{c, 2\}$. אז $2^{n^c} \leq 2^{n^{c'}} \leq (c')^{n^{c'}}$ (האי-שוויון האחרון כי $c' \geq 2$), ולכן $A \in \mathrm{DTime}\left((c')^{n^{c'}}\right)$, שהוא אחד מאיברי האיחוד. ■
שלב ד: $\bigcup_{c \geq 1} \mathrm{DTime}(c^{cn})$ — המחלקה שנופלת בין P ל-$\mathrm{DTime}(2^{n^6})$
גם המחלקה הזו אינה מטופלת בסיכום. נכתוב $c^{cn} = 2^{c \lg c \cdot n}$, ולכן
$$\bigcup_{c \geq 1} \mathrm{DTime}(c^{cn}) = \bigcup_{k \geq 1} \mathrm{DTime}\left(2^{kn}\right),$$
כלומר זו מחלקת הזמן **האקספוננציאלי הלינארי**: המעריך גדל לינארית ב-n, ורק המקדם משתנה.
נסמן אותה $\mathcal{E}$.
$\mathrm{P} \subseteq \mathcal{E}$: לכל d קבוע מתקיים $n^d = O(2^n)$, ולכן $\mathrm{DTime}(n^d) \subseteq \mathrm{DTime}(2^n)$ לכל d, ומכאן $\mathrm{P} \subseteq \mathrm{DTime}(2^n) \subseteq \mathcal{E}$.
$\mathcal{E} \subseteq \mathrm{DTime}(2^{n^6})$: לכל k קבוע ולכל n גדול מספיק מתקיים $kn \leq n^6$, ולכן $2^{kn} = O\left(2^{n^6}\right)$, ולפי משפט 1 גם $\mathrm{DTime}(2^{kn}) \subseteq \mathrm{DTime}(2^{n^6})$.
שלב ה: ההכלה $\mathrm{DTime}(2^{n^6}) \subseteq \mathrm{EXP}$ מיידית מההגדרה: $\mathrm{EXP} = \bigcup_{c \geq 1} \mathrm{DTime}(2^{n^c})$ והמחלקה שלנו היא האיבר $c = 6$.
שלב ו: שלוש ההכלות הן ממש
כאן נכנס משפט 2, ובכל פעם באותו ריקוד בן שלושה צעדים.
(1) $\mathrm{P} \subsetneq \mathcal{E}$. ראינו ש-$\mathrm{P} \subseteq \mathrm{DTime}(2^n)$. נבחר $f(n) = 2^{2n}$: היא ישימה בזמן, סופר-לינארית, ומתקיים $2^n = o(2^{2n})$ שכן $2^n / 2^{2n} = 2^{-n} \to 0$. לפי משפט 2,
$$\mathrm{DTime}(2^n) \subsetneq \mathrm{DTime}\left(\left(2^{2n}\right)^2\right) = \mathrm{DTime}\left(2^{4n}\right) \subseteq \mathcal{E},$$
ולכן קיימת שפה ב-$\mathcal{E}$ שאינה ב-$\mathrm{DTime}(2^n)$ ובפרט אינה ב-P.
(2) $\mathcal{E} \subsetneq \mathrm{DTime}(2^{n^6})$. ראשית, $\mathcal{E} \subseteq \mathrm{DTime}(2^{n^2})$: לכל k קבוע ולכל $n \geq k$ מתקיים $kn \leq n^2$. כעת נבחר $f(n) = 2^{n^3}$ — ישימה בזמן וסופר-לינארית — ומתקיים $2^{n^2} = o\left(2^{n^3}\right)$. לפי משפט 2,
$$\mathrm{DTime}\left(2^{n^2}\right) \subsetneq \mathrm{DTime}\left(2^{2n^3}\right) \subseteq \mathrm{DTime}\left(2^{n^6}\right),$$
כאשר ההכלה האחרונה היא משפט 1 עם $2n^3 \leq n^6$ לכל $n \geq 2$.
(3) $\mathrm{DTime}(2^{n^6}) \subsetneq \mathrm{EXP}$. נבחר $f(n) = 2^{n^7}$; אז $2^{n^6} = o\left(2^{n^7}\right)$, ולפי משפט 2
$$\mathrm{DTime}\left(2^{n^6}\right) \subsetneq \mathrm{DTime}\left(2^{2n^7}\right) \subseteq \mathrm{DTime}\left(2^{n^8}\right) \subseteq \mathrm{EXP}.$$

ההוכחה שהסיכום כותב במפורש: $\mathrm{P} \subsetneq \mathrm{DTime}(2^{n^6})$
הסיכום אינו עובר דרך $\mathcal{E}$ אלא מוכיח ישירות את ההכלה-ממש הזו, וכדאי לראות גם אותה כי היא מדגימה את הבחירה הנוחה של f:
תהא $A \in \mathrm{P}$, כלומר $A \in \mathrm{DTime}(n^c)$ עבור c כלשהו. מתקיים $n^c = O\left(2^{n^5}\right)$, ולכן $\mathrm{P} \subseteq \mathrm{DTime}\left(2^{n^5}\right)$. כעת $2^{n^5} = o\left(2^{n^6/2}\right)$, והפונקציה $2^{n^6/2}$ סופר-לינארית וישימה בזמן, ולכן לפי משפט ההיררכיה בזמן
$$\mathrm{DTime}\left(2^{n^5}\right) \subsetneq \mathrm{DTime}\left(\left(2^{n^6/2}\right)^2\right) = \mathrm{DTime}\left(2^{n^6}\right),$$
ומכאן $\mathrm{P} \subsetneq \mathrm{DTime}(2^{n^6})$. ■
ובאותו אופן, השרשרת שהסיכום מסמן בכחול כתקציר של כל התרגיל:
$$\mathrm{P} \subseteq \mathrm{DTime}(2^n) \subsetneq \mathrm{DTime}\left(2^{n^2}\right) \subseteq \mathrm{EXP}.$$
תרגיל 2 (מטלה 1, שאלה 3): המחלקה $\mathrm{TISP}(f, g)$
הנוסח. עבור שתי פונקציות $f, g : \mathbb{N} \to \mathbb{N}$ נגדיר את מחלקת הסיבוכיות $\mathrm{TISP}(f, g)$ כמחלקת השפות $A \subseteq \Sigma^*$ עבורן קיימת מכונת טיורינג M עם אלפבית קלט Σ כך שקיימים קבועים $c, d > 0$ כך ש-M מכריעה את A וגם לכל $x \in \Sigma^*$ מתקיים $\mathrm{time}_M(x) \le c \cdot f(|x|)$ וגם $\mathrm{space}_M(x) \le d \cdot g(|x|)$.
(א) הוכיחו או הפריכו: לכל פונקציה f מתקיים $\mathrm{TISP}(f, f) = \mathrm{DTime}(f)$.
התשובה: הטענה נכונה. תהא $f : \mathbb{N} \to \mathbb{N}$.
כיוון ראשון: $\mathrm{TISP}(f, f) \subseteq \mathrm{DTime}(f)$. תהא $A \in \mathrm{TISP}(f, f)$. לפי ההגדרה קיימת מכונה M וקיימים קבועים $c, d > 0$ כך ש-M מכריעה את A ולכל $x \in \Sigma^*$ מתקיים $\mathrm{time}_M(x) \le c \cdot f(|x|)$ וגם $\mathrm{space}_M(x) \le d \cdot f(|x|)$. נתבונן ב-$M$ ונתבונן ב-c. M מכריעה את A; יהי x; אז $\mathrm{time}_M(x) \le c \cdot f(|x|)$. אלה בדיוק שני התנאים בהגדרת $\mathrm{DTime}(f)$, ולכן $A \in \mathrm{DTime}(f)$.
.
שימו לב מה קרה כאן: פשוט **זרקנו** את חסם המקום. הכיוון הזה חינם.
כיוון שני: $\mathrm{DTime}(f) \subseteq \mathrm{TISP}(f, f)$. תהא $A \in \mathrm{DTime}(f)$. לפי ההגדרה קיימת מכונה M וקיים קבוע $c > 0$ כך ש-M מכריעה את A ולכל x מתקיים $\mathrm{time}_M(x) \le c \cdot f(|x|)$. נתבונן ב-$M$, נתבונן ב-$c$, ונבחר $d = c$. יהי x. אז מצד אחד $\mathrm{time}_M(x) \le c \cdot f(|x|)$, ומצד שני, לפי משפט 3 (הקשר בין מקום לזמן),
$$\mathrm{space}_M(x) \le \mathrm{time}_M(x) \le c \cdot f(|x|) = d \cdot f(|x|).$$
לכן M עם הקבועים c, d מעידה על $A \in \mathrm{TISP}(f, f)$. ■
מה הרעיון. החסם המשותף $\mathrm{TISP}(f, f)$ אינו מוסיף כלום מעל חסם הזמן, מפני שחסם הזמן **כבר כולל בתוכו** חסם מקום זהה. המחלקה מתחילה להיות מעניינת רק כאשר g קטנה ממש מ-f — למשל $\mathrm{TISP}(2^n, n^2)$, שבה יש מתח אמיתי בין שני המשאבים.
(ג) האם הטענה הבאה נכונה, אינה נכונה או שקולה לשאלה פתוחה? טענה:
$\bigcup_{c \ge 1} \mathrm{TISP}(n^c, n^c) = \mathrm{PSPACE}$.
התשובה: הטענה שקולה לשאלה פתוחה — לשאלה האם $\mathrm{P} = \mathrm{PSPACE}$.

הפתרון. לפי סעיף (א), לכל $c \geq 1$ מתקיים $\mathrm{TISP}(n^c, n^c) = \mathrm{DTime}(n^c)$. שוויון בין איברי שני איחודים גורר שוויון בין האיחודים, ולכן
$\bigcup_{c \geq 1} \mathrm{TISP}(n^c, n^c) = \bigcup_{c \geq 1} \mathrm{DTime}(n^c) = \mathrm{P}.$
מכאן שהטענה $\bigcup_{c \geq 1} \mathrm{TISP}(n^c, n^c) = \mathrm{PSPACE}$ שקולה בדיוק לטענה $\mathrm{P} = \mathrm{PSPACE}$, שהיא שאלה פתוחה. ■

חידוד שכדאי לכתוב במבחן. ההכלה $\mathrm{P} \subseteq \mathrm{PSPACE}$ **ידועה** (שיעור 2, משפט 5). לכן החלק הפתוח בטענה הוא רק ההכלה ההפוכה, $\mathrm{PSPACE} \subseteq \bigcup_{c} \mathrm{TISP}(n^c, n^c)$. הפירוק הזה — "איזה חלק מהשוויון ידוע ואיזה פתוח" — הוא בדיוק מה שהמרצה דרש בשיעור העוקב כשעסק בשאלה מאותו סוג ([01:22:18]–[01:23:54], הקלטת שיעור 24): "שוויון הוא טענת 'וגם', והוא מחביא בפנים שאחת הטענות ידועה והשנייה היא שאלה פתוחה".

תרגיל 3 (מטלה 1, שאלה 8): שני חסמים עליונים על NP

הנוסח. (א) הוכיחו כי $\mathrm{NP} \subseteq \mathrm{EXP}$ בעזרת ההגדרה של NP עם מכונת הכרעה אי-דטרמיניסטית.
(ב) הוכיחו כי $\mathrm{NP} \subseteq \mathrm{PSPACE}$ בעזרת ההגדרה של NP עם מכונת וידוא דטרמיניסטית.

הדגש בשאלה הוא על המילים "בעזרת ההגדרה": כל סעיף מחייב את **ההגדרה שלו**, גם אם הסעיף השני קל יותר.

(א) $\mathrm{NP} \subseteq \mathrm{EXP}$ דרך עץ הריצות

דיון פותח. תהא $A \in \mathrm{NP}$. אזי קיימת מכונה אי-דטרמיניסטית M וקיימים קבועים $c, d > 0$ כך ש-M מכריעה את A באופן אי-דטרמיניסטי ולכל x מתקיים $\mathrm{time}_M(x) \leq d \cdot |x|^c$.

מה יש לנו ביד. לפי משפט 5, עץ כל הריצות האפשריות של M על x הוא עץ שבו:
הקודקודים הם הקונפיגורציות המופיעות בריצות, והקשתות הן צעדי δ;
מספר הבנים של כל צומת חסום ב-$\alpha = |Q| \cdot |\Gamma| \cdot 2$ — **קבוע התלוי ב-M בלבד ולא ב-x**;
עומק העץ חסום ב-$d \cdot |x|^c$;
מספר הצמתים חסום ב- $1 + \alpha + \alpha^2 + \cdots + \alpha^{d|x|^c} = O\left(\alpha^{\,d|x|^c+1}\right) = O\left(2^{\,(\lg \alpha) \cdot d \cdot |x|^c \,+\, \lg \alpha}\right)$.

הבנייה. נבנה מכונה **דטרמיניסטית** $\widehat{M}$ באופן הבא. על קלט x:
$\widehat{M}$ תעבור בסריקת DFS על כל הריצות האפשריות של M על x. 1.1 אם קיים מסלול מקבל, כלומר קיימת ריצה אפשרית שבסופה M במצב מקבל — $\widehat{M}$ מקבלת.
אחרת, $\widehat{M}$ דוחה.

איך מיישמים את ה-DFS. בכל רגע $\widehat{M}$ מחזיקה על סרט העבודה את הקונפיגורציה הנוכחית ואת **מחסנית המסלול** מהשורש אליה: לכל רמה במסלול נשמרת השלישייה $t \in Q \times \Gamma \times \{L, R\}$ שנבחרה שם, כלומר איזה ענף כבר נוסה. אורך המסלול חסום בעומק העץ, ולכן המחסנית מחזיקה לכל היותר $d \cdot |x|^c$ רשומות, כל אחת בגודל $O(|\langle M \rangle|)$.

נכונות. M מכריעה את A באופן אי-דטרמיניסטי, כלומר: $x \in A$ אם ורק אם קיימת ריצה אפשרית מקבלת של M על x; וכן, בכל ריצה אפשרית M עוצרת, ולכן העץ סופי ו-$\widehat{M}$ תמיד מסיימת את הסריקה. אם $x \in A$, קיימת ריצה מקבלת; היא מסלול בעץ, וה-DFS סורק את כל המסלולים ולכן

יגיע אליה, ו-$\widehat{M}$ תקבל. אם $x \notin A$, אין ריצה מקבלת; שום עלה בעץ אינו מקבל, שלב 1.1 לא יופעל לעולם, ו-$\widehat{M}$ תדחה בשלב 2. לכן $\widehat{M}$ **מכריעה** את A.

ניתוח זמן ריצה. נפרק לשניים:

מחיר של צומת בודד. כדי לחשב את הבנים של קונפיגורציה, $\widehat{M}$ צריכה לאתר את הרשומות הרלוונטיות בטבלת המעברים של M ולכתוב את הקונפיגורציה החדשה. טבלת המעברים היא חלק מ-$\langle M \rangle$, וסריקה שלה עולה לכל היותר סדר גודל של $|\langle M \rangle|^2$. זהו **קבוע** — הוא תלוי ב-M בלבד, לא ב-x.

מספר הצמתים. חסום ב-$O\left(2^{(\lg \alpha) d |x|^c + \lg \alpha}\right)$ כפי שחישבנו.

בסך הכול, עם $d' = (\lg \alpha) \cdot d$ ועם בליעת הקבועים $|\langle M \rangle|^2$ ו-$2^{\lg \alpha}$,

$$\mathrm{time}_{\widehat{M}}(x) = O\left(2^{\,d' \cdot |x|^c}\right).$$

לבסוף, $d' \cdot |x|^c \le |x|^{c+1}$ לכל $|x|$ גדול מספיק, ולכן $\mathrm{time}_{\widehat{M}}(x) = O\left(2^{|x|^{c+1}}\right)$, כלומר $A \in \mathrm{DTime}\left(2^{n^{c+1}}\right) \subseteq \mathrm{EXP}$. ■

איפה בדיוק "נשרף" הזמן, ולמה זה בלתי נמנע בגישה הזו. לא בעומק העץ — הוא פולינומי — אלא ב**רוחב**: מספר הענפים מוכפל ב-α בכל רמה, ולכן העץ גדל כמו α^h, כאשר h הוא עומק העץ. כל אחד מהגורמים הוא תמים בפני עצמו; המכפלה שלהם היא האקספוננט.

(ב) $\mathrm{NP} \subseteq \mathrm{PSPACE}$ דרך מכונת הווידוא

הסיכום מסמן בחץ כחול שהסעיף הזה נפתר בשיעור, ומתמצת את הפתרון בשלוש שורות: **בניית מכונה שעוברת על כל העדים האפשריים; המכונה הזו רצה בזמן אקספוננציאלי; ולכן אותה הוכחה בדיוק מראה גם $\mathrm{NP} \subseteq \mathrm{EXP}$.**

הפתרון — ההוכחה המלאה נמצאת בשיעור 8, משפט 1, ולא נחזור עליה כאן. בקצרה: תהא $A \in \mathrm{NP}$ עם מוודא דטרמיניסטי M שזמן ריצתו חסום בפולינום p, ועם פולינום q החוסם את אורך העד. נגדיר מכונה דטרמיניסטית M_A שעל קלט x מחשבת את $q(|x|)$ ועוברת בסדר לקסיקוגרפי על כל $w \in \{0,1\}^{q(|x|)}$, מריצה את M על (x, w), ומקבלת אם M קיבלה; בסוף הלולאה היא דוחה.

הנקודה הקריטית: **מוחקים את סרט העבודה לפני כל איטרציה**, ולכן כל האיטרציות משתמשות באותם תאים והמקום אינו מצטבר. בסך הכול $\mathrm{space}_{M_A}(x) = O(q(|x|) + p(|x| + q(|x|)))$, שהוא פולינום.

התוספת שהשיעור הזה עושה. נסתכל על אותה מכונה במשקפי **זמן**. מספר האיטרציות הוא $2^{q(|x|)}$, וכל איטרציה עולה $p(|x| + q(|x|))$, ולכן

$$\mathrm{time}_{M_A}(x) = O\left(2^{q(|x|)} \cdot p\big(|x| + q(|x|)\big)\right) = O\left(2^{|x|^k}\right)$$

עבור k מתאים, שכן פולינום נבלע בקלות במעריך. לכן **אותה בנייה** מוכיחה גם $A \in \mathrm{EXP}$ — וזהו פתרון חלופי מלא לסעיף (א), שאינו נזקק לעץ הריצות כלל.

הערה: בהקלטת השיעור העוקב המרצה חוזר במפורש על הקשר הזה: כשנשאל למה מכונה שעוברת על כל העדים מזכירה משהו, הוא עונה "כשהראיתי ש-NP מוכלת ב-PSPACE אמרתי שאני יכול לעבור על כל העדים... כל איטרציה נעשית באותו מקום של האיטרציה הקודמת" ([01:02:35]–[01:03:39], הקלטת שיעור 24). המכניזם זהה; רק המשאב שסופרים משתנה.

תרגיל 4 (מבחן 2, שאלה 1א): $\mathrm{3SAT} \le_p \mathrm{4NAE}$

הנוסח. טענה: $\mathrm{3SAT} \le_p \mathrm{4NAE}$. אלגוריתם: בהינתן קידוד של נוסחה φ מצורת 3CNF נוסיף לכל אחד מהסגרי φ משתנה חדש x (אותו משתנה לכל ההסגרים) ונחזיר את הנוסחה המתקבלת **בצירוף השמה** הנותנת ל-x את הערך False.

התשובה: האלגוריתם כפי שנוסח אינו רדוקציה — אף שהטענה עצמה נכונה.

ההפרכה. אם הקלט הוא נוסחה φ מצורת 3CNF, האלגוריתם מחזיר **זוג**: נוסחה $\widehat{\varphi}$ מצורת 4CNF **והשמה**. אבל קלט חוקי של $\mathrm{4NAE}$ הוא נוסחת 4CNF בלבד; זוג של נוסחה והשמה אינו מופע של הבעיה. רדוקציה חייבת לשלוח מחרוזות למופעים של בעיית היעד, ולכן האלגוריתם הזה אינו מהווה רדוקציה בזמן פולינומי מ-$\mathrm{3SAT}$ ל-$\mathrm{4NAE}$.

מדוע בכלל נולד הרעיון להחזיר גם השמה, ולמה אין בו צורך. מי שכתב את האלגוריתם רצה "לכפות" על הפותר את הערך $x = \mathrm{False}$, כי בלי זה לא ברור איך לחלץ השמה מספקת ל-φ. אבל את הכפייה הזו מקבלים **בחינם** מהתכונה הסימטרית של ספיקות NAE:

> **התכונה החשובה לגבי ספיקות באופן NAE:** אם φ נוסחה ו-V השמה עבור משתני φ המספקת אותה באופן NAE, אזי ההשמה $\widehat{V}$, ההפכית ל-V בכל ערך, אף היא מספקת את φ באופן NAE (משפט 6).

הרדוקציה המתוקנת ופתרונה המלא. האלגוריתם: בהינתן $\varphi = \bigwedge_{i=1}^{m} (\ell_{i,1} \vee \ell_{i,2} \vee \ell_{i,3})$ מצורת 3CNF, נוסיף משתנה חדש יחיד x לכל ההסגרים ונחזיר **רק** את הנוסחה

$$\widehat{\varphi} = \bigwedge_{i=1}^{m} (\ell_{i,1} \vee \ell_{i,2} \vee \ell_{i,3} \vee x) .$$

זמן ריצה. עוברים על ההסגרים ומוסיפים ליטרל אחד לכל הסגר; סך הכול $O(|\langle\varphi\rangle|)$, ובוודאי פולינומי.

כיוון ראשון. נניח $\varphi \in \mathrm{3SAT}$, ותהא V השמה המספקת אותה. נרחיב אותה ל-$\widehat{V}$ על ידי $\widehat{V}(x) = \mathrm{False}$. בכל הסגר של $\widehat{\varphi}$ יש ליטרל אמת (כי V סיפקה את ההסגר המקורי) וגם ליטרל שקר (המשתנה x עצמו), ולכן ערכי הליטרלים בהסגר אינם כולם שווים. מכאן $\widehat{\varphi} \in \mathrm{4NAE}$.

כיוון שני. נניח $\widehat{\varphi} \in \mathrm{4NAE}$, ותהא U השמה המספקת אותה באופן NAE. אם $U(x) = \mathrm{True}$, נחליף את U בהשמה ההפכית $\widehat{U}$ — לפי משפט 6 גם היא מספקת את $\widehat{\varphi}$ באופן NAE, ובה $\widehat{U}(x) = \mathrm{False}$. לכן אפשר להניח בלי הגבלת הכלליות $U(x) = \mathrm{False}$. יהי i הסגר. אילו כל שלושת הליטרלים $\ell_{i,1}, \ell_{i,2}, \ell_{i,3}$ היו מקבלים False תחת U, אז כל ארבעת הליטרלים בהסגר היו שווים ל-False — בסתירה לספיקות NAE. לכן לפחות אחד מהם אמת, כלומר U מסופקת את ההסגר המקורי. הדבר נכון לכל הסגר, ולכן U מצומצמת למשתני φ מספקת את φ, ומכאן $\varphi \in \mathrm{3SAT}$. ■

המסר. הטענה נכונה; ההשמה שנוספה לפלט לא רק מיותרת אלא הורסת את הרדוקציה. כשמצרפים לפלט "עזרה" שאינה חלק ממופע של בעיית היעד, מפסיקים לפתור את בעיית היעד.

תרגיל 5 (מבחן 2, שאלה 1ד): $\text{MAX-IS} \leq_p \text{IS}$ בעזרת פונקציית הזהות

הנוסח. טענה: $\text{MAX-IS} \leq_p \text{IS}$. אלגוריתם: לכל קלט x החזר את x.

התשובה: הפונקציה אינה רדוקציה. נתבונן בגרף $G = (V, E)$ בעל שני קודקודים וללא קשתות, ובקבוע $k = 1$. אז:

$\langle G, 1 \rangle \notin \text{MAX-IS}$ — יש בגרף קבוצה בלתי תלויה בגודל 2 (שני הקודקודים גם יחד), ולכן הגודל המקסימלי הוא 2 ולא 1;

$\langle G, 1 \rangle \in \text{IS}$ — יש בגרף קבוצה בלתי תלויה בגודל 1 (כל אחד מהקודקודים לחוד).

פונקציית הזהות שולחת את $\langle G, 1 \rangle$ לעצמו, כלומר שולחת מופע **שאינו** ב-MAX-IS למופע **שכן** ב-IS. זו הפרה ישירה של הדרישה $x \in A \iff f(x) \in B$. לכן הפונקציה אינה רדוקציה בזמן פולינומי מ-MAX-IS ל-IS. ■

מה נשבר כאן מבחינה מושגית. IS שואלת "האם יש קבוצה **בגודל לפחות** k" (ולמעשה: בגודל k בדיוק, אבל אפשר תמיד להוריד קודקודים ולהישאר בלתי תלויים). MAX-IS שואלת "האם המקסימום **שווה בדיוק** k". שתי שאלות שונות על אותו אובייקט, ולכן אותה מחרוזת אינה יכולה לשמש כמופע לשתיהן.

תרגיל 6 (מבחן 2, שאלה 1ה): $\text{IS} \leq_p \text{MAX-IS}$ בעזרת פונקציית הזהות

הנוסח. טענה: $\text{IS} \leq_p \text{MAX-IS}$. אלגוריתם: לכל קלט x החזר את x.

התשובה: אותה טענה ואותו נימוק מהתרגיל הקודם, רק בכיוון ההפוך. עם אותו זוג $\langle G, 1 \rangle$ (G שני קודקודים ללא קשתות): $\langle G, 1 \rangle \in \text{IS}$ אך $\langle G, 1 \rangle \notin \text{MAX-IS}$, ולכן פונקציית הזהות שולחת מופע חיובי למופע שלילי, ואינה מתארת רדוקציה בזמן פולינומי מ-IS ל-MAX-IS. ■

הדיון המושגי שנספח לשני הסעיפים

הפרכת האלגוריתם אינה אומרת דבר על הטענות עצמן. הסיכום מותח קו ושואל את השאלה האמיתית:

האם בכלל מתקיים $\text{IS} \leq_p \text{MAX-IS}$? כן, וללא כל תנאי. $\text{IS} \in \text{NP}$ (שיעור 7, משפט 2), ו-MAX-IS היא NP-קשה (שיעור 22). לפי הגדרת NP-קשיות, **כל** שפה ב-NP נתנת לרדוקציה אליה, ובפרט $\text{IS} \leq_p \text{MAX-IS}$. שימו לב שהרדוקציה הזו קיימת מכוח משפט, ואיננו צריכים לכתוב אותה במפורש.

והאם מתקיים $\text{MAX-IS} \leq_p \text{IS}$? כאן התשובה מותנית: לפי מה שהוכח בשיעור 22 (ומנוסח כאן כמשפט 7),

$$\text{MAX-IS} \leq_p \text{IS} \quad \iff \quad \text{NP} = \text{coNP}.$$

כלומר: הכיוון האחד חינם, והכיוון השני שקול לשאלה פתוחה. זו אסימטריה חשובה בין $\leq_p$ לבין "שקילות", והיא בדיוק סוג הדבר שנשאל במבחן.

תרגיל 7 (מבחן 2, שאלה 1ו): $\text{SAT} \leq_p \text{IS}$

הנוסח. טענה: $\text{SAT} \leq_p \text{IS}$. אלגוריתם: בהינתן נוסחה φ מצורת CNF עם m הסגרים נחזיר את המחרוזת $\langle G, m \rangle$ כאשר $G = (V, E)$ גרף לא מכוון המוגדר כך:

קבוצת הקודקודים: לכל הסגר של φ יוגדר בגרף אוסף של קודקודים שמתאימים **לכל ההשמות עבור משתני ההסגר המספקות את ההסגר**.
קבוצת הקשתות: כל שני קודקודים המתאימים להשמות של אותו הסגר יחוברו בקשת. בנוסף יחוברו בקשת כל שני קודקודים שמתאימים להשמות של הסגרים שונים אשר סותרות זו את זו (כלומר, השמה אחת נותנת למשתנה מסוים ערך True והאחרת נותנת לו ערך False).
הדוגמה שמצורפת לשאלה: עבור $\left(\overline{x_1} \vee x_3\right) \wedge \left(x_1 \vee \overline{x_2} \vee x_3\right)$ יש 3 השמות למשתנים x_1, x_3 המספקות את ההסגר הראשון, ו-7 השמות למשתנים x_1, x_2, x_3 המספקות את ההסגר השני, ולכן יהיו בגרף 10 קודקודים.
ודאו את הדוגמה בעצמכם, זה שווה דקה. להסגר הראשון שני משתנים, כלומר $2^2 = 4$ השמות; היחידה שאינה מספקת אותו היא $x_1 = \mathrm{True}, x_3 = \mathrm{False}$, ולכן נשארות 3. להסגר השני שלושה משתנים, כלומר $2^3 = 8$ השמות; היחידה שאינה מספקת אותו היא $x_1 = \mathrm{False}, x_2 = \mathrm{True}, x_3 = \mathrm{False}$, ולכן נשארות 7. סך הכול 10.
התשובה: האלגוריתם אינו רדוקציה בזמן פולינומי — הוא כלל אינו רץ בזמן פולינומי.
ההפרכה. נתבונן בנוסחה בעלת הסגר יחיד:
$$\varphi = x_1 \vee x_2 \vee \cdots \vee x_n.$$
אורך הקידוד שלה הוא $|\langle\varphi\rangle| = O(n)$. מספר ההשמות למשתני ההסגר הוא 2^n, ומהן רק אחת אינה מספקת את ההסגר (זו שנותנת False לכל המשתנים). לכן האלגוריתם בונה $2^n - 1$ קודקודים, ובפרט כותב על סרט הפלט מחרוזת באורך אקספוננציאלי ב-n. מכאן שזמן הריצה של האלגוריתם בהכרח אינו פולינומי ב-$|\langle\varphi\rangle|$. ■
איפה הרעיון נכשל, ואיך הרדוקציה הנכונה עוקפת את זה. הרעיון "קודקוד לכל השמה מספקת של ההסגר" נכון סמנטית — הוא באמת מקודד נכון את הקשר בין ספיקות לקבוצה בלתי תלויה — אבל מספר ההשמות המספקות של הסגר ברוחב w הוא $2^w - 1$, ורוחב הסגר בנוסחת CNF כללית **אינו חסום בקבוע**. הרדוקציה התקינה, שנראתה בשיעור 22, בונה קודקוד לכל **מופע ליטרל** בהסגר ולא לכל השמה: מספר הקודקודים הוא אז $\sum_{i=1}^{m} |C_i| \le |\langle\varphi\rangle|$, כלומר לינארי. אותו רעיון בדיוק על הקשתות (קשת בתוך הסגר, קשת בין ליטרלים סותרים), אבל בגודל פולינומי.
המסר החוזר בשלושת התרגילים האחרונים. בכל אחד מהם הטענה נכונה והאלגוריתם שגוי, וכל אחד מהם נשבר בנקודה אחרת: **טיפוס הפלט** (תרגיל 4), **כיוון ההכרעה** (תרגילים 5–6), **זמן הריצה** (תרגיל 7). אלה שלושת הדברים שצריך לבדוק בכל רדוקציה — ובדיוק בסדר הזה.

הערות מהשיעור
למפגש הזה עצמו אין הקלטה בפלייליסט (ראו סעיף הפערים). ההערות שלהלן נלקחו מהקלטות המפגשים הסמוכים, שבהם המרצה פתר תרגילים מאותו סוג ובאותה שיטה, ומסומנות ככאלה.
[00:01:35]–[00:03:09], הקלטת שיעור 24 — הטכניקה שפותחת כל שאלת "מחלקה מוזרה".
שלב 1: לזהות מהי ההגדרה המוכרת הקרובה ביותר למה שכתוב. שלב 2: לכתוב את שתי ההגדרות **אחת מול השנייה** ולחפש ברמת התווים איפה הן נבדלות. שלב 3: להחליט אם אפשר לגשר על ההבדל. שלב 4: לכתוב. לדבריו, "השלב שנופלים עליו הוא דווקא הראשון" — הזיהוי, לא הטכניקה.

[00:05:45], הקלטת שיעור 24 — "לכתוב בסבלנות ולהיצמד לתבנית". התבנית שהוא דורש: מצטטים את ההגדרה כדי לקבל את המשתנים ("הגדרה שמבטיחה קיום — מציינת מכונה"), ואז "נתבונן ב-M", "נתבונן בקבוע", "יהי x", "נניח $x \in A$"... הוא מדגיש שהמטרה אינה פורמליות לשמה אלא **בהירות מחשבתית**: "לכם הרבה יותר קל לראות מה כתבתם ומה ההקשר של מה שכתבתם".

[00:26:21] ו-[00:32:54], הקלטת שיעור 24 — מעבר מ"לכל" ל"קיים". אפשר להסיק "קיים" מ"לכל" **רק** כשהקבוצה שעליה רצים אינה ריקה. הדוגמה הנגדית שלו: "כל מספר שהריבוע שלו שלילי מתחלק בשלוש" — טענה נכונה, ולא נובע ממנה שקיים מספר כזה. ההעדפה שלו במבחן: לא להסתמך על המעבר, אלא פשוט **להציג איבר קונקרטי** מהקבוצה.

[00:53:30]–[00:54:35], הקלטת שיעור 24 — שימוש נכון במשפט ההיררכיה. על תשובה בסגנון "ממשפט ההיררכיה קיימת שפה שאינה ב-NP": "הייתי מת על זה, אבל אני לא יודע אם זה היה מקבל את כל הנקודות — כי **איך** השתמשת במשפט ההיררכיה?" זו לא תשובה שגויה אלא תשובה **חסרה**. הניסוח שמקבל נקודות מלאות מפרט את הפונקציות ואת שלושת התנאים, בדיוק כפי שנעשה בתרגיל 1 כאן.

[00:55:06], הקלטת שיעור 24 — כמה להוכיח. "אני רוצה לכתוב את כל מה שאני חייב, אבל אני משתדל לא לכתוב יותר ממה שאני חייב." להוכיח יותר מהנדרש אינו שגוי מתמטית (וסטודנט שהעיר זאת קיבל אישור מפורש), אבל הוא מגדיל את שטח הפנים לטעויות.

[01:24:59]–[01:29:44], הקלטת שיעור 24 — למה "מספר קבוע של אפשרויות" אינו אקספוננציאלי. ההסבר על מספר הבחירות האי-דטרמיניסטיות: "נסמן ב-α את $2 \cdot |\Gamma| \cdot |Q|$... כל בחירה כזו אני יכול לתאר ב-$\lg \alpha$ ביטים". זהו בדיוק החישוב שמאחורי משפט 5 ותרגיל 3(א) כאן. השאלה שצריך תמיד לשאול היא "מעריכי **כפונקציה של מה**".

פערים בין הסיכום להקלטה

מקור: שיוך ההקלטות. **הפער:** ההקלטה שנמסרה כמקור ראשי (`sjTAzTgMpD0` , "שיעור 22", 11 ביוני) אינה עוסקת באף אחד מתרגילי הסיכום הזה: כולה פתרון **מטלה 2** — המחלקות C_5–C_1 המוגדרות מול NP — שהוא בדיוק תוכן הסיכום של שיעור 24 (עמוד 1 שלו נושא את הכותרת "פתרון מטלה 2"). ההקלטה השנייה (`2Ck_-XFD52E` , 15 ביוני) היא פתרון **מטלה 3**, שהוא תוכן הסיכום של שיעור 25. **ההכרעה:** שתיהן סומנו `coverage: none` עם הערה מפורשת, והקובץ נכתב מהסיכום. ההקלטה של המפגש שבו נפתרה מטלה 1 (ככל הנראה 8 ביוני) אינה קיימת בפלייליסט — בין 4 ביוני ל-11 ביוני אין וידאו.

מקור: ההקלטה של 11 ביוני, [00:59:55]. **הפער:** המרצה מפנה במפורש לחומר של הסיכום הזה — "לא כל מה שנראה מעריכי הוא מעריכי; ראינו את זה גם **שיעור שעבר** עם ה-n בחזקת 2 בחזקת c" — כלומר תרגיל 1 כאן נפתר במפגש הקודם. **ההכרעה:** האזכור שימש כאישור לשיוך התוכן, וצוטט בגוף הקובץ.

מקור: הסיכום, עמוד 1. **הפער:** בשורת הסיום של הכיוון השני נכתב $A \in \bigcup_{d \geq 1} \mathrm{DTime}(2^d) = \mathrm{P}$. **ההכרעה:** שגיאת כתיב מתמטית; הנוסח הנכון הוא $\bigcup_{d \geq 1} \mathrm{DTime}(n^d) = \mathrm{P}$, וכך נכתב כאן, עם הערה בגוף הפתרון.

מקור: הסיכום, עמודים 1–2. **הפער:** התרגיל מונה שבע מחלקות, אך הסיכום מטפל רק בשלוש מהזהויות ($\mathrm{P} = \bigcup \mathrm{DTime}(n^{2^c})$, $\mathrm{EXP} = \bigcup \mathrm{DTime}(n^{n^c})$, ו-$\mathrm{P} \subsetneq \mathrm{DTime}(2^{n^6})$); המחלקות $\bigcup_c \mathrm{DTime}(c^{cn})$ ו-$\bigcup_c \mathrm{DTime}(c^{n^c})$ אינן מוזכרות כלל, וגם לא הסידור המלא. **ההכרעה:** השלמתי את שתי המחלקות החסרות ואת כל ההכלות-ממש (שלבים ג–ו בתרגיל 1), באותה טכניקה שהסיכום משתמש בה; שלבים אלה הם תוספת שלי ואינם קריאה של הסיכום.

מקור: הסיכום, עמוד 5. **הפער:** בחישוב גודל עץ הריצות מופיע המעריך $|x|^2$ בשני מקומות ו-$|x|^c$ במקום שלישי, באותו חישוב. **ההכרעה:** החסם על זמן הריצה הוא $d \cdot |x|^c$, ולכן המעריך הנכון הוא c בכל המקומות; תוקן.

מקור: הסיכום, עמוד 5. **הפער:** אי-שוויונות בשורות בעברית נכתבים עם סימן שנראה הפוך לקורא שמאל-ימין (למשל "עומק העץ $\geq d|x|^c$"). **ההכרעה:** זהו שיקוף של סימן ההשוואה בשורת טקסט מימין לשמאל; המשמעות היא "עומק העץ **חסום ב-**$d|x|^c$", וכך נכתב.

מקור: הסיכום, עמוד 1. **הפער:** בשימוש במשפט ההיררכיה בזמן מצוין עבור $2^{n^6/2}$ רק שהיא "סופר-לינארית", בלי תנאי הישימות בזמן. **ההכרעה:** התנאי נדרש והוא מתקיים; הוסף במפורש, ומסומן כהשלמה.

מקור: הסיכום, עמודים 3–4. **הפער:** שאלה 3 מופיעה עם סעיפים (א) ו-(ג) בלבד; סעיף (ב) חסר לחלוטין. **ההכרעה:** לא שוחזר — אין בסיס לנחש את נוסחו. נרשם ב- `open_questions` .

מקור: הסיכום, עמוד 7, סעיף (ד). **הפער:** הגרף שצויר מראה שני קודקודים **מחוברים בקשת**, בעוד שהנימוק הכתוב לצדו — "יש קבוצה בלתי תלויה בגודל 2" — נכון רק לגרף חסר קשתות. בגרף עם קשת ו-$k = 1$ שני המופעים חיוביים ואין הפרכה. **ההכרעה:** הנימוק הכתוב הוא הקובע; הפתרון כאן משתמש בשני קודקודים ללא קשת. הפער נרשם גם ב- `open_questions` .

מקור: הסיכום, עמוד 7, סעיף (א). **הפער:** מילה אחת בשורת המסקנה אינה קריאה בוודאות. **ההכרעה:** המשמעות ברורה מההקשר ומהאלגוריתם המצוטט — הפלט הוא זוג של נוסחה והשמה, שאינו קלט חוקי של $4\mathrm{NAE}$ — וכך נוסח.

מקור: הסיכום, עמוד 7, שורת הסיום. **הפער:** נכתב "לפי מה שהראינו בשיעור שעבר, $\mathrm{MAX\text{-}IS} \leq_p \mathrm{IS}$ אם ורק אם $\mathrm{NP} = \mathrm{coNP}$", בלי חזרה על הטיעון. **ההכרעה:** הטיעון שוחזר בקצרה כמשפט 7 מתוך שיעור 22, שם הוא הוכח במלואו; לא הועתקה ההוכחה המלאה.

מקור: הסיכום, עמוד 5, ההערה הכחולה. **ההכרעה:** ההערה ("פתרון בשיעור — בניית מכונה שעוברת על כל העדים האפשריים; מכונה זו רצה בזמן אקספוננציאלי; ולכן אותה הוכחה בדיוק מראה $\mathrm{NP} \subseteq \mathrm{EXP}$") שולבה בגוף תרגיל 3(ב) כתוצאה עצמאית, כי היא ההוספה היחידה של השיעור מעל שיעור 8.

סיכום ונקודות למבחן

מה שחייבים לדעת בעל פה

הזהויות שמתמוטטות. $\bigcup_{c\geq 1} \mathrm{DTime}(n^{2^c}) = \mathrm{P}$; $\bigcup_{c\geq 1} \mathrm{DTime}(n^{n^c}) = \mathrm{EXP}$; $\bigcup_{c\geq 1} \mathrm{DTime}(c^{cn})$ היא הזמן האקספוננציאלי הלינארי, שיושבת ממש בין P ל-$\mathrm{DTime}(2^{n^6})$.

הריקוד של משפט ההיררכיה בשלושה צעדים: לחסום את המחלקה הקטנה במחלקה עדינה אחת; לבחור f ישימה בזמן וסופר-לינארית עם $g = o(f)$ ועם $\mathrm{DTime}(f^2)$ בתוך המחלקה הגדולה; להסיק. **תמיד לבדוק את שלושת התנאים בכתב.**

$\mathrm{space}_M(x) \le \mathrm{time}_M(x)$ — המשפט הקטן שפותר את כל תרגיל 2.

$\mathrm{TISP}(f, f) = \mathrm{DTime}(f)$, ולכן $\bigcup_c \mathrm{TISP}(n^c, n^c) = \mathrm{P}$.

מכונה אחת, שני חסמים: המכונה שעוברת על כל העדים מוכיחה גם $\mathrm{NP} \subseteq \mathrm{PSPACE}$ (מוחקים בין איטרציות) וגם $\mathrm{NP} \subseteq \mathrm{EXP}$ (סופרים איטרציות).

עץ הריצות: $\alpha = |Q| \cdot |\Gamma| \cdot 2$ בנים לכל צומת, עומק כזמן הריצה, גודל $O(\alpha^{T+1})$.

NAE סימטרית: ההשמה המשלימה מספקת באופן NAE כל נוסחה שההשמה המקורית סיפקה באופן NAE.

תמיד: $\mathrm{IS} \le_p \mathrm{MAX\text{-}IS}$; **אם ורק אם** $\mathrm{MAX\text{-}IS} \le_p \mathrm{IS}$ **.** $\mathrm{NP} = \mathrm{coNP}$

המלכודות הסטנדרטיות

"נראה מעריכי" $\neq$ "מעריכי". n^{2^c} הוא פולינום; c^{cn} אינו ב-P. תמיד לשאול: מעריכי **כפונקציה של אורך הקלט**?

"ממשפט ההיררכיה נובע" אינו טיעון. צריך לכתוב את f, את g, ואת שלושת התנאים.

שוויון בין מחלקות הוא טענת "וגם". כששואלים "האם הטענה נכונה, שגויה או שקולה לשאלה פתוחה", מפרקים לשתי הכלות ועונים על כל אחת בנפרד — לרוב אחת ידועה והשנייה פתוחה.

רדוקציה נבדקת בשלושה מקומות: (1) האם הפלט הוא **מופע חוקי** של בעיית היעד; (2) האם הכיוון נשמר **בשני הכיוונים** של האם-ורק-אם; (3) האם זמן הריצה — **כולל אורך הפלט** — פולינומי. שלושת התרגילים האחרונים כאן נשברים בדיוק בשלוש הנקודות האלה, אחת בכל אחד.

הפרכת אלגוריתם אינה הפרכת טענה. בכל שלוש הטענות שהופרכו כאן, הטענה עצמה נכונה. אם השאלה מבקשת רק לבדוק את האלגוריתם — לענות על מה שנשאל, ולציין בשורה אחת שהטענה עצמה נכונה.

מ"לכל" ל"קיים" רק כשהקבוצה אינה ריקה, ועדיף פשוט להציג איבר.

מה המרצה אמר על המבחן עצמו

הדברים הבאים נאמרו בהקלטת המפגש של 15 ביוני ([01:09:23]–[01:13:33]), והם נוגעים לכל ארבעת שיעורי החזרה:

סדר העדיפויות ברור. "לעבור על החומר זה הכי חשוב מהכול" — תרגילי בית, ותרגילים שנפתרו בכיתה. רק אם נשאר זמן, מבחנים משנים קודמות.

למה. שאלות אמנם חוזרות, אבל "אם 80% מהמבחן הוא על שאלות שראינו בקורס ויש עוד שאלה של 20 נקודות שהופיעה פעם במבחן קודם — האם שווה לפתור עכשיו 20 מבחנים על חשבון החומר?" ובנוסף: בסמסטרים קודמים לימדו לפעמים חומר אחר, ואפשר להיתקע על בעיה בלי לדעת שהיא בכלל לא בחומר. "אם אתם עושים אוברפיטינג למשהו, תעשו אוברפיטינג לחומר ולא לבחינות קודמות."

מה נחשב "ברמת תרגיל". "למעט שניים-שלושה משפטים — משפט ההיררכיה, משפט קוק-לוין ואולי עוד אחד — **כל מה שהוכחנו בשיעור הוא ברמת תרגיל מבחינתכם**." כלומר כל הוכחה שנראתה בכיתה היא הוכחה שאתם אמורים לדעת לשחזר.

רשימת בדיקה — מה צריך לדעת לעשות אחרי השיעור הזה

- [ ] לקבוע, בהינתן משפחת מחלקות מהצורה $\bigcup_c \mathrm{DTime}(h(n,c))$, למה היא שווה, על ידי חישוב סדר גודל אחד והפעלת משפט המונוטוניות.
- [ ] להוכיח הכלה ממש בין שתי מחלקות גסות באמצעות משפט ההיררכיה בזמן, כולל בחירת f ואימות שלושת התנאים.
- [ ] להוכיח $\mathrm{TISP}(f,f) = \mathrm{DTime}(f)$ ולהסיק ממנה טענות על איחודים.
- [ ] להוכיח $\mathrm{NP} \subseteq \mathrm{EXP}$ **בשתי הדרכים** — עץ ריצות של מכונה אי-דטרמיניסטית, ומעבר על כל העדים — ולדעת איזו הגדרה כל דרך דורשת.
- [ ] בהינתן אלגוריתם שמוצג כרדוקציה, לבדוק את שלוש הנקודות (טיפוס הפלט, שני כיווני האם-ורק-אם, זמן ריצה ואורך פלט) ולהציג מופע נגדי קונקרטי כשהוא נכשל.
- [ ] לתקן את הרדוקציה $3\mathrm{SAT} \le_p 4\mathrm{NAE}$ ולהוכיח אותה במלואה, כולל השימוש בהשמה המשלימה.
- [ ] להסביר מדוע $\text{MAX-IS} \le_p \text{IS}$ מתקיים תמיד ואילו הכיוון ההפוך שקול ל-$\mathrm{NP} = \mathrm{coNP}$.

שאלות שנשארו פתוחות

לשיעור זה אין הקלטה: שתי ההקלטות שנמסרו שייכות לשיעורים 24 ו-25, והמפגש שבו נפתרו התרגילים האלה (ככל הנראה ה-8 ביוני) חסר מהפלייליסט; הקובץ נשען על הסיכום בלבד.

עמוד 4 בסיכום עובר משאלה 3 סעיף (א) לסעיף (ג); סעיף (ב) של אותה שאלה אינו מופיע בסיכום כלל ולא שוחזר.

עמוד 7 בסיכום: הגרף שצויר לסעיף (ד) מראה קשת בין שני הקודקודים, אך הנימוק הכתוב לצדו ('יש קבוצה בלתי תלויה בגודל 2') מחייב גרף חסר קשתות; הלכתי אחרי הנימוק.

עמוד 7 בסיכום: מילה אחת בשורת המסקנה של סעיף (א) אינה קריאה בוודאות; המשמעות ('הפלט הוא זוג ולא נוסחה, ולכן אינו קלט חוקי של 4NAE') ברורה מההקשר.

החומר שעמוד 7 נשען עליו (MAX-IS היא coNP-קשה, ומכאן השקילות ל-NP=coNP) נפתר בהקלטה AGUI69L7aDA השייכת לשיעור 22; היא לא נמסרה לקובץ זה, וההפניה אליה היא דרך שיעור 22.

24 תרגול חזרה: אפיון מחלקות סיבוכיות ביחס ל-NP (שאלה 3, סעיפים א–ג)

שלושה אפיונים שנראים כמעט זהים להגדרת ה-verifier של NP — היפוך קבלה/דחייה, החלפת 'אם ורק אם' בשני תנאי קיום, וקיצור העד לאורך קבוע — ובכל אחד מהם מכריעים האם המחלקה מכילה את NP, מוכלת בה או שווה לה.

ביטחון: high

בקצרה

זהו מפגש **חזרה למבחן**: אין בו תיאוריה חדשה, אלא פתרון מלא של שאלה אחת מתרגיל הבית — שאלה שכולה ברמת **ההגדרה**, כדברי המרצה: "אין שם שום דבר פרט להגדרה" [00:00:30].

נתונות שלוש מחלקות $\mathrm{C}_1, \mathrm{C}_2, \mathrm{C}_3$, שכל אחת מהן נראית כמעט בדיוק כמו הגדרת ה-verifier של NP (שיעור 6), ולכל אחת יש להכריע **שלוש** שאלות נפרדות: האם היא מכילה את NP, האם היא מוכלת ב-NP, והאם היא שווה לה.

התשובות: $\mathrm{C}_1 = \mathrm{NP}$ (ההבדל היחיד הוא "דוחה" במקום "מקבלת", והוא ניתן לגישור על ידי היפוך מצבי הקבלה והדחייה); $\mathrm{NP} \subsetneq \mathrm{C}_2$, ולמעשה C_2 היא **מחלקת כל השפות** (ההבדל הוא "לכל" שהוחלף ב"קיים", והוא ניתן לגישור רק בכיוון אחד); $\mathrm{C}_3 = \mathrm{P}$ (העד מקוצר לאורך **קבוע**, ולכן אפשר לעבור על כולו), ולכן $\mathrm{C}_3 \subseteq \mathrm{NP}$ **נכון**, בעוד ש-$\mathrm{NP} \subseteq \mathrm{C}_3$ **שקול לשאלה הפתוחה** $\mathrm{P} = \mathrm{NP}$.

מעבר לתשובות, השיעור הוא בעיקרו שיעור **בשיטה**. המרצה מפרק את פתרון שאלות מהסוג הזה לארבעה שלבים קבועים, שניים מחשבתיים ושניים טכניים [00:05:45]–[00:06:17]; מי שמפנים אותם מקבל מתכון לכל שאלה כזו במבחן.

שני כשלים לוגיים חוזרים מתועדים כאן במפורש: המעבר מ"לכל" ל"קיים" **מותר רק כשהתחום אינו ריק** [00:32:54], והטענה "ממשפט ההיררכיה קיימת שפה שאינה ב-NP" בלי להסביר **איך** — תשובה חלקית בלבד [00:53:30].

קו הגבול העדין ביותר בשיעור: להוכיח **קיום** צריך להציג עצם אחד; להוכיח **הכלה** צריך לצטט את ההגדרה. המרצה מסרב במכוון להוכיח יותר ממה שנדרש, גם כשהטענה החזקה יותר נכונה [00:57:10].

רקע ותלויות

(א) בנוסח ה-verifier (ראו שיעור 6). זו ההגדרה שכל השאלה סובבת סביבה, ולכן היא מובאת כאן במלואה. שפה $A \subseteq \Sigma^*$ שייכת ל-NP אם קיים $c \geq 1$ וקיימת מכונת טיורינג **דטרמיניסטית** M עם זמן ריצה פולינומי, כך שלכל $x \in \Sigma^*$: $x \in A \iff \exists\, w \in \{0,1\}^{|x|^c} \ \text{s.t. } M \text{ accepts } (x, w)$.

M המכונה w נקראת **verifier**, המחרוזת w נקראת **עד** **(witness)**. שיעור 6 הוכיח שהגדרה זו שקולה להגדרה דרך מכונה אי-דטרמיניסטית פולינומית, כלומר $\mathrm{NP}' = \mathrm{NP}$; כאן נשתמש בשתי הצורות בלי להבדיל ביניהן.

שימו לב לניסוח: בשיעור 6 החסם על אורך העד נכתב כפולינום $q(|x|)$, וכאן הוא נכתב כ-$|x|^c$. **זה אותו דבר** — כל פולינום נחסם על ידי n^c עבור c גדול דיו, ואת מספר סופי של הערכים הקטנים אפשר תמיד "לצרוב" בתוך המכונה [00:22:12]. המרצה חוזר ומדגיש: **היצמדו לניסוח שבו נכתבה השאלה** [00:09:30] — אם השאלה כותבת $|x|^c$, כתבו $|x|^c$.

(ב) מכריעה" ומשמעות "מכריעה" (ראו שיעורים 1–2). $\mathrm{P} = \bigcup_{c \geq 1} \mathrm{DTime}(n^c)$. מכונה $\hat{M}$ **מכריעה** שפה A אם לכל x היא עוצרת, מקבלת אם $x \in A$ ודוחה אם $x \notin A$. הממשק חשוב: מכונה מכריעה מקבלת רק את x, ואילו verifier מקבל את הזוג (x, w) ולכן **אינו** מכריע דבר [00:30:17].

(ג) שרשרת ההכלות הגסות (ראו שיעורים 2–4). מהסיכום, עמוד 2, במסגרת מודגשת: $\mathrm{P} \subseteq \mathrm{NP} \subseteq \mathrm{PSPACE} \subseteq \mathrm{EXP} \subseteq \mathrm{EXPSPACE}, \qquad \mathrm{P} \subsetneq \mathrm{EXP}.$ הוכח בשיעור 2, $\mathrm{PSPACE} \subseteq \mathrm{EXP}$ בשיעורים 2–3, $\mathrm{P} \subseteq \mathrm{NP}$ בשיעור 4, $\mathrm{NP} \subseteq \mathrm{PSPACE}$ בשיעור 8, ו-$\mathrm{P} \subsetneq \mathrm{EXP}$ ממשפט ההיררכיה בזמן בשיעור 3.

(ד) R ו-HALT (מקורס החישוביות). R היא מחלקת השפות הכריעות, ו-HALT — בעיית העצירה — אינה בה. כדברי המרצה [00:42:15]: "בכל הקורס הזה היינו בתוך R, ופירקנו את R לכל מיני מחלקות כשהשאלה הייתה על **המחיר**". כל המחלקות שראינו — גם האי-דטרמיניסטיות, גם ההסתברותיות — הן מחלקות של שפות כריעות.

(ה) הרכבת פולינומים (ראו שיעור 6). סכום, מכפלה והרכבה של פולינומים הם פולינום. זהו הצעד השקוף שכל ניתוח זמן ריצה בקובץ הזה נשען עליו.

הגדרות

הגדרה 1: המחלקה C_1 (סעיף א' בשאלה)

C_1 היא מחלקת השפות $A \subseteq \Sigma^*$ עבורן קיים $c \geq 1$ כך שקיימת מכונת טיורינג **דטרמיניסטית** M עם זמן ריצה פולינומי, כך שלכל $x \in \Sigma^*$ מתקיים: $x \in A \iff \exists\, w \in \{0,1\}^{|x|^c} \ \text{s.t. } M \text{ rejects } (x, w)$.

אינטואיציה. זו מילה במילה הגדרת ה-verifier של NP, כשההבדל היחיד הוא שבמקום "M **מקבלת** את (x, w)" כתוב "M **דוחה** את (x, w)". במילים: העד אינו מחרוזת שמשכנעת את הבודק לומר "כן", אלא מחרוזת שגורמת לו לומר "לא". מכיוון שהמכונה דטרמיניסטית ופולינומית — ולכן **עוצרת תמיד** — "לא לקבל" ו"לדחות" הם אותו אירוע, ואפשר להחליף ביניהם על ידי החלפת שני מצבי העצירה.

מופע. $\mathrm{SAT} \in \mathrm{C}_1$: קחו את ה-verifier הרגיל של SAT (הצב את ההשמה w בנוסחה) והחליפו בו את מצב הקבלה במצב הדחייה. **אי-מופע (למראית עין):** אין כאן אף שפה שהיא ב-C_1 ולא ב-NP — זו בדיוק תוצאת סעיף א'.

הגדרה 2: המחלקה C_2 (סעיף ב' בשאלה)

C_2 היא מחלקת השפות $A \subseteq \Sigma^*$ עבורן קיים $c \geq 1$ כך שקיימת מכונת טיורינג דטרמיניסטית M עם זמן ריצה פולינומי, כך שלכל $x \in \Sigma^*$ מתקיים:

אם $x \in A$ אז $\exists\, w \in \{0,1\}^{|x|^c}$ שעבורו M מקבלת את (x, w);

אם $x \notin A$ אז $\exists\, w \in \{0,1\}^{|x|^c}$ שעבורו M דוחה את (x, w).

אינטואיציה. גם כאן ההשוואה היא ל-NP, וההבדל הוא **כמתי**: בהגדרת NP הצד השני הוא "אם $x \notin A$ אז **לכל** w המכונה דוחה", וכאן הוא הוחלף ב"**קיים** w שעבורו היא דוחה" [00:17:57]. זו החלשה דרמטית: תנאי "קיים" בשני הצדדים אינו מחייב את המכונה להבחין בין $x \in A$ ל-$x \notin A$ **בכלל**. די שהמכונה תדע לקבל על עד אחד ולדחות על עד אחר — וזה משהו שכל מכונה טיפשית יודעת לעשות.

מופע. כל שפה שהיא. **אי-מופע.** אין. זו בדיוק המסקנה שסטודנט העלה בכיתה [00:52:59]: "C_2 זה בעצם קבוצת כל השפות" — והמרצה אישר שהטענה נכונה, אך סירב להוכיח אותה כי אין בה צורך (ראו הערות).

הגדרה 3: המחלקה C_3 (סעיף ג' בשאלה)

C_3 היא מחלקת השפות $A \subseteq \Sigma^*$ עבורן קיים $c \geq 1$ כך שקיימת מכונת טיורינג דטרמיניסטית M עם זמן ריצה פולינומי, כך שלכל $x \in \Sigma^*$ מתקיים: $x \in A \iff \exists\, w \in \{0,1\}^{c} \ \text{s.t.}\ M \text{ accepts } (x, w)$.

אינטואיציה. ההגדרה זהה **אות באות** להגדרת NP, למעט מקום אחד: אורך העד הוא c ולא $|x|^c$ — כלומר **קבוע שאינו תלוי בקלט כלל** [00:58:53]. וזה משנה הכול: מספר העדים האפשריים הוא 2^c, שהוא קבוע, ולכן אפשר פשוט לעבור על כולם בזמן פולינומי. העד מפסיק להיות "עזרה מבחוץ" והופך לפרט טכני שאפשר לנחש בכוח.

מופע. כל שפה ב-P (הוכחה בתרגיל 3 להלן). **אי-מופע.** SAT, אלא אם $\mathrm{P} = \mathrm{NP}$ — כלומר אנחנו לא יודעים להצביע על אי-מופע קונקרטי, וזה בדיוק תוכן החלק האחרון של הסעיף.

הגדרה 4: HALT

$\mathrm{HALT} = \{\langle M, x\rangle \mid M \text{ halts on } x\}$. זו השפה שתשמש אותנו כ"עד" לכך ש-C_2 אינה מוכלת ב-NP.

משפטים והוכחות

משפט 1: היפוך מצבי הקבלה והדחייה

טענה. תהי M מכונת טיורינג דטרמיניסטית העוצרת על כל קלט, ותהי $\hat{M}$ המכונה המתקבלת מ-M על ידי **החלפת מצב הקבלה ומצב הדחייה** זה בזה. אזי לכל קלט a: $\hat{M}$ מקבלת את a אם ורק אם M דוחה את a; ו-$\mathrm{time}_{\hat{M}}(a) = \mathrm{time}_{M}(a)$.

הוכחה. $\hat{M}$ זהה ל-M בכל רכיביה — Q, q_{start}, Σ, Γ, δ — למעט תיוג שני מצבי העצירה. לכן על כל קלט a שתי המכונות עוברות **את אותה סדרת קונפיגורציות בדיוק**, ובפרט עוצרות באותו מספר צעדים ובאותו מצב עצירה. מכיוון ש-M עוצרת על כל קלט, מצב העצירה הוא בהכרח אחד משני המצבים q_{acc}, q_{rej}; ומכיוון שהתיוג הוחלף, $\hat{M}$ מקבלת בדיוק כאשר M דוחה. ■

> **הערה:** בהרצאה זה נאמר במשפט אחד — "כי המכונה דטרמיניסטית, אני יכול להפוך את ה-accept וה-reject" [00:03:41]; הפירוט כאן. שימו לב **היכן** נכנסת הדטרמיניסטיות: במכונה אי-דטרמיניסטית "לא מקבלת" פירושו "**כל** הריצות דוחות", ואילו "דוחה" של ריצה בודדת הוא אירוע אחר לגמרי — היפוך המצבים היה הופך "קיימת ריצה מקבלת" ל"קיימת ריצה דוחה", שאינה שלילת המקור. המשפט הזה **נכשל** למכונות אי-דטרמיניסטיות.

הערת סגנון של המרצה [00:07:20]–[00:08:27]. כשמציגים את $\hat{M}$ **אין** לכתוב "נגדיר מכונה"; הניסוח הנכון הוא "**נסמן** ב-$\hat{M}$ את המכונה המתקבלת מ-M על ידי החלפת מצבי הקבלה והדחייה". הסיבה: לא כתבנו אלגוריתם חדש, שינינו תיוג. "נגדיר" אינו טעות, זה עניין של סגנון — אבל הוא מטשטש את מה שבאמת קורה.

משפט 2: מ"לכל" ל"קיים" מעל תחום לא ריק

טענה. תהי S קבוצה **לא ריקה** ותהי φ תכונה. אם לכל $s \in S$ מתקיים $\varphi(s)$, אז קיים $s \in S$ שעבורו $\varphi(s)$.

הוכחה. $S \neq \emptyset$, ולכן קיים $s_0 \in S$. מההנחה $\varphi(s_0)$ מתקיים. ■

למה זה לא טריוויאלי, ולמה חייבים לומר את זה במפורש [00:32:54]. הטענה "כל מספר שריבועו שלילי מתחלק ב-3" היא **נכונה** (ריקנית), ובכל זאת לא קיים מספר שריבועו שלילי. לכן המעבר מ"לכל" ל"קיים" אינו כלל לוגי חופשי — הוא דורש את אי-ריקות התחום. בכל השימושים בקובץ הזה התחום הוא $\{0,1\}^{|x|^c}$, שהוא לעולם אינו ריק (יש בו $2^{|x|^c} \geq 1$ מחרוזות), ולכן המעבר תקף.

> **המלצת המרצה** [00:33:25]: במקום להסתמך על המעבר הזה, **פשוט הציגו איבר קונקרטי**. אם ידוע שכל w מקיים משהו וצריך להוכיח שקיים כזה — כתבו "נתבונן ב-$w = 0^{|x|^c}$". זה קצר יותר, נצמד לתבנית ההוכחה של טענת קיום, ואינו מסתמך על צעד לוגי שקל לשגות בו.

משפט 3: $\mathrm{HALT} \notin \mathrm{NP}$

טענה. $\mathrm{HALT} \notin \mathrm{NP}$.

הוכחה. לפי שיעור 8, $\mathrm{NP} \subseteq \mathrm{PSPACE}$. כל שפה ב-$\mathrm{PSPACE}$ ניתנת להכרעה — קיימת לה מכונה שעוצרת על כל קלט ומכריעה אותה במקום פולינומי — ולכן $\mathrm{PSPACE} \subseteq \mathrm{R}$. נשרשר: $\mathrm{NP} \subseteq \mathrm{PSPACE} \subseteq \mathrm{R}$. מקורס החישוביות $\mathrm{HALT} \notin \mathrm{R}$, ולכן $\mathrm{HALT} \notin \mathrm{NP}$. ■

מסלול חלופי שהוצג בכיתה [00:41:14]–[00:46:30]. אפשר לא לצאת מ-R בכלל. ממשפט ההיררכיה במקום (שיעור 3), באותה הוכחה בדיוק שנתנה $\mathrm{P} \subsetneq \mathrm{EXP}$, מקבלים $\mathrm{PSPACE} \subsetneq \mathrm{EXPSPACE}$: מראים $\mathrm{PSPACE} \subseteq \mathrm{DSpace}(2^n) \subsetneq \mathrm{DSpace}(2^{n^2}) \subseteq \mathrm{EXPSPACE}$, כשההכלה האמצעית ממש היא בדיוק משפט ההיררכיה. לכן קיימת $A \in \mathrm{EXPSPACE} \setminus \mathrm{PSPACE}$, ומכיוון ש-$\mathrm{NP} \subseteq \mathrm{PSPACE}$ נובע $A \notin \mathrm{NP}$. המרצה ציין שהוא מרגיש פחות בנוח עם המסלול הזה, אך הוא תקף לגמרי.

> **מה אי אפשר לעשות** [00:43:17]. אי אפשר להסיק ישירות מ-$\mathrm{P} \subsetneq \mathrm{EXP}$ שקיימת שפה מחוץ ל-NP: הכלה ממש בין הקצוות של שרשרת אינה אומרת לנו **איזו** מן ההכלות בפנים היא ממש, ולכן לא נובע ממנה כלום על NP עצמה. צריך משפט היררכיה שמפריד שתי מחלקות ש-NP יושבת בין הקטנה שבהן לבין עצמה.

משפט 4: $\mathrm{NP} \subseteq \mathrm{PSPACE}$ — הפניה לשיעור 8, והמכונה שנשתמש בה שוב

טענה. $\mathrm{NP} \subseteq \mathrm{PSPACE}$. **הוכחה: ראו שיעור 8, משפט 1.**

הסיבה שמזכירים אותה כאן היא לא הטענה אלא ה**מכונה**: בהינתן verifier M ופולינום q לאורך העד, בונים מכונה $\hat{M}$ שעל קלט x עוברת על **כל** $w \in \{0,1\}^{q(|x|)}$, מריצה את M על (x, w), ומקבלת אם אחת ההרצות קיבלה. מספר האיטרציות הוא $2^{q(|x|)}$ — מעריכי, ולכן מקבלים PSPACE ולא P.

בתרגיל 3 להלן נשתמש **באותו מנגנון בדיוק**, אך מספר האיטרציות יהיה 2^c — קבוע — ולכן נקבל P. כדברי המרצה [01:09:12]: "המכניזם הוא אותו מכניזם, רק שפה מספר האיטרציות של הלולאה קטן יותר".

דוגמאות ותרגילים מהשיעור

עמוד 1 נושא כותרת ירוקה — **"פתרון מטלה 2"** — וחמשת העמודים כולם הם פתרון של **שאלה 3** במטלה. ניסוח השאלה, כפי שהוא מודפס בראש עמוד 1:

> **3.** עבור כל אחת ממחלקות הסיבוכיות שלהלן קבעו האם היא מכילה את המחלקה NP, האם היא מוכלת בה, והאם היא שווה לה (אם ידוע; אחרת הוכיחו כי השאלה שקולה לשאלה פתוחה).

שימו לב שיש כאן **שלוש** שאלות נפרדות לכל מחלקה, ולא אחת. המרצה חזר על כך שלוש פעמים בסוף השיעור [01:19:38], [01:23:22], [01:24:27]: תשובה שמתייחסת רק לשוויון — גם אם היא נכונה — אינה עונה על מה שנשאל.

שיטת הפתרון בארבעה שלבים [00:05:45]–[00:06:17]:

לזהות איזו **הגדרה מוכרת** קרובה ביותר להגדרה שניתנה. (מחשבתי)

לכתוב את שתי ההגדרות **אחת מול השנייה**, ולאתר את ההבדל ברמת ה-pattern matching. (טכני)

להכריע האם אפשר **לגשר** על ההבדל, ובאיזה כיוון. (מחשבתי — כאן נמצא כל התוכן)

לכתוב את ההוכחה לפי התבנית. (טכני)

"החלק שנופלים עליו הוא דווקא השלב הקודם" [00:03:09] — כלומר שלב 2, ההשוואה. המרצה מדגיש שהוא עצמו כותב את שתי ההגדרות זו לצד זו על דף, כי הוא לא מסוגל לראות את ההבדל בראש [00:02:07].

תרגיל 1 (סעיף א'): C_1 — האם מכילה, מוכלת, שווה?

זיהוי ההבדל. ההגדרה הקרובה ביותר היא NP בנוסח ה-verifier. ההשוואה:

NP	C_1
$x \in A \iff \exists w \in \{0,1\}^{\|x\|^c}$	$x \in A \iff \exists w \in \{0,1\}^{\|x\|^c}$
כך ש-M **מקבלת** את (x, w)	כך ש-M **דוחה** את (x, w)

ההבדל הוא מילה אחת, וניתן לגשר עליו לפי **משפט 1**.

חלק א': $\mathrm{C}_1 \subseteq \mathrm{NP}$

תהא $A \in \mathrm{C}_1$. לכן קיימת מכונה M הרצה בזמן פולינומי, וכן קיים $c \geq 1$, כך שלכל $x \in \Sigma^*$: $x \in A \iff \exists\, w \in \{0,1\}^{|x|^c} \text{ s.t. } M \text{ rejects } (x, w)$.

נסמן ב-$\hat{M}$ את המכונה המתקבלת מ-M על ידי החלפת מצבי הקבלה והדחייה. לפי משפט 1, $\hat{M}$ רצה בזמן פולינומי (אותו זמן ריצה בדיוק), ולכל קלט a: $\hat{M}$ מקבלת את a אם ורק אם M דוחה אותו. **נתבונן ב-$\hat{M}$ ונתבונן ב-c.** אכן $\hat{M}$ רצה בזמן פולינומי, ואכן $c \geq 1$.

יהי $x \in \Sigma^*$.

כיוון ראשון. נניח $x \in A$. לכן קיים $w \in \{0,1\}^{|x|^c}$ כך ש-M דוחה את (x,w). **נתבונן ב-w זה.** אכן $w \in \{0,1\}^{|x|^c}$ (הוא התקבל מתוך ההגדרה של C_1, ולכן באורך הנכון), ומכיוון ש-M דוחה את (x,w), לפי משפט 1 המכונה $\hat{M}$ **מקבלת** את (x,w).

כיוון שני. נניח $x \notin A$. לפי ההגדרה של C_1 (בשלילת הצד הימני של האם-ורק-אם), לכל $w \in \{0,1\}^{|x|^c}$ המכונה M **אינה** דוחה את (x,w), ומכיוון שהיא עוצרת תמיד — היא מקבלת את (x,w). יהי $w \in \{0,1\}^{|x|^c}$; לפי משפט 1, $\hat{M}$ **דוחה** את (x,w).

סיכום התבנית. קיבלנו: קיימת מכונה $\hat{M}$ הרצה בזמן פולינומי וקיים $c \geq 1$ כך שלכל x — אם $x \in A$ אז קיים $w \in \{0,1\}^{|x|^c}$ ש-$\hat{M}$ מקבלת את (x,w), ואם $x \notin A$ אז לכל $w \in \{0,1\}^{|x|^c}$ המכונה $\hat{M}$ דוחה את (x,w). זו בדיוק הגדרת NP, ולכן $A \in \mathrm{NP}$.

מכאן $\mathrm{C}_1 \subseteq \mathrm{NP}$. ■

על שתי השורות האחרונות [00:13:44]. המרצה רשם את "סיכום התבנית" הזה **על הלוח בשחור**, מסגרת נפרדת, למרות שהוא רק חוזר על מה שהוכח. הסיבה: "כשמביאים את זה ככה, המבנה קופץ החוצה" — הקישור בין ההוכחה להגדרה נעשה ברמה תחבירית ולא ברמה של אינטואיציה. אפשר לכתוב במקום זה את הצורה המקוצרת ("ולכן לכל w המכונה $\hat{M}$ דוחה"), וזה נכון מתמטית ומקובל, אבל המבנה פחות נראה [00:14:47].

חלק ב': $\mathrm{NP} \subseteq \mathrm{C}_1$

הסיכום כותב "ובאותו אופן"; ההרצאה אמרה "הכיוון השני זה אותו דבר בדיוק, אני לא חושב שאנחנו צריכים" [00:16:56]. הנה הוא במלואו.

תהא $A \in \mathrm{NP}$. לכן קיימת מכונה M הרצה בזמן פולינומי וקיים $c \geq 1$ כך שלכל $x \in \Sigma^*$: $x \in A$ אם ורק אם קיים $w \in \{0,1\}^{|x|^c}$ ש-M מקבלת את (x,w). נסמן ב-$\hat{M}$ את המכונה המתקבלת מ-M בהחלפת מצבי הקבלה והדחייה; לפי משפט 1 היא פולינומית, ולכל a היא **דוחה** את a אם ורק אם M מקבלת אותו.

נתבונן ב-$\hat{M}$ ונתבונן ב-c. יהי $x \in \Sigma^*$.

אם $x \in A$: קיים $w \in \{0,1\}^{|x|^c}$ ש-M מקבלת את (x,w), ולכן $\hat{M}$ **דוחה** את (x,w) — כלומר קיים w שעבורו $\hat{M}$ דוחה.

אם $x \notin A$: לכל $w \in \{0,1\}^{|x|^c}$ המכונה M דוחה את (x,w), ולכן $\hat{M}$ **מקבלת** את (x,w) — כלומר אין אף w שעבורו $\hat{M}$ דוחה.

שני התנאים יחד נותנים בדיוק $x \in A \iff \exists w \in \{0,1\}^{|x|^c} : \ \hat{M} \text{ rejects } (x,w)$, כלומר $A \in \mathrm{C}_1$. מכאן $\mathrm{NP} \subseteq \mathrm{C}_1$. ■

התשובה לשלוש השאלות

$$\boxed{\mathrm{C}_1 = \mathrm{NP}}$$

האם C_1 מוכלת ב-NP? כן — חלק א'.

האם C_1 מכילה את NP? כן — חלק ב'.

האם C_1 שווה ל-NP? כן, משתי ההכלות. אף אחת מהשאלות אינה פתוחה.

תרגיל 2 (סעיף ב'): C_2 — האם מכילה, מוכלת, שווה?

זיהוי ההבדל [00:17:57]. שוב ההגדרה הקרובה היא NP. כשכותבים אותן זו מול זו:

NP	C_2
$x \in A \;\Rightarrow\; \exists w:\ M \text{ accepts } (x,w)$	$x \in A \;\Rightarrow\; \exists w:\ M \text{ accepts } (x,w)$
$x \notin A \;\Rightarrow\; \forall w:\ M \text{ rejects } (x,w)$	$x \notin A \;\Rightarrow\; \exists w:\ M \text{ rejects } (x,w)$

ההבדל: **"קיים" פעמיים במקום "לכל" ו"קיים"**. הגישור אפשרי רק **בכיוון אחד**: מ"לכל" ל"קיים" (משפט 2, התחום אינו ריק), ולא להפך. לכן התחושה המיידית היא $\mathrm{NP} \subseteq \mathrm{C}_2$, וכנראה הכלה ממש [00:26:54].

חלק א': $\mathrm{NP} \subseteq \mathrm{C}_2$

תהא $A \in \mathrm{NP}$. לכן קיימת מכונה M הרצה בזמן פולינומי וקיים $c \geq 1$ כך שלכל $x \in \Sigma^*$: $x \in A \iff \exists\, w \in \{0,1\}^{|x|^c} \text{ s.t. } M \text{ accepts } (x,w)$.

נתבונן ב-M ונתבונן ב-c — אותה מכונה ואותו קבוע, אין צורך לבנות דבר. אכן M רצה בזמן פולינומי ואכן $c \geq 1$.

יהי $x \in \Sigma^*$.

המקרה $x \in A$. לפי ההגדרה קיים $w \in \{0,1\}^{|x|^c}$ ש-M מקבלת את (x,w). **זו בדיוק הטענה שצריך להוכיח**, ולכן עוצרים כאן [00:31:21].

המקרה $x \notin A$. לפי ההגדרה, לכל $w \in \{0,1\}^{|x|^c}$ המכונה M אינה מקבלת את (x,w); מכיוון ש-M פולינומית ולכן עוצרת — היא דוחה את (x,w). עלינו להוכיח טענת **קיום**, ולכן נציג עד קונקרטי: **נתבונן ב-$w = 0^{|x|^c}$**. אכן $w \in \{0,1\}^{|x|^c}$ (זו מחרוזת בינרית באורך $|x|^c$), ולפי הנ"ל M דוחה את (x,w).

לכן $A \in \mathrm{C}_2$, ומכאן $\mathrm{NP} \subseteq \mathrm{C}_2$. ■

> **שאלת סטודנט** [00:35:29]: האם $1^{|x|^c}$ היה עובד גם? כן — **כל** מחרוזת בקבוצה עובדת, כי הטענה מתקיימת לכל w. $0^{|x|^c}$ ו-$1^{|x|^c}$ הן פשוט הכתיבות הקצרות ביותר.

חלק ב': $\mathrm{C}_2 \not\subseteq \mathrm{NP}$

צריך להציג שפה שהיא ב-C_2 ואינה ב-NP. **נתבונן ב-HALT.** לפי משפט 3, $\mathrm{HALT} \notin \mathrm{NP}$. נותר להראות $\mathrm{HALT} \in \mathrm{C}_2$.

נבנה מכונה M, שעל קלט (x,w):

אם התו הראשון של w הוא 1 — **קבל**.

אחרת — **דחה**.

נתבונן ב-M ונתבונן ב-$c = 1$. אכן $c \geq 1$. M רצה בזמן פולינומי בגודל הקלט — למעשה בזמן **קבוע**, היא קוראת תו אחד [00:50:13].

יהי x.

המקרה $x \in \mathrm{HALT}$. **נתבונן ב-$w = 1^{|x|}$.** אכן $w \in \{0,1\}^{|x|^1}$. התו הראשון של w הוא 1, ולכן M מקבלת את (x,w).

המקרה $x \notin \mathrm{HALT}$. **נתבונן ב-$w = 0^{|x|}$.** אכן $w \in \{0,1\}^{|x|^1}$. התו הראשון של w אינו 1, ולכן M דוחה את (x,w).

לכן HALT מקיימת את הגדרת C_2, כלומר $\mathrm{HALT} \in \mathrm{C}_2$. מכיוון ש-$\mathrm{HALT} \notin \mathrm{NP}$, נובע $\mathrm{C}_2 \not\subseteq \mathrm{NP}$. ■

> **השלמה: הקלט הריק.** אם $x = \varepsilon$ אז $|x| = 0$, העד היחיד הוא המחרוזת הריקה, ואין לה "תו ראשון". שלב 1 אינו מתקיים ולכן M דוחה — וזה בדיוק מה שצריך, כי בקידודים המקובלים ε אינו קידוד חוקי של זוג $\langle M, x \rangle$ ולכן $\varepsilon \notin \mathrm{HALT}$. שני המקורות עוברים על המקרה הזה בשתיקה; ראו סעיף הפערים.

מסקנה: $\mathrm{NP} \subsetneq \mathrm{C}_2$

מחלק א' $\mathrm{NP} \subseteq \mathrm{C}_2$, ומחלק ב' $\mathrm{C}_2 \not\subseteq \mathrm{NP}$, ולכן ההכלה ממש: $\boxed{\mathrm{NP} \subsetneq \mathrm{C}_2}$

האם C_2 מכילה את NP? כן, וממש.

האם C_2 מוכלת ב-NP? לא.

האם C_2 שווה ל-NP? לא. אף אחת מהשאלות אינה פתוחה.

מה באמת קורה כאן: C_2 היא מחלקת כל השפות

סטודנט הצביע על כך בכיתה [00:52:59], והמרצה אישר שהטענה נכונה [00:57:10]. הנימוק: אותה מכונה M בדיוק ("אם התו הראשון של w הוא 1 קבל, אחרת דחה") מקיימת את הגדרת C_2 עבור **כל** שפה A, כי היא כלל אינה מסתכלת על x — ולכל x יש עד שגורם לה לקבל ועד שגורם לה לדחות. תהא $A \subseteq \Sigma^*$ כלשהי: אם $x \in A$ ניקח $w = 1^{|x|}$ והמכונה מקבלת, ואם $x \notin A$ ניקח $w = 0^{|x|}$ והמכונה דוחה. לכן $A \in \mathrm{C}_2$, כלומר $\mathrm{C}_2 = \{A \mid A \subseteq \Sigma^*\}$.

ואף על פי כן המרצה סירב לכתוב את זה [00:57:10]. הסיבה מתודית: השאלה דורשת להוכיח **קיום** של שפה ב-$\mathrm{C}_2 \setminus \mathrm{NP}$, ותבנית ההוכחה של טענת קיום היא "נתבונן ב-HALT", לא "תהא A שפה כלשהי". הוכחת הטענה החזקה יותר אינה שגויה ואינה מפסידה נקודות — "בתנאי שאתה לא טועה שם" — אבל היא עבודה מיותרת שמגדילה את שטח הפנים לשגיאות.

תרגיל 3 (סעיף ג'): C_3 — האם מכילה, מוכלת, שווה?

זיהוי ההבדל [00:58:53]. ההגדרה זהה להגדרת NP למעט אורך העד: $w \in \{0,1\}^c$ במקום $w \in \{0,1\}^{|x|^c}$ — אורך **קבוע שאינו תלוי ב-x**.

הגישור. מספר העדים האפשריים הוא 2^c. "זה נראה מעריכי, זה מעריכי — אבל לא ב-x" [00:59:55]. מה שקובע הוא האם הביטוי מעריכי **כפונקציה של אורך הקלט**, ו-2^c הוא קבוע. לכן אפשר להריץ את ה-verifier על כל העדים ועדיין להישאר בזמן פולינומי. המרצה הפנה כאן לאחור, לשיעור הקודם, שבו נדון באותו הקשר הביטוי n^{2^c}: "לא כל מה שיש לו צורה מעריכית אומר שזה מעריכי" [00:59:55].

חלק א': $\mathrm{C}_3 \subseteq \mathrm{P}$

תהא $A \in \mathrm{C}_3$. לכן קיימת מכונה M הרצה בזמן פולינומי וקיים $c \geq 1$ כך שלכל $x \in \Sigma^*$: $x \in A \iff \exists\, w \in \{0,1\}^c \text{ s.t. } M \text{ accepts } (x, w)$.

נגדיר מכונה $\hat{M}$ באופן הבא, על קלט x:

לכל $w \in \{0,1\}^c$:

1.1 הרץ את M על (x, w).

1.2 אם M קיבלה — **קבל**.

דחה.

(שימו לב לממשק: $\hat{M}$ מקבלת **רק את** x, כי היא אמורה להכריע את A [01:01:32].)

ניתוח זמן ריצה. יהי $x \in \Sigma^*$.

לכל $w \in \{0,1\}^c$, זמן הריצה של M על (x,w) פולינומי ב-$|x| + |w| = |x| + c$. מכיוון ש-c קבוע, זהו פולינום ב-$|x|$.

$\hat{M}$ מריצה את M בדיוק 2^c פעמים. **מספר הפעמים אינו תלוי ב-**x — זהו קבוע של המכונה. כתיבת המונה ומעבר על $\{0,1\}^c$ עולים $O(c) = O(1)$.

סך הכול $\big(p(|x|+c) + O(1)\big)$, $\cdot\, 2^c \leq \mathrm{time}_{\hat{M}}(x)$, שהוא פולינום ב-$|x|$ (מכפלה בקבוע והרכבת פולינומים).

נכונות. יהי $x \in \Sigma^*$.

נניח $x \in A$. אז קיים $w \in \{0,1\}^c$ כך ש-M מקבלת את (x,w). מכיוון ש-$\hat{M}$ עוברת על **כל** $\{0,1\}^c$, קיימת בריצה שלה על x איטרציה שבה נבחר בדיוק ה-w הזה; באיטרציה זו שלב 1.2 מתקיים ו-$\hat{M}$ מקבלת את x.

נניח $x \notin A$. אזי **לכל** $w \in \{0,1\}^c$ המכונה M אינה מקבלת את (x,w), ומכיוון שהיא עוצרת — היא דוחה. יהי $w \in \{0,1\}^c$; שלב 1.2 אינו מתקיים באיטרציה שלו. מכיוון שזה נכון לכל w, הלולאה מסתיימת ו-$\hat{M}$ דוחה את x בשלב 2.

מכאן $\hat{M}$ מכריעה את A בזמן פולינומי, ולכן $A \in \mathrm{P}$. מכאן $\mathrm{C}_3 \subseteq \mathrm{P}$. ■

תיקון שעלה בכיתה [01:07:39]. בכתיבה הראשונה על הלוח המרצה כתב במקרה $x \notin A$ ישירות "M דוחה את (x,w)" בלי לכמת. סטודנט העיר שחסר "**יהי** $w \in \{0,1\}^c$" — כי כדי להסיק ש-$\hat{M}$ דוחה צריך להראות שהמקרה נכשל **לכל** w, לא ל-w אחד. המרצה קיבל: "אתה צודק, שאלה טובה". התיקון מופיע בגוף ההוכחה למעלה, וגם בסיכום.

הקשר לשיעור 8 [01:02:35], [01:09:12]. זו אותה מכונה בדיוק שבנינו כדי להוכיח $\mathrm{NP} \subseteq \mathrm{PSPACE}$ — "נבנה מכונה שתעבור על כל העדים". שם מספר האיטרציות היה $2^{q(|x|)}$, ולכן יכולנו לטעון רק על ה**מקום** (בתנאי שכל איטרציה משתמשת באותם תאים). כאן מספר האיטרציות קבוע, ולכן אנחנו מקבלים חסם על ה**זמן**. אילו אורך העד היה $|x|^c$ היו לנו $2^{|x|^c}$ איטרציות והטיעון היה קורס.

חלק ב': $\mathrm{P} \subseteq \mathrm{C}_3$

תהא $A \in \mathrm{P}$. לכן קיימת מכונה M המכריעה את A בזמן פולינומי.

נגדיר מכונה $\hat{M}$ באופן הבא, על קלט (x,w):

הרץ את M על x והחזר את אותה תשובה. (העד w נזרק.)

נתבונן ב-$\hat{M}$ **ונתבונן ב-**$c = 1$**.** אכן $c \geq 1$.

M רצה בזמן פולינומי ב-$|x|$, ומכיוון ש-$|x| \leq |(x,w)|$, המכונה $\hat{M}$ רצה בזמן פולינומי **בגודל הקלט שלה** [01:14:41]. (המרצה הדגיש שאין שום צורך "להיכנס פנימה" ולחלץ את הפולינום או הקבוע של M — מריצים את אותה מכונה על אותו קלט, ואין מה לנתח.)

יהי $x \in \Sigma^*$.

נניח $x \in A$. אזי M מקבלת את x. **נתבונן ב-**$w = 0$**.** אכן $w \in \{0,1\}^1 = \{0,1\}^c$, ו-$\hat{M}$ מריצה את M על x ומחזירה קבלה, כלומר $\hat{M}$ מקבלת את (x, w).
נניח $x \notin A$. אזי M דוחה את x. יהי $w \in \{0,1\}^1$. אזי $\hat{M}$ מריצה את M על x ומחזירה דחייה, כלומר $\hat{M}$ דוחה את (x, w). זה נכון לכל w.
לכן $x \in A \iff \exists w \in \{0,1\}^c : \ \hat{M} \text{ accepts } (x,w)$, כלומר $A \in \mathrm{C}_3$. מכאן $\mathrm{P} \subseteq \mathrm{C}_3$. ■

> **טעות בזמן אמת, ותיקונה** [01:16:26]–[01:16:56]. המרצה כתב תחילה $w = 0^c$, ומיד תיקן ל-$w = 0$: "חשבתי על ה-2^c מההוכחה הקודמת". מכיוון שבחרנו $c = 1$, קבוצת העדים היא $\{0,1\}^1 = \{0,1\}$, ולכן העד הוא **ביט בודד**. זו טעות טיפוסית שנולדת מהעתקת תבנית מהסעיף הקודם בלי לבדוק את הפרמטר שנבחר.

התשובה לשלוש השאלות
משני החלקים: $\boxed{\mathrm{C}_3 = \mathrm{P}}$
האם C_3 **מוכלת ב-**NP**? כן, וזו טענה ידועה.** $\mathrm{C}_3 \subseteq \mathrm{P} \subseteq \mathrm{NP}$ (שיעור 4). זו **אינה** שאלה פתוחה.
האם C_3 **מכילה את** NP**? שאלה פתוחה.** מכיוון ש-$\mathrm{C}_3 = \mathrm{P}$, הטענה $\mathrm{NP} \subseteq \mathrm{C}_3$ שקולה לטענה $\mathrm{NP} \subseteq \mathrm{P}$; ומכיוון ש-$\mathrm{P} \subseteq \mathrm{NP}$ תמיד, זו בדיוק השאלה $\mathrm{P} = \mathrm{NP}$.
האם C_3 **שווה ל-**NP**?** שקול ל-$\mathrm{P} = \mathrm{NP}$, כלומר **שאלה פתוחה**.

> **למה לפרק את השוויון לשתי הכלות** [01:19:08]–[01:24:27]. סטודנט שאל למה לא לכתוב פשוט "$\mathrm{C}_3 = \mathrm{NP}$ אם ורק אם $\mathrm{P} = \mathrm{NP}$, ולכן שאלה פתוחה". התשובה: זה **נכון ולא שגוי**, אבל הוא מחביא מידע. השוויון הוא צירוף של שתי הכלות, שאחת מהן **ידועה** (ונכונה) והשנייה פתוחה. השאלה במפורש ביקשה להתייחס לשלוש הטענות בנפרד, ולכן התשובה צריכה להצביע איזה **חלק** של השוויון הוא הפתוח. המרצה הודה שניסוח השאלה יכול היה להיות בהיר יותר [01:20:43].

תרגיל 4 (סעיף ה'): C_5 — נדון בעל פה בלבד
הסעיף הזה **אינו** בסיכום; הוא נפתר בעל פה בעשר הדקות האחרונות [01:24:27]–[01:29:44] לבקשת סטודנט, בלי לכתוב על הלוח. הוא מובא כאן בקצרה כי הוא משתמש בדיוק באותה טכניקה.
ההגדרה. C_5 היא מחלקת השפות A עבורן קיים קבוע c כך שקיימת מכונה **אי-דטרמיניסטית** N עם זמן ריצה פולינומי המכריעה את A, וכך שלכל $x \in \Sigma^*$ **מספר הבחירות האי-דטרמיניסטיות** בריצה על x אינו עולה על $c \log |x|$.
זיהוי ההבדל. ההגדרה הקרובה היא NP **בנוסח האי-דטרמיניסטי**, וההבדל הוא הגבלה על מספר נקודות הבחירה (לא על זמן הריצה, שנשאר פולינומי).
התשובה: $\mathrm{C}_5 = \mathrm{P}$**.** נזכיר מתסריט הריצה של שיעור 6: נסמן ב-$\alpha = \max_{q,\sigma} |\delta(q,\sigma)|$ את מספר האפשרויות המרבי בנקודת בחירה. α הוא **קבוע של המכונה** — הוא נחסם על ידי $2 \cdot |\Gamma| \cdot |Q|$ ואינו תלוי ב-x. לתיאור בחירה אחת דרושים $\lceil \log \alpha \rceil$ ביטים, ולכן לתיאור ריצה שלמה דרושים $\lceil \log \alpha \rceil \cdot c \log |x|$ ביטים, ומספר העדים האפשריים הוא $2^{\lceil \log \alpha \rceil \cdot c \log |x|} = |x|^{c \lceil \log \alpha \rceil}$, כלומר **פולינומי ב-**$|x|$. עכשיו מפעילים בדיוק את המכונה מחלק א' של תרגיל 3: עוברים על כל תסריטי

הריצה, מסמלצים את N על כל אחד מהם דטרמיניסטית, ומקבלים אם אחת הסימולציות קיבלה. מספר האיטרציות פולינומי וכל סימולציה פולינומית, ולכן הסימולציה כולה פולינומית, ומכאן $A \in \mathrm{P}$. הכיוון ההפוך, $\mathrm{P} \subseteq \mathrm{C}_5$, מיידי: מכונה דטרמיניסטית היא מכונה אי-דטרמיניסטית עם אפס בחירות.
האינטואיציה של המבוך [01:26:04]. מכונה אי-דטרמיניסטית היא מבוך; העד הוא רשימת ההוראות "בצומת הראשון שמאלה, בשני ימינה". ב-NP צריך הוראה לכל צעד — לכן העד ארוך פולינומית ומספר העדים מעריכי. כאן יש רק $c \log |x|$ צמתים שבהם בכלל יש ברירה, ולכן רשימת ההוראות קצרה לוגריתמית ומספר הרשימות האפשריות הוא רק פולינומי.

הערות מהשיעור
[00:00:30] רמת הקושי. "השאלות האלה אינן קלות, הן מאוד טריקיות — אבל מה שחשוב להבין הוא שהן ברמת ההגדרה בלבד. אין שם שום דבר פרט להגדרה." אין צורך בשום משפט מהקורס מעבר לתשתית; כל התוכן הוא השוואה מדוקדקת בין שתי הגדרות.
[00:02:07] הכלי הפיזי. המרצה כותב את שתי ההגדרות זו לצד זו על **דף**, ולא בראש: "אני באופן אישי לא מסוגל לראות את הדברים האלה בראש". ב-[00:25:17] הוא מסביר למה הוא כותב על דפים ולא על טאבלט — הוא רוצה הרבה דברים מול העיניים בו זמנית.
[00:04:12]–[00:05:14] מה זה בכלל עד. התשובה לשאלה "מה תפקידו של w": ה-verifier אינו מכריע את A; הוא מכונה שאם נותנים לה קצת עזרה היא יודעת **לוודא**. הדוגמה: לשכנע שמספר הוא פריק דורש פירוק לגורמים, שהוא יקר — אבל בהינתן גורם, מספיק חילוק ארוך. "NP זה כל הבעיות שבהינתן עד לא מאוד גדול אני יכול לוודא אותן בזמן פולינומי. השאלה P מול NP היא כמו לשאול מה יותר קשה — לפתור מבחן או לבדוק אותו" [00:05:14].
[00:10:00] סדר כמתים. אפשר להחליף בין שני כמתים **מאותו סוג** ($\exists\exists$ או $\forall\forall$) בלי לשנות את המשמעות; **אסור** להחליף בין כמתים משני סוגים. בהגדרות שכאן זה מתיר לכתוב "קיים c כך שקיימת M" או "קיימת M כך שקיים c" באותה מידה.
[00:19:32]–[00:22:43] מול פולינום q. סטודנטית שאלה למה מותר להחליף ביניהם, ובצדק: לא כל פולינום הוא מהצורה n^c. התשובה בשני חלקים: (א) לכל פולינום q קיים c כך ש-$q(n) \le n^c$ אסימפטוטית, ואם העד ארוך יותר — האלגוריתם פשוט מתעלם מהזנב; (ב) עבור מספר **סופי** של ערכי n קטנים שבהם החסם עדיין לא תופס, המכונה יכולה "לזכור בעל פה" את התשובות. מסקנה: שתי הצורות שקולות, ובכתיבה **נצמדים לניסוח של השאלה**.
[00:30:17] אזהרה חוזרת. ה-verifier M **אינה** מכריעה את A, וזה לא עניין של יעילות אלא של **ממשק**: הקלטים שלה הם זוגות (x, w), ולא אובייקטים שאנחנו שואלים לגביהם שייכות. "היא לא מקבלת בכלל את x ככלט" — זו מכונת verification.
[00:53:30]–[00:54:03] מה מקבל נקודות. לכתוב "ממשפט ההיררכיה קיימת A שאינה ב-NP" — **תשובה חסרה**, לא שגויה: "אתה צודק שזה נובע ממשפט ההיררכיה, אבל **איך**?". לכתוב "ממשפט ההיררכיה קיימת $A \in \mathrm{EXPSPACE}$ שאינה ב-PSPACE, ומכיוון ש-$\mathrm{NP} \subseteq \mathrm{PSPACE}$ היא אינה ב-NP" — תשובה מלאה.

[00:55:37]–[00:56:39] מה המכונה בסעיף ב' לא מתיימרת לעשות. סטודנטית התקשתה: המכונה שבנינו ל-HALT אינה מכריעה את HALT, אפילו לא חלקית, ולא מזהה בה כלום — אז מה בעצם הוכחנו? התשובה: הגדרת C_2 **אינה** דורשת הכרעה. היא דורשת רק ש-לכל x בשפה תהיה אפשרות שהמכונה תקבל, ולכל x מחוץ לשפה תהיה אפשרות שהיא תדחה. "אני מצייט להגדרה, אני לא צריך יותר מזה." זה בדיוק מה שמבלבל בתרגיל.

[01:16:26] אזהרה על העתקת תבניות. הטעות $w = 0^c$ במקום $w = 0$ בסעיף ג' נולדה מהעתקת הצורה $0^{|x|^c}$ מהסעיף הקודם. הלקח: אחרי שבוחרים c, לבדוק **פיזית** מהי קבוצת העדים שנוצרה.

[00:15:20] על הפורמליות. "המטרה אינה שזה יהיה מסודר כי זה קדוש. המטרה היא שזה ייצור לכם בהירות מחשבתית." מותר לכתוב זורם יותר אם אתם בטוחים — "על אחריות המשתמש".

פערים בין הסיכום להקלטה

מקור: ההקלטה, [01:24:27]–[01:29:44]. **הפער:** סעיף ה' של אותה שאלה (C_5 — הגבלת מספר הבחירות האי-דטרמיניסטיות ל-$c \log |x|$) נפתר בעל פה ואינו מופיע כלל בחמשת עמודי הסיכום. **ההכרעה:** נכלל כאן כתרגיל 4, בקצרה ובסימון מפורש שהוא לא נכתב על הלוח, כי הוא מדגים את אותה טכניקה בדיוק ועשוי להופיע במבחן.

מקור: ההקלטה, [01:29:44] מול הסיכום. **הפער:** סעיף ד' של השאלה נדחה במפורש לשיעור הבא ("אנחנו נתחיל בסעיף ד' בשיעור הבא") ואינו בסיכום ולא בהקלטה. **ההכרעה:** לא נכתב כאן דבר עליו. בדיקה שנעשתה לאחר מכן על פני כל הקורפוס העלתה שהסעיף אינו מופיע גם בסיכום 25 ולא בהקלטות 29 או 30: הקלטה 29 נפתחת כבר בתוך תרגיל 3, כלומר תחילת אותו מפגש אינה מוקלטת, ושם נלמד הסעיף ככל הנראה. המחלקות C_1–C_4 שבהקלטה 30 הן וריאציות הסתברותיות על ([00:29:05]) BPP — התנגשות שמות בלבד, ואינן קשורות לסעיף זה. **מסקנה: לסעיף ד' אין תיעוד בקורפוס.**

מקור: ההקלטה, [00:52:59]–[00:57:42]. **הפער:** הסיכום אינו מזכיר כלל ש-C_2 היא מחלקת **כל** השפות; זו תוצאה של דיון כיתה. **ההכרעה:** נכללה כתת-סעיף נפרד בתרגיל 2, יחד עם ההסבר המתודי מדוע המרצה בחר **לא** להוכיח אותה.

מקור: ההקלטה, [00:41:14]–[00:46:30]. **הפער:** הסיכום מנמק $\mathrm{HALT} \notin \mathrm{NP}$ רק דרך $\mathrm{NP} \subseteq \mathrm{PSPACE} \subseteq \mathrm{R}$; ההקלטה מציגה גם מסלול חלופי דרך משפט ההיררכיה במקום, ומזהירה מפני שימוש שגוי ב-$\mathrm{P} \subsetneq \mathrm{EXP}$. **ההכרעה:** שני המסלולים והאזהרה נכתבו במשפט 3.

מקור: הסיכום, עמוד 2, וההקלטה [00:47:35]–[00:52:28]. **הפער:** הבנייה "אם התו הראשון של w הוא 1 — קבל" אינה מטפלת בקלט $x = \varepsilon$, שעבורו $c = 1$ נותן עד ריק שאין לו תו ראשון. **ההכרעה:** הבנייה נשמרה כפי שהיא (שלב 2 דוחה במקרה זה), והוספה הערה מפורשת בגוף: המקרה תקין כי $\varepsilon \notin \mathrm{HALT}$ בקידודים המקובלים.

מקור: הסיכום, עמוד 1, סוף העמוד. **הפער:** הכיוון $\mathrm{NP} \subseteq \mathrm{C}_1$ נכתב כ"באותו אופן" בלבד, וההקלטה [00:16:56] דילגה עליו במפורש. **ההכרעה:** נכתב כאן במלואו (תרגיל 1, חלק ב'), לפי דרישת הפירוט המלא.

מקור: ההקלטה, [01:07:39]. **הפער:** בכתיבה על הלוח חסר היה הכימות "יהי $w \in \{0,1\}^c$" במקרה $x \notin A$ בהוכחת $\mathrm{C}_3 \subseteq \mathrm{P}$; סטודנט תיקן והמרצה אישר. הסיכום כן כולל את השורה. **ההכרעה:** נכתב עם הכימות, והתיקון תועד כהערה כי הוא מדגים בדיוק את סוג הפער שהתבנית נועדה למנוע.

מקור: ההקלטה, [01:16:26]. **הפער:** על הלוח נכתב לרגע $w = 0^c$ במקום $w = 0$ בהוכחת $\mathrm{P} \subseteq \mathrm{C}_3$. **ההכרעה:** בגוף נכתב $w = 0$ (שכן $c = 1$), והטעות תועדה כהערה — היא כשל טיפוסי של העתקת תבנית.

מקור: הסיכום, עמוד 1, כותרת ירוקה, מול ההקלטה [00:00:00]. **הפער:** הכותרת קצרה ומקוצרת. הקריאה שנבחרה היא "פתרון מטלה 2", והיא מאושרת מההקלטה — המרצה פותח ב"תפתחו את תרגיל הבית… נתתי לכם פה ארבע מחלקות", ובסוף השיעור [01:29:44] מכריז על מעבר ל"תרגיל שלוש", כלומר למטלה הבאה. **ההכרעה:** צוטטה בגוף כ"פתרון מטלה 2".

מקור: שני המקורות. **הפער:** אין בעמודים האלה שום נתון מזהה של סטודנט. **ההכרעה:** לא נדרש טיפול.

מקור: מוסכמות הסימון של הפרויקט. **הפער:** הסיכום כותב את שמות המחלקות ללא `\mathrm` . **ההכרעה:** בקובץ זה שמות מחלקות ובעיות נכתבו ב- `\mathrm` לפי §2a, בעוד שאותיות המשתנים (A, M, $\hat{M}$, c, w, x) נשמרו בדיוק כבמקור.

סיכום ונקודות למבחן

התוצאות שכדאי לזכור.

מחלקה	ההבדל מהגדרת NP	התשובה	מכילה את NP?	מוכלת ב-NP?	שווה?
C_1	"דוחה" במקום "מקבלת"	$\mathrm{C}_1 = \mathrm{NP}$	כן	כן	כן
C_2	"קיים" במקום "לכל" בצד השלילי	C_2 = כל השפות	כן, וממש	לא	לא
C_3	$w \in \{0,1\}^c$ במקום $\{0,1\}^{\|x\|^c}$	$\mathrm{C}_3 = \mathrm{P}$	**פתוח** ($\mathrm{P} = \mathrm{NP}$ vs)	כן	**פתוח**
C_5	$\le c \log \|x\|$ בחירות אי-דטרמיניסטיות	$\mathrm{C}_5 = \mathrm{P}$	**פתוח**	כן	**פתוח**

המנוע שמאחורי כל השורות. בכל שורה יש הבדל תחבירי אחד מהגדרת NP, והשאלה היחידה היא האם ניתן לגשר עליו ובאיזה כיוון:

היפוך קבלה/דחייה — ניתן לגישור בשני הכיוונים, כי המכונה דטרמיניסטית ועוצרת. שוויון.

החלפת $\forall$ ב-$\exists$ — ניתן לגישור בכיוון אחד בלבד (מ-$\forall$ ל-$\exists$, מעל תחום לא ריק). הכלה ממש.
קיצור העד לאורך שאינו תלוי בקלט — הופך את "לנחש" ל"לעבור על הכול" בזמן פולינומי. קריסה ל-P.

מלכודות סטנדרטיות.

לענות על שאלה אחת במקום שלוש. "האם היא שווה ל-NP" אינה מכסה את "האם היא מכילה" ואת "האם היא מוכלת". פרקו את השוויון לשתי הכלות ואמרו על כל אחת בנפרד: נכונה / שגויה / שקולה לשאלה פתוחה.

מעבר מ"לכל" ל"קיים" בלי לומר למה. אם אתם עושים אותו — כתבו "הקבוצה אינה ריקה". עדיף פשוט להציג עד קונקרטי.

"ממשפט ההיררכיה קיימת שפה מחוץ ל-NP" בלי לפרט את שרשרת ההכלות — תשובה חלקית.

בלבול בין $\mathrm{P} \subsetneq \mathrm{EXP}$ לבין הפרדה שימושית. הכלה ממש בין קצוות שרשרת אינה אומרת איזו הכלה פנימית היא ממש.

להעתיק את צורת העד מהסעיף הקודם. אחרי שבוחרים c, בדקו מהי בפועל הקבוצה $\{0,1\}^{\cdots}$.

לשכוח שהמכונה עוצרת. כל הטיעונים "אינה מקבלת $\Longleftarrow$ דוחה" נשענים על כך שהמכונה פולינומית ולכן עוצרת. במכונה אי-דטרמיניסטית זה נשבר.

רשימת בדיקה — מה צריך לדעת לעשות אחרי השיעור הזה.

- [ ] לכתוב את הגדרת ה-verifier של NP מהזיכרון, בדיוק, כולל שני החסמים הנפרדים (אורך העד וזמן האימות).
- [ ] בהינתן הגדרה חדשה שדומה ל-NP, לזהות את ההבדל התחבירי היחיד ולנסח בעצמכם האם ניתן לגשר עליו ובאיזה כיוון.
- [ ] להוכיח $\mathrm{C}_1 = \mathrm{NP}$ בשני הכיוונים, כולל ההצדקה מדוע היפוך המצבים חוקי דווקא במכונה דטרמיניסטית.
- [ ] להציג שפה מחוץ ל-NP בשתי דרכים: HALT דרך $\mathrm{R} \subseteq \mathrm{NP} \subseteq \mathrm{PSPACE}$, ושפה מ-$\mathrm{EXPSPACE} \setminus \mathrm{PSPACE}$ דרך משפט ההיררכיה במקום.
- [ ] לבנות את המכונה שעוברת על כל העדים, ולדעת בדיוק מתי היא נותנת PSPACE (עד פולינומי) ומתי P (עד קבוע או לוגריתמי).
- [ ] לנסח תשובה לשאלה "האם המחלקה שווה ל-NP" בצורה שמפרידה בין החלק הידוע לחלק הפתוח.

שאלות שנשארו פתוחות

סעיף ד' (C_4) של אותה שאלה נדחה במפורש לשיעור הבא ואינו נפתר באף מקום בקורפוס: לא בסיכום הזה, לא בסיכום 25 ולא בהקלטות 29 או 30. הבדיקה בוצעה: הקלטה 29 נפתחת כבר בתוך תרגיל 3 (תחילת המפגש חסרה מן ההקלטה), והמחלקות C_1–C_4 שבהקלטה 30 הן וריאציות הסתברותיות על BPP ([00:29:05]) ואינן קשורות ל-C_4 שכאן. המסקנה: הסעיף נלמד ככל הנראה בפתיחה החסרה של הקלטה 29, ואין לו תיעוד.

ההקלטה [00:59:55] מפנה לאחור ל'שיעור שעבר' ולביטוי n^{2^c} שנדון בו; תוכנו של שיעור 23 לא נבדק כאן, ולכן ההפניה הובאה כציטוט של המרצה ולא כתלות מפורשת.

בבניית המכונה עבור HALT $\in C_2$ הסיכום אינו מטפל בקלט הריק, שעבורו העד הוא המחרוזת הריקה ואין לה 'תו ראשון'. ההשלמה מופיעה בגוף; ראו סעיף הפערים.

ההקלטה מכנה את סעיף ה' 'C_5' ואת המחלקות בשאלה 'ארבע מחלקות'; המספור בין ההקלטה לסיכום אינו עקבי לחלוטין ולא ניתן לאמת אותו מתוך חמשת העמודים בלבד.

25 חזרה לקראת המבחן: תת-גרף מקסימלי חסר מעגלים, כיסוי בהיפרגרף 3-אחיד, חתך מכוון ואי-קירוב של Bin-Packing

פתרון מלא של ארבעה תרגילים מתרגיל בית 3 — שלושה אלגוריתמי קירוב (½ לתת-גרף חסר מעגלים, 3 לכיסוי בהיפרגרף 3-אחיד, ¼ לחתך מקסימלי בגרף מכוון), רדוקציה $\mathrm{VC}\le_p\mathrm{3H\text{-}VC}$, והוכחה שקיום אלגוריתם קירוב ביחס 1.49 ל-$\mathrm{BIN\text{-}PACKING}$ גורר $\mathrm{P}=\mathrm{NP}$.

ביטחון: high

בקצרה

זהו שיעור **חזרה**: ארבעה תרגילים מתרגיל בית 3, כל אחד נפתר על הלוח מקצה לקצה. אין כאן תיאוריה חדשה — יש כאן את התבניות שבהן הקורס בודק את החומר.

שלושת הדברים שכל אלגוריתם קירוב חייב חוזרים בכל תרגיל ומודגשים שוב ושוב: (1) זמן ריצה פולינומי, (2) הפלט הוא **פתרון אפשרי**, (3) יחס הקירוב. הפריט (2) הוא זה שנשכח הכי הרבה.

תרגיל 3 — פירוק קשתות גרף מכוון לפי סדר האינדקסים לשתי קבוצות חסרות מעגלים, ובחירת הגדולה מביניהן: אלגוריתם קירוב ביחס $\frac{1}{2}$ לבעיית תת-הגרף המקסימלי חסר המעגלים.

תרגיל 4 — הכללה של הכיסוי בקודקודים להיפרגרפים 3-אחידים: (א) $\mathrm{VC}\le_p\mathrm{3H\text{-}VC}$, ולכן $\mathrm{3H\text{-}VC}$ היא NP-קשה; (ב) אותו אלגוריתם חמדני של שיעור 13, עם 3 במקום 2 — אלגוריתם קירוב ביחס 3.

תרגיל 5 — חתך מקסימלי בגרף **מכוון**: מוחקים כיוונים, מריצים את אלגוריתם ה-$\frac{1}{2}$ ל-MAXCUT, ואז בוחרים בין U ל-$\bar{U}$. יחס $\frac{1}{4}$. זהו התרגיל שרוב הכיתה טעתה בו — בהגשה הוחזר ניתוח **בתוחלת**, וזה אינו אלגוריתם קירוב.

תרגיל 7 — אם קיים אלגוריתם קירוב ביחס 1.49 ל-$\mathrm{BIN\text{-}PACKING}$ אז $\mathrm{P}=\mathrm{NP}$. אותה תבנית בדיוק כמו אי-הקירוב של TSP משיעור 13: מניחים אלגוריתם קירוב, בונים ממנו אלגוריתם **הכרעה** לבעיה NP-קשה, ומסיקים.

הסף 1.49 אינו שרירותי: כל $\alpha < \frac{3}{2}$ עובד, ובדיוק $\frac{3}{2}$ כבר לא — כי מספר התאים הוא מספר שלם.

רקע ותלויות

הקובץ הזה אינו מוכיח כמעט שום דבר מאפס; הוא מרכיב תוצאות קיימות. להלן מה שצריך להיות בידיים, במלואו.

1. הגדרת אלגוריתם קירוב (שיעור 13, הגדרה 3). לבעיית **מינימיזציה** ועבור $\alpha \ge 1$: אלגוריתם שרץ בזמן פולינומי ב-$|I|$, מחזיר פתרון **אפשרי** $x \in X_I$, ומקיים $\mathrm{OPT}(I) \le v(x) \le \alpha \cdot \mathrm{OPT}(I)$. לבעיית **מקסימיזציה** ועבור $0 < \alpha \le 1$: אלגוריתם פולינומי המחזיר פתרון אפשרי ומקיים $\alpha \cdot \mathrm{OPT}(I) \le v(x) \le \mathrm{OPT}(I)$. בשני המקרים אחד משני אי-השוויונות טריוויאלי (הוא נובע מהפיזביליות של הפלט), וכל העבודה היא בשני.

2. הכיסוי בקודקודים (שיעור 10, הגדרה 1 ומשפט 2). $U \subseteq V$ היא כיסוי בקודקודים של $G = (V, E)$ אם $\forall e \in E:\ e \cap U \neq \emptyset$, והשפה היא $\mathrm{VC} = \{\langle G, k\rangle \mid \exists U \subseteq V \text{ vertex cover}, \ |U| \le k\}$. VC היא NP-שלמה (שיעור 10, משפט 2, דרך $\mathrm{IS} \le_p \mathrm{VC}$).

3. אלגוריתם ה-2-קירוב ל-VC (שיעור 13, משפט 1). כל עוד יש קשת $e = xy$ בגרף — מכניסים את **שני** קצותיה ל-C, מוסיפים את e ל-F, ומוחקים את x, y ואת כל הקשתות הנוגעות בהם. הניתוח: F היא קבוצת קשתות זרות בזוגות, ולכן $|C| = 2|F|$; וכן $|F| \le |C_{\mathrm{opt}}|$; ומכאן $|C| \le 2|C_{\mathrm{opt}}|$. תרגיל 4(ב) כאן הוא בדיוק ההכללה של האלגוריתם הזה.

4. אלגוריתם ה-$\frac{1}{2}$-קירוב ל-MAXCUT (שיעור 13, משפט 3; ובגרסה חמדנית שיעור 14, משפט 1). לשני האלגוריתמים אותה הבטחה: הם רצים בזמן פולינומי, מחזירים $U \subseteq V$, וגודל החתך המושרה מקיים $|F| \ge \frac{1}{2}|E| \ge \frac{1}{2}\mathrm{OPT}$. ההוכחה של שיעור 13 מסתמכת על $\mathrm{cut}(v) + \mathrm{other}(v) = \deg(v)$ ועל $\sum_v \deg(v) = 2|E|$ — שני הדברים נכונים גם ב**מולטיגרף**, ולכן האלגוריתם תקף גם על גרפים עם קשתות מקבילות. זה יהיה קריטי בתרגיל 5.

5. $\mathrm{PARTITION}$ ו-$\mathrm{BIN\text{-}PACKING}$ (שיעור 12). שואלת אם ניתן לפצל $a_1, \dots, a_n$ לשני חלקים שווי-סכום; היא NP-שלמה (משפט 2 שם). $\mathrm{BIN\text{-}PACKING}$ מקבלת $a_1, \dots, a_n \in (0, 1]$ ומספר k, ושואלת אם ניתן לארוז אותם ב-k תאים בעלי קיבולת 1; היא NP-שלמה (משפט 4 שם), ו**נשארת NP-קשה גם כאשר $k = 2$ קבוע** (משפט 5 שם).

6. תבנית אי-הקירוב (שיעור 13, משפט 4). ההוכחה ש"קירוב בכל יחס קבוע ל-TSP הכללית גורר $\mathrm{P} = \mathrm{NP}$" היא בדיוק התבנית של תרגיל 7: מניחים אלגוריתם קירוב, קוראים לו כתת-שגרה, ומתרגמים את **ערך** הפלט לתשובת כן/לא לבעיה NP-קשה. שימו לב שהאובייקט המתקבל אינו רדוקציית מיפוי אלא **אלגוריתם הכרעה**.

7. הטריק של "החלפת קודקוד חדש בשכן" (שיעור 19, משפט 4). ברדוקציה $\mathrm{VC} \le_p \mathrm{DS}$ הוספנו לכל קשת xy קודקוד חדש v_{xy}, ובכיוון ההפוך היינו צריכים להחליף כל קודקוד חדש בקבוצה בקודקוד ישן. תרגיל 4(א) משתמש באותו טריק בדיוק — המרצה קישר בין השניים ב-[00:34:33].

8. כיוון הרדוקציה — בעברית. $A \le_p B$ פירושו: קיימת פונקציה f הניתנת לחישוב בזמן פולינומי כך ש-$x \in A \iff f(x) \in B$. במילים: B **היא הבעיה הקשה לפחות כמו** A — אלגוריתם יעיל ל-B היה נותן אלגוריתם יעיל ל-A. בקובץ הזה נוכיח $\mathrm{VC} \le_p \mathrm{3H\text{-}VC}$, כלומר $\mathrm{3H\text{-}VC}$ היא הקשה מבין השתיים.

הגדרות

הגדרה 1: תת-גרף חסר מעגלים ובעיית האופטימיזציה שלו

יהי $G = (V, E)$ גרף **מכוון**. תת-קבוצת קשתות $E' \subseteq E$ נקראת **חסרת מעגלים** אם הגרף $G' = (V, E')$ אינו מכיל מעגל מכוון.

> **קלט:** גרף מכוון $G = (V, E)$. **פתרונות אפשריים:** כל $E' \subseteq E$ שעבורה (V, E') חסר מעגלים. **ערך:** $|E'|$. **מטרה:** מקסימיזציה.

אינטואיציה. מבקשים "לשבור" את כל המעגלים של הגרף בזריקת מספר מינימלי של קשתות — או, שקול, לשמור מספר מקסימלי של קשתות. הקבוצה הריקה היא תמיד פתרון אפשרי (גרף בלי קשתות בוודאי חסר מעגלים), ולכן שאלת המקסימום היא השאלה המעניינת.

מופע. על $V = \{1, 2, 3\}$ עם $E = \{(1, 2), (2, 3), (3, 1)\}$ — מעגל מכוון יחיד — כל תת-קבוצה של שתי קשתות היא פתרון אפשרי, ו-E עצמה אינה. לכן $\mathrm{OPT} = 2$.

אי-מופע. $E' = E$ בדוגמה שלמעלה **אינו** פתרון אפשרי, אף שהוא הגדול ביותר. זו בדיוק הנקודה שבה נופלים: פתרון גדול שאינו פיזבילי אינו פתרון.

הגדרה 2: היפרגרף 3-אחיד וכיסוי קודקודים בו

היפרגרף 3-אחיד הוא זוג $H = (V, E)$ שבו V קבוצת קודקודים ו-E הוא אוסף של תת-קבוצות של V **בגודל 3 כל אחת**. כל תת-קבוצה כזו נקראת **היפר-קשת**.

כיסוי קודקודים של H הוא קבוצה $S \subseteq V$ המקיימת $\forall e \in E : \quad e \cap S \neq \emptyset$.

השפה: $$\mathrm{3H\text{-}VC} = \left\{ \langle H, k \rangle \;\middle|\; \begin{array}{l} H \text{ a 3-uniform hypergraph},\ k \in \mathbb{N}, \\ \exists\, S \subseteq V \text{ a vertex cover of } H,\ |S| \leq k \end{array} \right\}$$

אינטואיציה. זו הכללה מדויקת של VC: גרף רגיל **הוא** היפרגרף 2-אחיד, כי כל קשת לא מכוונת היא בדיוק קבוצה בגודל 2 של קודקודים ([00:12:40]). ההגדרה של הכיסוי לא השתנתה כלל — אותה שורה $e \cap S \neq \emptyset$ מילה במילה. באופן כללי יותר: יש לנו אוסף תת-קבוצות, ומחפשים קבוצת איברים ה"נוגעת" בכל אחת מהן.

מופע. $V = \{1, 2, 3, 4, 5, 6\}$, $E = \{\{1, 2, 3\}, \{3, 4, 5\}, \{4, 5, 6\}\}$. אז $S = \{3, 4\}$ הוא כיסוי בגודל 2: 3 בשתי ההיפר-קשתות הראשונות, 4 בשתי האחרונות.

אי-מופע. $S' = \{1\}$ אינו כיסוי של אותו H: $S' \cap \{3, 4, 5\} = \emptyset$.

> **הערה על "בגודל k" מול "בגודל לכל היותר k" ([00:40:50]–[00:41:23]).** ניסוח התרגיל אומר "קיים ב-H כיסוי קודקודים בגודל k". שתי הצורות שקולות כאן, כי **על-קבוצה של כיסוי היא כיסוי** — אם יש כיסוי בגודל $j \leq k \leq |V|$ אפשר תמיד להשלים אותו לגודל k בדיוק בהוספת קודקודים שרירותיים. המרצה הדגיש שזה נכון ב-VC, ב-IS וב-CLIQUE (שם מורידים איברים במקום להוסיף), אבל **לא** ב-MAXCUT: שם אני בוחר קודקודים כדי לקבל קשתות, ובמספר הקשתות אין לי שליטה מדויקת. הקובץ הזה כותב את השפה עם $\leq k$; כל ההוכחות עוברות מילה במילה גם עם "בדיוק k".

הגדרה 3: החתך המושרה בגרף מכוון

יהי $G = (V, E)$ גרף פשוט **מכוון** ותהי $U \subseteq V$, ונסמן $\bar{U} = V \setminus U$. **החתך המושרה על ידי** U הוא $\delta(U) \;=\; \{\, (u, v) \in E \;\mid\; u \in U,\ v \in \bar{U} \,\}$, כלומר קבוצת הקשתות ש**זנבן** ב-U ו**ראשן** ב-$\bar{U}$.

> **קלט:** גרף פשוט מכוון $G = (V, E)$. **פתרונות אפשריים:** כל $U \subseteq V$. **ערך:** $|\delta(U)|$.
> **מטרה:** מקסימיזציה.

אינטואיציה — ההבדל מהמקרה הלא מכוון. בגרף לא מכוון U ו-$\bar{U}$ מגדירות **אותו** חתך. כאן זה נשבר לחלוטין: $\delta(U)$ סופרת רק את הקשתות שיוצאות מ-U, ו-$\delta(\bar{U})$ רק את אלה שנכנסות אליה. הא-סימטריה הזו היא כל מה שמייחד את התרגיל, והיא גם המקור לפקטור $\frac{1}{2}$ הנוסף שיעלה לנו במעבר מ-$\frac{1}{2}$ ל-$\frac{1}{4}$.

מופע. $V = \{a, b\}$, $E = \{(a, b)\}$. אז $\delta(\{a\}) = \{(a, b)\}$ בגודל 1, ואילו $\delta(\{b\}) = \emptyset$ בגודל 0. שתי הקבוצות המשלימות זו את זו, ושני החתכים שונים לגמרי — הנה ההבדל בשורה אחת.

אי-מופע. $U = \emptyset$ נותנת $\delta(\emptyset) = \emptyset$ — פתרון אפשרי לגמרי, פשוט גרוע. כמו ב-MAXCUT, **כל** תת-קבוצת קודקודים היא פיזבילית, ולכן כל העבודה בתרגיל 5 היא ביחס הקירוב.

הגדרה 4: גרסת האופטימיזציה של $\mathrm{BIN\text{-}PACKING}$

> **קלט:** $b_1, \ldots, b_n \in (0, 1]$. **פתרונות אפשריים:** כל פונקציה $f : \{1, \ldots, n\} \to \{1, \ldots, m\}$ (הקצאת פריטים לתאים) המקיימת $\sum_{i:\, f(i) = \ell} b_i \le 1$ לכל ℓ. **ערך:** מספר התאים בשימוש. **מטרה:** מינימיזציה.

אינטואיציה. לכל תא קיבולת 1; רוצים להשתמש במספר קטן ככל האפשר. שימו לב שהערך הוא **מספר שלם** — עובדה שנראית טריוויאלית וששוברת את כל התרגיל השביעי לטובתנו.

מופע. $\left(\frac{1}{3}, \frac{1}{3}, \frac{1}{3}, \frac{1}{2}, \frac{1}{2}\right)$ נארז בשני תאים: שלושת השלישים בתא אחד, שני החצאים בשני.

אי-מופע. $\left(\frac{3}{4}, \frac{3}{4}, \frac{3}{4}\right)$ אינו נארז בשני תאים — לפי שובך היונים תא אחד יקבל שניים מהם, וסכומם $\frac{3}{2} > 1$.

משפטים והוכחות

בשיעור חזרה, החלק הזה קצר בכוונה: הוא מחזיק רק את התוצאות שהתרגילים **נשענים** עליהן, ומצביע אחורה על השיעור שבו הן הוכחו. הפתרונות המלאים הם בסעיף הבא, שהוא לב הקובץ.

משפט 1: VC היא NP-שלמה

טענה. VC היא NP-שלמה.

מקור. שיעור 10, משפט 2: $\mathrm{IS} \le_p \mathrm{VC}$ דרך ההבחנה ש-U היא כיסוי בקודקודים אם ורק אם $V \setminus U$ בלתי תלויה, ובצירוף $\mathrm{VC} \in \mathrm{NP}$. אנחנו נשתמש רק ב-NP-קושי, בתרגיל 4(א). ■

משפט 2: $\mathrm{PARTITION}$ היא NP-שלמה, וכך גם $\mathrm{BIN\text{-}PACKING}$ עם $k = 2$ קבוע

טענה. $\mathrm{PARTITION}$ NP-שלמה, ובעיית האריזה בשני תאים בעלי קיבולת 1 (בלי ש-k הוא חלק מהקלט) היא NP-קשה.

מקור. שיעור 12, משפט 2 ($\mathrm{SUBSET\text{-}SUM} \le_p \mathrm{PARTITION}$) ומשפט 5. הרדוקציה של משפט 4 שם שולחת את **כל** הקלטים לתת-המרחב שבו $k = 2$, ולכן אותה רדוקציה עצמה מוכיחה את NP-הקושי של הגרסה עם k קבוע. אנחנו נשתמש בשתיהן בתרגיל 7 — ב-$\mathrm{PARTITION}$ בפתרון הכתוב, ובגרסה עם $k = 2$ בקיצור-הדרך שהמרצה הציע. ■

משפט 3: קיים אלגוריתם קירוב פולינומי ביחס $\frac{1}{2}$ ל-MAXCUT, גם במולטיגרפים

טענה. קיים אלגוריתם פולינומי המקבל גרף לא מכוון $\hat{G} = (V, \hat{E})$ — אפשר עם קשתות מקבילות — ומחזיר $U \subseteq V$ שהחתך המושרה על ידה מקיים $|(U, \bar{U})| \ge \frac{1}{2}|\hat{E}|$.

מקור והוכחה. שיעור 13, משפט 3 (חיפוש מקומי), או שיעור 14, משפט 1 (חמדני חד-מעברי). שניהם משיגים את אותה הבטחה. המרצה ציין את שניהם במפורש ב-[01:39:58] ואמר ש"האלגוריתם שראינו בשיעור" בפתרון מתייחס לכל אחד מהם.

> **הערה: למה זה עובד גם עם קשתות מקבילות ([01:27:23]).** ההוכחה של שיעור 13 בנויה משלוש טענות: $\mathrm{cut}(v) + \mathrm{other}(v) = \deg(v)$, אופטימליות מקומית $\mathrm{cut}(v) \geq \mathrm{other}(v)$, וספירה כפולה $\sum_v \mathrm{cut}(v) = 2|F|$. אף אחת מהשלוש אינה מניחה שהגרף פשוט — כולן ספירות של **מופעי** קשתות. לכן ההבטחה $|(U, \bar{U})| \geq \frac{1}{2}|\hat{E}|$ תקפה כשסופרים כל קשת מקבילה בנפרד. תרגיל 5 חייב את התכונה הזו. ■

משפט 4: $\mathrm{VC} \leq_p 3\mathrm{H}\text{-}\mathrm{VC}$, ולכן $3\mathrm{H}\text{-}\mathrm{VC}$ היא NP-קשה

זהו תרגיל 4(א). הניסוח והוכחתו המלאה נמצאים ב**דוגמאות ותרגילים**, סעיף "תרגיל 4(א)", כי שם מקומו: זו שאלת תרגיל בית שנפתרה על הלוח.

משפט 5: ההשלמה — $3\mathrm{H}\text{-}\mathrm{VC} \in \mathrm{NP}$

טענה. $3\mathrm{H}\text{-}\mathrm{VC} \in \mathrm{NP}$, ולכן יחד עם משפט 4 היא NP-**שלמה**.

הוכחה. התרגיל ביקש רק NP-קושי, וההשלמה קלה. ה-certificate הוא הקבוצה $S \subseteq V$ עצמה; אורכה לכל היותר $|V|$ שמות קודקודים ולכן פולינומי בגודל הקלט. המאמת בודק שני דברים: ש-$|S| \leq k$, ושלכל $e \in E$ מתקיים $e \cap S \neq \emptyset$. הבדיקה השנייה היא מעבר יחיד על E, ולכל היפר-קשת בדיקה של שלושה קודקודים מול S — סך הכול $O(|E| \cdot |S|)$, פולינומי. לפי ההגדרה של NP דרך מאמת (שיעור 6), $3\mathrm{H}\text{-}\mathrm{VC} \in \mathrm{NP}$. ■

> **הערה:** ההשלמה הזו לא נאמרה בהרצאה — התרגיל ביקש NP-קושי בלבד. היא נוספה כאן כי במבחן ניסוח מסוג "הוכיחו כי הבעיה NP-שלמה" הוא נפוץ לפחות כמו "NP-קשה", וההבדל הוא בדיוק השורה הזו.

דוגמאות ותרגילים מהשיעור

זהו לב הקובץ. ארבעת התרגילים לפי מספורם במקור.

תרגיל 3: תת-גרף מקסימלי חסר מעגלים

הניסוח (כפי שנמסר)

(א) יהי $G = (V, E)$ גרף מכוון עבורו $V = \{1, 2, \ldots, n\}$. נסמן ב-E_1 את קבוצת הקשתות ב-G אשר מכוונות ממספר טבעי למספר טבעי **גדול** ממנו, כלומר $E_1 = \{(i, j) \in E \mid i < j\}$, ונסמן ב-$G_1 = (V, E_1)$ את תת-הגרף המתאים של G. נסמן ב-E_2 את קבוצת הקשתות ב-G אשר מכוונות ממספר טבעי למספר טבעי **קטן** ממנו, כלומר $E_2 = \{(i, j) \in E \mid i > j\}$, ונסמן ב-$G_2 = (V, E_2)$ את תת-הגרף המתאים של G. הראו שהגרפים G_1, G_2 חסרי מעגלים (מכוונים).

(ב) נגדיר את בעיית האופטימיזציה הבאה:

> **קלט:** גרף מכוון $G = (V, E)$. **מטרה:** למצוא קבוצת קשתות $E' \subseteq E$ גדולה ככל האפשר, כך שהגרף $G' = (V, E')$ חסר מעגלים.

הציעו אלגוריתם עם זמן ריצה פולינומי אשר משיג יחס קירוב $\frac{1}{2}$ לבעיה. היעזרו בסעיף הקודם.
פתרון (א)

> **הערה מתודית ([00:01:34]).** סעיף (א) הוא טענה **קומבינטורית**, לא אלגוריתמית. אנחנו לא מציעים אלגוריתם למצוא את E_1 — אנחנו **מגדירים** אותה ומוכיחים עליה תכונה. ההבחנה הזו חשובה, ובסעיף (ב) נעבור בדיוק לצד השני.

נוכיח ש-G_1 חסר מעגלים; ההוכחה ל-G_2 סימטרית.
נניח בשלילה שקיים ב-G_1 מעגל מכוון $v_1 \to v_2 \to \cdots \to v_k \to v_1, \quad k \geq 2$ כלומר $(v_1,v_2),(v_2,v_3),\ldots,(v_{k-1},v_k),(v_k,v_1) \in E_1$.
לפי הגדרת E_1, כל קשת $(i,j) \in E_1$ מקיימת $i < j$. נפעיל זאת על כל קשתות המעגל בזו אחר זו: $v_1 < v_2 < v_3 < \cdots < v_k$. משרשור שני הדברים: $v_1 < v_2 < \cdots < v_k < v_1$, ומיחס הסדר החזק על הטבעיים נובע $v_1 < v_1$ — סתירה. לכן ב-G_1 אין מעגל מכוון. באופן סימטרי, כל קשת ב-E_2 מקיימת $i > j$, מעגל היה נותן $v_1 > v_2 > \cdots > v_k > v_1$ ולכן $v_1 > v_1$, סתירה; ולכן גם G_2 חסר מעגלים. ■

> **על המקרה $k=1$ (לולאה עצמית) ([00:03:21]).** המרצה הזכיר את הקונבנציה: אם לא נאמר אחרת, הגרף **פשוט**; "מכוון" אינו מבטל את "פשוט". לכן אין לולאות (i,i). אבל למעשה אין בכך צורך: לולאה (i,i) אינה מקיימת $i < i$ ואינה מקיימת $i > i$, ולכן אינה שייכת לא ל-E_1 ולא ל-E_2. הטענה נכונה גם אם מרשים לולאות ב-G.

הבחנה שנשתמש בה בסעיף (ב). בגרף פשוט מכוון כל קשת (i,j) מקיימת $i \neq j$, ולכן בדיוק אחד משני התנאים $i < j$,$i > j$ מתקיים. מכאן $E = E_1 \dot\cup E_2$,
ולכן
$|E_1| + |E_2| = |E|$.
פתרון (ב) — האלגוריתם

> **קלט:** גרף מכוון $G=(V,E)$ כאשר $V=\{1,2,\ldots,n\}$.
> $E_1 \leftarrow \emptyset$, $E_2 \leftarrow \emptyset$.
> לכל קשת $e=(i,j) \in E$:
> אם $i<j$ — הכנס את e ל-E_1;
> אחרת — הכנס את e ל-E_2.
> אם $|E_1| \geq |E_2|$ — החזר את E_1; אחרת — החזר את E_2.

שלושה דברים צריך להוכיח, תמיד ([00:04:56]–[00:06:00]): זמן ריצה פולינומי, פיזביליות הפלט, ויחס הקירוב.
(1) ניתוח זמן ריצה
שלב 1 לוקח זמן קבוע. מספר האיטרציות של הלולאה בשלב 2 הוא בדיוק $|E|$, ובכל איטרציה מבצעים השוואה יחידה בין שני מספרים והוספה לקבוצה — זמן קבוע. שלב 3 הוא השוואה יחידה בין שני גדלים שנצברו תוך כדי. סך הכול $O(|E|) = O(|G|)$, פולינומי בגודל הקלט. ■

(2) פיזביליות

נסמן ב-E' את הקבוצה שהאלגוריתם מחזיר. לפי שלב 3, $E' \in \{E_1, E_2\}$, ולפי בניית שלב 2 אלה בדיוק הקבוצות מסעיף (א). לפי סעיף (א) שני הגרפים (V, E_1) ו-(V, E_2) חסרי מעגלים, ולכן בכל מקרה (V, E') חסר מעגלים — כלומר E' הוא פתרון אפשרי לבעיה. ■

> **זה השלב שנשכח ([00:04:24]).** התשובה הראשונה בכיתה לשאלה "מה הקבוצה שאני מחזיר צריכה לקיים?" הייתה "לפחות חצי". המרצה עצר: **קודם כול** היא צריכה להיות פתרון אפשרי, ואת זה צריך גם להוכיח.

(3) יחס הקירוב

יהי $G = (V, E)$ ונסמן ב-$\hat{E}$ פתרון **אופטימלי** לבעיה על G, כלומר קבוצת קשתות חסרת מעגלים בגודל מקסימלי.

לפי ההבחנה בסוף סעיף (א), $|E| = |E_1| + |E_2|$. שני מספרים אי-שליליים שסכומם $|E|$ — לפחות אחד מהם גדול או שווה למחצית הסכום: $|E_1| \geq \frac{1}{2}|E|$.

או

$|E'| = |E_2| \geq \frac{1}{2}|E|$. האלגוריתם מחזיר את הגדולה מבין השתיים, ולכן בכל מקרה $\max\{|E_1|, |E_2|\} \geq \frac{1}{2}|E|$.

מצד שני, $\hat{E} \subseteq E$ ולכן $|\hat{E}| \leq |E|$ — זהו החסם העליון על האופטימום, ובעיית מקסימיזציה זה בדיוק מה שדרוש. משרשור: $|E'| \geq \frac{1}{2}|E| \geq \frac{1}{2}|\hat{E}|$. ומן הצד השני $|E'| \leq |\hat{E}|$, כי E' הוא פתרון אפשרי ו-$\hat{E}$ אופטימלי. יחד: $\frac{1}{2}|\hat{E}| \leq |E'| \leq |\hat{E}|$, ולפי הגדרה 3(ב) של שיעור 13 זהו אלגוריתם קירוב ביחס $\frac{1}{2}$ לבעיית תת-הגרף המקסימלי חסר המעגלים. ■

> **הכלי החוזר ([00:09:44]).** "יש לי שני מספרים, לפחות אחד מהם גדול-שווה לחצי מהסכום — תמיד." המרצה הוסיף מיד אזהרה: הטענה המקבילה ל**מכפלה** אינה נכונה — אי אפשר להסיק שאחד משני מספרים גדול מהשורש של המכפלה בלי הנחת אי-שליליות. הטענה הנכונה, זו שאנחנו כן משתמשים בה, נשענת על כך ששני הגדלים אי-שליליים.

תרגיל 4(א): $\mathrm{3H\text{-}VC}$ היא NP-קשה

הניסוח (כפי שנמסר)

היפרגרף 3-אחיד הוא זוג $H = (V, E)$ כאשר V קבוצת קודקודים ו-E אוסף של תת-קבוצות של V בגודל 3 כל אחת. כל תת-קבוצה כזו נקראת היפר-קשת (בעצם ניתן לחשוב על גרף רגיל כעל היפרגרף 2-אחיד, כיוון שכל קשת היא קבוצת קודקודים בגודל 2). כיסוי קודקודים של היפרגרף H הוא קבוצה $S \subseteq V$ המקיימת שבכל היפר-קשת ב-E יש קודקוד ששייך ל-S, כלומר לכל $e \in E$ מתקיים $e \cap S \neq \emptyset$.

(א) תהא $\mathrm{3H\text{-}VC}$ שפת כל הזוגות $\langle H, k \rangle$ של היפרגרף 3-אחיד H ומספר טבעי k עבורם קיים ב-H כיסוי קודקודים בגודל k. הוכיחו כי הבעיה $\mathrm{3H\text{-}VC}$ היא NP-קשה.

הרעיון, ולמה דווקא מ-VC
נראה $\mathrm{VC} \leq_p \mathrm{3H\text{-}VC}$ — כלומר, $\mathrm{3H\text{-}VC}$ היא הבעיה הקשה מבין השתיים. הבחירה ב-VC כבעיית המקור אינה מקרית: היא ה"בעיה הקרובה" ([00:14:49]) — ההגדרה של כיסוי קודקודים בהיפרגרף היא **מילה במילה** ההגדרה מ-VC. המרצה הציג את זה כשיטת עבודה: הניחוש הראשון הוא תמיד הבעיה הדומה ביותר; אם היא לא עובדת, אז מתחילים לחשוב על אחרות.
הקושי הטכני היחיד: הפלט חייב להיות היפרגרף **3-אחיד**, וקשתות של גרף רגיל הן בגודל 2. צריך "לנפח" כל קשת לגודל 3 מבלי לשנות את התשובה — ולכן מוסיפים לכל קשת קודקוד חדש משלה.
הרדוקציה (האלגוריתם R)

קלט: גרף לא מכוון $G = (V, E)$ ומספר $k \in \mathbb{N}$.
$\hat{V} \leftarrow V$, $\hat{E} \leftarrow \emptyset$.
לכל $e \in E$:
2.1 צור קודקוד חדש v_e (חדש, כלומר $v_e \notin V$ ושונה מכל קודקוד שנוצר קודם);
2.2 הוסף את v_e ל-$\hat{V}$;
2.3 הוסף את $e \cup \{v_e\}$ ל-$\hat{E}$.
החזר את $H = (\hat{V}, \hat{E})$ ואת **אותו** k.

הפלט הוא אינסטנס חוקי. לכל $e = \{x, y\} \in E$ מתקיים $x \neq y$ (הגרף פשוט) ו-$v_e \notin V$, ולכן $|e \cup \{v_e\}| = 3$ בדיוק. כל איברי $\hat{E}$ הם תת-קבוצות של $\hat{V}$ בגודל 3, כלומר H הוא היפרגרף 3-אחיד. הפלט הוא זוג $\langle$היפרגרף 3-אחיד, מספר טבעי$\rangle$ — בדיוק סוג הקלט של $\mathrm{3H\text{-}VC}$. ([00:15:53]: "שימו לב שאנחנו צריכים להחזיר היפרגרף — 3-אחיד".)
ניתוח זמן ריצה
יהי $G = (V, E)$ ויהי $k \in \mathbb{N}$. שלב 1 לוקח זמן קבוע — הוא רק מסמן שמות ואינו מעתיק שום דבר. מספר האיטרציות בלולאה הוא בדיוק $|E|$, ובכל איטרציה מייצרים שם חדש, מוסיפים אותו לקבוצת קודקודים ומוסיפים קבוצה בת שלושה איברים לקבוצת ההיפר-קשתות — זמן קבוע (או $O(\log)$ בייצוג סביר של שמות). שלב 3 הוא כתיבת הפלט. סך הכול $O(|G|)$, פולינומי בגודל הקלט.
גם **גודל** הפלט פולינומי: $|\hat{V}| = |V| + |E|$ ו-$|\hat{E}| = |E|$. זה נחוץ — אחרת לא היה אפשר לכתוב את הפלט בזמן פולינומי מלכתחילה.
ניתוח נכונות, כיוון ראשון: $\langle G, k\rangle \in \mathrm{VC} \Rightarrow \langle H, k\rangle \in \mathrm{3H\text{-}VC}$
נניח $\langle G, k\rangle \in \mathrm{VC}$. אז קיימת $U \subseteq V$ כיסוי בקודקודים של G עם $|U| \leq k$.
נתבונן באותה U בדיוק. שני דברים אנחנו מקבלים מיד, ואסור לדלג עליהם ([00:26:27]):
$U \subseteq V \subseteq \hat{V}$, ולכן U היא בכלל קבוצת קודקודים חוקית של H — רק בזכות זה יש בכלל **משמעות** לשאלה אם היא כיסוי של H;
$|U| \leq k$ לא השתנה.
תהא $\hat{e} \in \hat{E}$ היפר-קשת. לפי בניית שלב 2, **קיימת** קשת $e \in E$ כך ש-$\hat{e} = e \cup \{v_e\}$ — זהו הקישור שלנו חזרה לגרף המקורי, ובלעדיו אין הוכחה ([00:28:39]: "אי אפשר להגיד 'נסמן' על משהו שאני לא יודע שהוא קיים"). מכיוון ש-U כיסוי בקודקודים של G ו-$e \in E$, מתקיים $e \cap U \neq \emptyset$.
ומכיוון ש-$\hat{e} \supseteq e$, נובע $\hat{e} \cap U \supseteq e \cap U \neq \emptyset$.

מכיוון ש-$\hat{e}$ הייתה שרירותית, U היא כיסוי קודקודים של H בגודל $\leq k$, ולכן $\langle H, k\rangle \in \text{3H-VC}$. ■
ניתוח נכונות, כיוון שני: $\langle H, k\rangle \in \text{3H-VC} \Rightarrow \langle G, k\rangle \in \text{VC}$
נניח $\langle H, k\rangle \in \text{3H-VC}$. אז קיימת $\hat{U} \subseteq \hat{V}$ כיסוי קודקודים של H עם $|\hat{U}| \leq k$.

כאן נופלת ההוכחה הנאיבית ([00:31:54]–[00:34:33]). אי אפשר לקחת את $\hat{U}$ כמות שהיא. $\hat{U}$ מוכלת ב-$\hat{V}$, ו-$\hat{V}$ מכילה קודקודים שאינם ב-V; ייתכן ש-$\hat{U}$ מכילה כאלה, ואז היא **אינה תת-קבוצה של** V — ולשאלה "האם $\hat{U}$ כיסוי בקודקודים של G" אין אפילו משמעות. שימו לב לא-סימטריה מול הכיוון הראשון: שם קיבלנו קבוצה ב-V, וקבוצה ב-V היא אוטומטית קבוצה ב-$\hat{V}$; כאן הכיוון הפוך והוא נשבר.

נבנה קבוצה $U \subseteq V$ באופן הבא:

לכל $v \in \hat{U}$:
אם $v \in V$ — הכנס את v ל-U;
אחרת, מהבנייה קיימת קשת $xy \in E$ כך ש-$v = v_{xy}$ — הכנס את x ל-U.

הערה על "x" ([00:47:21]–[00:49:30]). הקשת xy היא קבוצה, ולכאורה אין בה "ראשון". אבל הקלט מגיע בסופו של דבר כמחרוזת, ובמחרוזת יש סדר; מה שלא מובטח לנו הוא **איזה** סדר. לכן "הקצה הראשון שמופיע בייצוג" הוא ביטוי חוקי לגמרי. בכל מקרה — הבחירה שרירותית והוכחה עוברת גם עם y.

הערה: אין צורך לנתח את זמן הריצה של הבנייה הזו ([00:36:39]). היא אינה חלק מהרדוקציה; היא חלק מה**הוכחה**. התיאור הוא אלגוריתמי רק כדי לבטא את הקבוצה בנוחות.

מיד מתקבלים שני דברים. ראשית, $U \subseteq V$ מהבנייה — כל איבר שהוכנס הוא או $v \in V$ או קצה של קשת ב-E. שנית, $|U| \leq |\hat{U}| \leq k$.

למה רק $\leq$ ולא $=$ ([00:39:16]–[00:40:20]). ההעתקה $\hat{U} \to U$ אינה בהכרח חד-חד-ערכית. אם למשל xy ו-xw הן שתי קשתות ב-E ושני הקודקודים v_{xy}, v_{xw} שייכים ל-$\hat{U}$, שניהם מתורגמים ל-x ונספרים פעם אחת. וכן ייתכן ש-x עצמו כבר היה ב-$\hat{U}$ וגם v_{xy} היה בה. אנחנו קיבלנו את $\hat{U}$ "מהשמיים" ואיננו רשאים להניח עליה מינימליות. אבל $k \leq$ מספיק לנו לגמרי, כי בכיסוי בקודקודים תמיד אפשר להשלים כלפי מעלה.

נראה ש-U כיסוי בקודקודים של G. תהא $e \in E$. אז קיימים $x, y \in V$ עם $e = \{x, y\}$, ומהבנייה $\{x, y, v_{xy}\} \in \hat{E}$. מכיוון ש-$\hat{U}$ כיסוי קודקודים של H, מתקיים $\{x, y, v_{xy}\} \cap \hat{U} \neq \emptyset$. נחלק לשני מקרים משלימים:
מקרה 1: $x \in \hat{U}$ או $y \in \hat{U}$. אז לפחות אחד מהם ב-V ושייך ל-$\hat{U}$, ולכן לפי הכלל הראשון של הבנייה הוא הוכנס ל-U. כלומר $x \in U$ או $y \in U$, ולכן $e \cap U \neq \emptyset$.
מקרה 2: $x \notin \hat{U}$ וגם $y \notin \hat{U}$. מכיוון שהחיתוך אינו ריק, בהכרח $v_{xy} \in \hat{U}$. $v_{xy} \notin V$, ולכן לפי הכלל השני של הבנייה הוכנס x ל-U. לכן $x \in U$ ומכאן שוב $e \cap U \neq \emptyset$.

בשני המקרים $e \cap U \neq \emptyset$. מכיוון ש-e הייתה שרירותית, U היא כיסוי בקודקודים של G בגודל $\leq k$, ולכן $\langle G, k \rangle \in \mathrm{VC}$. ■

מסקנה

R היא רדוקציה בזמן פולינומי מ-VC ל-3H-VC, כלומר $\mathrm{VC} \leq_p 3\text{H-VC}$. מכיוון ש-$\mathrm{VC}$ היא NP-קשה (משפט 1, שיעור 10), גם 3H-VC היא NP-קשה. ■

הערת כתיבה שהמרצה עצר עליה ([00:45:09]–[00:46:14]). המקרה השני נכתב **בדיוק כשלילה** של הראשון: "$x \notin \hat{U}$ וגם $y \notin \hat{U}$", ולא "נניח $v_{xy} \in \hat{U}$". שני הניסוחים נכונים כאן ואף אחד מהם אינו שגיאה — אבל כהרגל עבודה עדיף תמיד לחלק ל**שני** מקרים משלימים ("עצים בינריים של מקרים"), כי אחרת קל לפספס מקרה שלישי שלא חשבתם עליו. זה עניין של הימנעות מטעויות, לא של סגנון.

תרגיל 4(ב): אלגוריתם קירוב ביחס 3 לכיסוי המינימלי בהיפרגרף 3-אחיד

הניסוח (כפי שנמסר)

(ב) נסתכל על בעיית המינימיזציה שבה הקלט הוא היפרגרף 3-אחיד H והמטרה היא למצוא כיסוי קודקודים ב-H קטן ככל האפשר. הוכיחו כי קיים אלגוריתם עם זמן ריצה פולינומי לבעיה אשר משיג יחס קירוב 3.

הרעיון

זהו בדיוק אלגוריתם ה-2-קירוב ל-VC משיעור 13 (משפט 1), עם 3 במקום 2. הרעיון שלו לא השתנה כהוא זה: אוספים היפר-קשתות **זרות בזוגות**, משלמים על כל אחת את כל שלושת קודקודיה, ומשתמשים בקבוצת ההיפר-קשתות שנאספו כחסם תחתון על האופטימום. המרצה אמר את זה במפורש ([00:52:49]): "ראינו אלגוריתם קירוב ביחס 2 ל-VC, אז כבר עשינו את רוב העבודה."

האלגוריתם

קלט: היפרגרף 3-אחיד $H = (V, E)$.
אתחל $C \leftarrow \emptyset$, $F \leftarrow \emptyset$.
כל עוד יש ב-H היפר-קשת $e = \{x, y, z\} \in E$:
2.1 הוסף ל-C את x, y, z; הוסף ל-F את e;
2.2 מחק מ-H את x, y, z ואת כל ההיפר-קשתות המחוברות אליהן.
החזר את C.

הערה: F היא "משתנה רפאים" ([00:53:50], [00:56:27]). האלגוריתם אינו זקוק ל-F כדי לרוץ, והיא אינה משפיעה על הפלט. היא קיימת אך ורק לצורך הניתוח. המרצה ציין שברוב הספרים אין מסמנים אותה בתוך תיאור האלגוריתם אלא רק בהוכחה — שתי הדרכים תקינות.

הערה: למה מוחקים את הקודקודים ולא רק את ההיפר-קשתות ([00:57:33]). אפשר היה לכתוב "מחק את כל ההיפר-קשתות המחוברות ל-x, y, z" ולהשאיר קודקודים מבודדים; זה שקול לחלוטין. מחיקת הקודקודים נבחרה כי היא הופכת את **הזרות בזוגות** של F לגלויה לעין, וזרות זו היא לב הניתוח.

(1) ניתוח זמן ריצה

יהי $H = (V, E)$ ונריץ עליו את האלגוריתם. שלב 1 לוקח זמן קבוע.

מספר האיטרציות. בכל איטרציה נמחקת לפחות היפר-קשת אחת מהגרף — לכל הפחות e עצמה, שהרי כל שלושת קודקודיה נמחקים. מספר ההיפר-קשתות לעולם אינו גדל, ולכן מספר האיטרציות הוא $O(|E|)$.

עלות איטרציה בודדת. מציאת היפר-קשת ומחיקת שלושה קודקודים וכל ההיפר-קשתות הנוגעות בהם דורשות מעבר על כל הקודקודים ועל כל ההיפר-קשתות — $O(|V| \cdot |E|)$ בחסם גס.

סך הכול $O(|H|^2)$, פולינומי בגודל הקלט. ■

הערה ([01:00:46]–[01:01:20]). אפשר לנתח הדוק בהרבה: כל היפר-קשת "נוגעים" בה לכל היותר פעם אחת לאורך כל הריצה, ולכן אפשר לסכום את העלויות לאורך האיטרציות במקום להכפיל. המרצה העדיף במכוון את החסם הגס: "כל מה שמעניין אותי זה שזה פולינומי." סטודנט גם הצביע על כך שהניתוח $O(|V| \cdot |E|)$ לאיטרציה הוא רופף כי אפשר לעבור רק על שכני x, y, z — המרצה אישר שגם זה נכון וגם זה מספיק.

(2) פיזביליות

יהי $H = (V, E)$, ונסמן ב-C את הפלט. ראשית, $C \subseteq V$ — כל מה שהוכנס ל-C הוא קודקוד של היפר-קשת קיימת.

תהא $e \in E$ היפר-קשת של הקלט המקורי. האלגוריתם עוצר רק כאשר אין יותר היפר-קשתות ב-H, ולכן **במהלך הריצה** e **נמחקה**. זו נקודת המוצא של כל הטיעון.

מתי נמחקת היפר-קשת? רק בשלב 2.2, וזה קורה בדיוק כאשר **אחד מקודקודיה** נמחק מהגרף. וקודקוד נמחק אך ורק בשלב 2.2, ובאותו רגע (שלב 2.1 של אותה איטרציה) הוא הוכנס ל-C. לכן קיים $u \in e$ עם $u \in C$, כלומר $e \cap C \neq \emptyset$.

מכיוון ש-e הייתה שרירותית, C היא כיסוי קודקודים של H, ובפרט פתרון אפשרי לבעיה. ■

הערה: אין צורך בחלוקה למקרים ([01:06:11]–[01:07:13]). בכיתה הוצע לחלק ל"או ש-e היא זו שנבחרה, או שנמחקה בגלל שכנה". המרצה הראה שזה מיותר: **בשני המקרים** הסיבה למחיקה זהה — אחד מקודקודי e נכנס ל-C. חלוקה למקרים שאינה נדרשת אינה שגיאה, אבל הטיעון האחיד קצר ובטוח יותר.

(3) יחס הקירוב

נסמן ב-C_{opt} כיסוי קודקודים מינימלי של H, וב-F את קבוצת ההיפר-קשתות שהאלגוריתם צבר.

שלב א: F זרה בזוגות. יהיו $e, \hat{e} \in F$ שונות, ונניח בלי הגבלת הכלליות ש-e נבחרה קודם. באיטרציה שבה נבחרה e נמחקו כל שלושת קודקודיה מהגרף יחד עם כל ההיפר-קשתות הנוגעות בהם. לכן $\hat{e}$, שנבחרה מאוחר יותר ולכן הייתה עדיין בגרף, אינה מכילה אף אחד מקודקודי e; כלומר $e \cap \hat{e} = \emptyset$.

שלב ב: התאמה חד-חד-ערכית מ-F ל-C_{opt}. תהא $e \in F$. מכיוון ש-$F \subseteq E$ ומכיוון ש-C_{opt} הוא כיסוי קודקודים של H, מתקיים $e \cap C_{\text{opt}} \neq \emptyset$, כלומר קיים $x \in e$ עם $x \in C_{\text{opt}}$. נגדיר $\varphi : F \to C_{\text{opt}}$, $\varphi(e) = \text{some } x \in e \cap C_{\text{opt}}$ (אם יש כמה — בוחרים אחד שרירותית). φ מוגדרת היטב בדיוק בזכות היות C_{opt} כיסוי.

φ חד-חד-ערכית: אם $e \neq \hat{e}$ ב-F, אז לפי שלב א הן זרות; $\varphi(e) \in e$ ו-$\varphi(\hat{e}) \in \hat{e}$, ולכן בהכרח $\varphi(e) \neq \varphi(\hat{e})$.

קיום פונקציה חד-חד-ערכית מ-F ל-C_{opt} נותן $|F| \leq |C_{\text{opt}}|$.

שלב ג: הקשר בין $|C|$ ל-$|F|$. בכל איטרציה מוסיפים ל-F היפר-קשת אחת, ול-C בדיוק **שלושה** קודקודים — והם חדשים, כי מיד לאחר מכן הם נמחקים מהגרף ולא יופיעו שוב באף היפר-קשת שתיבחר. לכן $|C| = 3|F|$.

החיבור. מצד אחד C הוא כיסוי (טענה 2) ו-C_{opt} מינימלי, ולכן $|C_{\text{opt}}| \leq |C|$. מצד שני $|C| = 3|F| \leq 3|C_{\text{opt}}|$. יחד: $|C_{\text{opt}}| \leq |C| \leq 3|C_{\text{opt}}|$, ולפי הגדרה 3(א) של שיעור 13 זהו אלגוריתם קירוב ביחס 3 לבעיית הכיסוי המינימלי בהיפרגרף 3-אחיד. ■

> **מאיפה בא ה-3.** בדיוק מ-$|C| = 3|F|$, כלומר מכך שהיפר-קשת מכילה שלושה קודקודים ואנחנו משלמים על כולם. באותה הוכחה בדיוק, על היפרגרף r-אחיד, מתקבל יחס קירוב r; המקרה $r = 2$ הוא ה-2-קירוב ל-VC משיעור 13.

> **הערה: מהות מול ערך ([01:07:46]–[01:09:23]).** שאלה שעלתה: האם צריך להוכיח שהפלט הוא "פתרון" מעבר לכך שהוא כיסוי? התשובה של המרצה: בכל בעיית אופטימיזציה יש **מהות** (מה הופך אובייקט לפתרון אפשרי) ויש **ערך** (מה שממקסמים או ממזערים). מזהים את הערך בקלות — הוא הדבר שעליו עושים מקסימום/מינימום; **כל השאר הוא מהות**. כאן הערך הוא הגודל, והמהות היא "להיות כיסוי קודקודים". ב-MAXCUT הערך הוא גודל החתך והמהות היא רק "להיות קבוצת קודקודים", ולכן שם כל קבוצה פיזבילית — וזה בדיוק מקור הבלבול.

תרגיל 5: חתך מקסימלי בגרף מכוון — קירוב $\frac{1}{4}$

הניסוח (כפי שנמסר)

עבור קבוצת קודקודים $U \subseteq V$ בגרף **מכוון** $G = (V, E)$, החתך המושרה על ידי U, שיסומן $\delta(U)$, הוא קבוצת כל הקשתות בגרף היוצאות מ-U, כלומר הזנב שלהן ב-U והראש שלהן ב-$\bar{U}$. שימו לב שבניגוד לגרף לא מכוון, החתכים המושרים על ידי U ו-$\bar{U}$ אינם בהכרח שווים. נגדיר בעיית מקסימיזציה באופן הבא:

> **קלט:** גרף פשוט מכוון $G = (V, E)$. **מטרה:** למצוא בגרף G קבוצת קודקודים $U \subseteq V$ עבורה הגודל של $\delta(U)$ מקסימלי.

הוכיחו כי קיים אלגוריתם עם זמן ריצה פולינומי לבעיה אשר משיג יחס קירוב $\frac{1}{4}$.
הטעות שרוב הכיתה עשתה — ולמה היא טעות

[01:19:25]–[01:21:00]. הפתרון שהוגש על ידי הרוב המוחלט היה: "לכל קודקוד באופן בלתי תלוי, בהסתברות $\frac{1}{2}$, נכניס אותו ל-U", ואז חישוב $\mathbb{E}[|\delta(U)|] = \frac{1}{4}|E|$. **זה אינו אלגוריתם קירוב.** אלגוריתם קירוב חייב להבטיח את היחס **בכל ריצה אפשרית**; הניתוח ההסתברותי מבטיח אותו רק **בתוחלת**, והאלגוריתם אינו דטרמיניסטי. נכון שראינו איך לדה-רנדם ניתוח כזה בשיטת התוחלות המותנות (שיעור 20, משפט 7) — אבל אז צריך לכתוב את זה. המרצה הוסיף כלל אצבע: הדבר הראשון שבודקים במדעי המחשב הוא **טיפוס**; ודאו שמה שאתם מחזירים הוא מהטיפוס שהתבקשתם להחזיר.

החישוב עצמו, לצורך הבנת המספרים: קשת מכוונת (u, v) שייכת ל-$\delta(U)$ אם ורק אם $u \in U$ **וגם** $v \notin U$, ובניסוי האחיד זה קורה בהסתברות $\frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}$. לפי לינאריות התוחלת $\mathbb{E}[|\delta(U)|] = \frac{1}{4}|E|$. זו טענה נכונה ומעניינת (השוו לשיעור 19, משפט 1, שם המקרה הלא מכוון נותן $\frac{1}{2}|E|$) — היא פשוט אינה עונה על השאלה שנשאלה.

הצעה נוספת שנפסלה ([01:23:38]–[01:25:13]). סטודנט הציע גרסה חמדנית: להכניס כל קודקוד לצד שמגדיל את "החתך" הכי הרבה. בגרף מכוון יש עכשיו **ארבעה** סוגי קשתות ($U \to \bar{U}$, $\bar{U} \to U$, $U \to U$, $\bar{U} \to \bar{U}$), ולכן "החתך" אינו מוגדר היטב: איזה חתך מגדילים? יש שתי דרכים לתקן — או למקסם את **סכום** שני החתכים המכוונים, או להתעלם לגמרי מהכיוונים ולספור קשתות ללא כיוון. הכוונה של הסטודנט הייתה נכונה, אבל המרצה עמד על כך שבכתיבה **חייבים** לומר איזו: "אני לא חי אצלכם בראש."

האלגוריתם

קלט: גרף מכוון $G = (V, E)$.
נסמן ב-$\hat{G} = (V, \hat{E})$ את הגרף הלא מכוון המתקבל מ-G על ידי **מחיקת כיווני הקשתות** (שומרים כל קשת בנפרד — ראו ההערה מיד).
נריץ את אלגוריתם הקירוב ביחס $\frac{1}{2}$ שראינו בשיעור לבעיית MAXCUT על $\hat{G}$; נסמן ב-U את פלט האלגוריתם.
אם $|\delta(U)| \geq |\delta(\bar{U})|$ ב-G — החזר את U; אחרת — החזר את $\bar{U}$.

הערה קריטית: $\hat{G}$ הוא מולטיגרף ([01:27:23]). G פשוט **מכוון**, ולכן ייתכן שגם $(u, v) \in E$ וגם $(v, u) \in E$. אחרי מחיקת הכיוונים אלה שתי קשתות **מקבילות** בין u ל-v, ואנחנו שומרים את שתיהן. זה אינו פרט טכני: אנחנו זקוקים לכך ש-$|\hat{E}| = |E|$ בדיוק. אילו היינו ממזגים קשתות מקבילות, ההבטחה $|(U, \bar{U})| \geq \frac{1}{2}|\hat{E}|$ הייתה מדברת על מספר קטן יותר, והחסם הסופי $\frac{1}{4}|E|$ היה נשבר. לפי משפט 3 לעיל, אלגוריתם ה-$\frac{1}{2}$-קירוב אכן עובד על מולטיגרפים.

(1) ניתוח זמן ריצה
שלב 1 הוא מעבר יחיד על E שבו מוחקים את הכיוון מכל קשת: $O(|E|)$.
שלב 2 רץ בזמן פולינומי בגודל $\hat{G}$, כי אלגוריתם הקירוב שראינו בשיעור הוא פולינומי (שיעור 13, משפט 3 — $O(|G|^2)$). מכיוון ש-$|\hat{G}| = O(|G|)$, זהו זמן פולינומי ב-$|G|$.
שלב 3 דורש חישוב של $|\delta(U)|$ ושל $|\delta(\bar{U})|$: מעבר יחיד על E שבו לכל קשת (u, v) בודקים לאיזה צד שייכים u ו-v ומגדילים את המונה המתאים — $O(|E|)$, ליניארי.
סך הכול פולינומי בגודל הקלט. ■

> **[01:38:51]:** את חשבון שלב 3 סטודנט הוא שהעיר שחסר, והמרצה אישר: "אתה צודק, צריך להוסיף את זה — להגיד שזה קורה בזמן ליניארי." הסיכום הכתוב מדלג על השלב הזה; כאן הוא נכתב במפורש.

(2) פיזביליות
הפלט הוא U או $\bar{U}$, ושתיהן תת-קבוצות של V. מכיוון ש**כל** תת-קבוצה של V היא פתרון אפשרי לבעיה (הגדרה 3), הפלט אפשרי תמיד. ■

> שימו לב שקבוצת הקודקודים לא השתנתה בשלב 1 — $\hat{G}$ מוגדר על אותה V — ולכן הפלט של אלגוריתם ה-MAXCUT הוא קבוצת קודקודים חוקית גם ב-G, ואפשר לחזור איתה לגרף המכוון ([01:27:57]).

(3) יחס הקירוב
יהי $G = (V, E)$ גרף מכוון, ויהי $\hat{G} = (V, \hat{E})$ הגרף הלא מכוון (המולטיגרף) המתקבל ממנו במחיקת הכיוונים, כך ש-$|\hat{E}| = |E|$.
נסמן ב-U את פלט אלגוריתם ה-MAXCUT על $\hat{G}$, וב-$(U, \bar{U})$ את החתך המושרה על ידי U ב-$\hat{G}$ (כלומר, כל הקשתות הלא מכוונות שקצה אחד שלהן ב-U והשני ב-$\bar{U}$). נסמן ב-$\delta(U), \delta(\bar{U})$ את שני החתכים המכוונים ב-G.
שלב א — ההבטחה של אלגוריתם ה-MAXCUT. לפי משפט 3, $|(U, \bar{U})| \geq \frac{1}{2}|\hat{E}| = \frac{1}{2}|E|$.
שלב ב — הזהות המרכזית. תהי $\hat{e} \in (U, \bar{U})$ קשת בחתך הלא מכוון, ותהי $(u, v) \in E$ הקשת המכוונת שממנה היא נוצרה. שני קצותיה נמצאים בצדדים מנוגדים, ולכן בדיוק אחת משתי האפשרויות מתקיימת: או ש-$u \in U$ ו-$v \in \bar{U}$, ואז $(u, v) \in \delta(U)$; או ש-$u \in \bar{U}$ ו-$v \in U$, ואז $(u, v) \in \delta(\bar{U})$. ולהפך, כל קשת ב-$\delta(U)$ או ב-$\delta(\bar{U})$ מניבה קשת בחתך הלא מכוון. שתי הקבוצות $\delta(U), \delta(\bar{U})$ זרות. לכן $|(U, \bar{U})| = |\delta(U)| + |\delta(\bar{U})|$.
זהו בדיוק מה ש"נשבר" במעבר מגרף לא מכוון למכוון: החתך הלא מכוון מתפצל לשני חתכים מכוונים, ואנחנו מקבלים רק את אחד מהם.
שלב ג — בחירת הצד הטוב. שני מספרים אי-שליליים שסכומם $|(U, \bar{U})|$; לפחות אחד מהם גדול-שווה למחצית הסכום: $|\delta(U)| \geq \frac{1}{2}|(U, \bar{U})|$
או

$|\delta(\bar{U})| \geq \frac{1}{2}|(U,\bar{U})|$. שלב 3 של האלגוריתם בוחר בדיוק את הגדול מבין השניים. נסמן ב-$\tilde{U}$ את הפלט; אז $\tilde{U} \subseteq V$ ולכן פתרון אפשרי, ומתקיים $|\delta(\tilde{U})| \geq \frac{1}{2}|(U,\bar{U})| \geq \frac{1}{2}\cdot\frac{1}{2}|E| = \frac{1}{4}|E|$.

שלב ד — השוואה לאופטימום. נסמן ב-U_{opt} פתרון אופטימלי. מכיוון ש-$\delta(U_{\text{opt}}) \subseteq E$, מתקיים $|\delta(U_{\text{opt}})| \leq |E|$. לכן, $|\delta(U_{\text{opt}})| \leq |E| \leq 4|\delta(\tilde{U})|$ ומצד שני $|\delta(\tilde{U})| \leq |\delta(U_{\text{opt}})|$, כלומר $\tilde{U}$ פתרון אפשרי ו-U_{opt} אופטימלי. יחד: $\frac{1}{4}|\delta(U_{\text{opt}})| \leq |\delta(\tilde{U})| \leq |\delta(U_{\text{opt}})|$, כלומר אלגוריתם קירוב ביחס $\frac{1}{4}$. ■

> **הרעיון בשורה אחת ([01:37:47]):** לקחת אלגוריתם שאני כבר מכיר, ולעשות עליו **עוד שלב אחד**. כל אחד משני השלבים "עולה" פקטור $\frac{1}{2}$, וסך הכול $\frac{1}{4}$.

דוגמה מספרית קטנה

$V = \{1,2,3,4\}$ ו-$E = \{(1,3),(3,1),(2,4),(4,2)\}$ — שני זוגות אנטי-מקבילים. אז $|E| = 4$ ו-$\hat{G}$ הוא מולטיגרף עם ארבע קשתות: שתיים בין 1 ל-3 ושתיים בין 2 ל-4.

נניח שאלגוריתם ה-MAXCUT החזיר $U = \{1,2\}$. אז החתך הלא מכוון מכיל את כל ארבע הקשתות, $|(U,\bar{U})| = 4 \geq \frac{1}{2}\cdot 4$ — ההבטחה מתקיימת. בגרף המכוון: $\delta(\{1,2\}) = \{(1,3),(2,4)\}$, $\delta(\{3,4\}) = \{(3,1),(4,2)\}$, $|(U,\bar{U})| = 4 = 2+2$ — כלומר הזהות של שלב ב. שלב 3 מחזיר U (שוויון), והתוצאה $|\delta(U)| = 2 \geq \frac{1}{4}\cdot 4 = 1$.

ואילו אילו **מיזגנו** קשתות מקבילות היינו מקבלים $\hat{E}$ בגודל 2, ההבטחה הייתה נותנת רק $|(U,\bar{U})| \geq 1$, ומכאן רק $|\delta(\tilde{U})| \geq \frac{1}{2}$ — חסם חסר תועלת. זו בדיוק הסיבה לשמור על הקשתות המקבילות.

תרגיל 7: קירוב 1.49 ל-BIN-PACKING גורר $\text{P} = \text{NP}$

הניסוח (כפי שנמסר)

הוכיחו כי אם קיים אלגוריתם קירוב עם יחס קירוב 1.49 לבעיית BIN-PACKING אז $\text{P} = \text{NP}$.

איך מגיעים לרעיון

[01:43:22]–[01:43:52]. השאלה מהכיתה הייתה "איך אני אמור בכלל לזהות מה לעשות כאן?". התשובה של המרצה: ראינו משהו דומה — אי-הקירוב של בעיית **הסוכן הנוסע** (שיעור 13, משפט 4). התבנית: מניחים שקיים אלגוריתם קירוב, ומראים שבעזרתו אפשר **להכריע** בעיה NP-קשה בזמן פולינומי; מכאן $\mathrm{P} = \mathrm{NP}$.

[01:59:22] — שיטת החיפוש הממצה. "עוברים על **כל** מה שאני יודע על הבעיה ובודקים מה יעזור." מה אנחנו יודעים על BIN-PACKING? (א) את הגדרתה; (ב) שקיים לה אלגוריתם קירוב ביחס 2 (First-Fit, שיעור 14) — לא יעזור, כי זו תוצאה **חיובית** ואנחנו מחפשים תוצאת **קושי**; (ג) את הרדוקציה $\text{PARTITION} \leq_p \text{BIN-PACKING}$ (שיעור 12). זהו — הרשימה קצרה, ולכן החיפוש הממצה יעיל כאן. (ג) הוא הכיוון.

[01:57:46] — קיצור-דרך שהמרצה הציע. אפשר לעצור צעד אחד קודם: שיעור 12, משפט 5, כבר קבע ש-BIN-PACKING עם $k = 2$ **קבוע** היא NP-קשה. אפשר להכריע ישירות את הבעיה הזו — האלגוריתם מקבל $b_1, \ldots, b_n \in (0, 1]$, מריץ את אלגוריתם הקירוב ומקבל אם ורק אם התוצאה 2 — ולא לחזור כל הדרך אחורה ל-PARTITION. הפתרון הכתוב בסיכום עושה את המסלול המלא, וכך גם הקובץ הזה.

[01:46:36] — "נניח", לא "נניח בשלילה". השאלה מנוסחת כ"אם... אז...". אין כאן שום דבר שמוביל לסתירה; מניחים את המקדמה ומוכיחים את המסקנה.

האלגוריתם המכריע את PARTITION

נניח שקיים אלגוריתם קירוב A ביחס 1.49 לבעיית BIN-PACKING. נתבונן באלגוריתם הבא:

קלט: $a_1, \ldots, a_n \in \mathbb{N}$.

נסמן $S = \sum_{i=1}^{n} a_i$.

אם S אי-זוגי, **או** קיים $1 \leq i \leq n$ כך ש-$a_i > \dfrac{S}{2}$ — **דחה**.

לכל $1 \leq i \leq n$ נסמן $b_i = \dfrac{2a_i}{S}$.

הרץ את A על $b_1, \ldots, b_n$. אם מספר התאים בפלט שווה 2 — **קבל**; אחרת — **דחה**.

למה שלב 2 נחוץ

זו הייתה שאלת הכיתה המרכזית ([01:53:33]–[01:55:04]), והתשובה מלמדת עיקרון כללי.

החלק "S אי-זוגי": אם S אי-זוגי אז $S/2$ אינו שלם, ואף סכום חלקי של שלמים אינו יכול להשתוות לו — הקלט ודאי אינו ב-PARTITION, ולכן דחייה נכונה.

החלק "$a_i > S/2$": שתי סיבות, ושתיהן הכרחיות.

נכונות: אם $a_i > S/2$ אז כל צד המכיל את a_i עובר את המחצית, ולכן הקלט ודאי אינו ב-PARTITION — דחייה נכונה.

חוקיות הקלט ל-A: הקלט של BIN-PACKING חייב להיות ב-$(0,1]$. מתקיים $b_i = 2a_i/S \le 1$ אם ורק אם $a_i \le S/2$. ללא הבדיקה היינו שולחים ל-A קלט **לא חוקי**, ואז אין לנו שום הבטחה על מה שיחזור.

הדוגמה הקונקרטית מהלוח ([01:54:03]): $(a_1,a_2,a_3)=(1,1,3)$. אז $S=5$ ו- $b_3 = \frac{2\cdot 3}{5} = \frac{6}{5} > 1$ — מחוץ לתחום. ואכן $(1,1,3) \notin \text{PARTITION}$.

העיקרון הכללי ([01:55:04]): "כשאתם שולחים משהו לאלגוריתם, ודאו שזה קלט חוקי לאלגוריתם. האלגוריתם אינו אמור לוודא את זה."

הערה (לא נאמרה בהרצאה): בקורס $\mathbb{N}$ הוא קבוצת הטבעיים החיוביים, ולכן $a_i \ge 1$ ובפרט $b_i > 0$; זה מה שמבטיח $b_i \in (0,1]$ ולא רק $b_i \le 1$.

(1) ניתוח זמן ריצה

יהיו $a_1,\dots,a_n \in \mathbb{N}$.

שלבים 1–2 דורשים $O(n)$ צעדים: $n-1$ חיבורים של מספרים באורך לכל היותר אורך הקלט, בדיקת זוגיות אחת ו-n השוואות.

שלב 3 דורש $O(n)$ צעדים. כל b_i הוא רציונלי המיוצג כזוג שלמים — מונה $2a_i$ ומכנה S — ואורך כל אחד מהם פולינומי באורך הקלט.

שלב 4 מתבצע בזמן פולינומי בגודל הקלט **מההנחה**: אלגוריתם קירוב הוא מעצם הגדרתו אלגוריתם פולינומי.

סך הכול זמן ריצה פולינומי בגודל הקלט. ■

הערה חשובה על "גודל הקלט" ([02:02:32]–[02:03:37]). שאלה מהכיתה: כשמדובר במספרים, האם אין בעיה של ייצוג לוגריתמי? התשובה: כאן אנחנו נשארים **בתוך עולם המספרים** לכל אורך הדרך — הקלט מספרים, הפלט של שלב 3 מספרים — ולכן "פולינומי בגודל הקלט" מתגלגל ישירות. הזהירות נדרשת ב**מעברים** בין סוגי אובייקטים: אילו היינו בונים גרף עם S קודקודים, גודלו היה **מעריכי** באורך הייצוג של S. וכן ([02:03:37]) המעבר בין בסיס 10 לבסיס 2 אינו מהותי — הוא משנה את האורך בפקטור קבוע $\log 10 / \log 2$.

(2) ניתוח נכונות, כיוון ראשון: אם $(a_1,\dots,a_n) \in \text{PARTITION}$ אז האלגוריתם מקבל נניח $(a_1,\dots,a_n) \in \text{PARTITION}$. אז קיימת $I \subseteq [n]$ כך ש $\sum_{i\in I} a_i = \frac{S}{2} = \sum_{i\notin I} a_i$.

שלב 2 אינו דוחה. מכיוון ש-$S/2 = \sum_{i\in I} a_i$ הוא סכום של שלמים, S זוגי. וכן לכל $i \in [n]$ מתקיים $a_i \le S/2$, שכן a_i נמצא באחד משני הצדדים והוא לכל היותר סכום כל אותו צד (כל האיברים חיוביים).

הפלט של שלב 3 חוקי. לכל i מתקיים $0 < b_i = 2a_i/S \le 1$, כלומר $b_i \in (0,1]$. וכן $\sum_{i=1}^{n} b_i = \frac{2}{S}\sum_{i=1}^{n} a_i = \frac{2S}{S} = 2$.

האופטימום הוא בדיוק 2.

חסם עליון $\mathrm{OPT} \le 2$: נכניס לתא הראשון את הפריטים שאינדקסם ב-I ולשני את השאר. אז $\sum_{i \in I} b_i = \frac{2}{S} \cdot \frac{S}{2} = 1 \le 1, \qquad \sum_{i \notin I} b_i = 1 \le 1,$ כלומר זו אריזה חוקית בשני תאים.
חסם תחתון $\mathrm{OPT} \ge 2$: סכום כל הפריטים הוא $2 > 1$, ולכן תא יחיד אינו יכול להכיל את כולם. לכן $\mathrm{OPT}(b_1, \dots, b_n) = 2$.
מה A מחזיר. A הוא אלגוריתם קירוב ביחס 1.49 לבעיית מינימיזציה, ולכן הפלט שלו הוא אריזה **אפשרית** שמספר התאים בה, נסמנו ALG, מקיים $\mathrm{OPT} \le \mathrm{ALG} \le 1.49 \cdot \mathrm{OPT} = 1.49 \cdot 2 = 2.98.$ כלומר $2 \le \mathrm{ALG} \le 2.98$. אבל ALG הוא **מספר שלם**, ולכן בהכרח $\mathrm{ALG} = 2$.
לכן שלב 4 **מקבל**. ■

[01:49:52]: סטודנטית העירה שגם $\mathrm{ALG} = 1$ בלתי אפשרי — נכון, וזה בדיוק החסם התחתון $\mathrm{OPT} \ge 2$ שכתבנו. לכן התנאי "שווה 2" ו"קטן-שווה 2" שקולים כאן.

[01:48:48] — דיוק בניסוח. אילו היה אלגוריתם הקירוב מחזיר רק את **הערך** ולא אריזה, הניסוח המדויק של שלב 4 היה "אם המספר שחזר קטן מ-3". לפי ההגדרה שלנו אלגוריתם קירוב תמיד מחזיר פתרון אפשרי, ולכן שתי הגרסאות תקינות. אבל שווה לזכור שאפשר להגדיר אלגוריתם קירוב שמחזיר רק ערך.

(3) ניתוח נכונות, כיוון שני: אם האלגוריתם מקבל אז $(a_1, \dots, a_n) \in \mathrm{PARTITION}$

הסיכום הכתוב מסתפק כאן ב"(כך גם ההיפך)". המרצה השאיר את הכיוון לבית ואמר ב-[02:10:30] שהניסוח הנוח ביותר הוא דווקא **הקונטרפוזיטיבי**: "אם האלגוריתם קיבל, אז לא יכול להיות שזה קרה ולא יכול להיות שזה קרה" — כלומר להסיק מקבלה, במקום להתחיל מ"לא בפרטישן" ולפצל למקרים. כך נכתב כאן.

נניח שהאלגוריתם קיבל.
מסקנה א. שלב 2 לא דחה, ולכן S זוגי ולכל i מתקיים $a_i \le S/2$. מכאן שכל $b_i \in (0, 1]$ ושהקלט ל-A חוקי, וכן $\sum_{i=1}^{n} b_i = 2$ כמו קודם.
מסקנה ב. שלב 4 קיבל, ולכן A החזיר אריזה **אפשרית** של $b_1, \dots, b_n$ בשני תאים בדיוק. כלומר קיימת $f : [n] \to \{1, 2\}$ עם $\sum_{i:\, f(i)=1} b_i \le 1, \qquad \sum_{i:\, f(i)=2} b_i \le 1.$
מסקנה ג — אין מרווח. סכום שני האגפים השמאליים הוא $\sum_{i=1}^{n} b_i = 2$. אילו אחד מהם היה קטן ממש מ-1, הסכום היה קטן ממש מ-2 — סתירה. לכן $\sum_{i:\, f(i)=1} b_i = 1 = \sum_{i:\, f(i)=2} b_i$. זו בדיוק ה"צמידות המוחלטת" שהיא מנוע הרדוקציה של שיעור 12: מחלקים ב-$S/2$ כדי שהסכום הכולל יהיה 2 בדיוק, ואז אריזה בשני תאים אפשרית אם ורק אם החלוקה היא 1 ו-1 במדויק.
מסקנה ד — חזרה ל-a_i. נסמן $I = f^{-1}(1)$. אז $\sum_{i \in I} b_i = \frac{2}{S} \sum_{i \in I} a_i = 1 \quad \Longrightarrow \quad \sum_{i \in I} a_i = \frac{S}{2},$ ובאופן זהה $\sum_{i \notin I} a_i = S/2$. לכן $(a_1, \dots, a_n) \in \mathrm{PARTITION}$. ■
בשילוב שני הכיוונים: האלגוריתם מקבל את $(a_1, \dots, a_n)$ **אם ורק אם** $(a_1, \dots, a_n) \in \mathrm{PARTITION}$.

מסקנה
האלגוריתם שבנינו מכריע את $\mathrm{PARTITION}$ בזמן פולינומי, ולכן $\mathrm{PARTITION} \in \mathrm{P}$. לפי משפט 2 (שיעור 12), $\mathrm{PARTITION}$ היא NP-קשה, ולכן לכל $L \in \mathrm{NP}$ מתקיים $L \leq_p \mathrm{PARTITION}$; הרכבת הרדוקציה הפולינומית עם האלגוריתם הפולינומי נותנת $L \in \mathrm{P}$. לכן $\mathrm{NP} \subseteq \mathrm{P}$, ויחד עם ההכלה הטריוויאלית $\mathrm{P} \subseteq \mathrm{NP}$: $\blacksquare$ $\mathrm{P} = \mathrm{NP}$.
למה דווקא 1.49, ומה קורה ב-1.5
זו השאלה שסטודנטית הצביעה עליה כקושי האמיתי של התרגיל ([01:57:13]): "מה שהיה קשה זה להגיע מזה ש-1.49 יכול להכריע חלוקה לשני תאים."
ההוכחה השתמשה ב-1.49 רק בשורה אחת: $\mathrm{ALG} \leq 1.49 \cdot 2 = 2.98 < 3$. מכיוון ש-$\mathrm{ALG}$ שלם, זה כופה $\mathrm{ALG} \leq 2$. לכן:
כל $\alpha < \frac{3}{2}$ עובד באותה הוכחה מילה במילה, כי $2\alpha < 3$.
$\alpha = \frac{3}{2}$ בדיוק **אינו** עובד: אז $\mathrm{ALG} \leq 3$, והאלגוריתם רשאי להחזיר 3 תאים גם על קלט שאפשר לארוז בשניים — ואיננו יכולים להסיק דבר.
זהו הסף החד המוכר: אלא אם $\mathrm{P} = \mathrm{NP}$, אין לבעיית $\mathrm{BIN\text{-}PACKING}$ אלגוריתם קירוב ביחס $\frac{3}{2} - \varepsilon$ לשום $\varepsilon > 0$. שימו לב שאין בכך סתירה לאלגוריתם ה-2-קירוב First-Fit של שיעור 14 — $2 > \frac{3}{2}$.

הערות מהשיעור
[00:01:34] טענה קומבינטורית מול טענה אלגוריתמית. סעיף (א) של תרגיל 3 מגדיר קבוצה ומוכיח עליה תכונה; אין בו אלגוריתם. סעיף (ב) הוא שאלה אלגוריתמית. ההבחנה הזו חוזרת בכל הקורס.
[00:03:21] קונבנציית "גרף פשוט". אם לא נאמר אחרת — הגרף פשוט. "מכוון" אינו מבטל את "פשוט"; גרף מכוון פשוט הוא עדיין בלי לולאות ובלי קשתות כפולות באותו כיוון.
[00:04:56]–[00:06:00] שלושת הדברים. על כל אלגוריתם קירוב צריך להוכיח: זמן ריצה פולינומי, שהפלט הוא פתרון אפשרי, ויחס הקירוב. "השאלה הזו לא מאוד קשה, אבל לכתוב אותה צריך להקפיד על הכול. לא לדלג."
[00:08:07]–[00:09:12] מה מותר בהוכחה ומה מותר לאלגוריתם. בשלב ה**הוכחה** יש לי גישה חופשית לפתרון אופטימלי: "נסמן $\hat{E}$ פתרון אופטימלי" הוא ביטוי חוקי, כי פתרון אופטימלי תמיד קיים בבעיות שאנחנו לומדים. ל**אלגוריתם** אין גישה כזו — מציאת אופטימום היא בדיוק הבעיה הקשה. אותו הבדל בדיוק כמו בין "נניח $x \in L$, אז קיים certificate" לבין "האלגוריתם ימצא certificate".
[00:09:44]–[00:10:16] הכלי של "לפחות אחד מהשניים". שני מספרים אי-שליליים — אחד מהם לפחות חצי מהסכום. תמיד. האנלוגיה למכפלה (אחד מהם לפחות שורש המכפלה) **אינה** נכונה ללא הנחות. השתמשנו בכלי הזה פעמיים בקובץ: בתרגיל 3 ובתרגיל 5.
[00:14:49] בחירת בעיית המקור לרדוקציה. "אני עושה רדוקציה מ-VC כי זו בעיה **קרובה**. אם זה לא עובד אולי אתחיל לחשוב על דברים אחרים, אבל זה הניחוש הראשון שלי."

[00:18:02] למה מוסיפים סימונים לאלגוריתם. אפשר היה לכתוב "נוסיף את הקודקוד לגרף ונוסיף אותו לקשת" בלי לתת לו שם. זה תיאור מדויק ואפשר להריץ אותו. הסימון v_e קיים כי בשלב ההוכחה נוח בהרבה לדבר על אובייקט שיש לו שם.

[00:34:33] אותו טריק כמו ב-$\mathrm{VC} \leq_p \mathrm{DS}$ (שיעור 19). גם שם הוספנו לכל קשת קודקוד חדש וחיברנו אותו לשני קצותיה, וגם שם בכיוון ההפוך היינו צריכים להחליף כל קודקוד חדש בשכן שלו. "עשינו כבר את הטריק הזה."

[00:40:50]–[00:41:23] "בגודל k" מול "בגודל $\leq k$". ב-VC אפשר תמיד להוסיף קודקודים כדי להשלים לגודל מדויק; ב-IS וב-CLIQUE אפשר תמיד להוריד. ב-MAXCUT **אי אפשר** — שם בוחרים קודקודים ומודדים קשתות, ובמספר הקשתות אין שליטה מדויקת.

[00:45:09]–[00:46:14] דיסציפלינת חלוקה למקרים. תמיד לחלק לשני מקרים, והמקרה השני צריך להיות **בדיוק השלילה** של הראשון. "אני רוצה עצים בינריים של מקרים." זה לא עניין של סגנון — זה מה שמונע פספוס מקרה.

[00:48:25] יש סדר, הוא פשוט לא מובטח. על קבוצה במחשב "אין סדר" הוא ניסוח לא מדויק; הניסוח המדויק הוא **"לא מובטח לי סדר"**. תיאורטית אפשר להיכנס לזיכרון ולקרוא את האיבר הראשון. לכן "נבחר את הקצה הראשון של הקשת" הוא ביטוי חוקי כשמדובר בהוכחה ולא באלגוריתם.

[00:52:15] תכתבו גם את מה שברור לכם. "אל תגידו 'זה ברור, אני אכתוב את זה כשאבין את שאר התשובה'. זו שגיאה כדרך עבודה — כי כשאני כותב את מה שברור לי, הרבה פעמים דברים אחרים מתחילים להיות ברורים."

[01:07:46]–[01:09:23] מהות מול ערך. הערך הוא הדבר שעליו עושים אופטימיזציה; **כל השאר הוא מהות**, ועליו צריך להוכיח פיזביליות. ב-MAXCUT המהות היא רק "קבוצת קודקודים", ולכן שם הפיזביליות טריוויאלית — ובגלל זה מתבלבלים ומדלגים עליה גם במקומות שבהם היא לא טריוויאלית.

[01:09:55]–[01:13:33] עצה למבחן. "לעבור על החומר זה הכי חשוב מהכול: שיעורים ותרגילי בית. אם נשאר לכם זמן — קחו בחינות משנה-שנתיים אחרונות. אל תתחילו משם; זו לא נקודת התחלה טובה, זו נקודת סיום." ובהמשך: "אם אתם עושים אוברפיטינג למשהו, תעשו אוברפיטינג לחומר ולא לבחינות קודמות." המרצה ציין שלמעט משפט ההיררכיה ומשפט קוק–לוין, כל מה שהוכח בשיעור הוא "ברמת תרגיל" מבחינת הנבחנים.

[01:19:25]–[01:21:00] הטעות של תרגיל 5. אלגוריתם הסתברותי שמשיג את היחס **בתוחלת** אינו אלגוריתם קירוב. אלגוריתם קירוב חייב את ההבטחה בכל ריצה. "הדבר הראשון שבודקים במדעי המחשב הוא טיפוס: מה הקלט, מה הפלט."

[01:26:15] תיאור אלגוריתם. "אני לא חי אצלכם בראש." תיאור אלגוריתם צריך להיות מדויק מספיק כדי שאפשר יהיה לבצע עליו הרצה יבשה — לא ברמת קוד, אבל ברמה שבה אני יודע להריץ אותו.

[01:38:51] שאלת סטודנט שתפסה חור בכתיבה. בשלב 3 של תרגיל 5 צריך להשוות בין שני חתכים, וזה דורש מעבר על הקשתות; זמן הריצה של השלב הזה נשמט מהסיכום, והמרצה אישר שצריך להוסיפו ("זה קורה בזמן ליניארי").

[01:39:58] שני האלגוריתמים ל-MAXCUT. בקורס ראינו שניים: **חיפוש מקומי** (מתחילים מפתרון ומזיזים קודקודים; שיעור 13) ו**חמדני** (מתחילים מכל הקודקודים בחוץ ומכניסים אחד-אחד לפי איפה שהחתך גדל; שיעור 14). שניהם משיגים $\frac{1}{2}$, ובתרגיל 5 אפשר להשתמש בכל אחד מהם.
[01:41:02] אקראיות אינה קורית במקרה. "אקראיות זה לא משהו שקורה בדרך אגב — זה משהו שצריך לקרות **explicitly**." אלגוריתם חמדני דטרמיניסטי מנותח ב-worst case, לא בתוחלת; אין מקום למילה "תוחלת" כשלא הגרלנו כלום.
[01:46:36] "נניח" ולא "ננניח בשלילה". שאלה מהצורה "אם X אז Y" אינה מזמינה הנחה בשלילה. מתחילים ב"ננניח X".
[01:50:22]–[01:51:26] "לא הבנתי כלום" אינו קיים. תגובה לסטודנטית שאמרה שלא הבינה כלום: "הבנת איך מריצים את האלגוריתם. מה שלא הבנת זה **איך הגיעו** לזה, ולמה זה נותן משהו." הכלל: לא לבטל את מה שכן יודעים. ובהמשך ([01:51:57]) — "זה בדיוק הרדוקציה שראינו בשיעור מ-$\mathrm{PARTITION}$ ל-$\mathrm{BIN\text{-}PACKING}$; זה לא המצאה מחדש, זה היה בהישג ידך."
[01:57:46] הקיצור דרך $\mathrm{BIN\text{-}PACKING}$ עם $k = 2$. בשיעור 12 הודגש שלוש פעמים שהרדוקציה מוכיחה NP-קושי גם עבור $k = 2$ קבוע. אפשר להשתמש בזה ישירות ולחסוך את המסלול חזרה ל-$\mathrm{PARTITION}$. "זו הבעיה NP-קשה הכי קרובה ל-$\mathrm{BIN\text{-}PACKING}$ שראינו."
[02:03:05]–[02:04:11] מתי גודל הקלט הופך למהותי. כל עוד נשארים בעולם המספרים, "פולינומי בגודל הקלט" מתגלגל. במעבר בין מספרים לגרפים (או להפך) צריך לעצור ולבדוק — גרף עם S קודקודים הוא מעריכי באורך הייצוג של S. ולעניין בסיסי ספירה: כל בסיס שאינו אונרי שקול, כי המעבר בין בסיס 10 לבסיס 2 הוא פקטור קבוע.

פערים בין הסיכום להקלטה

מקור: הסיכום. **הפער:** שמונת העמודים מכילים את תרגילים 3, 4, 5 ו-7 בלבד; תרגילים 1, 2 ו-6 של אותו תרגיל בית אינם בהם. **ההכרעה:** ההקלטה מסבירה את היעדרו של 6 — ב-[01:41:35] המרצה דוחה אותו במפורש ("שש מאוד דומה למה שעשינו בשיעור") ועובר ישירות מ-5 ל-7. תרגילים 1–2 אינם מוזכרים בהקלטה כלל, וסביר שנפתרו במפגש קודם. הקובץ מכסה בדיוק את מה שבעמודים, ואינו מנחש.
מקור: ההקלטה. **הפער:** ההקלטה נפתחת ב-[00:00:00] **באמצע** פתרון סעיף (א) של תרגיל 3, בלי שום פתיחה, ואף מסכמת את הסעיף במשפט אחד ("אין כל כך מה לעשות אותה עכשיו") כאילו כבר נדון. כלומר תחילת המפגש חסרה בהקלטה. בפרט, שני הנושאים שנדחו בסוף המפגש הקודם — סעיף ד של שאלה 3 במטלה 2 (המחלקה C_4) ושאלה על רדוקציות בזמן מעריכי — **אינם מופיעים בהקלטה הזו כלל**; סריקת מילות מפתח על כל הקובץ לא מצאה אף אזכור שלהם. **ההכרעה:** לא נוסף כאן חומר שאינו בהקלטה ואינו בעמודים. החומר הדחוי אינו שייך לשיעור הזה, ויש לחפשו במפגש אחר.
מקור: ההקלטה. **הפער:** כל הדיון על הטעות הנפוצה בתרגיל 5 — הפתרון ההסתברותי שהוגש על ידי רוב הכיתה, ולמה ניתוח בתוחלת אינו אלגוריתם קירוב — אינו בסיכום כלל. **ההכרעה:** נכנס במלואו לפתרון תרגיל 5, לפני האלגוריתם, כי זה עיקר הערך של השיעור לגבי התרגיל הזה.

מקור: ההקלטה. **הפער:** גם ההצעה החמדנית שנפסלה ([01:23:38]) — "להכניס כל קודקוד לצד שמגדיל את החתך" — ולמה היא לא מוגדרת היטב בגרף מכוון, אינה בסיכום. **ההכרעה:** נכנסה כהערה בתרגיל 5.

מקור: הסיכום, עמוד 6. **הפער:** נכתב ישירות $|(U, \bar{U})| \geq \frac{1}{2}|E|$, בלי להסביר למה מותר להחליף את $|E|$ ב-$|\hat{E}|$. **ההכרעה:** הצעד תקף רק אם שומרים קשתות מקבילות ב-$\hat{G}$, כך ש-$|\hat{E}| = |E|$; ההקלטה נוגעת בכך ב-[01:27:23] ("יכולות להיות פתאום קשתות מקבילות... ראינו את MAXCUT כשהגרף לא פשוט"). הפירוט נכתב כאן במפורש, כולל דוגמה נומרית שמראה שמיזוג קשתות שובר את החסם.

מקור: הסיכום, עמוד 6. **הפער:** ניתוח זמן הריצה אינו כולל את שלב 3 (חישוב שני החתכים). **ההכרעה:** נוסף כאן, לפי [01:38:51] שבו סטודנט העלה את זה והמרצה אישר.

מקור: הסיכום, עמוד 7. **הפער:** נכתב "האלגוריתם יחזיר חלוקה שבה פחות **או יותר** מ-2.98 תאים" — ניסוח שאינו נכון מתמטית; אלגוריתם קירוב אינו יכול להחזיר יותר מ-$\alpha \cdot \mathrm{OPT}$. **ההכרעה:** ההקלטה אומרת בבירור ב-[02:09:26] "לכל היותר 2.98", וכך נכתב כאן. מדובר בהשמטת מילה בסיכום, לא בטעות מתמטית.

מקור: הסיכום, עמוד 8. **הפער:** הכיוון השני של תרגיל 7 מסוכם בסוגריים אחת בלבד. **ההכרעה:** נכתב כאן במלואו, בניסוח הקונטרפוזיטיבי שהמרצה המליץ עליו ב-[02:10:30] (מניחים שהאלגוריתם קיבל ומסיקים).

מקור: הסיכום, עמוד 2. **הפער:** ניסוח התרגיל משתמש ב-S עבור כיסוי הקודקודים בהיפרגרף, בעוד הפתרון בכתב יד משתמש ב-U. **ההכרעה:** זהו שינוי סימון מכוון שנדון בכיתה ב-[00:25:23]; ההגדרה בקובץ שומרת על S והפתרון על U ו-$\hat{U}$, כמו במקור.

מקור: הסיכום, עמוד 3. **הפער:** נכתב "לכן U כיסוי בקודקודים בגודל קטן או שווה ל-k", בעוד שהגדרת השפה בעמוד 2 אומרת "בגודל k". **ההכרעה:** אין כאן סתירה — שתי הצורות שקולות (על-קבוצה של כיסוי היא כיסוי), וההקלטה עוסקת בכך במפורש ב-[00:40:50]. הקובץ מגדיר את השפה עם $\leq k$ ומוסיף הערה.

מקור: הסיכום, עמוד 5. **הפער:** נכתב "$|C| = 3|F|$" ו-"$|F| \leq |C_{\mathrm{opt}}|$" בלי לפרט מדוע ההתאמה חד-חד-ערכית ומדוע שלושת הקודקודים חדשים. **ההכרעה:** ההקלטה ([01:15:07]–[01:16:42]) מפרטת; ההוכחה נכתבה כאן במלואה בשני שלבים נפרדים.

מקור: קונבנציות. **הפער:** §2a של המפרט קובע תיקון של רביעיית המכונה. **ההכרעה:** בשיעור הזה אין ולו מכונת טיורינג אחת — כל התוכן הוא אלגוריתמי קירוב ורדוקציה בין שפות — ולכן הכלל אינו חל. שמות מחלקות ובעיות נכתבו ב-‹· לפי המפרט; שמות המשתנים ($\hat{V}, \hat{E}, \hat{U}, C_{\mathrm{opt}}, \delta(U), (U, \bar{U})$) נשמרו בדיוק כפי שהם בסיכום.

מקור: פרטיות. **הפער:** אין. **ההכרעה:** לא נמצאו בעמודים מספרי זהות, שמות סטודנטים או פרטים מזהים אחרים. בהקלטה נזכרים שמות פרטיים של סטודנטים בכיתה; הם הושמטו, ושאלות הסטודנטים מובאות כאן ללא ייחוס אישי.

סיכום ונקודות למבחן

זהו שיעור חזרה, ולכן הסעיף הזה חשוב במיוחד.

התבנית שחוזרת בכל שלושת אלגוריתמי הקירוב

לכל אלגוריתם קירוב **שלושה** דברים, בסדר הזה:

זמן ריצה פולינומי — מספר איטרציות $\times$ עלות איטרציה. חסם גס מספיק, ובלבד שהוא נכון.

פיזביליות — הפלט הוא פתרון אפשרי לבעיה. זהו השלב הנשכח.

יחס הקירוב — שני אי-שוויונות, שאחד מהם טריוויאלי ונובע מ-(2).

והטכניקה בשלב (3) היא תמיד אותה טכניקה: האלגוריתם אינו יכול לחשב את OPT, ולכן בונים **גודל עזר** שהאלגוריתם שולט בו, מוכיחים שהוא חוסם את OPT מהצד הנכון, ומשווים אליו את הפלט.

תרגיל	גודל העזר	הכיוון
3 (תת-גרף חסר מעגלים, מקסימיזציה)	$\|E\|$	חוסם את OPT **מלמעלה**
4(ב) (כיסוי בהיפרגרף, מינימיזציה)	$\|F\|$ (היפר-קשתות זרות בזוגות)	חוסם את OPT **מלמטה**
5 (חתך מכוון, מקסימיזציה)	$\|E\|$	חוסם את OPT **מלמעלה**

התוצאות שכדאי לזכור

$E = E_1 \dot\cup E_2$ לפי כיוון האינדקסים, ושתי הקבוצות חסרות מעגלים — ולכן קירוב $\frac{1}{2}$ לתת-הגרף המקסימלי חסר המעגלים.

$\mathrm{VC} \le_p \mathrm{DS}$. $3\text{H-}\mathrm{VC} \le_p \mathrm{VC}$ בהוספת קודקוד חדש לכל קשת. אותו טריק כמו

אלגוריתם ה"היפר-קשתות הזרות" נותן קירוב r להיפרגרף r-אחיד; $r = 2$ הוא ה-VC המוכר, $r = 3$ הוא התרגיל.

$|\delta(U)| + |\delta(\bar U)| = |(U, \bar U)|$ — הזהות שמתרגמת חתך לא מכוון לשני חתכים מכוונים, והמקור לפקטור $\frac{1}{4}$.

אם קיים אלגוריתם קירוב ביחס $\alpha < \frac{3}{2}$ ל-BIN-PACKING אז $\mathrm{P} = \mathrm{NP}$. הסף חד בגלל שלמות מספר התאים.

המלכודות הסטנדרטיות

לשכוח את הפיזביליות. במיוחד בבעיות שבהן היא נראית טריוויאלית — ואז שוכחים אותה גם במקום שבו היא לא.

ניתוח בתוחלת במקום אלגוריתם קירוב. אם הרצתם ניסוי אקראי, יש לכם טענה קיומית או אלגוריתם הסתברותי — לא אלגוריתם קירוב. כדי לקבל אלגוריתם קירוב צריך לדה-רנדם (שיעור 20), ולכתוב את זה.

לקחת קבוצה מהצד הקשה של הרדוקציה כמו שהיא. ב-$3\text{H-}\mathrm{VC}$ הקבוצה $\hat U$ אינה בהכרח מוכלת ב-V, ולכן השאלה "האם היא כיסוי של G" אפילו לא מוגדרת. תמיד לבדוק לאיזו קבוצה שייך האובייקט שבידיכם.

לשלוח לאלגוריתם קלט לא חוקי. אם קוראים לאלגוריתם כתת-שגרה, האחריות לחוקיות הקלט היא שלכם. זו כל הסיבה לשלב 2 בתרגיל 7.

לאבד את $|\hat E| = |E|$ במחיקת כיוונים. מיזוג קשתות אנטי-מקבילות שובר את החסם.

לכתוב "יותר מ-" במקום "לכל היותר". אלגוריתם קירוב חוסם את הפלט **מלמעלה** ביחס ל- $\alpha \cdot \mathrm{OPT}$ ומלמטה ב-OPT.

רשימת יכולות אחרי השיעור

אחרי השיעור הזה צריך לדעת:

להוכיח שגרף מכוון שכל קשתותיו מונוטוניות באינדקסים הוא חסר מעגלים, ולבנות ממנה אלגוריתם קירוב $\frac{1}{2}$.

לבנות רדוקציה מ-VC לבעיה על היפרגרפים, כולל הטיפול בכיוון ההפוך שבו יש להחליף קודקודים חדשים בישנים.

להכליל את אלגוריתם ה-2-קירוב ל-VC לכל r, ולנתח אותו במלואו.

להשתמש באלגוריתם קיים כתת-שגרה ולהוסיף עליו שלב יחיד, כולל חשבון מלא של מה שהשלב הנוסף עולה ביחס הקירוב.

להוכיח תוצאת אי-קירוב מותנית בתבנית "מניחים אלגוריתם קירוב $\Rightarrow$ מכריעים בעיה NP-קשה $\Rightarrow \mathrm{P} = \mathrm{NP}$", כולל זיהוי הבעיה ה-NP-קשה הנכונה להתחיל ממנה.

לדעת מתי "בגודל k" ו"בגודל $\leq k$" שקולים ומתי לא.

שאלות שנשארו פתוחות

הכותרת הירוקה בראש עמוד 1 נקראה כ"תרגיל מספר 3", כלומר תרגיל בית 3; שאלות 1, 2 ו-6 של אותו תרגיל בית אינן מופיעות בשמונת העמודים.

עמוד 1 בסיכום, שורת זמן הריצה: הסימן שאחרי $O(|E|)$ נקרא בקושי ופורש כאן כ-$O(|G|)$, כלומר פולינומי בגודל הקלט.

עמוד 4 בסיכום, שלב 2 של האלגוריתם: הסימן בין e ל-xyz אינו חד-משמעי; נקרא כאן כ-$e=\{x,y,z\}\in E$, וזו גם הגרסה שנאמרה בהקלטה ב-[00:54:53].

עמוד 8 בסיכום: המילים בסוגריים אחרי סיום הכיוון הראשון נקראו כ"(כך גם ההיפך)"; הכיוון השני נכתב כאן במלואו לפי ההקלטה ב-[02:10:30].

ההקלטה נפתחת באמצע פתרון תרגיל 3(א) ואין בה פתיחה; החומר שנדחה מהמפגש הקודם (המחלקה C_4) ורדוקציות בזמן מעריכי) אינו מופיע בה כלל, ולכן אינו נכלל בקובץ.

ה-slug "exam-review-3" מתאר את מיקום השיעור בסדרת החזרות ולא את תוכנו; התוכן כולו הוא אלגוריתמי קירוב ותוצאת אי-קירוב אחת, כפי שמופיע ב-title_he.

26 חזרה למבחן ד׳: פתרון מטלה 4 — סגירות BPP לחיתוך, וארבעה אפיונים של המחלקות האקראיות

השיעור האחרון בקורס פותר את מטלה 4: מוכיחים ש-BPP סגורה לחיתוך (עם העצמה מוקדמת ל-9/10, כי $(2/3)^2$ קטן מחצי), ומכריעים ארבע וריאציות על ההגדרה ההסתברותית — שתיים מהן מתגלות כ-RP ו-P, אחת כמחלקת כל השפות, ואחת ככזו ששוויונה ל-NP שקול לשאלה הפתוחה P=NP.

ביטחון: high

בקצרה

זהו **המפגש האחרון של הקורס**, וכולו פתרון תרגילים: מטלה 4, שאלה 1 סעיף (ג) ושאלה 3 על כל סעיפיה. אין בו תיאוריה חדשה — רק שימוש מדויק בהגדרות של שיעורים 16–17.

התוצאה המרכזית: BPP **סגורה לחיתוך**. ההוכחה איננה "נריץ את שתי המכונות ונחזיר AND" בלבד — הצירוף הזה **מכפיל את הסתברויות ההצלחה**, ו-$\left(\frac{2}{3}\right)^2 = \frac{4}{9}$ קטן אפילו מ-$\frac{1}{2}$. לכן חייבים **להעצים קודם** ל-$\mathrm{BPP}\left(\frac{9}{10}, \frac{9}{10}\right)$, ורק אז $\left(\frac{9}{10}\right)^2 = \frac{81}{100} \geq \frac{2}{3}$.

שאלה 3 נותנת ארבע מחלקות $\mathrm{C}_1, \ldots, \mathrm{C}_4$ שכל אחת היא שינוי קטן בהגדרה ההסתברותית, ומבקשת להכריע לכל טענה: **נכונה, שגויה, או שקולה לטענה פתוחה**.

התשובות. $\mathrm{C}_1 = \mathrm{BPP}(\alpha, 1)$, ולכן עבור $\alpha = \frac{1}{10}$ מתקיים $\mathrm{C}_1 = \mathrm{RP}$ — **נכונה**, ישירות מהעצמה חד-צדדית. $\mathrm{C}_2 = \mathrm{BPP}(\alpha, \alpha)$, ולכן עבור $\alpha = \frac{1}{10}$ היא **מחלקת כל השפות** ובפרט $\mathrm{C}_2 \neq \mathrm{BPP}$ — הטענה **שגויה**; אבל עבור $\alpha = 1$ מתקיים $\mathrm{C}_2 = \mathrm{P}$ — **נכונה**.

C_3 היא BPP שבה המחרוזת האקראית באורך **קבוע** 5. עבור $\alpha = \frac{2}{3}$ מתקיים $\mathrm{C}_3 = \mathrm{P}$ — **נכונה**: עוברים על כל 32 המחרוזות ומצביעים רוב. שני התנאים חיוניים: $\alpha > \frac{1}{2}$ (אחרת אין רוב) ואורך קבוע (אחרת זו בדיוק השאלה הפתוחה $\mathrm{P} = \mathrm{BPP}$).

C_4 דורשת הסתברות טעות קטנה מ-$\frac{1}{|\Omega|}$, ולכן **קבוצת ה-r-ים השגויים ריקה** — מכאן $\mathrm{C}_4 = \mathrm{P}$, והטענה "$\mathrm{C}_4 = \mathrm{NP}$" **שקולה לשאלה הפתוחה** $\mathrm{P} = \mathrm{NP}$.

הרעיון החוזר בכל הסעיפים: **תרגמו הסתברות לספירה**. במרחב אחיד סופי $|E| = \Pr[E] \cdot |\Omega|$, וגודל של קבוצה הוא מספר שלם — זה מה שהופך "הסתברות גדולה מספיק" ל"כל האפשרויות" או ל"רוב מוחלט".

הרבע האחרון של ההקלטה [01:19:20]–[01:27:10] הוא **הנחיות המרצה לקראת המבחן**; הן מרוכזות בסעיף האחרון של הקובץ.

אזהרת שמות. המחלקות $\mathrm{C}_1, \ldots, \mathrm{C}_4$ של השיעור הזה הן וריאציות על ההגדרה **ההסתברותית** $\mathrm{BPP}(\alpha, \beta)$. הן **אינן** המחלקות $\mathrm{C}_1, \ldots, \mathrm{C}_5$ של שיעור 24, שהן וריאציות על הגדרת ה-verifier של NP. השמות זהים במקרה — שתי המטלות מספרו את המחלקות שלהן באותו אופן — והתוצאות אינן ניתנות להצלבה.

רקע ותלויות

כל התרגילים כאן נשענים על שיעורים 16 ו-17. להלן כל מה שנשתמש בו, במלואו, כדי שלא תצטרכו לקפוץ.

משפחת המחלקות $\mathrm{BPP}(\alpha,\beta)$ (שיעור 16, הגדרה 3). יהיו $\alpha,\beta\in[0,1]$. $A\in\mathrm{BPP}(\alpha,\beta)$ אם מתקיים אחד משני התנאים השקולים:

נוסח א (מכונה אקראית). קיימת מכונת טיורינג **אקראית** M הרצה בזמן פולינומי בגודל הקלט כך שלכל x: $x\in A \implies \Pr\left[M \text{ accepts } x\right]\geq\alpha, \qquad x\notin A \implies \Pr\left[M \text{ rejects } x\right]\geq\beta.$

נוסח ב (מכונה דטרמיניסטית וסרט אקראי). קיימת מכונת טיורינג **דטרמיניסטית** M הרצה בזמן פולינומי בגודל הקלט וקיים פולינום p כך שלכל x: $x\in A \implies \Pr_{r\in\{0,1\}^{p(|x|)}}\left[M \text{ accepts } (x,r)\right]\geq\alpha, \qquad x\notin A \implies \Pr_{r\in\{0,1\}^{p(|x|)}}\left[M \text{ rejects } (x,r)\right]\geq\beta.$

מרחב ההסתברות. האקראיות היא **אך ורק** המטבעות של המכונה, כלומר $\Omega=\Omega(x)=\{0,1\}^{p(|x|)}$. הקלט x **אינו** אקראי; הוא נתון ושרירותי. המרצה חזר על זה גם השיעור: "שים לב, אקראיות זה משהו שצריך להיכנס באופן מפורש. לא כתבתי פה שאני בוחר את x באקראי" [00:20:21].

השמות (שיעור 16, הגדרה 4). $\mathrm{BPP}=\mathrm{BPP}\left(\frac{2}{3},\frac{2}{3}\right), \qquad \mathrm{RP}=\mathrm{BPP}\left(\frac{1}{2},1\right), \qquad \mathrm{coRP}=\mathrm{BPP}\left(1,\frac{1}{2}\right).$

עוד משיעור 16 שנשתמש בו: מונוטוניות המשפחה (משפט 1), $\mathrm{BPP}\subseteq\mathrm{PSPACE}$ (משפט 4), והעובדה ש-$\mathrm{BPP}\left(\frac{1}{2},\frac{1}{2}\right)$ מכילה **כל** שפה (הערה שאחרי הגדרה 3).

משיעור 17: משפט ההעצמה החד-צדדית (משפט 1) ומשפט ההעצמה הדו-צדדית (משפט 2), וכן הצבעת הרוב (הגדרה 3).

משיעור 2: PSPACE מוגדרת דרך מכונות ש**מכריעות** את השפה, ולכן כל שפה ב-PSPACE היא כריעה; HALT אינה כריעה, ולכן $\mathrm{HALT}\notin\mathrm{PSPACE}$ (ראו שם את אי-הדוגמה שאחרי הגדרה 1).

הגדרות

השאלה מתחילה ב-"יהי $\alpha\in[0,1]$. נגדיר את מחלקות הסיבוכיות הבאות." ארבע ההגדרות מובאות כאן כלשונן בדף המודפס, **פרט לתיקון** $x\mapsto(x,r)$ ב-C_3 ו-C_4 שהמרצה עשה בעצמו בשיעור [00:36:21] ושמופיע גם בכתב יד על גבי העמוד.

הגדרה 1: המחלקות C_1 ו-C_2

C_1 היא מחלקת כל השפות A עבורן קיימת מכונת טיורינג **הסתברותית** M הרצה בזמן פולינומי בגודל הקלט, כך שלכל x: $x\in A \implies \Pr\left[M \text{ accepts } x\right]\geq\alpha, \qquad x\notin A \implies \Pr\left[M \text{ rejects } x\right]=1.$

C_2 היא אותה מחלקה בדיוק, אלא שהתנאי השני מוחלף ב-$\Pr\left[M \text{ rejects } x\right]\geq\alpha$.

התרגום המיידי. על גבי עמוד 3 בסיכום, בצד ההגדרות, כתוב בכתב יד בדיוק זה: $\mathrm{C}_1 = \mathrm{BPP}(\alpha, 1), \qquad \mathrm{C}_2 = \mathrm{BPP}(\alpha, \alpha).$ אחד-לאחד מול נוסח א של הגדרת $\mathrm{BPP}(\alpha, \beta)$. המרצה הקדיש לזה שלב מפורש בפתרון: "השלב הראשון: ברמת ה-pattern matching אני בודק האם זה זהה להגדרה או לא, ואיפה ההבדל" [00:28:33]. עבור C_1 ו-C_2 **אין** הבדל, ולכן "אין לי מה לשחק עם זה יותר" [00:27:31].

אינטואיציה. C_1 היא טעות **חד-צדדית**: על no-instance המכונה לעולם אינה טועה. C_2 היא טעות **דו-צדדית** עם אותו סף בשני הצדדים.

מופע. כל שפה ב-P שייכת ל-C_1 ול-C_2 עבור כל α: המכונה הדטרמיניסטית שמכריעה אותה היא בפרט מכונה אקראית שאינה מטילה מטבעות, וההסתברויות שלה הן $\alpha \geq 1$.

אי-מופע מאלף. עבור $\alpha \leq \frac{1}{2}$ המחלקה C_2 מפסיקה להיות אי-מופע של משהו — היא נהיית **מחלקת כל השפות**. זה בדיוק תוכן סעיף (ב) להלן.

הגדרה 2: המחלקה C_3

C_3 היא מחלקת כל השפות A עבורן קיימת מכונת טיורינג **דטרמיניסטית** M הרצה בזמן פולינומי בגודל הקלט, כך שלכל x: $x \in A \implies \Pr_{r \in \{0,1\}^5}\left[M \text{ accepts } (x, r)\right] \geq \alpha, \qquad x \notin A \implies \Pr_{r \in \{0,1\}^5}\left[M \text{ rejects } (x, r)\right] \geq \alpha.$

מה השתנה. זהו בדיוק **נוסח ב** של $\mathrm{BPP}(\alpha, \alpha)$, אלא שאורך המחרוזת האקראית אינו $p(|x|)$ עבור פולינום כלשהו אלא **הקבוע** 5. לכן מרחב המדגם קבוע: $|\Omega| = 2^5 = 32$, ללא תלות ב-x.

למה המכונה דטרמיניסטית. המרצה הסביר שהבחירה מכוונת: "כשאני רוצה לעבור מ-C_3 ל-P אני רוצה מכונה דטרמיניסטית, אז אני מעדיף שמראש תהיה לי מכונה דטרמיניסטית — ולכן הגדרתי את C_3 עם מכונה דטרמיניסטית. וגם היה לי חשוב להראות שהיא עם חמישה ביטים" [00:37:27].

מופע. $A = \Sigma^*$ שייכת ל-C_3 לכל α: המכונה שמתעלמת מ-r ומקבלת תמיד נותנת הסתברות 1.

אי-מופע. אף שפה **לא כריעה** אינה ב-C_3, כי לפי סעיף (ד) $\mathrm{C}_3 = \mathrm{P}$ כאשר $\alpha = \frac{2}{3}$. שימו לב שזה **לא** נכון ל-C_2 עם $\alpha = \frac{1}{10}$ — ובדיוק שם ההבדל בין השניים.

הגדרה 3: המחלקה C_4

C_4 היא מחלקת כל השפות A עבורן קיימת מכונת טיורינג **דטרמיניסטית** M הרצה בזמן פולינומי בגודל הקלט, כך ש**קיים פולינום** p שעבורו לכל x: $x \in A \implies \Pr_{r \in \{0,1\}^{p(|x|)}}\left[M \text{ accepts } (x, r)\right] \geq 1 - \frac{1}{2^{p(|x|)+1}},$ $x \notin A \implies \Pr_{r \in \{0,1\}^{p(|x|)}}\left[M \text{ rejects } (x, r)\right] \geq 1 - \frac{1}{2^{p(|x|)+1}}.$

הלב של ההגדרה. אותו פולינום p מופיע פעמיים: פעם כאורך המחרוזת האקראית, ופעם במכנה של הסתברות הטעות. סטודנט זיהה את זה בכיתה [00:28:02]: "הפולינומים תלויים אחד בשני — הם מבוטאים אחד באמצעות השני". זה לא קישוט: $|\Omega| = 2^{p(|x|)}$, והסתברות הטעות חסומה ב-$\frac{1}{2|\Omega|} = \frac{1}{2 \cdot 2^{p(|x|)}}$ — כלומר **קטנה מ-**$\frac{1}{|\Omega|}$. משם נובע הכול.

אינטואיציה. "הסתברות ההצלחה גבוהה יותר מ-1 פחות 1 חלקי גודל מרחב המדגם, ולכן אין לי אפילו מספיק הסתברות כדי שיהיה r **אחד** שעליו אני טועה" [01:20:57].

הסעיף הזה מרכז את התוצאות ש**התרגילים נשענים עליהן**. את מה ששיעור קודם הוכיח במלואו אני מנסח כאן במדויק ומפנה אליו, ומוכיח כאן רק את מה שנחוץ ולא הוכח שם.

משפט 1: מונוטוניות במשפחה $\mathrm{BPP}(\alpha,\beta)$ — שיעור 16, משפט 1

ניסוח. אם $\hat{\alpha}\geq\alpha$ ו-$\hat{\beta}\leq\beta$ אז $\mathrm{BPP}(\hat{\alpha},\hat{\beta})\subseteq\mathrm{BPP}(\alpha,\beta)$.

ההוכחה בשורה (המלאה בשיעור 16): **אותה מכונה בדיוק** מקיימת את התנאי החלש יותר, כי $\Pr[\dots]\geq\hat{\alpha}\geq\alpha$. $\square$

משפט 2: העצמה דו-צדדית — שיעור 17, משפט 2

ניסוח. לכל פולינום q: $\mathrm{BPP}=\mathrm{BPP}\left(\frac{1}{2}+\frac{1}{q(n)},\ \frac{1}{2}+\frac{1}{q(n)}\right)=\mathrm{BPP}\left(1-\frac{1}{2^{q(n)}},\ 1-\frac{1}{2^{q(n)}}\right)$.

ההוכחה הכללית עוברת באי-שוויון צ'רנוף ואינה נדרשת בקורס; שיעור 17 הוכיח במלואו את המקרה הפרטי $\mathrm{BPP}=\mathrm{BPP}\left(\frac{4}{5},\frac{4}{5}\right)$ בחישוב בינומי ידני. **מותר ונדרש להשתמש במשפט הזה בשם**, ואפילו במילה אחת: "אמפליפיקציה" [00:11:22].

מסקנה 2.1 — הצורה שנשתמש בה בפועל. $\boxed{\mathrm{BPP}=\mathrm{BPP}\left(\frac{9}{10},\frac{9}{10}\right)}$

הוכחה. נפעיל את משפט 2 עם הפולינום הקבוע $q\equiv 4$ ונקבל $\mathrm{BPP}=\mathrm{BPP}\left(\frac{15}{16},\frac{15}{16}\right)$. כעת שרשרת שתי הכלות ממשפט 1: $\mathrm{BPP}\left(\frac{15}{16},\frac{15}{16}\right)\subseteq\mathrm{BPP}\left(\frac{9}{10},\frac{9}{10}\right)\subseteq\mathrm{BPP}\left(\frac{2}{3},\frac{2}{3}\right)=\mathrm{BPP}$, הראשונה כי $\frac{9}{10}\geq\frac{15}{16}=0.9375$, והשנייה כי $\frac{9}{10}\geq\frac{2}{3}$. האגף השמאלי ביותר שווה ל-BPP, ולכן כל ההכלות בשרשרת הן שוויונות. $\blacksquare$

> **הערה:** בהרצה זה נאמר בקיצור — "ממשפט מהשיעור, A ו-B שייכות ל-BPP תשע עשיריות תשע עשיריות. סתם זרקתי מספר" [00:11:22]. הפירוט כאן הוא ההצדקה למה מותר "לזרוק מספר", ולמה דווקא מספר כזה.

משפט 3: $\mathrm{HALT}\notin\mathrm{BPP}$

ניסוח. בעיית העצירה אינה שייכת ל-BPP.

הוכחה. לפי שיעור 16, משפט 4, $\mathrm{BPP}\subseteq\mathrm{PSPACE}$. לפי הגדרת PSPACE (שיעור 2, הגדרות 1 ו-4), כל שפה בה **מוכרעת** על ידי מכונה דטרמיניסטית שעוצרת על כל קלט; בפרט כל שפה ב-PSPACE היא כריעה. HALT אינה כריעה, ולכן $\mathrm{HALT}\notin\mathrm{PSPACE}$, ולכן $\mathrm{HALT}\notin\mathrm{BPP}$. $\blacksquare$

למה HALT ולא משהו אחר. המרצה ציין שיש עוד המון אפשרויות — "BPP מוכלת ב-PSPACE, אני יכול לקחת שפה ב-$\mathrm{EXPSPACE}$ שאינה ב-PSPACE" — "אבל HALT תמיד מאוד נוחה בקטע הזה, כי אני יודע וברור שהיא לא שייכת" [00:31:07]. וכלל אצבע: "תמיד יותר קל לי להראות אי-שייכות למחלקות **דטרמיניסטיות**" [00:31:38].

משפט 4: העצמה חד-צדדית — שיעור 17, משפט 1

ניסוח. לכל פולינום q מתקיים $\mathrm{RP}=\mathrm{BPP}\left(\frac{1}{q(n)},1\right)$.

מה המשפט אומר. בטעות **חד-צדדית**, הסתברות ההצלחה בצד ה-yes יכולה להיות קטנה כרצוננו — ובלבד שהיא לפחות $1/\mathrm{poly}$ — והמחלקה לא משתנה. ההוכחה המלאה בשיעור 17: מריצים $q(|x|)$ פעמים בלתי-תלויות ומקבלים אם התקבל accept **ולו פעם אחת**; הכלל הזה חוקי בדיוק מפני

שבצד ה-no אין טעות כלל, ולכן accept אחד הוא **הוכחה** ולא עדות סטטיסטית.
מסקנה 4.1. עם הפולינום הקבוע $q \equiv 10$: $\mathrm{BPP}\left(\frac{1}{10}, 1\right) = \mathrm{RP}$. □
משפט 5: מהסתברות לספירה במרחב אחיד סופי
ניסוח. יהי Ω מרחב מדגם סופי עם התפלגות אחידה, ותהי $E \subseteq \Omega$. אזי $|E| = \Pr[E] \cdot |\Omega|$.
הוכחה. התפלגות אחידה מוגדרת על ידי $\Pr[E] = \frac{|E|}{|\Omega|}$; כפל בשני האגפים ב-$|\Omega|$ נותן את הטענה. ■

> **הערה:** סטודנט שאל בכיתה "האם יש משפט שאומר שהגודל של הקבוצה הוא כמות המאורעות כפול ההסתברות?" והתשובה הייתה: "זה לא משפט. זו **ההגדרה** של התפלגות אחידה" [01:18:49]. הפורמליות הזאת נראית זניחה, אבל היא הצעד היחיד בכל שלושת הסעיפים (ג), (ד) ו-(ה) שבו עוברים מעולם ההסתברות לעולם הקומבינטורי — ובלעדיו אין הוכחה.

מסקנה 5.1 (הכלי שנשתמש בו פעמיים). אם $\Pr[E] < \frac{1}{|\Omega|}$ אז $E = \emptyset$. אכן, $|E| = \Pr[E] \cdot |\Omega| < 1$, ו-$|E|$ הוא מספר שלם אי-שלילי, ולכן $|E| = 0$. □

דוגמאות ותרגילים מהשיעור
תרגיל 1, סעיף (ג): לכל $A, B \in \mathrm{BPP}$ מתקיים $A \cap B \in \mathrm{BPP}$
הניסוח כפי שנתון. *"הוכיחו את הטענות הבאות. (ג) לכל $A, B \in \mathrm{BPP}$ מתקיים $A \cap B \in \mathrm{BPP}$".*
הניסיון הראשון, שנכשל — ולמה חשוב לראות אותו
השיעור התחיל בדיוק כמו שסטודנט היה מתחיל: פותחים את ההגדרה עם הקבועים המקוריים $\frac{2}{3}$, בונים את המכונה הטבעית "הרץ את שתיהן וקבל אם שתיהן קיבלו", ואז מגיעים לניתוח הסמנטי ומקבלים $\Pr[M \text{ accepts } x] = \left(\frac{2}{3}\right)^2 = \frac{4}{9}$. זה לצערנו לא מספיק טוב. זה קטן ממש משני שליש — זה אפילו קטן מחצי" [00:10:10]. כלומר המכונה שבנינו גרועה ממטבע.
השלב הבא הוא הלקח המתודי המרכזי של השיעור [00:14:07]: **חוזרים אחורה ומחפשים איפה נשארה חירות שלא נוצלה.** החירות היא ההעצמה — לא היינו חייבים להתחיל מ-$\frac{2}{3}$. "לא להיבהל מזה. הוכחה, כשאני מתכנן אותה, יכולה להיות הרבה קדימה ואחורה."
כמה בדיוק צריך? נדרש $\alpha^2 \geq \frac{2}{3}$, כלומר $\alpha \geq \sqrt{2/3} \approx 0.8165$. שימו לב שאפילו $\frac{4}{5}$ **אינו מספיק**: $\left(\frac{4}{5}\right)^2 = \frac{16}{25} = 0.64 < \frac{2}{3}$ (אם כי כן גדול מ-$\frac{1}{2}$). $\frac{9}{10}$ עובד, ובנוחות: $\left(\frac{9}{10}\right)^2 = \frac{81}{100} = 0.81 \geq \frac{2}{3}$.
ההוכחה המלאה
תהיינה $A, B \in \mathrm{BPP}$.
שלב 0 — העצמה. לפי מסקנה 2.1, $\mathrm{BPP} = \mathrm{BPP}\left(\frac{9}{10}, \frac{9}{10}\right)$, ולכן $A, B \in \mathrm{BPP}\left(\frac{9}{10}, \frac{9}{10}\right)$.
שלב 1 — פתיחת ההגדרות. לפי נוסח א, קיימת מכונה אקראית M_A הרצה בזמן פולינומי בגודל הקלט, כך שלכל x: $x \in A \implies \Pr\left[M_A \text{ accepts } x\right] \geq \frac{9}{10}, \qquad x \notin A \implies \Pr\left[M_A \text{ rejects } x\right] \geq \frac{9}{10}$. כמו כן קיימת מכונה אקראית M_B הרצה בזמן פולינומי בגודל הקלט,

כך שלכל x: $x \in B \implies \Pr\left[M_B \text{ accepts } x\right] \geq \frac{9}{10}$, $\quad x \notin B \implies \Pr\left[M_B \text{ rejects } x\right] \geq \frac{9}{10}$.

שלב 2 — הבנייה. נבנה מכונה M באופן הבא. על קלט x:

הרץ את M_A על x.

הרץ את M_B על x, **באופן בלתי תלוי בשלב 1**.

אם M_A קיבלה את x וגם M_B קיבלה את x — קבל; אחרת — דחה.

שלב 3 — ניתוח זמן ריצה. יהי x. זמן הריצה של M_A על x פולינומי ב-$|x|$; זמן הריצה של M_B על x פולינומי ב-$|x|$; שלב 3 הוא השוואה בעלות $O(1)$. סכום של שני פולינומים הוא פולינום, ולכן $\text{time}_M(x)$ פולינומי ב-$|x|$.

שלב 4 — ניתוח סמנטי. יהי x.

מקרה א: $x \in A \cap B$. אז $x \in A$ וגם $x \in B$, ולכן $\Pr\left[M_A \text{ accepts } x\right] \geq \frac{9}{10}$, $\quad \Pr\left[M_B \text{ accepts } x\right] \geq \frac{9}{10}$. לפי שלב 3 בבנייה, M מקבלת את x אם ורק אם M_A מקבלת את x **וגם** M_B מקבלת את x. לכן $\Pr\left[M \text{ accepts } x\right] = \Pr\left[M_A \text{ accepts } x \ \wedge \ M_B \text{ accepts } x\right] = \Pr\left[M_A \text{ accepts } x\right] \cdot \Pr\left[M_B \text{ accepts } x\right] \geq \left(\frac{9}{10}\right)^2 = \frac{81}{100} \geq \frac{2}{3}$.

המעבר האמצעי — פירוק המכפלה — **חוקי בזכות שלב 2 בבנייה בלבד**: שתי ההרצות משתמשות בסיביות אקראיות טריות, ולכן שני המאורעות בלתי תלויים.

חשבון תקציב הטעות, במפורש. הסתברות הטעות של M על yes-instance היא $1 - \frac{81}{100} = \frac{19}{100} = 0.19 \leq \frac{1}{3}$. לחלופין, בלי להיעזר באי-תלות כלל, חסם האיחוד נותן $\Pr\left[M \text{ rejects } x\right] = \Pr\left[M_A \text{ rejects } x \ \vee \ M_B \text{ rejects } x\right] \leq \Pr\left[M_A \text{ rejects } x\right] + \Pr\left[M_B \text{ rejects } x\right] \leq \frac{1}{10} + \frac{1}{10} = \frac{1}{5} \leq \frac{1}{3}$. זה הלב הכמותי של כל הסעיף: **הצירוף מכפיל את הסתברויות ההצלחה ולכן מחבר את הסתברויות הטעות.** עם $\frac{2}{3}$ מקבלים תקציב טעות $\frac{2}{3} = \frac{1}{3} + \frac{1}{3}$ — יותר מהכול, ולכן שום דבר. עם $\frac{9}{10}$ מקבלים תקציב $\frac{1}{5}$, ונשאר מרווח. ההעצמה היא בדיוק הכלי שקונה את המרווח הזה.

מקרה ב: $x \notin A \cap B$. אז $x \notin A$ **או** $x \notin B$. זו טענת "או", והיא **משרה** את החלוקה למקרים.

מקרה ב.1: $x \notin A$. אז $\Pr\left[M_A \text{ rejects } x\right] \geq \frac{9}{10}$. לפי שלב 3 בבנייה ולפי דה-מורגן, M דוחה את x אם ורק אם M_A דוחה את x **או** M_B דוחה את x. לכן $\Pr\left[M \text{ rejects } x\right] = \Pr\left[M_A \text{ rejects } x \ \vee \ M_B \text{ rejects } x\right] \geq \Pr\left[M_A \text{ rejects } x\right] \geq \frac{9}{10} \geq \frac{2}{3}$. אי-השוויון הראשון הוא **מונוטוניות ההסתברות**: המאורע $\{M_A \text{ rejects } x\}$ **מוכל** במאורע $\{M_A \text{ rejects } x \vee M_B \text{ rejects } x\}$, ואם $E \subseteq F$ אז $\Pr[E] \leq \Pr[F]$. במקרה הזה **אין צורך באי-תלות כלל**.

מקרה ב.2: $x \notin B$. בדומה, בהחלפת התפקידים $A \leftrightarrow B$ ו-$M_A \leftrightarrow M_B$ בלבד: $\Pr\left[M \text{ rejects } x\right] \geq \Pr\left[M_B \text{ rejects } x\right] \geq \frac{9}{10} \geq \frac{2}{3}$.

בשני המקרים $\Pr[M \text{ rejects } x] \geq \frac{2}{3}$.

מסקנה. M היא מכונה אקראית פולינומית שמקיימת את שני תנאי $\text{BPP}\left(\frac{2}{3}, \frac{2}{3}\right)$ עבור $A \cap B$, ולכן $A \cap B \in \text{BPP}$. ■

שלוש הערות שנולדו משאלות בכיתה

(1) "מי אמר שאין תלות?" [00:08:29]. אי-תלות אינה מתנה — צריך **לבנות** אותה ולציין אותה. התשובה: "תמיד אפשר, כי אני פשוט לוקח source של אקראיות ומושך ממנו מחדש" [00:09:04]. ולכן המילים "באופן בלתי תלוי" בשלב 2 אינן קישוט; בלעדיהן שלב הכפל בניתוח הסמנטי אינו מוצדק.

(2) למה רק בשלב 2 כתוב "באופן בלתי תלוי"? [00:16:44]. כי M_A רצה **ראשונה** ואין לה במה להיות תלויה. המודל שהמרצה נתן: "תחשבו על האקראיות כאילו יש לי מטבעות. האלגוריתם כל פעם מטיל מטבע, ואני אומר ל-M_B: תתעלמי מכל המטבעות שהוטלו עד עכשיו — צריכה מטבע? תטילי מטבע חדש" [00:17:15]. מבחינה **הסתברותית** התמונה סימטרית, אבל מבחינה **אלגוריתמית** יש סדר ביצוע, וההערה שייכת למקום שבו התלות הייתה יכולה להיווצר.

(3) הווריאציה עם קיצור דרך. סטודנט הציע לנסח את המכונה כ-"הרץ את M_A; אם דחתה — דחה; אחרת הרץ את M_B והחזר את תשובתה" [00:14:07]. המרצה: "בעיקרון הניתוח יעבוד, אבל אתה צודק שהייתי מעדיף לעשות ככה." ההצדקה: אפשר לחשוב שתיאורטית מריצים את שתיהן מראש, והמכונה פשוט לא משתמשת בהרצה השנייה — ההתפלגות אינה משתנה. "זה לא באמת משפיע על הניתוח ההסתברותי, אבל **יותר קשה לראות את זה**" [00:15:42]. המסקנה המעשית: במבחן, נסחו את הבנייה בצורה שהניתוח שלה מיידי.

(4) "אפשר במקום להעצים פשוט להריץ הרבה פעמים?" [00:15:42]. אפשר — אבל אז אתם מוכיחים את משפט ההעצמה מחדש בידיים. "אני מעדיף להימנע, אם יש לי את זה כבר מוכן. זה בעצם השלב שהכנסתי לתוך קופסה שחורה" [00:16:14].

תרגיל 3: פתיחה — איך ניגשים לארבע המחלקות

לפני כל סעיף, המרצה עשה שלב שהוא שווה תרגיל בפני עצמו: **סריקה של ארבע ההגדרות מול ההגדרות המוכרות, בלי לטעון דבר** [00:27:01]–[00:29:05].

מחלקה	היחס להגדרה המוכרת	ההבדל
C_1	$= \mathrm{BPP}(\alpha, 1)$	אין הבדל — התאמה אחד-לאחד
C_2	$= \mathrm{BPP}(\alpha, \alpha)$	אין הבדל — התאמה אחד-לאחד
C_3	דומה ל-$\mathrm{BPP}(\alpha, \alpha)$ נוסח ב	אורך r **קבוע** (5) ולא $p(\|x\|)$
C_4	דומה ל-BPP נוסח ב	הסף אינו קבוע, **ואותו** p מופיע באורך r ובמכנה הטעות

"עכשיו אני יודע ש-C_3 ו-C_4 אינן זהות להגדרות של BPP בשום צורה ועם שום הסתברויות, ואני יודע גם **איפה** ההבדל. עכשיו השאלה מה אני יכול להגיד על זה" [00:29:05].

תרגיל 3, סעיף (א): אם $\alpha = \frac{1}{10}$ אז $\mathrm{C}_1 = \mathrm{RP}$ — **נכונה**

פתרון. לפי הגדרה 1, $\mathrm{C}_1 = \mathrm{BPP}\left(\frac{1}{10}, 1\right)$. לפי משפט 4 (שיעור 17, משפט 1) עם הפולינום הקבוע $q \equiv 10$: $\mathrm{BPP}\left(\frac{1}{10}, 1\right) = \mathrm{RP}.$ ■

זהו כל הפתרון. "הטענה נכונה. למה? כי הוכחנו אותה בשיעור. במילה אחת: **אמפליפיקציה**" [00:29:36]. סעיף זה נפתר בעל פה בלבד ואינו בסיכום.

ההרחבה שהמרצה נתן. בטעות **חד-צדדית** אפשר להעצים גם מהסתברות הצלחה זעירה: "אם זה היה $\mathrm{BPP}\left(\frac{1}{n},1\right)$ זה עדיין היה RP, כי הטעות חד-צדדית" [00:30:07]. לעומת זאת בטעות **דו-צדדית** נדרש ששני הצדדים יהיו גדולים מ-$\frac{1}{2}$ **באופן משמעותי** — "חצי ועוד 1 חלקי פולינום; זה לא יכול להיות חצי ועוד $\frac{1}{2^n}$" [00:30:07]. ההבדל הזה הוא בדיוק ההבדל בין משפט 4 למשפט 2, והוא הנקודה שהסעיפים (א) ו-(ב) בונים עליה יחד.

תרגיל 3, סעיף (ב): אם $\alpha = \frac{1}{10}$ אז $\mathrm{C}_2 = \mathrm{BPP}$ — **שגויה**

זהו הסעיף הראשון שנפתר בכתב, בעמוד 3 בסיכום.

מה צריך להראות. אי-שוויון בין קבוצות, כלומר: **שפה השייכת לאחת ולא לשנייה** [00:31:07]. הכיוון הנוח הוא למצוא שפה ב-C_2 שאינה ב-BPP.

נתבונן ב-HALT.

חלק ראשון: $\mathrm{HALT} \notin \mathrm{BPP}$. זה משפט 3 לעיל: $\mathrm{HALT} \notin \mathrm{PSPACE}$ ולכן $\mathrm{HALT} \notin \mathrm{BPP}$.

חלק שני: $\mathrm{HALT} \in \mathrm{C}_2$. נגדיר מכונה אקראית M באופן הבא. על קלט x:

הגרל $r \in \{0,1\}$ באופן אחיד.

אם $r = 1$ — קבל; אחרת — דחה.

זמן ריצה. M מטילה מטבע אחד ומחליטה; זמן הריצה שלה **קבוע**, ובפרט פולינומי ב-$|x|$.

ניתוח סמנטי. יהי x.

אם $x \in \mathrm{HALT}$: $\Pr\left[M \text{ accepts } x\right] = \frac{1}{2} \geq \frac{1}{10}$.

אם $x \notin \mathrm{HALT}$: $\Pr\left[M \text{ rejects } x\right] = \frac{1}{2} \geq \frac{1}{10}$.

שני התנאים של C_2 עם $\alpha = \frac{1}{10}$ מתקיימים, ולכן $\mathrm{HALT} \in \mathrm{C}_2$.

מסקנה. $\mathrm{HALT} \in \mathrm{C}_2 \setminus \mathrm{BPP}$, ולכן $\mathrm{C}_2 \neq \mathrm{BPP}$. הטענה **שגויה**. ■

מה באמת קרה כאן. המכונה M **אפילו לא מסתכלת בקלט**. הניסוח של המרצה: "אם הסתברות ההצלחה היא סך הכול גדולה שווה עשירית — I might as well flip a coin" [00:34:48]. למעשה ההוכחה מראה יותר מהנדרש: **לכל** שפה A (ולא רק HALT) אותה מכונה מוכיחה $A \in \mathrm{C}_2$, ולכן עבור כל $\alpha \leq \frac{1}{2}$ המחלקה $\mathrm{C}_2 = \mathrm{BPP}(\alpha,\alpha)$ היא **מחלקת כל השפות** — בדיוק כפי ששיעור 16 ציין עבור $\mathrm{BPP}\left(\frac{1}{2},\frac{1}{2}\right)$.

> **הערה על אנלוגיה שהמרצה הזכיר.** ב-[00:34:48] הוא ציין ש"זה מאוד מזכיר את מה שעשינו עם NP בפעם הקודמת, עם ה'קיים וקיים'" — שם גם כן מחלקה שנראתה כמו NP התגלתה כמחלקת כל השפות, ו-HALT שימשה כעד. זו אנלוגיה **מתודית** בלבד; המחלקה ההיא (שיעור 24) היא אובייקט אחר לגמרי, ואין להצליב את התוצאות.

תרגיל 3, סעיף (ג): אם $\alpha = 1$ אז $\mathrm{C}_2 = \mathrm{P}$ — **נכונה**

סעיף זה נפתר בעל פה [00:35:19]–[00:36:21] ואינו בסיכום. $\mathrm{C}_2 = \mathrm{BPP}(1,1)$.

כיוון $\mathrm{C}_2 \subseteq \mathrm{P}$. תהא $A \in \mathrm{BPP}(1,1)$. לפי **נוסח ב** קיימת מכונה דטרמיניסטית M_A הרצה בזמן פולינומי וקיים פולינום p כך שלכל x: $x \in A \implies \Pr_{r \in \{0,1\}^{p(|x|)}}\left[M_A \text{ accepts } (x,r)\right] \geq 1$, $\quad x \notin A \implies \Pr_{r \in \{0,1\}^{p(|x|)}}\left[M_A \text{ rejects } (x,r)\right] \geq 1$. הסתברות אינה עולה על 1, ולכן

אלה **שוויונות**. במרחב אחיד סופי, מאורע בהסתברות 1 הוא כל המרחב (משפט 5 עם המשלים): קבוצת ה-r-ים שעליהם המכונה טועה היא בגודל $0 \cdot 2^{p(|x|)} = 0$, כלומר ריקה. לכן **לכל** $r \in \{0,1\}^{p(|x|)}$ המכונה M_A עונה נכון על (x, r).

נבנה מכונה דטרמיניסטית M. על קלט x:

חשב $p(|x|)$ וכתוב $r = 0^{p(|x|)}$.

הרץ את M_A על (x, r) והחזר את תשובתה.

זמן ריצה. p פולינום קבוע וניתן לחישוב בזמן פולינומי, וכתיבת $0^{p(|x|)}$ אורכת $O(p(|x|))$; הרצת M_A על (x, r) פולינומית ב-$|x| + p(|x|)$, שהוא פולינומי ב-$|x|$. לכן $\mathrm{time}_M(x)$ פולינומי ב-$|x|$.

ניתוח סמנטי. לפי הקודם M_A צודקת על **כל** r, ובפרט על $r = 0^{p(|x|)}$. לכן M מקבלת את x אם ורק אם $x \in A$, כלומר M מכריעה את A בזמן פולינומי, ולכן $A \in \mathrm{P}$. $\square$

כיוון $\mathrm{P} \subseteq \mathrm{C}_2$**.** תהא $A \in \mathrm{P}$ ותהי M_A מכונה דטרמיניסטית פולינומית שמכריעה אותה. היא בפרט מכונה **אקראית** שאינה מטילה אף מטבע, ולכן לכל x: אם $x \in A$ אז $\Pr[M_A \text{ accepts } x] = 1$, ואם $x \notin A$ אז $\Pr[M_A \text{ rejects } x] = 1$. שני התנאים של $\mathrm{BPP}(1,1)$ מתקיימים, ולכן $A \in \mathrm{C}_2$. $\square$

מכאן $\mathrm{C}_2 = \mathrm{P}$. $\blacksquare$

הניסוח של המרצה [00:36:21]: "אם הסתברות ההצלחה היא אחת, גם בדחייה וגם בקבלה — היא תמיד צודקת. איך אני מראה שזה P? אני בונה מכונה דטרמיניסטית שפשוט מכניסה למכונה האקראית **מחרוזת אקראית קבועה**, ובגלל שהסתברות ההצלחה היא אחת אני יודע שזה יחזיר את התשובה הנכונה."

תרגיל 3, סעיף (ד): אם $\alpha = \frac{2}{3}$ אז $\mathrm{C}_3 = \mathrm{P}$ — **נכונה**

זהו הסעיף הארוך בסיכום (עמודים 4–5) ובהקלטה [00:45:18]–[01:10:14].

כיוון ראשון: $\mathrm{C}_3 \subseteq \mathrm{P}$

תהא $A \in \mathrm{C}_3$. אזי קיימת מכונת טיורינג **דטרמיניסטית** M_A הרצה בזמן פולינומי בגודל הקלט, כך שלכל x: $x \in A \implies \Pr_{r \in \{0,1\}^5}\left[M_A \text{ accepts } (x,r)\right] \geq \frac{2}{3}$, $\quad x \notin A \implies \Pr_{r \in \{0,1\}^5}\left[M_A \text{ rejects } (x,r)\right] \geq \frac{2}{3}$.

נבנה מכונה **דטרמיניסטית** M באופן הבא. על קלט x:

לכל $r \in \{0,1\}^5$: 1.1. הרץ את M_A על (x, r).

החזר את התשובה של M_A שחזרה על עצמה הכי הרבה פעמים (**הצבעת רוב**).

ניתוח זמן ריצה. בהרצת M על x, מספר האיטרציות בלולאה הוא $|\{0,1\}^5| = 2^5 = 32$ — **קבוע**, שאינו תלוי ב-x, כי אורך r קבוע. זמן הריצה של כל איטרציה: M_A רצה על (x, r) שאורכו $|x| + 5$, ולכן פולינומי ב-$|x|$. ניהול שני המונים עולה $O(1)$ לאיטרציה. לכן $\mathrm{time}_M(x) \leq 32 \cdot \mathrm{poly}(|x|) + O(1) = \mathrm{poly}(|x|)$.

> **הערה:** בהרצה הנקודה הזאת עוררה ויכוח קצר [00:50:18]: "זמן קבוע?" — "לא, הזמן אינו קבוע, כי אני מריץ את המכונה על כל r, והמכונה רצה בזמן פולינומי. **מספר האיטרציות** הוא הקבוע." הבחנה קטנה, אבל היא בדיוק ההבדל בין טענה נכונה לטענה שגויה.

ניתוח סמנטי. יהי x.

מקרה א: $x \in A$. אז $\Pr_{r\in\{0,1\}^5}\left[M_A \text{ accepts } (x,r)\right] \geq \frac{2}{3}$. כאן עוברים מהסתברות לקומבינטוריקה (משפט 5), כי r נדגם אחיד ממרחב בגודל 32: $\left|\left\{r \in \{0,1\}^5 \ : \ M_A \text{ accepts } (x,r)\right\}\right| = \Pr_r\left[M_A \text{ accepts } (x,r)\right] \cdot 32 \geq \frac{2}{3} \cdot 32 = \frac{64}{3} > 16.$
בסך הכול יש 32 מחרוזות, ויותר מ-16 מהן מובילות ל-accept; לכן accept היא **הרוב המוחלט**, ולכן M מקבלת את x.

מקרה ב: $x \notin A$. בדומה, בהחלפת accept ב-reject: $\left|\left\{r \in \{0,1\}^5 \ : \ M_A \text{ rejects } (x,r)\right\}\right| \geq \frac{2}{3} \cdot 32 > 16,$
ולכן reject היא הרוב המוחלט ו-M דוחה את x.
לכן M מכריעה את A בזמן פולינומי, כלומר $A \in \mathrm{P}$. $\square$
כיוון שני: $\mathrm{P} \subseteq \mathrm{C}_3$
תהא $A \in \mathrm{P}$. אזי קיימת מכונה דטרמיניסטית M_A שמכריעה את A בזמן פולינומי בגודל הקלט.
נבנה מכונה דטרמיניסטית M **שהקלט שלה הוא הזוג** (x,r):
הרץ את M_A על x והחזר את אותה תשובה (התעלם מ-r).
ניתוח זמן ריצה. בריצתה על (x,r), M מריצה את M_A על x; זמן הריצה פולינומי ב-$|x|$, ובפרט פולינומי ב-$|(x,r)| = |x| + 5$.
ניתוח סמנטי. יהי x.
אם $x \in A$: M_A מקבלת את x, ולכן M מקבלת את (x,r) עבור **כל** r, ומכאן $\Pr_{r\in\{0,1\}^5}\left[M \text{ accepts } (x,r)\right] = 1 \geq \frac{2}{3}$.
אם $x \notin A$: M_A דוחה את x, ולכן M דוחה את (x,r) עבור כל r, ומכאן $\Pr_{r\in\{0,1\}^5}\left[M \text{ rejects } (x,r)\right] = 1 \geq \frac{2}{3}$.
לכן $A \in \mathrm{C}_3$. $\square$
משני הכיוונים: $\mathrm{C}_3 = \mathrm{P}$. $\blacksquare$
ארבע מלכודות בסעיף הזה, כולן מההקלטה
(1) הממשק — המלכודת המרכזית [01:04:12], [01:05:19]. בכיוון $\mathrm{P} \subseteq \mathrm{C}_3$ מפתה לכתוב "נתבונן ב-M_A עצמה". זה **שגוי**. "האינטרפייס שלה עם העולם הוא לא האינטרפייס הנכון. אני חייב מכונה שהקלט שלה הוא הזוג" — הגדרת C_3 מדברת על $\Pr_r[M \text{ accepts } (x,r)]$, ולכן M **חייבת** לקבל (x,r). "הקלט של M צריך להיות x ו-r. זה החזות של המחלקה הזאת. על זה לא ליפול."
(2) "יהי x" ולא "יהי (x,r)" [01:07:32]. בניתוח הסמנטי של הכיוון השני, מה הכמת הראשון? "תשימו לב להגדרה של C_3: כתוב **לכל** x. אז אם אני רוצה להוכיח ש-$A \in \mathrm{C}_3$ אני אתחיל ב'יהי x' ולא ב'יהי x ו-r'. בסופו של דבר הכול חוזר להגדרה; השאלה היא רק על איזו הגדרה להסתכל."
(3) למה $\alpha > \frac{1}{2}$ הכרחי [00:42:41]–[00:45:18]. סטודנט שאל אם ל-α יש בכלל משמעות. יש — **הוא חייב להיות גדול מחצי**, אחרת אין רוב. נניח $\alpha = \frac{1}{10}$: כל מה שנתון הוא שהתשובה הנכונה חוזרת לפחות ב-$\frac{1}{10}$ מהמקרים. "היא יכולה להיות עשירית, היא יכולה להיות שלושת רבעי — אני לא יודע. אני לא יודע אם היא יותר מחצי או פחות מחצי." ולכן:
כלל "קבל אם קיים r אחד שמקבל" אינו עובד בטעות דו-צדדית: גם על $x \notin A$ קיימת הסתברות חיובית ש-M_A תקבל, ואז תיפול על אותו r ותטעה.

כלל הרוב עובד רק כאשר $\alpha > \frac{1}{2}$: אז "התשובה הנכונה תחזור על עצמה לפחות שני שלישים מהפעמים, ולכן היא **בהכרח** תהיה התשובה שחזרה הכי הרבה פעמים."

הערה מעניינת [00:45:18]: אילו היה נתון ש-ההסתברות שווה **בדיוק** $\frac{1}{10}$, אפשר היה לקחת את התשובה שחזרה **הכי מעט** פעמים — כלומר לעשות flip — ולקבל הסתברות הצלחה $\frac{9}{10}$. "בשוויון, ה-1 פחות נשאר עם שוויון; ב-'גדול שווה' ה-1 פחות הופך ל-'קטן שווה'." זה בדיוק המקום שבו כמת $\geq$ הורס את הטיעון.

(4) למה אורך r **הקבוע הכרחי, ומה בדיוק הגבול** [00:51:24]–[00:52:59]. שאלת סטודנט: מה היה קורה אילו $|r|$ לא היה קבוע?

אם $|r| = p(|x|)$ **פולינומי:** מספר האיטרציות הוא $2^{p(|x|)}$ — מעריכי, וההוכחה קורסת. ולא במקרה: זו בדיוק הוכחת $\mathrm{BPP} \subseteq \mathrm{PSPACE}$ משיעור 16, ו-"$\mathrm{P} = \mathrm{BPP}$? זו **שאלה פתוחה**."

אם $|r| = c \cdot \log|x|$**:** אז מספר האיטרציות הוא $2^{c \log |x|} = |x|^c$ — פולינומי. מכפלה של פולינום (מספר איטרציות) בפולינום (זמן לאיטרציה) היא פולינום. **ההוכחה עדיין עוברת**, ולכן גם עם אורך אקראיות לוגריתמי המחלקה שווה ל-P.

(5) "קבוע הוא פולינום, אז אפשר להגיד מיד $\mathrm{C}_3 \subseteq \mathrm{BPP}$**?"** [00:55:43]–[00:56:44]. כן, ובצדק: 5 הוא פולינום קבוע, ולכן לפי נוסח ב מתקיים $\mathrm{C}_3 \subseteq \mathrm{BPP}$ ישירות מההגדרה. אבל "כל קבוע הוא פולינום; **לא** כל פולינום הוא קבוע", ולכן ההכלה היא בכיוון אחד בלבד והיא **לא הדוקה**. "הקבוע נותן לי אקסטרה אינפורמציה, ולכן אני יכול להוכיח משהו יותר חזק" — והמשהו החזק הוא $\mathrm{C}_3 = \mathrm{P}$.

(6) קאונטר מפורש מול "רוב" [00:59:31]–[01:01:36]. בשיעור מוקדם יותר בסמסטר, בהוכחה מקבילה, המרצה כתב במפורש מונה והשווה ל-$\frac{2}{3} \cdot 2^{p(|x|)}$; כאן הוא כתב פשוט "החזר את התשובה שחזרה הכי הרבה פעמים". שתי הצורות נכונות. הנימוק להבדל: "אז היה שלב מוקדם יותר בסמסטר ורציתי להדגיש איך אני עושה את זה; שם המספר היה $2^{p(|x|)}$ ורציתי על הדרך להזכיר לכם שאני צריך להיות מסוגל **לחשב** את $p(|x|)$ בזמן ובמקום. עכשיו אנחנו גדולים יותר ואפשר לעשות את זה טיפה יותר אימפליציטית." הכלל שנשאר: כל פונקציה מספרית שאתם מחשבים בתוך בנייה — ודאו שהיא ישימה בזמן ובמקום, ואמרו את זה כשזה מהותי. כאן זה לא: 16 **הוא קבוע**.

תרגיל 3, סעיף (ה): $\mathrm{C}_4 = \mathrm{NP}$ — **שקולה לטענה פתוחה**

סעיף זה נפתר בעל פה [01:10:48]–[01:19:20] ואינו בסיכום.

הטענה שנוכיח. $\mathrm{C}_4 = \mathrm{P}$.

כיוון ראשון: $\mathrm{C}_4 \subseteq \mathrm{P}$

תהא $A \in \mathrm{C}_4$ עם מכונה דטרמיניסטית פולינומית M_A ופולינום p כבהגדרה 3. יהי x, ונסמן $\Omega = \{0,1\}^{p(|x|)}, \quad |\Omega| = 2^{p(|x|)}$, ותהי $E \subseteq \Omega$ קבוצת ה-r-ים שעליהם M_A **טועה** — כלומר דוחה את (x, r) כאשר $x \in A$, או מקבלת את (x, r) כאשר $x \notin A$. הקלט x קבוע, ולכן "מקבלת" ו"דוחה" הם מאורעות משלימים באותו מרחב (שיעור 16, ההערה שאחרי הגדרה 3), ולכן בשני המקרים $\Pr_{r \in \Omega}[r \in E] \leq 1 - \left(1 - \frac{1}{2^{p(|x|)+1}}\right) = \frac{1}{2^{p(|x|)+1}}$. לפי משפט 5: $|E| = \Pr[E] \cdot |\Omega| \leq \frac{1}{2^{p(|x|)+1}} \cdot 2^{p(|x|)} = \frac{1}{2}$, ולכן $|E| = 0$ הוא מספר שלם אי-שלילי שקטן או שווה ל-$\frac{1}{2}$. כלומר: M_A **צודקת על כל** $r \in \Omega$, ללא יוצא מן הכלל (מסקנה 5.1).

לכן נבנה מכונה דטרמיניסטית M. על קלט x:

חשב $p(|x|)$ וכתוב $r = 0^{p(|x|)}$.

הרץ את M_A על (x, r) והחזר את תשובתה.
זמן ריצה. כמו בסעיף (ג): חישוב $p(|x|)$ וכתיבת המחרוזת פולינומיים, והרצת M_A על קלט באורך $|x| + p(|x|)$ פולינומית ב-$|x|$.
ניתוח סמנטי. מהחלק הקודם, M_A צודקת על (x, r) עבור כל r, ובפרט עבור $r = 0^{p(|x|)}$. לכן M מכריעה את A, ומכאן $A \in \mathrm{P}$. $\square$
כיוון שני: $\mathrm{P} \subseteq \mathrm{C}_4$
תהא $A \in \mathrm{P}$ עם מכונה דטרמיניסטית פולינומית M_A שמכריעה אותה. נבחר $p(n) = 1$ ונגדיר מכונה M שעל קלט (x, r) מריצה את M_A על x ומחזירה את תשובתה. אז לכל x, הסתברות התשובה הנכונה היא 1, ובוודאי $1 \geq 1 - \frac{1}{2^{p(|x|)+1}}$. לכן $A \in \mathrm{C}_4$. $\square$
מכאן $\mathrm{C}_4 = \mathrm{P}$.
ומכאן ההכרעה של הטענה
הטענה "$\mathrm{C}_4 = \mathrm{NP}$" שקולה לטענה "$\mathrm{P} = \mathrm{NP}$", שהיא **בעיה פתוחה**. לכן התשובה בסעיף היא: **שקולה לטענה פתוחה**. ■
מה זה לא שקול לו [01:19:54]–[01:20:26]. סטודנט הציע שאולי אפשר לקשור את זה ל-$\mathrm{P} = \mathrm{BPP}$. המרצה: "לא. C_4 הוא P — אין קשר ל-BPP. אתה לא תצליח להראות שזה שקול בלי להראות ש-$\mathrm{P} = \mathrm{BPP}$, ואת זה אני לא יודע." כלומר: ברגע שהראינו $\mathrm{C}_4 = \mathrm{P}$, כל שאלה על C_4 מול מחלקה $\mathcal{D}$ מתורגמת לשאלה "$\mathrm{P} = \mathcal{D}$?" — ולכן צריך לבחור את הבעיה הפתוחה **הנכונה**.
דוגמה: תרגיל הצעצוע שהמרצה הוציא מהחישוב
כדי לבודד את הרעיון של סעיף (ה) מהפרמטרים, המרצה נתן את המקרה הבא [01:14:04]–[01:18:19].
הנתון. תהי $A \subseteq \{1, 2, \ldots, 10\}$ קבוצה **שרירותית** — לא ידוע עליה דבר, והיא **אינה** אקראית. נתון שאם דוגמים x אחיד מ-$\{1, \ldots, 10\}$ אז $\Pr[x \in A] \geq \frac{19}{20}$.
מה אפשר להסיק? ש-$A = \{1, \ldots, 10\}$.
הפתרון. נסמן $B = \{1, \ldots, 10\} \setminus A$. אז $\Pr[x \in B] \leq 1 - \frac{19}{20} = \frac{1}{20}$, ולפי משפט 5 שלם אי-שלילי, ולכן $|B| = 0$, ולכן $A = \{1, \ldots, 10\}$. $|B| \; |B| \; = \; \Pr[x \in B] \cdot 10 \; \leq \; \frac{1}{20} \cdot 10 \; = \; \frac{1}{2}$. ■
ההתאמה לסעיף (ה). $\{0,1\}^{p(|x|)} \leftrightarrow \{1, \ldots, 10\}$, $\frac{1}{2^{p(|x|)+1}} \leftrightarrow \frac{1}{20}$, B קבוצת ה-r-ים השגויים. בשני המקרים החסם על ההסתברות קטן מ-$\frac{1}{|\Omega|}$, ולכן הקבוצה החריגה ריקה.

הערות מהשיעור

[00:02:05] "ברגע שהתחלתי לכתוב אני בתנועה." ההנחיה החוזרת ביותר בשיעור: לכתוב את ההגדרות במלואן, גם את מה שנראה מובן מאליו. "לא להסתפק ב'אוקיי, אני יודע את ההגדרה, אבל איך אני אמשיך?' — ברגע שהתחלתי לכתוב אני בתנועה, ואז אני רק צריך לשמור על אינרציה. לא לדלג על השלב הזה."
[00:14:07] ההוכחה אינה קו ישר. "מה שקרה זה שהתחלתי, נתקעתי, חזרתי אחורה לראות איפה אני יכול לתקן, איפה יש לי עדיין חופש שלא השתמשתי בו. לא להיבהל מזה." זו הסיבה שהוא **בכוונה** התחיל מ-$\frac{2}{3}$ ולא מ-$\frac{9}{10}$.

[00:05:50] "נכונות" מול "ניתוח סמנטי". המרצה מעדיף את המונח "ניתוח סמנטי": "נכונות יכול להיות כל דבר, זה תלוי מה אני רוצה להגיד. ניתוח סמנטי אומר מה אני בעצם רוצה לעשות פה."
[00:18:49] חלוקה למקרים. "כשאתם עושים חלוקה למקרים, תמיד תדאגו לעשות מקרה **בשלילתו** — אלא אם כן החלוקה למקרים מובנית בתוך ההוכחה. ברגע שיש לי טענת **או**, היא משרה לי חלוקה למקרים; אני לא צריך להגיד 'נניח x לא שייך ל-A, נניח x כן שייך ל-A'."
[00:19:51] מה בכלל אקראי כאן. לשאלה "האם צריך לכתוב את ההסתברות בהינתן ש-$x \notin A$?" — "לא, זה לא נתון. הדבר הזה לא אקראי בכלל. הקלט אינו אקראי, הוא שרירותי; השייכות שלו אינה אקראית. זה שאני לא יודע את התשובה לא אומר שזה אקראי. **אקראיות היא משהו שצריך להיכנס באופן מפורש.**"
[00:21:24] מתי צריך אי-תלות ומתי לא. "המקום היחיד שהתלות משחקת בו תפקיד הוא כשאני רוצה **'וגם'** ולכפול. באי-תלות במקרה של האיחוד — היא לא נכנסת בכלל למשחק." לשאלת סטודנט "אבל המאורעות לא זרים" — נכון, ולכן אסור לכתוב סכום; אבל כאן צריך רק ש-$E \subseteq F \Rightarrow \Pr[E] \leq \Pr[F]$, "וזה הוכחנו ביחד".
[00:24:00] מתי מותר לכתוב "בדומה". "אם ההוכחות זהות **עד כדי שינוי אותיות** אתה יכול לכתוב 'בדומה'. כל דבר אחר — תכתוב את ההוכחה." טוב לדעת שאפשר להשתמש בזה במבחן, אם נזהרים.
[00:11:22] האם צריך לצטט את המשפט שהשתמשתם בו. כשמשתמשים במשפט שהוכח בשיעור אין חובה לנקוב בשמו הרשמי, "אבל מה שכן שווה לכתוב, רק כדי לוודא, זה **'אמפליפיקציה'**".
[00:36:21] המרצה מתקן את דף התרגיל שלו. "זו הייתה טעות שלי. ב-C_3 וב-C_4 היה צריך להיות 'M מקבלת את (x, r)' ו-'M דוחה את (x, r)', כי המכונה **דטרמיניסטית** והיא צריכה לקבל את r מבחוץ."
[00:38:30] שתי הדרכים לטפל באקראיות. "יש לי שתי דרכים: אחת — מכונה אקראית, ואז אני משחק עם ההסתברויות; והשנייה — מכונה **דטרמיניסטית** שמקבלת את הקלט האקראי מבחוץ, כלומר אני מעביר את האקראיות החוצה." ולשאלת סטודנטית: "המכונה עם שני הסרטים והסרט האקראי היא בעצם מכונה דטרמיניסטית, ומי שדואג לאקראיות הוא מי שממלא את הסרט השני. אני עושה סוג של **דלגציה** לאקראיות החוצה."
[01:07:32] הכלל שמסכם את כל שאלה 3. "בסופו של דבר הכול חוזר להגדרה. השאלה היא רק על **איזו** הגדרה להסתכל."
[01:21:28] דחייה אינה כישלון. "תחשוב שדחייה זה **הצלחה**. זה מבלבל כי זה נשמע שלילי, אבל דחייה כש-$x \notin A$ היא הצלחה. לא לבלבל בין דחייה לכישלון."
[01:18:19] פורמליות שאינה עולה כלום. על השאלה אם $|E| = \Pr[E] \cdot |\Omega|$ הוא משפט: "זה לא משפט, זו ההגדרה של התפלגות אחידה: $\Pr[A] = \frac{|A|}{|\Omega|}$, ולכן $|A| = \Pr[A] \cdot |\Omega|$."

פערים בין הסיכום להקלטה

מקור: הדף המודפס של שאלה 3, עמוד 3 בסיכום. **הפער:** בהגדרות C_3 ו-C_4 כתוב "M accepts x" ו-"M rejects x", אף שהמכונה דטרמיניסטית וההסתברות נלקחת על פני r. **ההכרעה:** זו טעות שהמרצה תיקן בעצמו בכיתה [00:36:21] ושתוקנה בכתב יד על גבי העמוד; הגוף כאן מביא את

הנוסח המתוקן (x, r) בכל מקום.
מקור: ההקלטה [00:10:10]–[00:13:34] מול עמוד 1 בסיכום. **הפער:** הסיכום מציג את ההוכחה כשהיא כבר מועצמת ל-$\frac{9}{10}$; ההקלטה מראה שהניסיון הראשון היה עם $\frac{2}{3}$ ונכשל ($\left(\frac{2}{3}\right)^2 = \frac{4}{9} < \frac{1}{2}$). **ההכרעה:** הניסיון הכושל נכלל כאן במפורש, כי הוא ההצדקה היחידה לכך שהמספר $\frac{9}{10}$ אינו שרירותי; הוספתי גם את החישוב שמראה ש-$\frac{4}{5}$ אינו מספיק ואת הסף המדויק $\sqrt{2/3}$.
מקור: ההקלטה [00:11:22]. **הפער:** המרצה קרא ל-$\frac{9}{10}$ "סתם זרקתי מספר" ולא הצדיק מאיזה משפט העצמה בדיוק הוא נובע. **ההכרעה:** מסקנה 2.1 כאן מוכיחה $\mathrm{BPP} = \mathrm{BPP}\left(\frac{9}{10}, \frac{9}{10}\right)$ בשתי שורות ממשפט 17.2 עם $q \equiv 4$ וממונוטוניות (16.1).
מקור: ההקלטה [00:31:38]. **הפער:** התמלול האוטומטי מפיל את השלילה וכותב "הלט שייכת ל-PSPACE, לכן הלט לא שייכת ל-BPP" — מה שאינו עקבי בפני עצמו. **ההכרעה:** הסיכום (עמוד 3) כותב את הנוסח הנכון, "$\mathrm{HALT} \notin \mathrm{PSPACE}$ ולכן $\mathrm{HALT} \notin \mathrm{BPP}$", והוא זה שנכתב כאן (משפט 3).
מקור: הסיכום, עמודים 1–2 מול ההקלטה. **הפער:** הסיכום מסתמך על אי-תלות בלבד, ואינו מזכיר את חסם האיחוד. **ההכרעה:** הצגתי את חשבון הטעות בשתי הדרכים — המכפלה $\left(\frac{9}{10}\right)^2$ כמו במקור, וגם חסם האיחוד $\frac{1}{5} = \frac{1}{10} + \frac{1}{10}$, שאינו זקוק לאי-תלות כלל. שתיהן נותנות טעות $\leq \frac{1}{3}$.
מקור: הסיכום, עמוד 1. **הפער:** הסיכום מציין רק "באופן בלתי תלוי" ליד שלב 2, בלי הסבר. **ההכרעה:** ההסבר מההקלטה [00:08:29]–[00:09:37] ו-[00:16:44] נוסף בגוף — כולל מדוע ההערה מיותרת בשלב 1.
מקור: ההקלטה מול הסיכום, כיסוי. **הפער:** בסיכום מופיעים רק שני סעיפים משאלה 3 — (ב) ו-(ד). סעיפים (א), (ג) ו-(ה) נפתרו בעל פה בלבד: (א) ב-[00:29:05], (ג) ב-[00:35:19], (ה) ב-[01:10:48]. **ההכרעה:** שוחזרו מההקלטה ונכתבו כאן במלואם, עם ציון מפורש שאינם בסיכום. הניסוח המילולי המדויק שלהם אינו זמין; ראו `open_questions`.
מקור: ההקלטה, סביב [00:35:50] ו-[00:41:07]. **הפער:** בהקלטה יש בלבול חוזר בין "סעיף ג'" של שאלה 1 לבין "סעיף ג'" של שאלה 3, והמרצה מתקן את עצמו פעמיים. **ההכרעה:** המספור כאן צמוד לשאלה: "תרגיל 1 סעיף (ג)" מול "תרגיל 3 סעיף (ג)".
מקור: הסיכום, עמוד 1 שורה ראשונה. **הפער:** הסיכום נפתח באמצע שאלה 1, ישירות בסעיף (ג); סעיפים (א) ו-(ב) של אותה שאלה אינם בו, וההקלטה מתחילה כשסעיף (ג) כבר על הלוח. **ההכרעה:** לא שוחזרו, ולא הומצאו.
מקור: ההקלטה [00:51:24]–[00:52:59] ו-[00:55:43]–[00:56:44]. **הפער:** שתי הרחבות מהותיות לסעיף (ד) — הגבול $|r| = c \log |x|$, וההכלה הלא-הדוקה $\mathrm{C}_3 \subseteq \mathrm{BPP}$ — אינן בסיכום כלל. **ההכרעה:** נכללו כמלכודות (4) ו-(5) בסעיף התרגיל, כי הן בדיוק סוג ההרחבה שנשאלת במבחן.
מקור: עמוד 6 בסיכום. **הפער:** העמוד ריק לחלוטין. **ההכרעה:** אין ממה לשחזר; לא נכתב עליו דבר.
מקור: קונבנציית הסימון של הקורס (§2a). **הפער:** בעמודים אלה לא מופיעה שום שביעיית מכונה מפורשת, ולכן אין מקום שבו הושמט q_{start}. **ההכרעה:** אין תיקון נדרש; כל שמות המחלקות והבעיות נכתבו כאן ב- (כולל HALT), גם היכן שהסיכום כתב אותם בכתב יד רגיל.

מקור: שמות המחלקות. **הפער:** C_4–C_1 כאן חולקות שם עם C_5–C_1 של שיעור 24, שהן אובייקטים שונים לחלוטין (וריאציות על NP ולא על BPP). **ההכרעה:** נוספה אזהרה בראש הקובץ, וההצלבה היחידה לשיעור 24 היא אנלוגיה מתודית שהמרצה עצמו עשה, המסומנת ככזו במפורש.

סיכום ונקודות למבחן

מה לזכור בעל פה

BPP **סגורה לחיתוך** (וגם לאיחוד ולמשלים, באותה טכניקה) — אבל **רק אחרי העצמה**. הצירוף "וגם" מכפיל הסתברויות הצלחה; $\left(\frac{2}{3}\right)^2 = \frac{4}{9} < \frac{1}{2}$, ואפילו $\left(\frac{4}{5}\right)^2 = 0.64 < \frac{2}{3}$. הסף המדויק הוא $\alpha \geq \sqrt{2/3} \approx 0.8165$, ו-$\frac{9}{10}$ הוא הבחירה הנוחה.

$\mathrm{BPP}(\alpha, 1) = \mathrm{RP}$ **לכל** $\alpha \geq \frac{1}{q(n)}$ (העצמה חד-צדדית, שיעור 17 משפט 1), אבל $\mathrm{BPP}(\alpha, \alpha)$ **עם** $\alpha \leq \frac{1}{2}$ **היא מחלקת כל השפות**. זה ההבדל היחיד והמכריע בין טעות חד-צדדית לדו-צדדית.

$\mathrm{BPP}(1, 1) = \mathrm{P}$: הסתברות 1 במרחב סופי משמעה **כל** r, ולכן אפשר לקבע r שרירותי.

אקראיות באורך קבוע (או לוגריתמי) אינה אקראיות: עוברים על כל המחרוזות ומצביעים רוב, ומקבלים P. אקראיות באורך פולינומי — זו כבר BPP, ו-$\mathrm{P} = \mathrm{BPP}$ פתוחה.

הסתברות טעות קטנה מ-$\frac{1}{|\Omega|}$ **פירושה אפס טעויות.** $|E| = \Pr[E] \cdot |\Omega| < 1$ ו-$|E|$ שלם.

$\mathrm{BPP} \subseteq \mathrm{PSPACE}$**, ולכן כל שפה ב-**$\mathrm{BPP}$ **כריעה**, ולכן HALT היא העד המהיר ביותר לכך שמחלקה כלשהי **אינה** BPP.

מלכודות סטנדרטיות

להריץ שתי מכונות ולשכוח את תקציב הטעות. הבדיקה בת השורה: חשבו את הסתברות הטעות המצטברת ובדקו שהיא $\leq \frac{1}{3}$.

לכפול הסתברויות בלי לומר "בלתי תלוי". שלב הכפל אינו חוקי בלי זה.

לחבר הסתברויות של מאורעות לא זרים. במקרה ה-"או" צריך **מונוטוניות** ($E \subseteq F \Rightarrow \Pr[E] \leq \Pr[F]$) ולא סכום.

ממשק שגוי של המכונה הנבנית. להוכחת שייכות למחלקה שמנוסחת עם $\Pr_r[M(x, r)]$ — המכונה חייבת לקבל את **הזוג**. להוכחת שייכות ל-P — המכונה חייבת לקבל את x **בלבד**, ולכן הלולאה על r נכנסת אליה.

לפתוח ניתוח סמנטי ב-"יהי (x, r)**".** הכמת נקבע על ידי ההגדרה שאתם מוכיחים אליה, וזו כתובה "לכל x".

לחשוב ש-x **אקראי.** האקראיות היא רק המטבעות. x נתון, שרירותי, גרוע ביותר.

להצביע רוב כאשר $\alpha \leq \frac{1}{2}$**.** אין רוב. ולהפך — לקבל על סמך r **אחד** כאשר הטעות דו-צדדית.

לבלבל בין "דחייה" ל"כישלון". על no-instance, דחייה היא הצלחה.

צ'ק-ליסט: מה צריך לדעת לעשות אחרי השיעור הזה

לתרגם מחלקה מנוסחת-מילולית ל-$\mathrm{BPP}(\alpha, \beta)$ תוך זיהוי **איפה** ההבדל מההגדרה המוכרת (pattern matching), לפני שטוענים משהו.

להוכיח סגירות של BPP לפעולה בוליאנית, כולל בחירת רמת ההעצמה הנכונה והצדקתה.

לעבור מהסתברות לספירה במרחב אחיד ובחזרה, ולנצל את שלמות הגודל.

להכריע בין שלוש התשובות האפשריות — נכונה / שגויה / שקולה לטענה פתוחה — ולדעת **לאיזו** בעיה פתוחה השקילות היא.
לבנות מכונה עם הממשק הנכון לכיוון ההכלה שמוכיחים, ולנתח זמן ריצה במפורש (מספר איטרציות × זמן לאיטרציה).
הנחיות המרצה לקראת המבחן [01:19:20]–[01:27:10]
מבנה המבחן [01:21:59]. *שלוש שעות.* **שתי שאלות פתוחות ושש שאלות סגורות** (אמריקאיות); ייתכן שיהיו סעיפים בשאלות הפתוחות. חלוקת הניקוד לא נמסרה — "אתם צריכים לענות על הכול" [01:22:31].
איך ללמוד [01:23:01]. "כל השיעורים, כל מה שעשינו בשיעור, כל תרגילי הבית — לעבור, לראות שאתם יודעים אותם פרפקט." לגבי מבחנים קודמים: "שאלות ממבחנים לפעמים חוזרות על עצמן, אבל בערך **80% מהמבחן הוא שאלות שמבוססות על החומר**, ובערך 20% משהו שהיה פעם באיזה מבחן. לעבור על מלא מבחנים ולהזניח את הלימוד של החומר זה לא הדבר הנכון מבחינת השקעת משאבים." והמשפט שהוא אומר כל סמסטר: "כל סמסטר אחרי המבחן מגיעים אליי סטודנטים ואומרים 'אתה לא מבין כמה מבחנים חרשתי ועדיין היה לי קשה' — כן, כי לא למדתם כמו שאמרתי ללמוד. **תלמדו את החומר של הקורס**; אחרי שתדעו אותו, תפתרו מבחנים כמה שתרצו."
איך לגשת לשאלות האמריקאיות [01:24:34]. "תתייחסו אליהן **כמו לשאלות פתוחות**. ההבדל היחיד הוא שאני לא צריך לכתוב את ההוכחה למישהו אחר שיקרא. כל סעיף בשאלה סגורה — תחשבו עליו כאילו הוא שאלה פתוחה, ותפתרו אותו כך. לא לחשוב על זה בכלל בתור שאלות סגורות." לגבי ההיסקים: מסתכלים על התשובות האפשריות ושואלים "מה הייתי מוכיח, או מפריך, אילו זו הייתה שאלה פתוחה".
חלוקת הזמן [01:26:40]. "קצת יותר מחצי מהזמן על השאלות הפתוחות, קצת פחות מחצי על הסגורות — בערך שעתיים ושעה. **לא להקדיש פחות מעשר דקות לשאלה סגורה.** לא לנסות להמר, לא לנסות אלימינציה. לעבור על הסעיפים ולראות שאתם יודעים **למה** אתם בוחרים את מה שאתם בוחרים."
והמשפט האחרון של הקורס [01:27:10]: "שיהיה לכולנו בהצלחה."

שאלות שנשארו פתוחות

התנגשות שמות: המחלקות C_1–C_4 כאן הן וריאציות הסתברותיות על BPP(α,β), ואינן קשורות למחלקות C_1–C_5 של שיעור 24, שהן וריאציות על הגדרת ה-verifier של NP. אין להצליב תוצאות בין שני הקבצים.

הסיכום פותח באמצע שאלה 1, בסעיף (ג); סעיפים (א) ו-(ב) של אותה שאלה אינם בסיכום, וההקלטה מתחילה כשסעיף (ג) כבר על הלוח.

הניסוח המילולי המדויק של סעיפי (א), (ג) ו-(ה) בשאלה 3 אינו מופיע בסיכום — הם נפתרו בעל פה בלבד; שוחזרו מההקלטה, ובפרט הערך α=1/10 בסעיף (א) נלמד מכך שהמרצה נימק אותו ב-BPP(1/2,1)=BPP(1/10,1).

הדף המודפס של שאלה 3 כותב בהגדרות C_3 ו-C_4 'M accepts x' במקום 'M accepts (x,r)'; זו טעות שהמרצה תיקן בעצמו [00:36:21] ושתוקנה בכתב יד על גבי העמוד. הגוף כאן מביא את הנוסח המתוקן.

עמוד 6 בסיכום ריק לחלוטין.