חישוביות וסיבוכיות
מצגת 7- מבוא לסיבוכיות, המחלקות P, NP ועוד

סיבוכיות זמן - מבוא

- בחצי הראשון של הקורס, חישוביות, עסקנו בשאלה "מה בכלל אפשר לחשב בעזרת מכונות?"
  - אלו פונקציות ניתנות לחישוב ואלו לא?
  - אלו שפות ניתנות להכרעה (לזיהוי) ואלו לא?

סיבוכיות זמן - מבוא

- בחצי הראשון של הקורס, חישוביות, עסקנו בשאלה "מה בכלל אפשר לחשב בעזרת מכונות?"
  - אלו פונקציות ניתנות לחישוב ואלו לא?
  - אלו שפות ניתנות להכרעה (לזיהוי) ואלו לא?
- בחצי השני של הקורס, סיבוכיות, נעסוק רק בפונקציות הניתנות לחישוב ובשפות הכריעות, ונדון בשאלה של כמויות המשאבים הדרושות לחישובים
  - דנים בעיקר במשאבי הזמן והזיכרון הדרושים

המודל - מכונות טיורינג

- אנחנו נלמד בעיקר על סיבוכיות זמן
  – מהו הזמן הדרוש למימוש כל אלגוריתם

המודל - מכונות טיורינג

- אנחנו נלמד בעיקר על סיבוכיות זמן
  – מהו הזמן הדרוש למימוש כל אלגוריתם
- המודל החישובי שבו נשתמש ממשיך להיות מכונות טיורינג. הסיבות לכך הן (בין היתר):

המודל - מכונות טיורינג

- אנחנו נלמד בעיקר על סיבוכיות זמן
  – מהו הזמן הדרוש למימוש כל אלגוריתם
- המודל החישובי שבו נשתמש ממשיך להיות מכונות טיורינג. הסיבות לכך הן (בין היתר)
  – סיבוכיות הזמן נמדדת כרגיל כפונקציה של גודל הקלט. במכונות טיורינג גודל הקלט מוגדר היטב
    - מספר התאים הדרוש לרישום הקלט על הסרט

המודל - מכונות טיורינג

- אנחנו נלמד בעיקר על סיבוכיות זמן
  – מהו הזמן הדרוש למימוש כל אלגוריתם
- המודל החישובי שבו נשתמש ממשיך להיות מכונות טיורינג. הסיבות לכך הן (בין היתר):
  – סיבוכיות הזמן נמדדת כרגיל כפונקציה של גודל הקלט. במכונות טיורינג גודל הקלט מוגדר היטב-
    - מספר התאים הדרוש לרישום הקלט על הסרט.
  – זמן הריצה יוגדר כמספר הצעדים שמבצעת המכונה במהלך ריצתה.
    - צעד חישוב במכונת טיורינג מוגדר היטב.

דוגמה לחישוב זמן ריצה

- **דוגמה**: כמה זמן נדרש להכריע שייכות לשפה $\{a^m b^m \mid m \geq 0\}$ במכונת טיורינג חד-סרטית?
- $M_1 =$ "על מילת קלט w:
  1. עבור על הקלט עד סופו, ודחה אם יש a מימין ל-b.
  2. כל עוד יש a-ים ו-b-ים, עבור על תוכן הסרט, ומחק a אחד ו-b אחד בכל מעבר כזה.
  3. אם נמחקו כל ה-a-ים וכל ה-b-ים, קבל. אחרת, דחה."
- מהו זמן הריצה של המכונה M_1?

זמן ריצה דטרמיניסטי

- זמן הריצה של M_1 הוא $O(n^2)$ כאשר n הוא גודל הקלט.
- **הגדרה**: תהי M מכונת טיורינג דטרמיניסטית,
ותהי $t: \mathbb{N} \rightarrow \mathbb{N}$ פונקציה.
אומרים שזמן הריצה של M הוא $t(n)$,
אם לכל קלט w באורך n,
מספר צעדי הריצה של M על w הוא לכל היותר $t(n)$
- ההגדרה מטפלת בזמן הריצה במקרה הגרוע ביותר.

מחלקה של שפות

- **הגדרה**: תהי $t:\mathbb{N}\rightarrow\mathbb{N}$ פונקציה.
מחלקת השפות $DTIME(t(n))$ היא מחלקת השפות שיש להן מכונת טיורינג דטרמיניסטית מכריעה שזמן הריצה שלה הוא $O(t(n))$.

$$DTIME\big(t(n)\big) = \{L|L\ is\ a\ language,\ decided\ by\ an\ O\big(t(n)\big) - time\ DTM\}$$

- **דוגמה**: לפי מה שראינו, השפה $\{a^m b^m|m \geq 0\}$ שייכת ל-$DTIME(n^2)$.

אפשר יותר טוב?

- **שאלה**: האם אפשר להכריע את השפה הזו מהר יותר?

אפשר יותר טוב?

- **שאלה**: האם אפשר להכריע את השפה הזו מהר יותר?
- $M_2 =$ "על מילת קלט w:
  1. עבור על הקלט, ודחה אם יש a מימין ל-b.
  2. חזור על הפעולות הבאות כל עוד יש a-ים ו-b-ים:
     - עבור על תוכן הסרט, ובדוק האם המספר הכולל של ה-a-ים וה-b-ים הוא אי-זוגי. אם כן, דחה.
     - עבור על תוכן הסרט, מחק את ה-a הראשון, השלישי, החמישי, וכך הלאה, וכך גם ביחס ל-b-ים
  3. אם נמחקו כל ה-a-ים וכל ה-b-ים, קבל. אחרת, דחה."

הוכחת נכונות וחישוב הזמן

- **תרגיל**: הראו ש-M_2 באמת מכריעה את השפה $\{a^m b^m | m \geq 0\}$
- **תרגיל**: הראו שזמן הריצה של M_2 הוא $O(n \cdot \log(n))$

הוכחת נכונות וחישוב הזמן

- **תרגיל**: הראו ש-M_2 באמת מכריעה את השפה $\{a^m b^m | m \geq 0\}$
- **תרגיל**: הראו שזמן הריצה של M_2 הוא $O(n \cdot \log(n))$
- **מסקנה**: השפה $\{a^m b^m | m \geq 0\}$ שייכת למחלקה $DTIME(n \cdot \log(n))$ (וגם ל-$DTIME(n^2)$)

הוכחת נכונות וחישוב הזמן

- **תרגיל**: הראו ש-M_2 באמת מכריעה את השפה $\{a^m b^m | m \geq 0\}$
- **תרגיל**: הראו שזמן הריצה של M_2 הוא $O(n \cdot \log(n))$
- **מסקנה**: השפה $\{a^m b^m | m \geq 0\}$ שייכת למחלקה $DTIME(n \cdot \log(n))$ (וגם ל-$DTIME(n^2)$)
- **תרגיל**: האם כל שפה ששייכת ל-$DTIME(n \cdot \log(n))$ שייכת גם ל-$DTIME(n^2)$?

אפשר עוד יותר טוב?

- **משפט**: אם $t_1(n) = O(t_2(n))$, אז $DTIME(t_1(n)) \subseteq DTIME(t_2(n))$
- **שאלה**: האם אפשר להכריע את $\{a^m b^m \mid m \geq 0\}$ עוד יותר מהר?
  - כלומר, בזמן שהוא $o(n \cdot \log(n))$?

אפשר עוד יותר טוב?

- **משפט**: אם $t_1(n) = O(t_2(n))$, אז $DTIME(t_1(n)) \subseteq DTIME(t_2(n))$
- **שאלה**: האם אפשר להכריע את $\{a^m b^m \mid m \geq 0\}$ עוד יותר מהר?
  - כלומר, בזמן שהוא $o(n \cdot \log(n))$?
- **תשובה**: לא במכונה עם סרט אחד!

משפט: שפה שניתנת להכרעה בזמן $o(n \cdot \log(n))$ במכונה עם סרט אחד היא בהכרח רגולרית.

מכונה עם שני סרטים

- למה שלא נבנה מכונה עם שני סרטים להכרעת השפה?
- **תרגיל**: תארו מכונה עם שני סרטים להכרעת $\{a^m b^m | m \geq 0\}$, והראו שזמן הריצה שלה הוא $O(n)$.

מכונה עם שני סרטים

- למה שלא נבנה מכונה עם שני סרטים להכרעת השפה?
- **תרגיל**: תארו מכונה עם שני סרטים להכרעת $\{a^m b^m | m \geq 0\}$, והראו שזמן הריצה שלה הוא $O(n)$.
- **מסקנה**: אפשר להכריע שייכות ל-$\{a^m b^m | m \geq 0\}$ במכונה עם שני סרטים בזמן שהוא $O(n)$.
במכונה חד-סרטית הזמן הטוב ביותר הוא $O(n \cdot \log(n))$.

הבדל בין חישוביות וסיבוכיות

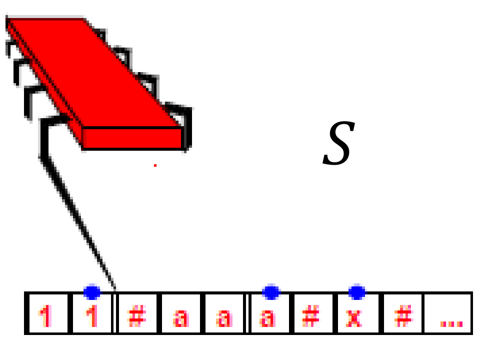
- בתורת החישוביות כל המודלים הסבירים שקולים.
  - כל מה שאפשרי לביצוע באחד המודלים אפשרי לביצוע גם בכל המודלים האחרים.
  - זוהי התזה של צ'רץ' וטיורינג.

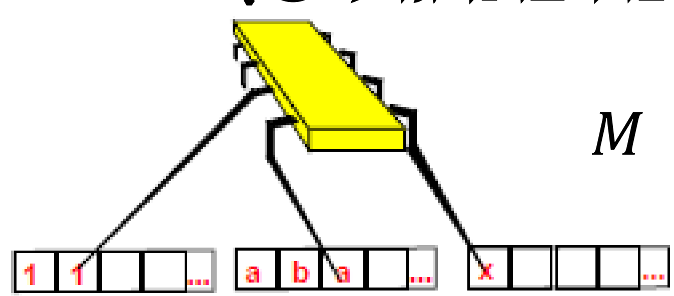
הבדל בין חישוביות וסיבוכיות

- בתורת החישוביות כל המודלים הסבירים שקולים.
  - כל מה שאפשרי לביצוע באחד המודלים אפשרי לביצוע גם בכל המודלים האחרים.
  - זוהי התזה של צ'רץ' וטיורינג.
- כאשר דנים בסיבוכיות, בחירת המודל משפיעה על זמן הריצה.
  - לבחירת המודל (מכונה עם סרט אחד או מכונה עם כמה סרטים) יש השפעה על זמן הריצה.

בעיה: תלות במודל

- **בעיה**: באיזה מודל נבחר לצורך סיווג שפות לפי זמן הריצה של המכונות המכריעות אותן?
- למזלנו, הזמן הדרוש איננו שונה באופן מהותי במודלים דטרמיניסטיים שונים.
- ניזכר כיצד הוכחנו שמכונה עם כמה סרטים שקולה בכוח החישוב שלה למכונה עם סרט אחד (הוכח בתרגול ☺)





תזכורת: הערה על זמן הריצה

- כדי לחקות צעד אחד של פעולת M, S עוברת על הסרט שלה מספר פעמים שחסום על-ידי קבוע.

תזכורת: הערה על זמן הריצה

- כדי לחקות צעד אחד של פעולת M, S עוברת על הסרט שלה מספר פעמים שחסום על-ידי קבוע.
- אם מספר הצעדים של M הוא $t(n)$, ($n = |w|$), אז מספר התאים המקסימלי שעליהם הראש של S עובר במעבר אחד על הסרט הוא $O(t(n))$
  - **תרגיל**: למה?

תזכורת: הערה על זמן הריצה

- כדי לחקות צעד אחד של פעולת M, S עוברת על הסרט שלה מספר פעמים שחסום על-ידי קבוע.
- אם מספר הצעדים של M הוא $t(n)$, ($n = |w|$), אז מספר התאים המקסימלי שעליהם הראש של S עובר במעבר אחד על הסרט הוא $O(t(n))$
  - **תרגיל**: למה?
- **מסקנה**: זמן הסימולציה של מכונה מרובת סרטים על-ידי מכונה חד-סרטית הוא ריבועי לכל היותר ($O(t(n)^2)$)

הפער הריבועי הוא הדוק

- כמו שראינו, הפער בין מכונה מרובת סרטים למכונה עם סרט אחד הוא לכל היותר ריבועי.

למעשה, יש שפות שהוכח עליהן שזהו הפער.

– למשל, שפת הפלינדרומים מעל $\{a, b\}$

  - ניתנת להכרעה במכונה דו-סרטית בזמן שהוא $O(n)$ (איך?)
  - ניתנת להכרעה במכונה חד-סרטית בזמן שהוא $O(n^2)$ (איך?)
  - לא ניתנת להכרעה במכונה חד-סרטית בזמן שהוא $o(n^2)$ (הוכח!)

מודלים לא דטרמיניסטיים

- הראינו שזמן הריצה איננו שונה באופן מהותי במודלים דטרמיניסטיים שונים.
- מה קורה במודלים לא דטרמיניסטיים?

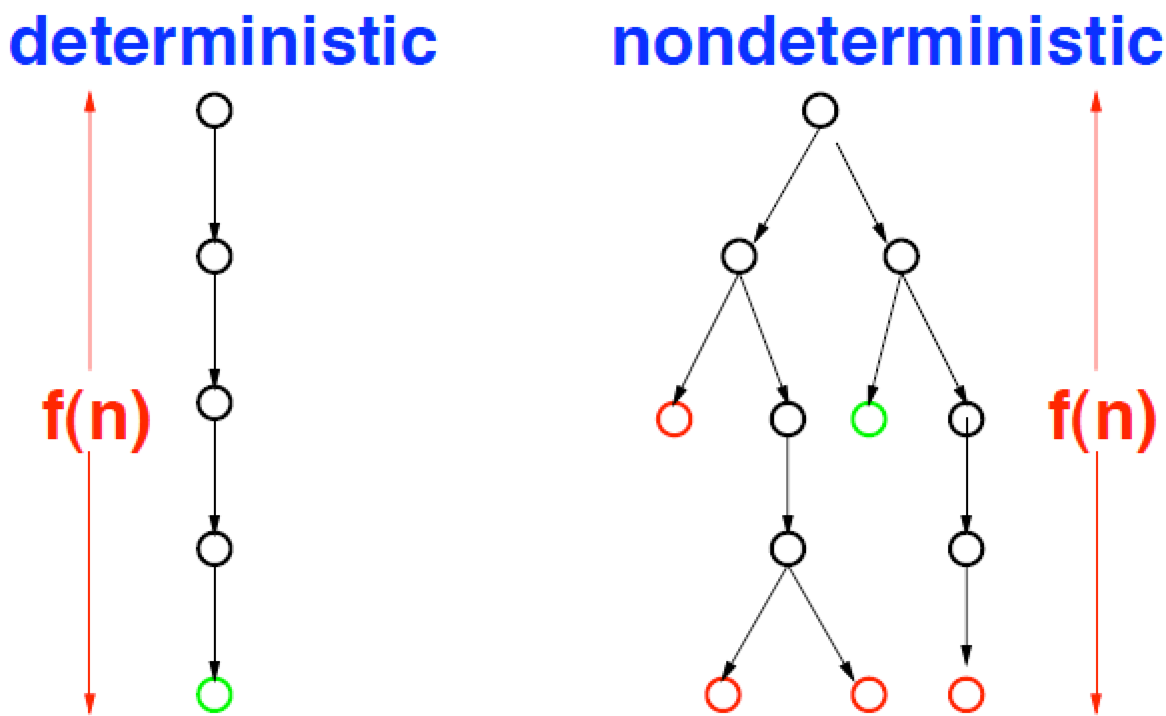
מודלים לא דטרמיניסטיים

- הראינו שזמן הריצה איננו שונה באופן מהותי במודלים דטרמיניסטיים שונים.
- מה קורה במודלים לא דטרמיניסטיים?
- תחילה עלינו להגדיר מהו זמן הריצה במקרה זה.
  - נדבר רק על מכונות מכריעות
    - כל ענפי החישוב מסתיימים בעצירה
      - במצב המקבל או במצב הדוחה
  - נסתכל על זמן החישוב הארוך ביותר

זמן ריצה לא דטרמיניסטי

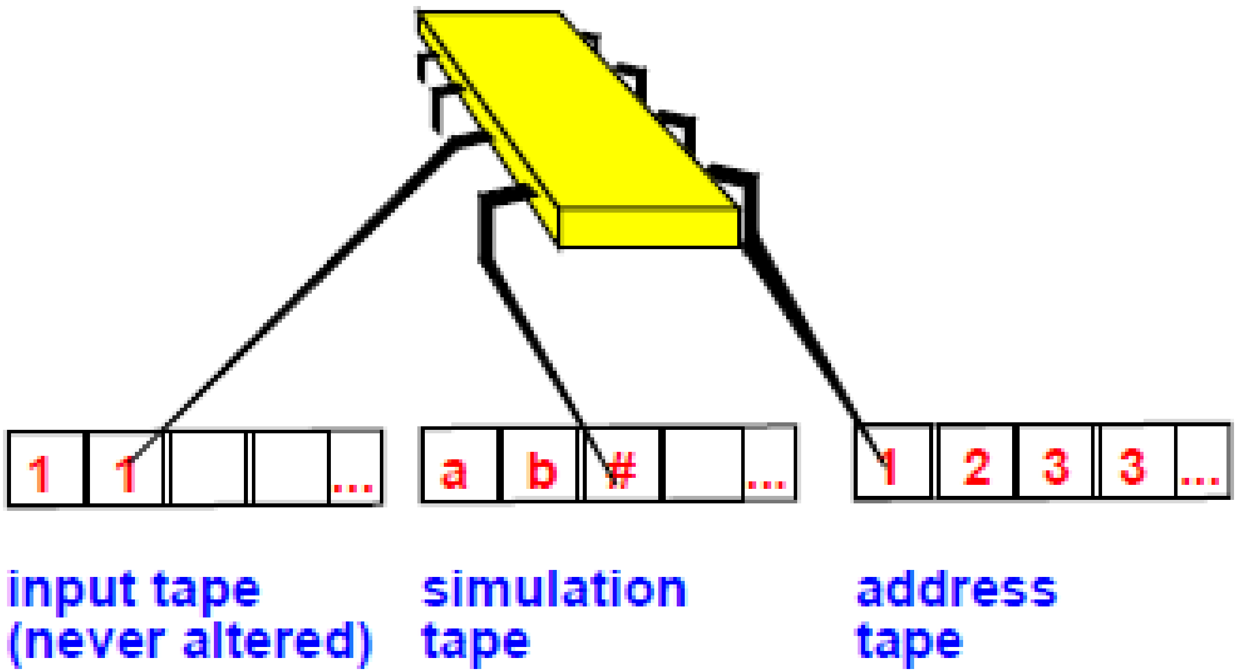
- **הגדרה**: תהי N מכונת טיורינג לא דטרמיניסטית,
ותהי $t: \mathbb{N} \to \mathbb{N}$ פונקציה.
אומרים שזמן הריצה של N הוא $t(n)$,
אם לכל קלט w באורך n,
מספר צעדי הריצה של N על w הוא לכל היותר
$t(n)$, בכל אחד ממסלולי החישוב של N על w.
- **הערה**: מסתכלים על זמן הריצה של כל מסלולי החישוב, גם של אלה שמסתיימים בדחייה.

דטרמיניסטי ולא דטרמיניסטי



שימו לב שבמסלולי חישוב לא מקבלים, המכונה הלא דטרמיניסטית חייבת להגיע ל- q_{reject} בתוך מגבלת הזמן

תזכורת לסימולציה



המכונה D שמסמלצת את המכונה הלא דטרמיניסטית N

תזכורת: הערה על זמן הריצה

- המכונה D שתיארנו לא יעילה מבחינת זמן הריצה
  - יש בה חזרות על חלקים של חישובים.
- אפשר לייעל את פעולתה של D, אך עדיין זמן הריצה של כל סימולציה אפשרית של מכונה לא דטרמיניסטית על-ידי מכונה דטרמיניסטית הוא לפחות מעריכי (אקספוננציאלי) בזמן הריצה של המכונה הלא דטרמיניסטית
  - זמן הריצה של מכונה לא דטרמיניסטית מכריעה N על מילה w מוגדר כמספר הצעדים במסלול החישוב הארוך ביותר של N על w (מקבל או דוחה, לא משנה).

אבחנה חשובה

- לכל היותר פער פולינומיאלי בין מכונה מרובת סרטים ומכונה עם סרט אחד.
  לכל היותר פער אקספוננציאלי בין מכונה לא דטרמיניסטית ומכונה דטרמיניסטית.
- יש הבדל עצום בין הגידול של זמני ריצה פולינומיאליים טיפוסיים כמו n^3,
  ובין הגידול של זמני ריצה אקספוננציאליים טיפוסיים כמו 2^n.

הטוב, הרע והמכוער

	10	20	30	40	50	60
n	.00001 second	.00002 second	.00003 second	.00004 second	.00005 second	.00006 second
n^2	.00001 second	.00004 second	.00009 second	.00016 second	.00025 second	.00036 second
n^3	.00001 second	.00008 second	.027 second	.064 second	.125 second	.216 second
n^5	.1 second	3.2 seconds	24.3 seconds	1.7 minute	5.2 minutes	13.0 minutes
2^n	.001 second	1.0 second	17.9 minutes	12.7 days	35.7 years	366 centuries
3^n	.059 second	58 minutes	6.5 years	3855 centuries	$2 \cdot 10^8$ centuries	$1.3 \cdot 10^{13}$ centuries

פולינומיאלי ואקספוננציאלי

- זמן ריצה אקספוננציאלי מצביע, כרגיל, על סריקה ממצה של כל מרחב הפתרונות. אלגוריתם בעל זמן ריצה פולינומיאלי מצביע על הבנה מעמיקה יותר של הבעיה.
- כל המודלים החישוביים הדטרמיניסטיים "הסבירים" שקולים פולינומיאלית.
  - כל אחד מהם יכול לסמלץ כל אחד אחר בהפסד זמן פולינומיאלי.
    - כרגיל, הפסד הזמן הוא לא יותר מאשר ריבועי.

השגת אי-תלות במודל

- התשובה לשאלה "האם זמן הריצה הוא ליניארי, ריבועי וכדומה?" תלויה במודל.
- לעומת זאת, התשובה לשאלה "האם זמן הריצה פולינומיאלי?" לא תלויה במודל.
- בסופו של דבר אנחנו מעוניינים במדד לקושי של חישובים (מבחינת זמן הריצה, כרגע), ולא בהתמקדות במודל כזה או אחר.
- לכן נבחין בין זמן ריצה פולינומיאלי ובין זמן ריצה על-פולינומיאלי.

הגדרה: מכונת טיורינג פולינומית

- מ״ט דטרמיניסטית M תיקרא **פולינומית**, אם קיים פולינום $p(n) = n^c$, $c \in \mathbb{R}$ כך שלכל $x \in \Sigma^*$, M עוצרת על x בתוך לכל היותר $p(|x|)$ צעדים.

- $p(n) = n^c$ יקרא **חסם זמן הריצה** של M.

הגדרה: מכונת טיורינג פולינומית

- מ״ט דטרמיניסטית M תיקרא **פולינומית**, אם קיים פולינום $p(n) = n^c$, $c \in \mathbb{R}$ כך שלכל $x \in \Sigma^*$, M עוצרת על x בתוך לכל היותר $p(|x|)$ צעדים.
- בדומה, מ״ט **אי דטרמיניסטית** M תיקרא **פולינומית**, אם קיים פולינום $p(n) = n^c$ כך שלכל $x \in \Sigma^*$, M עוצרת על x בתוך לכל היותר $p(|x|)$ צעדים, **בכל מסלולי החישוב שלה**.

- $p(n) = n^c$ יקרא **חסם זמן הריצה** של M.

מבנה הוכחת נכונות של מכונה פולינומית

- **מכונה דטרמיניסטית פולינומית (מכריעה):**

א. הוכחת נכונות:

$$x \in L \ \Rightarrow M(x) = 1$$
$$x \notin L \ \Rightarrow M(x) = 0$$

ב. הוכחת סיבוכיות: להוכיח שלכל קלט x זמן הריצה של המכונה על x חסום ע"י פולינום כלשהו $p(|x|)$.

מבנה הוכחת נכונות של מכונה פולינומית

- **מכונה דטרמיניסטית פולינומית (מכריעה):**

א. הוכחת נכונות:

$$x \in L \;\Rightarrow M(x) = 1$$
$$x \notin L \;\Rightarrow M(x) = 0$$

ב. הוכחת סיבוכיות: להוכיח שלכל קלט x זמן הריצה של המכונה על x חסום ע"י פולינום כלשהו $p(|x|)$.

- **מכונה אי דטרמיניסטית פולינומית (מכריעה):**

א. הוכחת נכונות:

אם $x \in L$ אז **קיים** מסלול **מקבל** בעץ החישוב של המכונה על x.

אם $x \notin L$ אז **כל** המסלולים בעץ החישוב של המכונה על x **דוחים**.

ב. הוכחת סיבוכיות: להוכיח שלכל קלט x, **ולכל מסלול בעץ החישוב**, זמן הריצה של המכונה על x חסום ע"י פולינום כלשהו $p(|x|)$.

הפסקה

המחלקה P

- **הגדרה**: $\boldsymbol{P}$ היא מחלקת השפות שיש להן מכונת טיורינג דטרמיניסטית מכריעה שזמן הריצה שלה פולינומיאלי (בגודל הקלט)

$$\boldsymbol{P} = \cup_{k\geq 0} DTIME(n^k)$$

- שפה L שייכת למחלקה $\boldsymbol{P}$, אם יש אלגוריתם בעל זמן ריצה פולינומיאלי להכרעת השייכות ל-L.
  - כלומר, קיים אלגוריתם שזמן ריצתו $O(n^k)$ ל-k קבוע טבעי כלשהו.

חשיבות המחלקה P

- המחלקה P היא מחלקה חשובה של שפות.
  - שייכות של שפה למחלקה אינה תלויה במספר הסרטים של המכונה שמכריעה שייכות לשפה.
  - השייכות של שפה למחלקה לא תלויה במודל החישובי, כל עוד הוא שקול פולינומיאלית למכונת טיורינג.
  - המחלקה מתאימה למחלקת הבעיות הפתירות באופן מעשי במחשב.

המחלקה מתאימה למציאות

- **שאלה**: ומה אם זמן הריצה הוא $O(n^{100})$?

המחלקה מתאימה למציאות

- **שאלה** : ומה אם זמן הריצה הוא $O(n^{100})$?
- **תשובה** : זה ייחשב זמן ריצה פולינומיאלי.
אבל במציאות זמן הריצה של אלגוריתמים הוא או פולינומיאלי עם פולינום צנוע או על-פולינומיאלי.
- הניסיון מראה שהסף שאותו צריך לעבור הוא המעבר מזמן ריצה אקספוננציאלי לפולינומיאלי.
ברגע שהמעבר הזה קורה, נמצאים אלגוריתמים יותר ויותר יעילים.

דוגמאות לבעיות ב- P

- **אריתמטיקה**: חיבור, חיסור, כפל, חילוק עם שארית.
- **מספרים**: מציאת מחלק משותף מקסימלי.
- **חקר ביצועים**: זרימה ברשתות, תכנון ליניארי.
- **אלגברה**: כפל מטריצות, חישוב דטרמיננטה, פתרון מערכת משוואות ליניאריות, מציאת מטריצה הופכית.
- **גרפים**: חיפוש לעומק, חיפוש לרוחב, מציאת עץ פורש מינימלי, מעגל אוילר.

ניתוח טיפוסי של זמן ריצה

- מחלקים את האלגוריתם לשלבים.
- מראים שזמן הריצה של כל שלב פולינומיאלי.
- מראים שמספר הפעמים שכל שלב מתבצע הוא פולינומיאלי.
- מסיקים שזמן הריצה של האלגוריתם כולו פולינומיאלי:
  - סכום של פולינומים הוא פולינום
    כפל של פולינומים הוא פולינום
    הרכבת פולינומים הוא פולינום

קידוד הקלט (1)

- זמן הריצה מוגדר כפונקציה של גודל הקלט.
  לכן צריך לבחור קידוד סביר לקלט, ולא קידוד שיגדיל באופן מלאכותי את גודל הקלט
  - (למרות שאז זמן הריצה ייראה טוב יותר. זה נקרא "ריפודי")

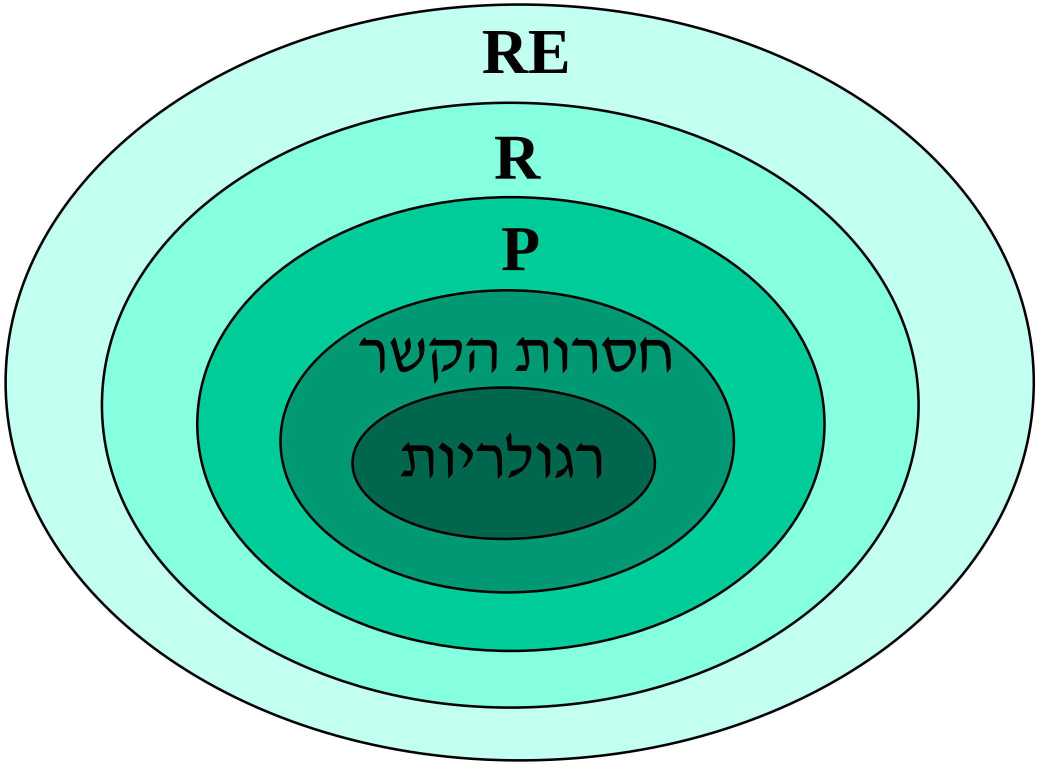
קידוד הקלט (1)

- זמן הריצה מוגדר כפונקציה של גודל הקלט.
לכן צריך לבחור קידוד סביר לקלט, ולא קידוד שיגדיל באופן מלאכותי את גודל הקלט
  - (למרות שאז זמן הריצה ייראה טוב יותר. זה נקרא "ריפודי")
    - **דוגמה**: קידוד של גרף: רשימה של צמתים ורשימה של קשתות, או מטריצת שכנויות.
  - אפשר לעבור מקידוד מסוים לקידוד אחר בזמן פולינומיאלי, והגודל של כל קידוד פולינומיאלי בגודל של הקידוד האחר.
  - רגילים לחשב את זמן הריצה כפונקציה של מספר הצמתים.
זה לא גודל הקלט, אבל גודל הקלט פולינומיאלי במספר הזה.
  - נגיד: גרף הנתון כמטריצת שכנויות, הקלט בגודל $O(|V|^2)$.

קידוד הקלט (2)

– **דוגמה**: מספרים יכולים להיות מיוצגים בבינארי או בעשרוני, אבל לא באונרי.
  - הגודל של הקידוד האונרי אקספוננציאלי בגודל של הקידוד הבינרי (או העשרוני).
– אלגוריתם על מספרים ייחשב פולינומיאלי אם זמן הריצה שלו פולינומיאלי בכמות הספרות המייצגות את המספרים (ולא אם הזמן פולינומיאלי במספרים עצמם המיוצגים על-ידי הספרות)
  - פולינומיאליות בגודל הקלט.
  - **דוגמה**: אם $n = 1000000$ (ייצוג בינרי), אז זמן הריצה צריך להיות פולינומיאלי ב-7 (ולא ב-128).

תמונת עולם של המחלקות



כל ההכלות בין המחלקות הן הכלות ממש

תכונות סגירות של P

- **תרגיל**: הוכיחו שהמחלקה $\boldsymbol{P}$ סגורה ל-
  - איחוד
  - חיתוך
  - משלים
  - שרשור
- $\boldsymbol{P}$ סגורה גם לאיטרציה
  - הוכחה בעזרת אלגוריתם מסוג תכנות דינמי

המחלקה NP

- **תזכורת**: תהי $t: \mathbb{N} \to \mathbb{N}$ פונקציה.
מחלקת השפות $DTIME(t(n))$ היא מחלקת השפות שיש להן מכונת טיורינג דטרמיניסטית מכריעה שזמן הריצה שלה הוא $O(t(n))$.
$DTIME\big(t(n)\big) = \{L | L\ is\ a\ language,$
$decided\ by\ an\ O\big(t(n)\big) - time\ DTM\}$
- אפשר להגדיר הגדרה מקבילה כאשר המכונה לא דטרמיניסטית!

המחלקה NTIME($t(n)$)

- **הגדרה**: תהי $t\colon \mathbb{N} \to \mathbb{N}$ פונקציה.
מחלקת השפות $NTIME(t(n))$ היא מחלקת השפות שיש להן מכונת טיורינג לא דטרמיניסטית מכריעה שזמן הריצה שלה הוא $O(t(n))$.
$$NTIME\big(t(n)\big) = \{L | L \text{ } is \text{ } a \text{ } language, \\ decided \text{ } by \text{ } an \text{ } O\big(t(n)\big) - time \text{ } NTM\}$$
- **תזכורת**: זמן הריצה של מכונה לא דטרמיניסטית מוגדר לפי מסלול החישוב הארוך ביותר על המילה.

המחלקה NP

- במקביל להגדרה של המחלקה $\boldsymbol{P}$ מגדירים את מחלקת השפות $\boldsymbol{NP}$:
  $\boldsymbol{NP}$ היא מחלקת השפות שיש להן מכונת טיורינג לא דטרמיניסטית מכריעה שזמן הריצה שלה פולינומיאלי (בגודל הקלט)

$$\boldsymbol{NP} = \cup_{k \geq 0} NTIME(n^k)$$

הסבר לא פורמלי של NP

- באופן לא פורמלי, שפה L שייכת למחלקה $\boldsymbol{NP}$ אם לכל מילה w בשפה יש דרך לוודא במהירות ש-w שייכת לשפה.
  - "במהירות" = בזמן פולינומיאלי בגודל הקלט.
  - לכל מילה בשפה יש "תעודת שייכות" שמשכנעת שהמילה שייכת לשפה.
  - לכל מילה שלא שייכת לשפה אין תעודת שייכות כזו.
  - לפעמים נקרא לתעודה זו "עד" (witness).

תכונות של המחלקות P,NP

- $P,NP \subseteq R$

הסבר: מכיוון ששתי ההגדרות של P ו-NP מתייחסות למכונות טיורינג **המכריעות** שפות.

- $P \subseteq NP$

רעיון ההוכחה: הוכחנו שהמודל הדטרמיניסטי שקול למודל הלא דטרמיניסטי. ובפרט ראינו שקל להפוך כל מכונה דטרמיניסטית למכונה לא דטרמיניסטית.

אבל, כעת צריך לשים לב **לחסם הפולינומי** לזמן הריצה של המכונה.

הוכחה- $P \subseteq NP$

תהי $L \in P$, ותהי M_L מכונת טיורינג דטרמיניסטית פולינומית המכריעה את L. יהי $p(n)$ חסם זמן הריצה הפולינומי של M_L.

נתאר מכונה לא דטרמיניסטית פולינומית $M_L{}'$ המכריעה את L. המכונה $M_L{}'$ תהיה זהה ל-M_L למעט שינוי פורמלי בהגדרת פונקציית המעברים של המכונה M_L (כדי שתתאים למודל הלא דטרמיניסטי).

נשים לב שלכל קלט $x \in \Sigma^*$ עומק העץ חסום ע"י החסם של המכונה המקורית, $p(|x|)$.

נכונות: (השלימו)

האם $P \supseteq NP$?

- במילים אחרות- האם אפשר להמיר מ״ט לא דטרמיניסטית פולינומית למ״ט דטרמיניסטית **פולינומית**?

האם $P \subseteq NP$?

- במילים אחרות- האם אפשר להמיר מ״ט לא דטרמיניסטית פולינומית למ״ט דטרמיניסטית **פולינומית**?
- כשהוכחנו בשיעור הקודם שניתן לסמלץ מכונה לא דטרמיניסטית ע״י מכונה דטרמיניסטית, התעלמנו מכמות המשאבים הדרושים לכך.

האם $P \subseteq NP$?

- במילים אחרות- האם אפשר להמיר מ״ט לא דטרמיניסטית פולינומית למ״ט דטרמיניסטית **פולינומית**?
- כשהוכחנו בשיעור הקודם שניתן לסמלץ מכונה לא דטרמיניסטית ע״י מכונה דטרמיניסטית, התעלמנו מכמות המשאבים הדרושים לכך.
- אם נרצה לסרוק את כל עץ החישוב של המכונה הלא דטרמיניסטית הפולינומית, נקבל זמן ריצה פרופורציונלי לגודל העץ, כלומר $\Omega(2^{p(n)})$ – אקספוננציאלי!

האם $P \subseteq NP$?

- במילים אחרות- האם אפשר להמיר מ״ט לא דטרמיניסטית פולינומית למ״ט דטרמיניסטית **פולינומית**?
- כשהוכחנו בשיעור הקודם שניתן לסמלץ מכונה לא דטרמיניסטית ע״י מכונה דטרמיניסטית, התעלמנו מכמות המשאבים הדרושים לכך.
- אם נרצה לסרוק את כל עץ החישוב של המכונה הלא דטרמיניסטית הפולינומית, נקבל זמן ריצה פרופורציונלי לגודל העץ, כלומר $\Omega(2^{p(n)})$ – אקספוננציאלי!
- השאלה הזו נקראת גם שאלת $\boldsymbol{P = NP}$? זו **שאלה פתוחה**, שעדיין לא הצליחו להוכיח או להפריך אותה.
- בהמשך נראה ניסוח/ים שונים לשאלה הזו.

דוגמא לשפה ב- NP

$$IS = \{< G, k > | G \text{ is a graph that contains an independent set of size } k\}$$

טענה: $\boldsymbol{IS \in R}$

רעיון ההוכחה: אלגוריתם של **חיפוש מלא** יכול לעבור על כל האפשרויות לבחירת k קודקודים מהגרף, ולכל אפשרות כזו, לבדוק האם היא קבוצה בלתי תלויה (לבדוק שכל זוג של קודקודים בקבוצה לא מחוברים בצלע).

אם מצאנו כזו – להחזיר כן.

ואם עברנו על כל האפשרויות ולא מצאנו – להחזיר לא.

דוגמא לשפה ב- NP

$$IS = \{< G, k > | G \text{ is a graph that contains an independent set of size } k\}$$

טענה: $\boldsymbol{IS \in R}$

רעיון ההוכחה: אלגוריתם של **חיפוש מלא** יכול לעבור על כל האפשרויות לבחירת k קודקודים מהגרף, ולכל אפשרות כזו, לבדוק האם היא קבוצה בלתי תלויה (לבדוק שכל זוג של קודקודים בקבוצה לא מחוברים בצלע).

אם מצאנו כזו – להחזיר כן.

ואם עברנו על כל האפשרויות ולא מצאנו – להחזיר לא.

טענה: $\boldsymbol{IS \in NP}$

רעיון ההוכחה: במקום חיפוש מלא, ניתן **לנחש** קבוצה המועמדת להיות קבוצה בלתי תלויה בגרף (ולבדוק רק אותה).

טענה: $IS \in NP$

הוכחה: נתאר מכונה לא דטרמיניסטית פולינומית המכריעה את IS

N על קלט $< G,k >$:

1. נחש תת קבוצה S של קודקודי G. (בדוק שגודל הקבוצה הינו k)
2. לכל זוג $v_1,v_2 \in S$ בדוק ש-$E(G)$ $\{v_1,v_2\} \notin$
   – אם לאחת הצלעות גילינו ש-$\{v_1,v_2\} \in E(G)$ -דחה.
3. אם עברנו על כל הזוגות ולא דחינו – קבל.

טענה: $IS \in NP$

המשך : **<u>נכונות</u>** האלגוריתם:

- אם IS $\langle G,k\rangle \in$ אזי **קיימת** תת קבוצה $S \subseteq V$ בגודל k שהיא בלתי תלויה.

אזי, קיים מסלול חישוב שבו המכונה N מנחשת בדיוק את הקבוצה S.

במסלול זה, הבדיקה של N את הקבוצה S יוצאת תקינה, ולכן N מקבלת.

כלומר, קיים מסלול מקבל, ולכן $\langle G,k\rangle \in L(N)$.

טענה: $IS \in NP$

המשך: **<u>נכונות</u>** האלגוריתם:

- אם IS $\langle G,k\rangle \in$ אזי **קיימת** תת קבוצה $S \subseteq V$ בגודל k שהיא בלתי תלויה.

אזי, קיים מסלול חישוב שבו המכונה N מנחשת בדיוק את הקבוצה S.

במסלול זה, הבדיקה של N את הקבוצה S יוצאת תקינה, ולכן N מקבלת.

כלומר, קיים מסלול מקבל, ולכן $\langle G,k\rangle \in L(N)$.

- אם IS $\langle G,k\rangle \notin$ אזי **לכל** תת קבוצה $S \subseteq V$ בגודל k, מתקיים ש-S תלויה (כלומר מכילה צלע ששתי קצותיה ב-S).

אזי, לכל ניחוש של קבוצה S כנ"ל, N תזהה שקיימת צלע "בתוך" S ותדחה.

כלומר, כל המסלולים בעץ החישוב דוחים, ולכן $\langle G,k\rangle \notin L(N)$.

טענה: $IS \in NP$

הסיבוכיות של ניחוש הוא כגודל הניחוש.

(למשל, הסיבוכיות של ניחוש של קבוצה בגודל k הוא $O(k)$)

המשך: <u>סיבוכיות האלגוריתם</u>:

ראשית, גודל הקלט שלנו הינו $O(n^2)$, כאשר n הינו מספר הקודקודים בגרף. בנוסף אפשר להניח ש-n $k \le$ (כי אחרת השאלה טריוויאלית).

בשלב 1, ניחוש קבוצה בגודל k, לכן $O(k)$.

בשלב 2, עוברים על $O\left(\binom{k}{2}\right) = O(k^2)$ זוגות.

סה"כ: $O(k^2 + k) = O(k^2)$ – פולינומי.

הגדרה שקולה למחלקה NP

שפה L שייכת ל-NP אם קיים יחס דו מקומי R_L המכיל זוגות (x,y) כך שמתקיים:

- $x \in L$
- y הינו **עד** עבור x (כלומר, y הוא אוביקט המעיד על השייכות של x ל-L).

<u>R_L מקיים</u>:

1. R_L חסום פולינומית.

   כלומר: לכל זוג $(x,y) \in R_L$ קיים פולינום $p(\cdot)$ כך שמתקיים $|y| \leq p(|x|)$.

2. R_L ניתן לזיהוי דטרמיניסטי פולינומי. כלומר קיימת מכונת טיורינג דטרמיניסטית פולינומית V המוודאת (=מכריעה) את היחס. (לכל זוג (x,y) המכונה תענה אם הזוג שייך ליחס או לא.) V נקרא **מאמת**.

הגדרה שקולה למחלקה NP

3. השפה L מקיימת

$$L = \{x \in \Sigma^* | \exists y \ s.t. \ (x,y) \in R_L\}$$

כלומר לכל מילה בשפה **קיים** עד פולינומי, ולכל מילה שאיננה בשפה **לא קיים** עד פולינומי.

ביתר פירוט:

$$x \in L \rightarrow \exists \ p(\cdot), \exists \ y \in \Sigma^{p(|x|)} \ : (x,y) \in R_L$$

$$x \notin L \rightarrow \forall p(\cdot), \forall \ y \in \Sigma^{p(|x|)} \ : (x,y) \notin R_L$$

הוכחת $IS \in NP$ ע״י ההגדרה השנייה

- עד עבור IS יהיה קבוצה בלתי תלויה בגודל k.
- היחס R_{IS} מכיל זוגות מהצורה $(< G,k > , < S >)$
- גודל העד הוא $O(k)$ –פולינומי בגודל הגרף G.
- התנאי השלישי:

אם $\langle G,k\rangle \in IS$ אזי קיימת תת קבוצה $S \subseteq V$ בגודל k שהיא בלתי תלויה. אז נבחר אותה להיות העד .

אם $\langle G,k\rangle \notin IS$ אזי **לכל** תת קבוצה $S \subseteq V$ בגודל k, מתקיים ש-S תלויה (כלומר מכילה צלע ששתי קצותיה ב-S). לכן, לכל תת קבוצה שנבחר להיות העד, לא יתקבל זוג אשר שייך ליחס R_{IS} .

- תרגיל: כתבו פסודו קוד של פעולת המאמת V.

ניסוח שקול לשאלת $P = NP$

האם וידוא יעיל גורר חיפוש יעיל?

וידוא יעיל הוא מאפיין מרכזי של NP. (כלומר, בהינתן הצעה לפתרון אפשרי, ניתן בזמן פולינומי לוודא שהפתרון המוצע נכון).

דוגמא: משחק סדוקו, בהינתן פתרון של סדוקו אפשר בקלות יחסית (=באופן פולינומי) לוודא שהפתרון נכון.

השאלה היא אם התכונה הנ"ל גם אומרת **שמציאת** הפתרון יכולה להתבצע ביעילות?

<u>דוגמא לבעיה כריעה שאיננה ב-NP:</u> משחק שחמט. אם במהלך המשחק יציגו לנו צעד שאותו יש לבצע כדי לנצח, אין לנו אפשרות לדעת בקלות שהצעד המדובר באמת יביא לנו ניצחון. (כלומר גם **בדיקה** של פתרון אופציונלי דורשת הרבה עבודה.)

הפסקה

טענה: שתי ההגדרות של NP הן שקולות

- **הוכחה:**

ראשית, נסמן:

NP_1 = המחלקה NP לפי ההגדרה הראשונה – כלומר כל השפות שיש להן מכונת טיורינג לא דטרמיניסטית פולינומית מכריעה.

NP_2 = המחלקה NP לפי ההגדרה המשתמשת ביחס. כלומר כל השפות כך שקיים עבורן יחס R_L שהוא חסום פולינומית, ניתן לזיהוי יעיל, וכן לכל מילה בשפה **קיים** עד פולינומי, ולכל מילה שאיננה בשפה **לא קיים** עד פולינומי.

כיוון ראשון - $NP_2 \subseteq NP_1$

תהי $L \in NP_2$.

תהי V מכונה פולינומית דטרמיניסטית המוודאת את היחס R_L, יהי $p_1(n)$ חסם פולינומי לזמן הריצה של V, ויהי $p_2(n)$ חסם פולינומי לגודל העדים ב-R_L.

נתאר מכונה לא דטרמיניסטית המכריעה את L :

N על קלט x :

1. מנחשת y באורך לכל היותר $p_2(|\mathrm{x}|)$.
2. מסמלצת את ריצת V על הזוג (x,y) ועונה כמוה.

כיוון ראשון $NP_2 \subseteq NP_1$

נכונות:

- אם $x \in L$ אזי קיים עד y באורך פולינומי ומתקיים $(x,y) \in R_L$.

לכן קיים ניחוש נכון של y בעץ החישוב של N על x, ובמסלול של הניחוש הנכון, N מקבלת את x.

- אם $x \notin L$ אזי לכל ניחוש של y מתקיים שהזוג $(x,y) \notin R_L$,

לכן לכל ניחוש y בעץ החישוב של N על x, N תדחה את x.

כיוון ראשון $NP_2 \subseteq NP_1$

נכונות:

- אם $x \in L$ אזי קיים עד y באורך פולינומי ומתקיים $(x,y) \in R_L$.

לכן קיים ניחוש נכון של y בעץ החישוב של N על x, ובמסלול של הניחוש הנכון, N מקבלת את x.

- אם $x \notin L$ אזי לכל ניחוש של y מתקיים שהזוג $(x,y) \notin R_L$,

לכן לכל ניחוש y בעץ החישוב של N על x, N תדחה את x.

סיבוכיות: בשלב 1, $O(p_2(|x|))$

בשלב 2, $O(p_1(|x|) + p_2(|x|))$

סה"כ $O(p_1(|x|) + p_2(|x|))$ פולינומי ב-$|x|$ כנדרש. (כי סכום פולינומים הוא גם פולינום)

מ.ש.ל כיוון ראשון.

כיוון שני - $NP_1 \subseteq NP_2$

תהי $L \in NP_1$

תהי N מכונת טיורינג לא דטרמיניסטית המכריעה את L, ויהי $p(n)$ חסם פולינומי לזמן הריצה של N (כלומר לעומק של עצי החישוב שלה).

יחס R_L עבור השפה L:

- לכל $x \in L$ ניקח **מסלול ריצה מקבל** בעץ החישוב של N על x להיות עד.

נייצג כל מסלול ריצה כזה כמחרוזת בינארית (ע"י למשל 0= פניה שמאל 1=פניה ימינה)

- האורך של כל מחרוזת כזו חסום על ידי $p(|x|)$.
- ניתן לבדוק בקלות (כלומר, בחישוב דטרמיניסטי בזמן פולינומי) אם המסלול שניתן לנו כעד, מסתיים/לא מסתיים במצב מקבל. (זה בעצם המאמת V).

טענה: שתי ההגדרות של NP הן שקולות

- **לסיום**:

אם $x \in L$ אז **קיים** מסלול מקבל בעץ החישוב של N על x.

מכאן קיים עד y שאורכו חסום על ידי פולינום ב- $|x|$. לכן הזוג (x,y) שייך ליחס R_L.

אם $x \notin L$ אז כל המסלולים בעץ החישוב של N על x דוחים.

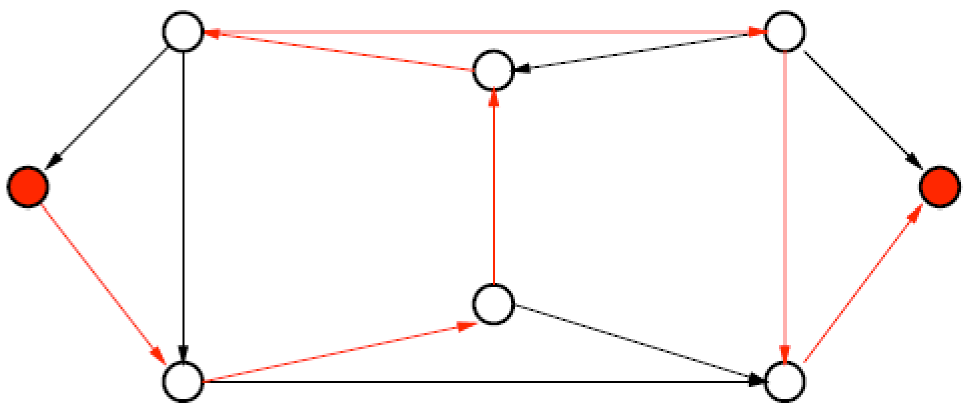
מכאן **לכל** עד y, הזוג (x,y) איננו שייך ליחס R_L.

מ.ש.ל כיוון שני

- נראה דוגמאות נוספות לשפות ב-NP.

מסלול המילטון

- מסלול המילטון בגרף מכוון D הוא מסלול פשוט (ללא מעגלים) שמבקר בכל צומת פעם אחת ויחידה



$$HAMPATH = \{< D, s, t > | D\ is\ a\ directed\ graph\ with\ a\ Hamiltonian\ path\ from\ s\ to\ t\}$$

$HAMPATH$

- **תרגיל**: תארו מאמת בעל זמן ריצה פולינומיאלי לשפה $HAMPATH$
- **תרגיל**: תארו מכונת טיורינג לא דטרמיניסטית מכריעה ל- $HAMPATH$שרצה בזמן פולינומיאלי

$HAMPATH$

- **תרגיל**: תארו מאמת בעל זמן ריצה פולינומיאלי לשפה $HAMPATH$
- **תרגיל**: תארו מכונת טיורינג לא דטרמיניסטית מכריעה ל- $HAMPATH$ שרצה בזמן פולינומיאלי
- **מסקנה**: $HAMPATH$ שייכת ל-$\boldsymbol{NP}$.

$HAMPATH$

- **תרגיל**: תארו מאמת בעל זמן ריצה פולינומיאלי לשפה $HAMPATH$
- **תרגיל**: תארו מכונת טיורינג לא דטרמיניסטית מכריעה ל- $HAMPATH$ שרצה בזמן פולינומיאלי
- **מסקנה**: $HAMPATH$ שייכת ל-$\boldsymbol{NP}$.
- **שאלה**: האם $HAMPATH$ שייכת ל-$\boldsymbol{P}$?

$HAMPATH$

- **תרגיל**: תארו מאמת בעל זמן ריצה פולינומיאלי לשפה $HAMPATH$
- **תרגיל**: תארו מכונת טיורינג לא דטרמיניסטית מכריעה ל- $HAMPATH$שרצה בזמן פולינומיאלי
- **מסקנה**: $HAMPATH$ שייכת ל-$\boldsymbol{NP}$**.**
- **שאלה**: האם $HAMPATH$ שייכת ל-$\boldsymbol{P}$?
  תשובה: לא ידוע.
  – לא ידוע על אלגוריתם פולינומיאלי להכרעת השייכות לשפה, וגם לא הוכח שאלגוריתם כזה לא קיים.

COMPOSITES

- מספר טבעי נקרא **פריק**, אם הוא מכפלה של שני מספרים טבעיים גדולים מ-1.

$$COMPOSITES = \{< n > | n \ is \ composite\}$$

- **תרגיל**: הוכיחו שהשפה $COMPOSITES$ שייכת ל-$\boldsymbol{NP}$.
  - **תזכורת**: זמן הריצה צריך להיות פולינומיאלי בכמות הספרות שמייצגות את המספר n.

COMPOSITES

- מספר טבעי נקרא **פריק**, אם הוא מכפלה של שני מספרים טבעיים גדולים מ-1.

$$COMPOSITES = \{< n > | n \text{ is composite}\}$$

- **תרגיל**: הוכיחו שהשפה $COMPOSITES$ שייכת ל-$\boldsymbol{NP}$.
  – **תזכורת**: זמן הריצה צריך להיות פולינומיאלי בכמות הספרות שמייצגות את המספר n
- **שאלה**: האם השפה הזו שייכת ל-$\boldsymbol{P}$?

COMPOSITES

- מספר טבעי נקרא פריק, אם הוא מכפלה של שני מספרים טבעיים גדולים מ-1.

$$COMPOSITES = \{< n > | n\ is\ composite\}$$

- **תרגיל**: הוכיחו שהשפה $COMPOSITES$ שייכת ל-$\boldsymbol{NP}$.
  - **תזכורת**: זמן הריצה צריך להיות פולינומיאלי בכמות הספרות שמייצגות את המספר n
- **שאלה**: האם השפה הזו שייכת ל-$\boldsymbol{P}$?

תשובה (2002): כן!

PRIMES

- **שאלה**: מה עם שפת המספרים הראשוניים?

$PRIMES = \{< n > \mid n\ is\ prime\}$

PRIMES

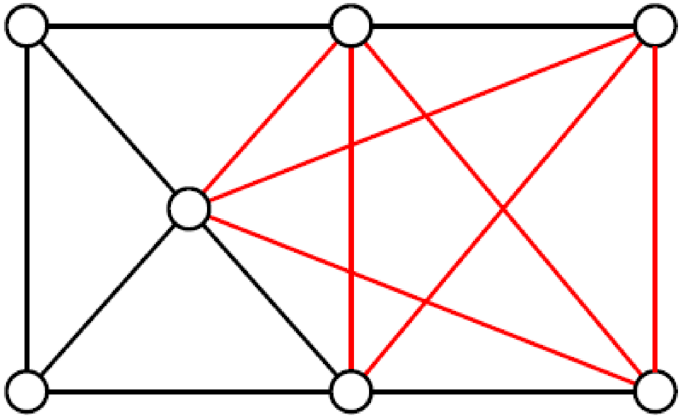
- **שאלה**: מה עם שפת המספרים הראשוניים?
$$PRIMES = \{< n > \mid n \; is \; prime\}$$
- **תשובה**: מכיוון ש-$COMPOSITES$ שייכת ל-$\boldsymbol{P}$, אז גם $PRIMES$ שייכת ל-$\boldsymbol{P}$ ($\boldsymbol{P}$ סגורה למשלים). אבל כבר ב-1975 הוכח ש-$PRIMES$ שייכת ל-$\boldsymbol{NP}$.
  - זה "החשיד" שהשפות $COMPOSITES$ ו-$PRIMES$ שייכות ל-$\boldsymbol{P}$.
    - שפה שגם היא וגם המשלימה שלה שייכות ל-$\boldsymbol{NP}$ "חשודה" כשייכת ל-$\boldsymbol{P}$ (בהמשך יובן למה).

$CLIQUE$

- קליקה בגרף לא מכוון G היא קבוצה של צמתים שיש קשת בין כל שניים מהם.

$$CLIQUE = \{< G,k > | G \text{ is an undirected graph with a } k - \text{clique}\}$$

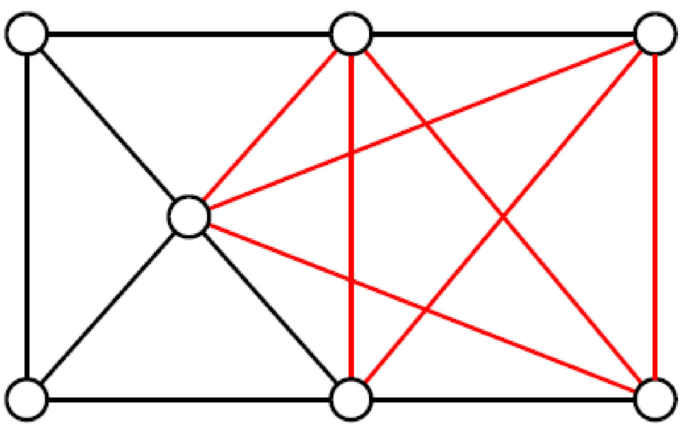
- **תרגיל**: הוכיחו ש-$CLIQUE$ שייכת ל-$\boldsymbol{NP}$
- **שאלה**: האם היא שייכת ל-$\boldsymbol{P}$?



$CLIQUE$

- קליקה בגרף לא מכוון G היא קבוצה של צמתים שיש קשת בין כל שניים מהם.

$$CLIQUE = \{< G,k > | G \text{ is an undirected graph with a } k-\text{clique}\}$$



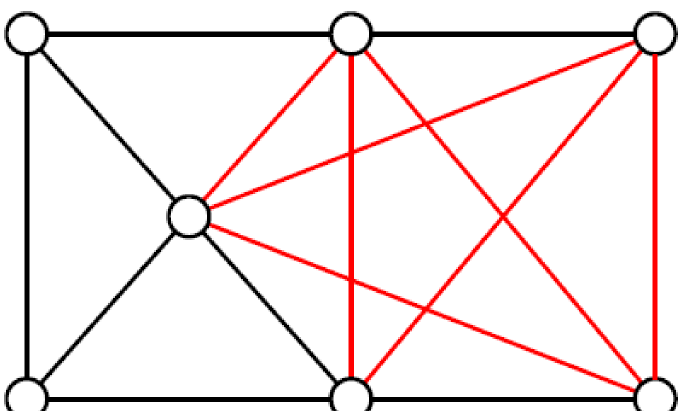
- **תרגיל**: הוכיחו ש-$CLIQUE$ שייכת ל-$\boldsymbol{NP}$
- **שאלה**: האם היא שייכת ל-$\boldsymbol{P}$?

תשובה: לא ידוע.

$CLIQUE$

- קליקה בגרף לא מכוון G היא קבוצה של צמתים שיש קשת בין כל שניים מהם.

$$CLIQUE = \{< G, k > | G \text{ is an undirected graph with a } k - \text{clique}\}$$



- **תרגיל**: הוכיחו ש-$CLIQUE$ שייכת ל-$\boldsymbol{NP}$
- **שאלה**: האם היא שייכת ל-$\boldsymbol{P}$?
  תשובה: לא ידוע.
- שאלה: האם IS היא המשלימה של $CLIQUE$?

INDEPENDENT-SET

- קבוצה בלתי תלויה של צמתים בגרף לא מכוון G היא קבוצת צמתים שאין קשת בין כל שניים מהם

$IS = \{< G, k >|G \; is \; a \; graph \; that \; contains \; an \; independent \; set \; of \; size \; k\}$

- הראנו כבר (שקפים +63) שמתקיים $IS \in NP$.
- **שאלה**: האם היא שייכת ל-**P**?

INDEPENDENT-SET

- **קבוצה בלתי תלויה** של צמתים בגרף לא מכוון G היא קבוצת צמתים **שאין קשת** בין כל שניים מהם

$IS = \{< G, k >| G \text{ is a graph that contains an independent set of size } k\}$

- הראנו כבר (שקפים 63+) שמתקיים $IS \in NP$.
- **שאלה**: האם היא שייכת ל-**P**?

  תשובה: לא ידוע.
- **הערה**: שימו לב היטב **לקלט** בשתי הבעיות האחרונות
  - גרף G **ומספר טבעי** k (ולא רק הגרף G)

SUBSET-SUM

- הקלט לבעיה: קבוצה S של מספרים ומספר t
  השאלה: האם יש ל-S תת-קבוצה שהסכום שלה t?

$$Subset - Sum = \{< S, t > | S = \{x_1, \dots, x_n\},$$
$$\exists\{y_1, \dots, y_k\} \subseteq \{x_1, \dots, x_n\}\ s.t \sum y_i = t\}$$

- **תרגיל**: הוכיחו ש-*SUBSET-SUM* שייכת ל-$\boldsymbol{NP}$.

SUBSET-SUM

- הקלט לבעיה: קבוצה S של מספרים ומספר t
השאלה: האם יש ל-S תת-קבוצה שהסכום שלה t?

$$Subset-Sum=\{<S,t>|S=\{x_1,\ldots,x_n\},$$
$$\exists\{y_1,\ldots,y_k\}\subseteq\{x_1,\ldots,x_n\}\ s.t\ \sum y_i=t\}$$

- **תרגיל**: הוכיחו ש-*SUBSET-SUM* שייכת ל-$\boldsymbol{NP}$.
- **שאלה**: האם היא שייכת ל-$\boldsymbol{P}$?

$SUBSET\text{-}SUM$

- הקלט לבעיה: קבוצה S של מספרים ומספר t
השאלה: האם יש ל-S תת-קבוצה שהסכום שלה t?

$$Subset - Sum = \{< S, t > | S = \{x_1, \dots, x_n\}, \exists\{y_1, \dots, y_k\} \subseteq \{x_1, \dots, x_n\}\ s.t \sum y_i = t\}$$

- **תרגיל**: הוכיחו ש-$SUBSET\text{-}SUM$ שייכת ל-$\boldsymbol{NP}$.
- **שאלה**: האם היא שייכת ל-$\boldsymbol{P}$?
תשובה: לא ידוע.

הבהרה של כללי המשחק

- **שאלה**: משהו פה לא ברור. אם מישהו מספק לנו את ההוכחה לשייכות של המילה לשפה, אז האם לא כל שפה שייכת ל-$\boldsymbol{NP}$?
  - האם לא תמיד אפשר לספק "תעודת שייכות" קצרה לכל מילה בשפה?
    - "קצרה" = בעלת אורך פולינומיאלי באורך המילה.

הבהרה של כללי המשחק

- **שאלה**: משהו פה לא ברור. אם מישהו מספק לנו את ההוכחה לשייכות של המילה לשפה, אז האם לא כל שפה שייכת ל-$\boldsymbol{NP}$?
  - האם לא תמיד אפשר לספק "תעודת שייכות" קצרה לכל מילה בשפה?
    - "קצרה" = בעלת אורך פולינומיאלי באורך המילה.
- **תשובה**: הסתכלו במשלימה של $CLIQUE$ או של $HAMPATH$ או של $INDEPENDENT\text{-}SET$ האם תוכלו להראות שהן שייכות ל-$\boldsymbol{NP}$?

הבהרה של כללי המשחק

- **שאלה**: משהו פה לא ברור. אם מישהו מספק לנו את ההוכחה לשייכות של המילה לשפה, אז האם לא כל שפה שייכת ל-$\boldsymbol{NP}$?
  - האם לא תמיד אפשר לספק "תעודת שייכות" קצרה לכל מילה בשפה?
    - "קצרה" = בעלת אורך פולינומיאלי באורך המילה.
- **תשובה**: הסתכלו במשלימה של *CLIQUE* או של *HAMPATH* או של *INDEPENDENT-SET* האם תוכלו להראות שהן שייכות ל-$\boldsymbol{NP}$?
  - לא נורא. לא רק אתם לא הצלחתם. איש (עדיין?) לא הצליח.

המחלקה $coNP$

- מחלקת השפות $\boldsymbol{coNP}$: השפות שהמשלימה שלהן שייכת ל-$\boldsymbol{NP}$
- $\boldsymbol{coNP} = \{L|\bar{L} \in \boldsymbol{NP}\}$
- באופן לא פורמלי, שפה L שייכת למחלקה $\boldsymbol{coNP}$ אם לכל מילה w שלא שייכת ל-L יש דרך מהירה לוודא ש-w לא שייכת ל-L

המחלקה $coNP$

- מחלקת השפות $\boldsymbol{coNP}$: השפות שהמשלימה שלהן שייכת ל-$\boldsymbol{NP}$
- $\boldsymbol{coNP} = \{L | \bar{L} \in \boldsymbol{NP}\}$
- באופן לא פורמלי, שפה L שייכת למחלקה $\boldsymbol{coNP}$ אם לכל מילה w שלא שייכת ל-L יש דרך מהירה לוודא ש-w לא שייכת ל-L
- **תרגיל** : אלו שפות נראות קשות יותר, אלה שב-$\boldsymbol{NP}$ או אלה שב-$\boldsymbol{coNP}$?

זכרונות נעימים (למי?)

- המחלקות $\boldsymbol{P}$, $\boldsymbol{NP}$ ו-$\boldsymbol{coNP}$ מזכירות מחלקות מתורת החישוביות
  - $\boldsymbol{P}$ מקבילה למחלקת השפות הכריעות.
    - יש לשפה מכונה מכריעה (במהירות)

זכרונות נעימים (למי?)

- המחלקות $\boldsymbol{P}$, $\boldsymbol{NP}$ ו-$\boldsymbol{coNP}$ מזכירות מחלקות מתורת החישוביות
  - $\boldsymbol{P}$ מקבילה למחלקת השפות הכריעות.
    - יש לשפה מכונה מכריעה (במהירות)
  - $\boldsymbol{NP}$ מקבילה למחלקת השפות ב-RE.
    - יש לשפה מאמת (מהיר)

זכרונות נעימים (למי?)

- המחלקות $\boldsymbol{P}$, $\boldsymbol{NP}$ ו-$\boldsymbol{coNP}$ מזכירות מחלקות מתורת החישוביות
  - $\boldsymbol{P}$ מקבילה למחלקת השפות הכריעות.
    - יש לשפה מכונה מכריעה (במהירות)
  - $\boldsymbol{NP}$ מקבילה למחלקת השפות ב-RE.
    - יש לשפה מאמת (מהיר)
  - $\boldsymbol{coNP}$ מקבילה למחלקת השפות שהמשלימה שלהן ב-RE.

זכרונות נעימים (למי?)

- המחלקות $\boldsymbol{P}$, $\boldsymbol{NP}$ ו-$\boldsymbol{coNP}$ מזכירות מחלקות מתורת החישוביות
  - $\boldsymbol{P}$ מקבילה למחלקת השפות הכריעות.
    - יש לשפה מכונה מכריעה (במהירות)
  - $\boldsymbol{NP}$ מקבילה למחלקת השפות ב-RE.
    - יש לשפה מאמת (מהיר)
  - $\boldsymbol{coNP}$ מקבילה למחלקת השפות שהמשלימה שלהן ב-RE.
- **משפט**: $\boldsymbol{P \subseteq coNP}$.

שאלות פתוחות

- לא ידוע האם $P = NP$ או $P \subset NP$.
  - האם יש שוויון בין המחלקות או שיש הכלה ממש?
  - זו אולי השאלה הפתוחה החשובה ביותר בתורת הסיבוכיות
  - רוב מוחלט של החוקרים סוברים ש- $P \neq NP$ (למה?)

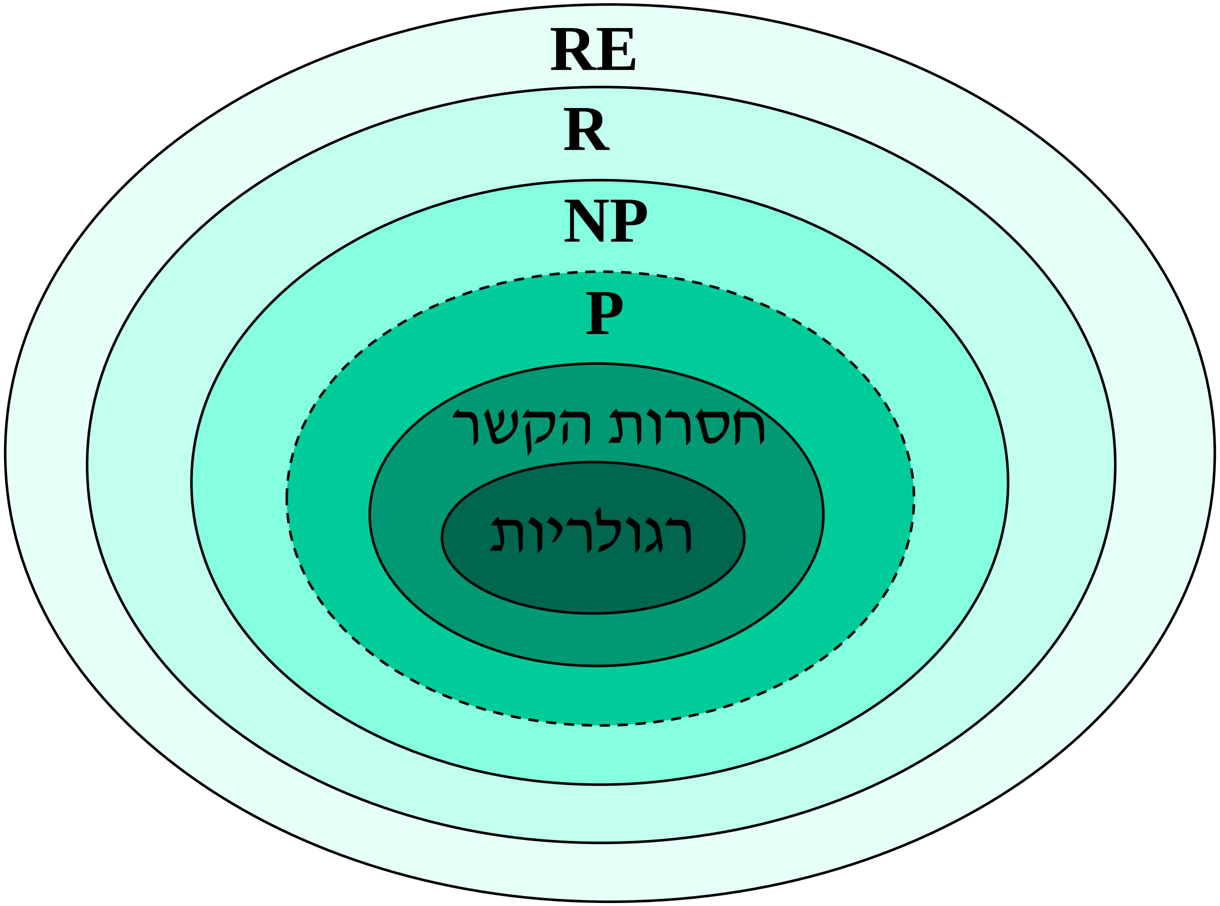
שאלות פתוחות

- לא ידוע האם $P = NP$ או $P \subset NP$.
  - האם יש שוויון בין המחלקות או שיש הכלה ממש?
  - זו אולי השאלה הפתוחה החשובה ביותר בתורת הסיבוכיות
  - רוב מוחלט של החוקרים סוברים ש- $P \neq NP$ (למה?)
- לא ידוע האם $NP = coNP$
  - הסבירו היטב את משמעות השוויון הזה!

שאלות פתוחות

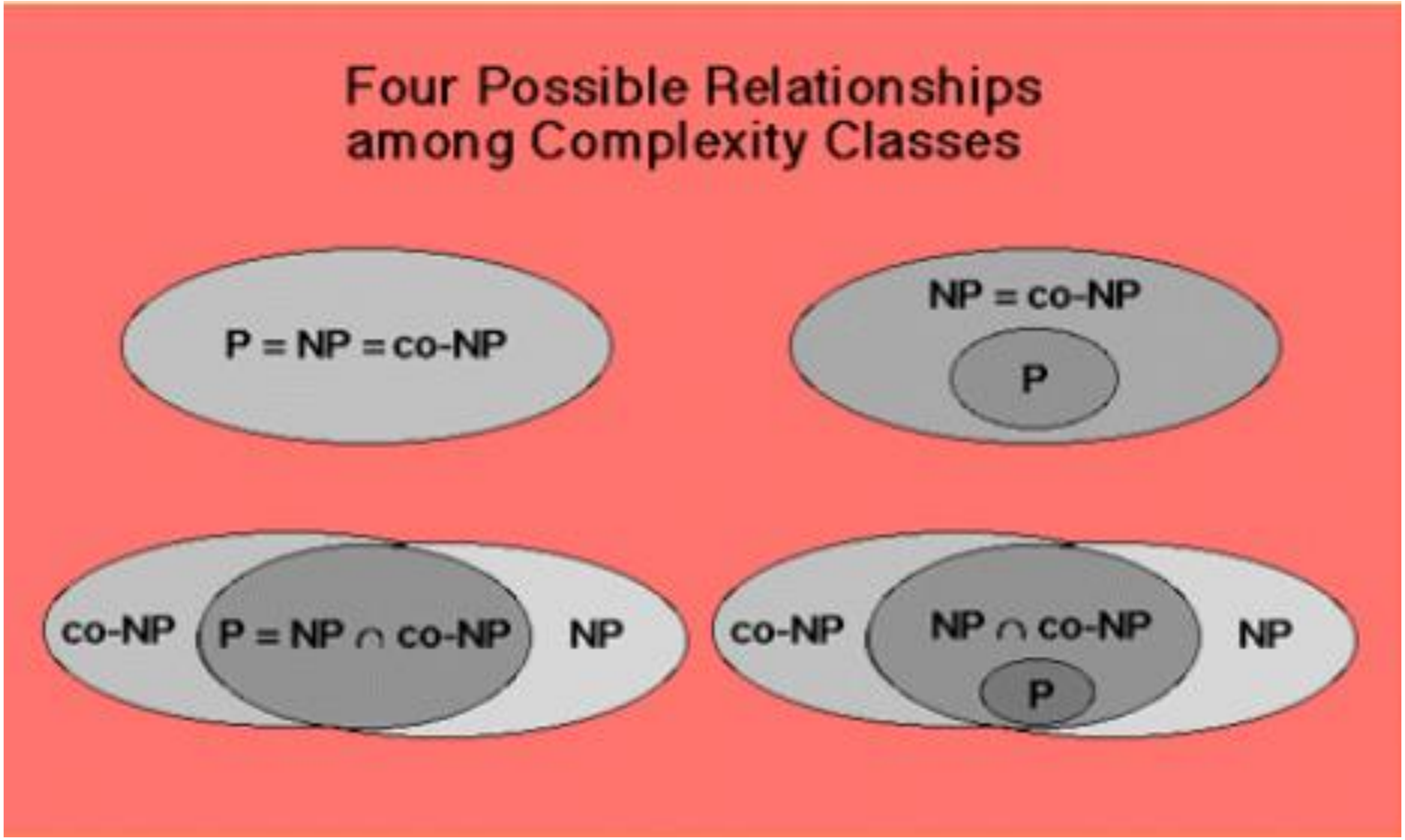
- לא ידוע האם $\boldsymbol{P = NP}$ או $\boldsymbol{P \subset NP}$.
  - האם יש שוויון בין המחלקות או שיש הכלה ממש?
  - זו אולי השאלה הפתוחה החשובה ביותר בתורת הסיבוכיות
  - רוב מוחלט של החוקרים סוברים ש- $\boldsymbol{P \neq NP}$ (למה?)
- לא ידוע האם $\boldsymbol{NP = coNP}$
  - הסבירו היטב את משמעות השוויון הזה!
- לא ידוע האם $\boldsymbol{P = NP \cap coNP}$
  - הסבירו היטב מהי המחלקה $\boldsymbol{NP \cap coNP}$
  - הראו ש-$\boldsymbol{P \subseteq NP \cap coNP}$.

תמונת עולם של המחלקות



האם כל ההכלות בין המחלקות הן הכלות ממש?

P, NP ו- $coNP$: יחסים אפשריים



תכונות סגור של NP

- **תרגיל**: הוכיחו שהמחלקה $\boldsymbol{NP}$ סגורה ל-
  - איחוד
  - חיתוך
  - שרשור
  - איטרציה
- לא ידוע האם $\boldsymbol{NP}$ סגורה למשלים
  - לא ידוע האם $\boldsymbol{NP = coNP}$.