9.6.2025 | ***מודלים חישוביים***

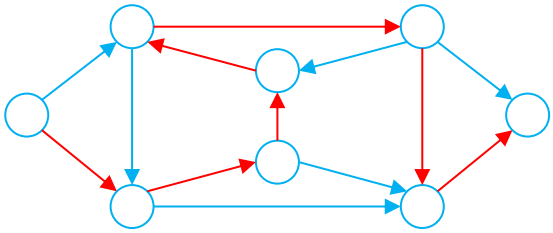
הרצאה 11: חישוב אקראי

Based on previous iterations of this course, given by Nir Bitansky, Rotem Oshman, Iftach Haitner, and Omer Paneth.

מרצה: אורי שטמר

<u>תזכורת:</u> מסלול המילטוני בגרף מכוון G הוא מסלול שמבקר בכל צומת בדיוק פעם אחת.

לדוגמה:



$HAMPATH = \{(G,s,t) : t$ ל s מ מסלול המילטוני עם מכוון גרף $G\}$

<u>טענה:</u> $3SAT \leq_p HAMPATH$

<u>מסקנה:</u> $HAMPATH \in NPC$

<u>הוכחת הטענה:</u>

נתאר רדוקציה f עם התכונות הבאות:

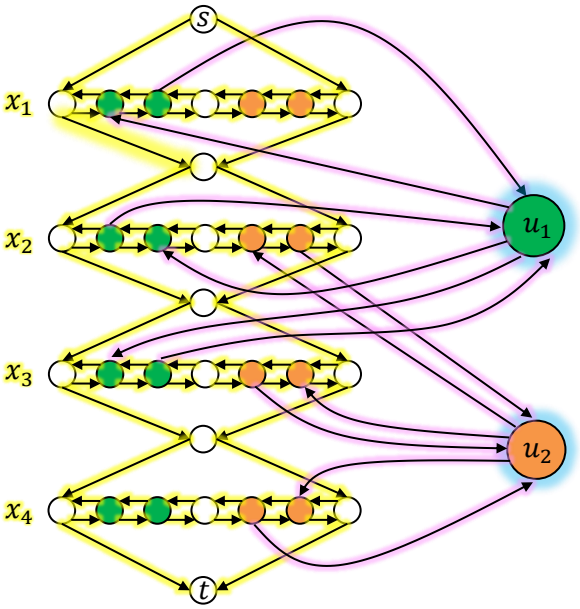
<u>קלט:</u> $\varphi =$ נוסחת 3CNF עם משתנים $x_1, \dots, x_n$ ופסוקיות $c_1, \dots, c_m$

<u>פלט:</u> $(G,s,t) =$ גרף מכוון וזוג קודקודים המוגדרים באופן הבא:

1. לכל פסוקית c_j נוסיף לגרף G צומת u_j
2. לכל משתנה x_i נוסיף לגרף G "יהלום" שניתן לעבור אותו מימין לשמאל או משמאל לימין. בשכבה האמצעית יהיו $3m+1$ צמתים, זוג לכל פסוקית עם צומת רווח בין הזוגות.
3. כל היהלומים האלה מחוברים בשרשרת בין s ל t.
4. לכל ליטרל $z \in \{x_i, \overline{x_i}\}$ ולכל פסוקית c_j שמכילה את z נוסיף "גישה" מהיהלום של x_i לצומת u_j. <u>אם</u> $z = x_i$ הגישה היא בנתיב מימין לשמאל ואם $z = \overline{x_i}$ אז הגישה היא בנתיב משמאל לימין

דוגמה:

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



ניתוח נכונות: כיוון ראשון

תהי φ נוסחת 3CNF ספיקה. נקבע השמה מספקת ל φ ונבנה ממנה מסלול המילטוני מ s ל t ב G:

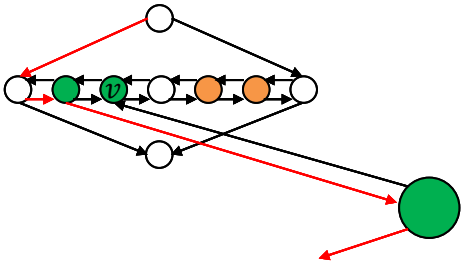
- לכל משתנה x_i נחצה את היהלום שלו מימין לשמאל אם $x_i = 1$ ומשמאל לימין אם $x_i = 0$.
- לכל פסוקית c_j נבחר ליטרל אחד $z \in \{x_i, \overline{x_i}\}$ שמסתפק ונרחיב את המסלול דרך היהלום של x_i כך שנבקר דרך u_j (זה אפשרי כי z מספתק ולכן אנחנו חוצים את היהלום בכיוון המתאים)
- מהבנייה נובע כי זהו מסלול המילטוני מ s ל t ב G.

כיוון שני

נקבע מסלול המילטוני מ s ל t ב G ונבנה ממנו השמה מספקת ל φ:

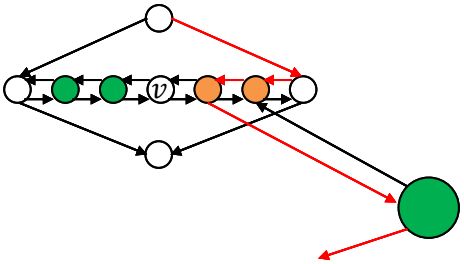
- נאמר שהמסלול הוא נורמלי אם בכל יציאה לקודקוד פסוקית u_j המסלול חוזר מיד לאותו יהלום
- אם המסלול נורמלי אז נבנה ממנו השמה מספקת באופן הבא:
  - אם המסלול נורמלי אז כיוון החציה של כל יהלום מוגדר היטב
  - נציב $x_i = 1$ אם המסלול חוצה את היהלום של x_i מימין לשמאל ואחרת נציב $x_i = 0$.
  - המסלול המילטוני ולכן מגיע לכל צומת u_j דרך היהלום של משתנה x_i כלשהו
  - בגלל כיוון הגישה, ההשמה ל- x_i מספקת את הפסוקית c_j.
- נותר להראות שכל מסלול המילטוני מ s ל t ב G חייב להיות נורמלי.
  - נניח בשלילה שיש לנו מסלול המילטוני לא נורמלי ונסתכל על הפעם הראשונה שהמסלול מפסיק להיות נורמלי.

מקרה א: המסלול יוצא אל קודקוד פסוקית כלשהו דרך "הנתיב הנכון" של יהלום כלשהו, אך לא חוזר מיד לאותו יהלום. בציור:



איך המסלול יגיע ל v? הדרך היחידה להגיע אליו כעת היא דרך הקוד' שמימינו ביהלום, אבל אז המסלול יתקע ב v ולא יוכל להמשיך ל- t.

מקרה ב: המסלול יוצא אל קודקוד פסוקית כלשהו דרך "הנתיב הלא הנכון" של יהלום כלשהו. בציור:



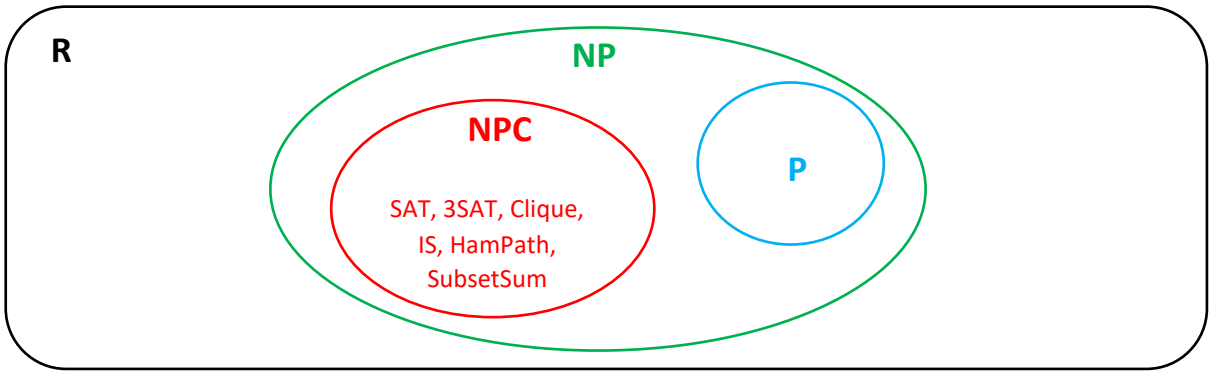
איך המסלול יגיע ל v? הדרך היחידה להגיע אליו כעת היא דרך הקוד' שמשמאלו ביהלום, אבל אז המסלול יתקע ב v ולא יוכל להמשיך ל- t.

הערה: זאת הסיבה לכך שהשארנו "צמתי רווח" בתוך היהלומים שלנו.

מ.ש.ל.

מה יש בין *NP* ל *R* ?

ציור חלקי של תמונת העולם שלנו:



<u>המחלקה coNP</u>

<u>הגדרה:</u>

$$coNP := \{\overline{L} : L \in NP\}$$

מכיוון שאנחנו מכירים 2 הגדרות שקולות ל NP, אז אנחנו גם מקבלים כאן 2 הגדרות שקולות ל coNP:

- שפה L היא ב coNP אם"ם יש מטל"ד שמכריעה את $\overline{L}$ בזמן פולינומי
- שפה L היא ב coNP אם"ם ל- $\overline{L}$ יש אלג' וידוא פולינומי. כלומר ניתן לוודא ביעילות עד לכך שקלט x הוא <u>לא</u> בשפה L.

<u>דיון:</u> עבור מכונות <u>דטר'</u> אנחנו יודעים שאם אפשר להכריע שפה מסויימת בזמן $O(t(n))$ אז גם את $\overline{L}$ אפשר להכריע בזמן $O(t(n))$, ע"י זה שניקח מכריע עבור L ונהפוך את ההחלטה שלו. אבל עבור מטל"ד זה הרבה פחות ברור. מדוע? כי מטל"ד מקבלת קלט אם קיים עלה מקבל בעץ החישוב שלה ולכן אנחנו לא יכולים פשוט "להפוך" את כל ההחלטות של המטל"ד. לכן ייתכן (ומאמינים שזה כך) שיהיו שפות $L \in NP$ כך ש- $\overline{L} \notin NP$.

<u>דוגמה:</u>

$$\overline{CLIQUE} = \{(G,k) : k \text{ גרף לא מכוון שאין בו קליק בגודל } G\} \in coNP$$

לא ידוע האם $\overline{CLIQUE} \in NP$.
באופן כללי לא ידוע האם $NP = coNP$ אך אנו משערים שלא.
כעת נראה שתחת ההנחה כי $NP \neq coNP$ אז $coNP$ לא מכילה שפות NP-שלמות.

<u>טענה:</u> לכל זוג שפות A, B כך ש- $A \leq_p B$ מתקיים:
(א) אם $B \in NP$ אז גם $A \in NP$
(ב) אם $B \in coNP$ אז גם $A \in coNP$

<u>הוכחה:</u>
אם $A \leq_p B$ אז גם $\overline{A} \leq_p \overline{B}$ ולכן (ב) נובע מ (א).
נותר להוכיח את (א).
תהי f רדוקציית מיפוי מ- A ל- B החשיבה בזמן $p_f(n)$.
תהי N_B מטל"ד המכריעה את B בזמן $p_B(n)$.
נבנה מטל"ד N_A שמכריעה את A:

N_A בהינתן קלט x באורך n: מחשבת את $f(x)$ ואז מריצה את $N_B(f(x))$ ומקבלת אם"ם N_B מקבלת.

N_A רצה בזמן פולינומי ולכל x מתקיים ש- $x \in A$ אם"ם $f(x) \in B$ אם"ם $N_B(f(x))$ מקבלת.

<u>מסקנה:</u> תהי $L \in NPC$. מתקיים:

$$L \in coNP \iff NP = coNP$$

<u>הוכחה:</u>
כיוון ראשון ברור (אם $NP=coNP$ אז ברור ש- L גם ב- $coNP$)

כיוון שני – נניח כי $L \in NP$ ונראה כי $NP = coNP$:

- לכל $L' \in NP$ מתקיים $L' \leq_p L$ ולכן $L' \in coNP$.
- באופן דומה, לכל $L' \in coNP$ מתקיים $\overline{L'} \leq_p L$ ולכן $\overline{L'} \in coNP$, כלומר $L' \in NP$.

<u>שאלה:</u> כשדיברנו על RE ועל $coRE$ אז התקיים ש $R = RE \cap coRE$. האם גם עכשיו באופן אנלוגי מתקיים $P = NP \cap coNP$?
<u>תשובה:</u> מאמינים שלא.

<u>הבהרה:</u> שפה L נמצאת ב $NP \cap coNP$ אם ניתן לוודא ביעילות עד לכך ש- $x \in L$ וגם לכך ש- $x \notin L$.

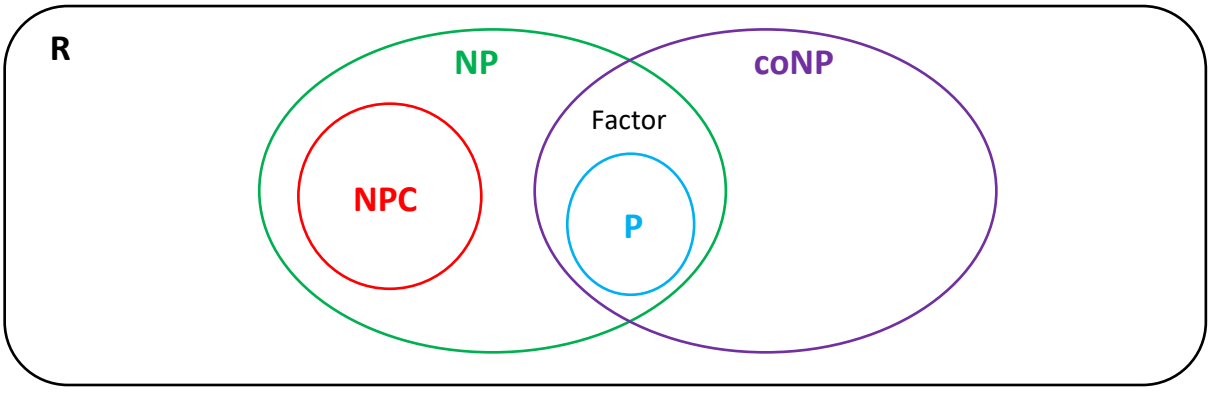
תזכורת:

$$FACTOR = \{\langle N, k\rangle : \text{קיים } 1 < d \leq k \text{ המחלק את } N\}$$

<u>טענה:</u> $FACTOR \in NP \cap coNP$
<u>רעיון:</u> בין אם $\langle N, k\rangle \in FACTOR$ או לא, הפירוק של N לגורמים ראשוניים הוא עד לכך.

אנו משערים ש- $FACTOR \notin P$

תמונת עולם מעודכנת:



מחלקה נוספת שנתעניין בה:

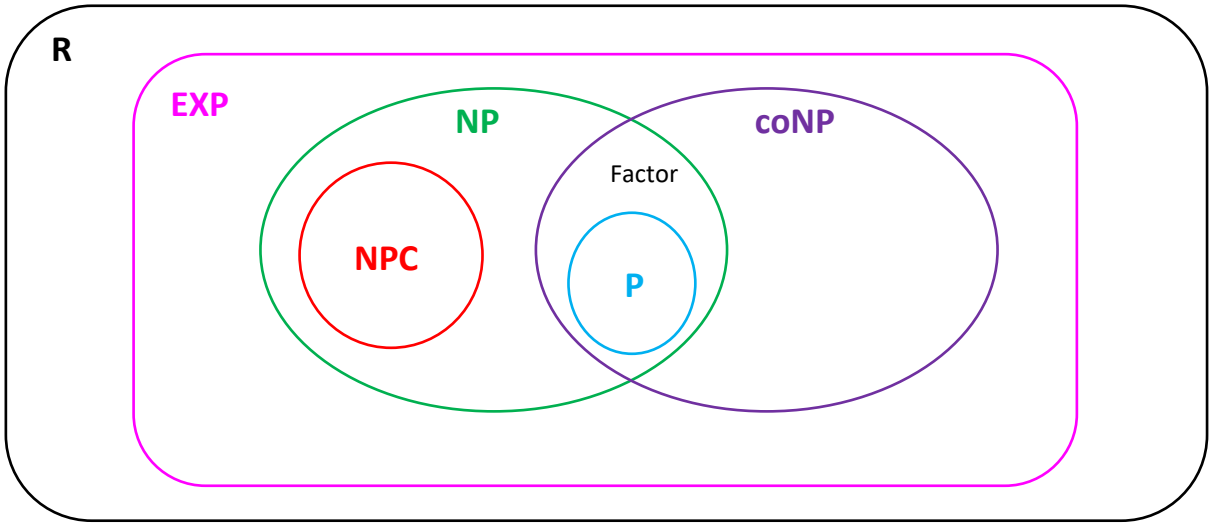
$$EXP \coloneqq \bigcup_{c\in\mathbb{N}} DTime\left(2^{n^c}\right)$$

מחלקת השפות שניתנות להכרעה בזמן אקספוננציאלי על מ"ט דטרמיניסטית.

<u>תזכורת:</u> לכל מטל"ד N שרצה בזמן $t(n)$ קיימת מ"ט דטרמיניסטית M שרצה בזמן $2^{O(t(n))}$ כך ש- $L(M) = L(N)$.

<u>מסקנה:</u> $NP \cup coNP \subseteq EXP$

תמונת עולם מעודכנת:



מה אנחנו יודעים בוודאות לגבי התמונה הזאת?

1. $P \subseteq NP \cap coNP$
2. $Factor \in NP \cap coNP$
3. $P \subsetneq EXP \subsetneq R$. השוני בין המחלקות האלה נובע מהיררכיית הזמן.
4. $NP \cup coNP \subseteq EXP$

כל השאר אנחנו לא יודעים בוודאות, אלא רק מאמינים. למשל:

5. $P \neq NP$, $P \neq coNP$
6. $NP \neq coNP$, $NPC \cap coNP = \emptyset$
7. $NP \cup coNP \subsetneq EXP$. למשל עבור השפה הבאה, שהיא ב *EXP*, מאמינים שהיא לא ב $NP \cup coNP$: בהינתן (קידוד של) מ"ט *M*, קלט *x*, ומספר *k* בייצוג בינארי, האם *M(x)* עוצרת תוך לכל היותר *k* צעדים? השפה הזאת היא ב *EXP* כי בזמן $k \approx$ אפשר לסמלץ את *M* ולבדוק אם היא עוצרת. זה דורש זמן אקספ' כי *k* ניתן לנו בבינארי. מאמינים שהשפה הזאת לא ב $NP \cup coNP$. לא ברור איך "לשכנע" בעזרת עד קצר כי *M(x)* עוצרת...

חישוב אקראי

אחת המטרות העיקריות שלנו בקורס היא להבין מה אפשר לעשות בעזרת חישוב פיזבילי. בהרצאות האחרונות התכנסנו להגדרה של המחלקה P שכוללת את כל הבעיות שאפשר להכריע בזמן פולינומי ע"י מ"ט.
עכשיו אנחנו רוצים להרחיב את ההגדרה שלנו עבור מהו חישוב פיזבילי גם לחישובים שכוללים אקראיות. למשל quicksort הוא אלגוריתם מאוד יעיל אבל הוא לא נכלל תחת המטרייה של מ"ט כמו שהגדרנו אותה כי הוא משתמש בארקראיות.

<u>הגדרה לא פורמלית (נפרמל בהמשך):</u> אלגוריתם אקראי הוא אלגוריתם שלאורך החישוב יכול להטיל מטבעות ולהמשיך בחישוב על פי תוצאת המטבע.

דוגמה: כפל מטריצות

<u>הגדרה:</u>

$$MATMULT = \{(A,B,C) : A \cdot B = C \text{ ומתקיים } A,B,C \in \mathbb{Z}^{n\times n}\}$$

- בעזרת אלגוריתם נאיבי לכפל מטריצות ניתן להכריע את $MATMULT$ בזמן $O(n^3)$
- האלג' הטוב ביותר לכפל מטריצות כיום רץ בזמן $O(n^{2.371552})$

נתאר אלגוריתם אקראי M שרץ בזמן $O(n^2)$ כך ש:
- בהינתן $(A,B,C) \in MATMULT$ תמיד מקבל
- בהינתן $(A,B,C) \notin MATMULT$ דוחה בהסתברות לפחות $1-2^{-100}$

כלומר אנחנו מאבדים פה את הוודאות בנכונות תשובת האלגוריתם. הרצנו אלג' ויש לנו הסת' שהוא טעה. פילוסופית זה מעיק. מעשית, מאורע בהסתברות 2^{-100} לא יקרה. לצורך השוואה: ההסתברות לזכות בלוטו 4 מקום ראשון פעמים ברצף היא יותר גדולה מ 2^{-100}. ההסתברות הזאת היא בערך 2^{-92}.

<u>M בהינתן קלט (A,B,C):</u>
- נחזור על הבדיקה הבאה 100 פעמים:
  - נגריל ווקטור אקראי $r \in \{0,1\}^n$
  - נחשב $x_r = A \cdot B \cdot r$ ואת $y_r = C \cdot r$
  - אם $x_r \neq y_r$ אז נדחה
- נקבל

זמן ריצה $O(n^2)$ (הכפלת מטריצה בווקטור)

נכונות:
- אם $A \cdot B = C$ אז לכל r מתקיים $x_r = y_r$ ולכן M תמיד יקבל.
- נותר להראות שאם $A \cdot B \neq C$ אז M דוחה בהסתברות לפחות $1-2^{-100}$.
- מספיק להראות שבכל איטרציה M דוחה בהסתברות לפחות 0.5.

<u>טענה:</u> לכל $D \in \mathbb{Z}^{n\times n}$ שאינה זהותית אפס מתקיים: $\Pr_{r\leftarrow\{0,1\}^n}[D \cdot r \neq 0] \geq 0.5$

מהטענה נובע שאם $A \cdot B \neq C$ אז בכל איטרציה M דוחה בהסתברות
$$\Pr_{r \leftarrow \{0,1\}^n}[x_r \neq y_r] = \Pr_{r \leftarrow \{0,1\}^n}[(A \cdot B - C) \cdot r \neq 0] \geq 0.5$$

<u>הוכחת הטענה:</u> תהי $D \in \mathbb{Z}^{n \times n}$ שאינה זהותית אפס. נניח בה"כ כי $D_{1,1} \neq 0$.
נספור עבור כמה ווקטורים r יתכן שמתקיים $D \cdot r = 0$.
נקבע את $r_2, r_2, \dots, r_n$. מהי הקואורדינטה הראשונה של $D \cdot r$?

$$\sum_{i=1}^{n} D_{1,i} \cdot r_i = D_{1,1} \cdot r_1 + \underbrace{\sum_{i=2}^{n} D_{1,i} \cdot r_i}_{\substack{\text{קבענו את } r_2,\dots,r_n \\ \text{ולכן הסכום קבוע.} \\ \text{נסמן אותו ב } b}}$$

אם $D \cdot r = 0$ אז בפרט הקואו' הראשונה בתוצאה שווה אפס ולכן
$$D_{1,1} \cdot r_1 + b = 0$$
כלומר
$$r_1 = \frac{-b}{D_{1,1}}$$

לכל היותר אחת מהאפשרויות $r_1 \in \{0,1\}$ תקיים את השוויון

(אם למשל $\frac{-b}{D_{1,1}} = 2.5$ אז אף בחירה של r_1 לא תקיים את זה...)

מסקנה: לכל בחירה של $r_2, r_3, \dots, r_n$ קיימת לכל היותר בחירה אחת של r_1 כך ש- $D \cdot r = 0$.

לכן יש לכל היותר 2^{n-1} ווקטורים r כך ש- $D \cdot r = 0$.

לכן,
$$\Pr_{r \leftarrow \{0,1\}^n}[D \cdot r \neq 0] \geq \frac{2^{n-1}}{2^n} = \frac{1}{2}$$

דוגמה נוספת: זהות פולינומים

תזכורת: פולינום במשתנה אחד הוא סכום סופי מהצורה
$$f(x) = a_0 + a_1 \cdot x + a_2 \cdot x^2 + \cdots + a_d \cdot x^d$$

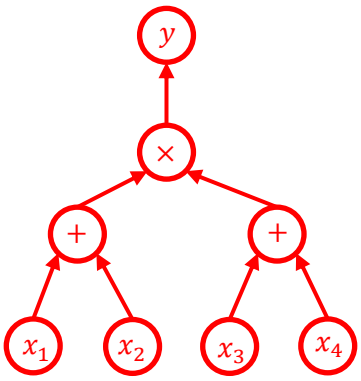
<u>הגדרה:</u> פולינום ב n משתנים הוא סכום של מונומים, כאשר כל מונום הוא מהצורה:
$$a \cdot x_1^{e_1} \cdot x_2^{e_2} \cdots x_n^{e_n}$$
כאשר $e_i \geq 0$ שלם עבור כל i.
דרגת המונום היא $\sum e_i$
דרגת הפולינום: מקסימום דרגם המונומים בפולינום.

דוגמה: פולינום מדרגה 3

$$f(x,y,z) = 5x^2y + z^3 + 9yz + 4$$

אנחנו נתעניין בבעיה הבאה הנקראת Polynomial Identity Testing. בצורה לא פורמלית, בהינתן פולינום, המטרה שלנו היא להכריע האם זהו פולינום האפס או לא. העניין הוא שהפולינום לא ניתן לנו בצורה מפורשת (כלומר אנחנו לא מקבלים רשימה של כל המקדמים) אלא אנחנו מקבלים את הפולינום בצורה "דחוסה", על ידי נוסחה אריטמטית (AF) מהצורה

$$(x_1 + 7x_2) \cdot (x_3 + x_4 + 3x_5) \cdot x_2 \cdot (x_5 - x_6) + x_2 \cdot x_4(2x_3 + 3\,x_5)$$



הגדרה: נוסחה אריטמטית (AF) היא נוסחה (מעגל עם fan-out=1) עם שערי $+, \times, 0, 1$. כלומר אנחנו מרשים שערי כפל, חיבור, ושערים קבועים 0 ו- 1.

למשל, המעגל משמאל מגדיר את הנוסחה הבאה:

$$\phi(x_1,x_2,x_3,x_4) = (x_1 + x_2)(x_3 + x_4)$$
$$= x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4$$

הגדרה:

$$PIT = \{\phi : \phi \text{ is an } AF \text{ and } \phi \equiv 0\}$$

הערה: מעל שדות אינסופיים (כמו הממשיים) מתקיים שפולינום הוא זהותית אפס אם"ם כל המקדמים שלו הם אפס. לכן אם היו נותנים לנו את הפולינום בצורה מפורשת אז היה לנו קל להחליט אם הוא פולינום האפס. (זה לא בהכרח נשאר נכון גם מעל שדות סופיים, אבל היום נדבר רק על פולינומים מעל הממשיים).

שאלה: איך מראים שמעל הממשיים פולינום הוא זהותית אפס אם"ם כל המקדמים שלו הם אפס?
תשובה: הוכחה באינדוקציה על מספר המשתנים:

- בסיס: נסו להשתכנע שבפולינום במשתנה אחד, אם יש מקדם לא אפס אז הפולינום הוא לא זהותית אפס, כלומר יש קלטים עליהם הפולינום לא מתאפס.
- צעד: בהינתן פולינום מדרגה n, נחשוב עליו כפולינום במשתנה אחד x_n שהמקדמים שלו הם פולינומיים בשאר המשתנים.
- כלומר

$$f(x_1,\dots,x_n) = \sum_{i=0}^{d} q_i(x_1,\dots,x_{n-1}) \cdot x_n^i$$

כאשר לפחות אחד ה q_i מכיל מקדם לא-אפס.

- לפי הנחת האינדוקציה, קיימים ערכים $a_1,\dots,a_{n-1}$ עבורם $q_i(a_1,\dots,a_{n-1}) \neq 0$.
- כעת קיבלנו פולינום במשתנה אחד $r(x_n) = f(a_1,\dots,a_{n-1},x_n)$ שיש לו מקדם לא אפס, ולכן יש קביעה של x_n עבורה f לא מתאפס.

<u>בדיקת שפיות:</u> מה הבעיה עם האלגוריתם אשר בהינתן נוסחה, "פותח" את כל הסוגריים ומחשב את הייצוג המפורש של הפולינום ואז רואה האם כל המקדמים הם אפס?

<u>תשובה:</u> זה יכול לקחת זמן אקספוננציאלי. למשל עבור הנוסחה
$(x_1 + x_2)(x_3 + x_4)(x_5 + x_6) \cdots (x_{2n-1} + x_{2n})$
אם נפתח את הסוגריים אז נקבל 2^n מונומים...

האם $PIT \in P$? כלומר האם קיים אלג' דטר' פולינומי שמכריע את PIT?
לא ידוע! מאמינים שכן, אבל לא יודעים להראות אלגוריתם כזה. נכון להיום ידועים רק אלג' למקרים פרטיים של הבעיה, תחת הגבלות מסויימות על הנוסחאות האפשריות.

נראה אלג' אקראי ל PIT שרץ בזמן פולינומי.

<u>הרעיון:</u> נעריך את הפולינום בנקודות אקראיות, ואם בכל הנסיונות הוא ישתערך לאפס אז "נשתכנע" שזהו פולינום האפס.

בשביל שזה יפעל אנחנו נסתמך על העובדות הבאות שמראות שאם פולינום הוא לא זהותית אפס אז מספר הנקודות עליהן הוא מתאפס הוא קטן יחסית. ספציפית:

<u>תזכורת – משפט מאלגברה (סקיצת הוכחה באפנדיקס):</u> לפולינום במשתנה 1 מדרגה לכל היותר d יש לכל היותר d שורשים, אלא אם הוא פולינום האפס.

האם גם לפולינום עם כמה משתנים יש מספר חסום של שורשים? לא. למשל:
$p(x_1, x_2) = (x_1 - 3)(x_2 - 5)$
יש אינסוף שורשים. כל הנקודות מהצורה $(a, 5)$ ו- $(3, b)$ לכל a, b.

כלומר מספר השורשים יכול להיות לא חסום גם כאשר הדרגה חסומה. מה כן אפשר להגיד?

<u>למה "שוורץ-זיפל" (הוכחה באפנדיקס):</u> יהי $p(x_1, \dots, x_n)$ פולינום שאינו זהותית אפס ב- n משתנים שדרגתו $d \geq$ ויהי m מספר טבעי. תהי $S \subseteq \mathbb{R}$ בגודל $|S| = m$. אז מספר השורשים של $p(x_1, \dots, x_n)$ בקבוצה S^n הוא לכל היותר $d \cdot m^{n-1}$.

<u>מסקנה:</u>

$$\Pr_{(x_1,\dots,x_n)\leftarrow S^n}[p(x_1, \dots, x_n) = 0] \leq \frac{d \cdot m^{n-1}}{m^n} = \frac{d}{m}$$

<u>לדוגמה:</u> נסתכל על $p(x, y) = x \cdot y$. זהו פולינום מדרגה 2. עבור $S = \{0,1,2, \dots,9\}$ מתקיים שיש ל p בדיוק 19 שורשים בקבוצה S^2:
$(0,0), (0,1), \dots, (0,9), (1,0), \dots, (9,0)$
ולכן, אם נגריל נקודה מהקבוצה S^2, ההסתברות שנפגע בשורש היא לכל היותר
$$\frac{19}{100} = 0.19 < \frac{2 \cdot 10}{100} = 0.2$$
כנדרש.

נתאר אלג' אקראי לבעיית PIT:

- בהינתן ϕ נבחר $S \subseteq \mathbb{R}$ כך ש- $|S| > 100 \cdot \deg(\phi)$
- נגריל $x = (x_1, \dots, x_n) \leftarrow S^n$ ונקבל אם"ם $\phi(x) = 0$.

אם $\phi \equiv 0$ אז נקבל תמיד.
אם $\phi \not\equiv 0$ אז נקבל בהסתברות לכל היותר

$$\frac{\deg(\phi)}{|S|} = \frac{\deg(\phi)}{100 \cdot \deg(\phi)} = \frac{1}{100}$$

שאלה למחשבה: איך בהינתן ϕ מחשבים חסם על הדרגה.

המודל הפורמלי ומח' סיבוכיות

<u>הגדרה:</u> מ"ט אקראית עם זמן ריצה $t(n)$ היא מ"ט דו-סרטית:

- סרט עבורה שמכיל בתחילת הריצה את הקלט x
- סרט אקראיות שמכיל בתחילת הריצה מחרוזת $r \in \{0,1\}^{t(|x|)}$.

<u>סימונים:</u>

- נסמן ב- $M(x;r)$ ריצה של מ"ט אקראית M עם קלט x ואקראיות r
- לעיתים נתייחס ל- $M(x;r)$ כאינדיקטור: 1 אם $M(x;r)$ מקבלת ו- 0 אם דוחה
- נסמן ב- $M(x)$ את המשתנה המקרי $M(x;r)$ כאשר r מחרוזת אקראית באורך $t(|x|)$

<u>הגדרה (randomized polynomial time):</u>

תהי $\alpha: \mathbb{N} \to [0,1]$. שפה L שייכת למחלקה $RP(\alpha(n))$ אם קיימת מ"ט אקראית M שרצה בזמן פולינומי $t(n)$ כך שלכל n מספיק גדול ולכל קלט x באורך n מתקיים:

- אם $x \in L$ אז

$$\Pr_{r \leftarrow \{0,1\}^{t(n)}}[M(x;r) = 1] \geq \alpha(n)$$

- אם $x \notin L$ אז

$$\Pr_{r \leftarrow \{0,1\}^{t(n)}}[M(x;r) = 1] = 0$$

כלומר $RP(\alpha(n))$ היא מחלקת כל השפות שניתנות להכרעה בזמן פולינומי על ידי מ"ט אקראית עם שגיאה חד-צדדית לכל היותר $(1 - \alpha(n))$ על קלטים בשפה.

<u>אבחנות:</u>

1. אם $\alpha(n) \leq \beta(n)$ לכל n אזי $RP(\beta(n)) \subseteq RP(\alpha(n))$
2. לכל $\alpha(n) \in [0,1]$ מתקיים $P = RP(1) \subseteq RP(\alpha(n))$. מדוע?
3. לכל $\alpha(n) \in (0,1]$ מתקיים $RP(\alpha(n)) \subseteq NP$. מדוע? העד הוא r כך ש- $M(x;r) = 1$...

שאלה: האם *PIT* שייכת ל *RP*?
תשובה: מה שאנחנו הראינו זה שקיים אלג' עם טעות חד-כיוונית בכיוון ההפוך...

<u>הגדרה:</u> $coRP(\alpha(n)) \coloneqq \{\overline{L} : L \in RP(\alpha(n))\}$

כלומר, $coRP(\alpha(n))$ היא מחלקת השפות שניתנות להכרעה בזמן פולינומי ע"י מ"ט אקראית עם שגיאה חד-צדדית לכל היותר $(1-\alpha(n))$ על קלטים <u>לא</u> בשפה. כלומר:

- *RP*: לעולם לא טועים עבור $x \notin L$
- *coRP*: לעולם לא טועים עבור $x \in L$

הדוגמאות שראינו היום מוכיחות: $PIT \ , \ MATMULT \in coRP(0.99)$

<u>צמצום שגיאה חד-צדדית:</u>

<u>טענה:</u> לכל $d, c \in \mathbb{N}$ מתקיים

$$RP(n^{-c}) = RP(1 - 2^{-}n^{d})$$

<u>הוכחה:</u>

הכיוון $RP(n^{-c}) \supseteq RP(1 - 2^{-}n^{d})$ ברור.

בכיוון השני, תהי $L \in RP(n^{-c})$ ותהי M מ"ט אקראית שרצה בזמן פולינומי $t(n)$ אשר מקבלת $x \in L$ בהסתברות לפחות n^{-c} ודוחה $x \notin L$ בהסתברות 1.

נגדיר מ"ט אקראית M' שרצה בזמן $O(t(n) \cdot n^{c+d})$:

M' בהינתן קלט x באורך n:
• מריצה $\ell = n^{c+d}$ פעמים את $M(x)$ ובכל הרצה משתמשת באקראיות חדשה
• מקבלת אם"ם לפחות אחת מהריצות קיבלה.

ניתוח:

- אם $x \notin L$ אז $M(x)$ תמיד דוחה ולכן גם $M'(x)$ תמיד דוחה
- אם $x \in L$ אז $M'(x)$ דוחה רק אם <u>כל</u> הריצות של $M(x)$ דחו, מה שקורה בהסתברות לכל היותר

$$(1 - n^{-c})^{\ell} \leq \left(e^{-n^{-c}}\right)^{\ell} = e^{-n^{-c} \cdot \ell} = e^{-n^{d}} \leq 2^{-n^{d}}$$

- ולכן $L \in RP(1 - 2^{-}n^{d})$

<u>מוסכמה:</u>

$$coRP = coRP(1/2) \quad , \quad RP = RP(1/2)$$

<u>הגדרה (bounded-error probabilistic polynomial time):</u>

יהיו $\alpha, \beta: \mathbb{N} \to [0,1]$. שפה L שייכת למחלקה $BPP(\alpha(n), \beta(n))$ אם קיימת מ"ט אקראית M שרצה בזמן פולינומי כך שלכל n מספיק גדול ולכל קלט x באורך n מתקיים:

- אם $x \in L$ אז

$$\Pr_{r \leftarrow \{0,1\}^{t(n)}}[M(x;r) = 1] \geq \beta(n)$$

- אם $x \notin L$ אז

$$\Pr_{r \leftarrow \{0,1\}^{t(n)}}[M(x;r) = 1] \leq \alpha(n)$$

מוסכמה:

$$BPP = BPP\left(\frac{1}{4}, \frac{3}{4}\right)$$

כלומר *BPP* היא מחלקת כל השפות הניתנות להכרעה בזמן פולינומי ע"י מ"ט אקראית עם שגיאה דו-צדדית לכל היותר רבע.

מתקיים:

$$coRP\big(\alpha(n)\big) = BPP(1-\alpha(n), 1) \quad , \quad RP(\alpha(n) = BPP\big(0, \alpha(n)\big)$$

צמצום שגיאה דו-צדדית:

טענה: לכל $c, d \in \mathbb{N}$ ו- $\alpha(n)$ חשיבה בזמן פולינומי כך ש- $n^{-c} \leq \alpha(n) \leq 1 - n^{-c}$ מתקיים:

$$BPP(\alpha(n) - n^{-c}, \alpha(n) + n^{-c}) \subseteq BPP\left(2^{-n^d}, 1 - 2^{-n^d}\right)$$

לשם פשטות נוכיח גרסה מוחלשת של הטענה: נראה כי $\boldsymbol{BPP \subseteq BPP\left(2^{-0.2d}, 1 - 2^{-0.2d}\right)}$

הוכחה: נריץ את M (המ"ט עם שגיאה דו-צדדית רבע) ℓ פעמים על הקלט x ונענה לפי החלטת הרוב. נסמן ב- p את ההסתברות ש M טועה על x (בריצה אחת). אנחנו יודעים כי $p \leq 1/4$. נקבל:

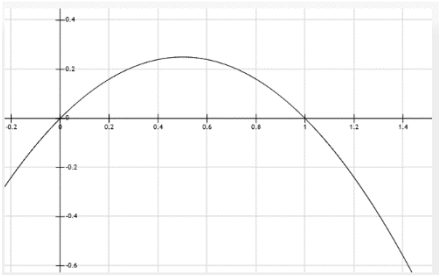
$$\Pr\begin{bmatrix}\text{החלטת}\\ \text{הרוב}\\ \text{טועה}\end{bmatrix} = \sum_{t=\frac{\ell+1}{2}}^{\ell} \Pr\begin{bmatrix}M \text{ טועה}\\ t \text{ פעמים}\end{bmatrix} = \sum_{t=\frac{\ell+1}{2}}^{\ell} \binom{\ell}{t} p^t (1-p)^{\ell-t}$$

נשים לב. בטור הזה, ככל ש t גדל אנחנו מעבירים משקל מ *(1-p)* ל *p* מה שמקטין את האיברים. נסמן $t' = \frac{\ell+1}{2}$ ואז הטור הזה קטן מ:

$$\leq \sum_{t=t'}^{\ell} \binom{\ell}{t} p^{t'} (1-p)^{\ell-t'} = p^{t'} (1-p)^{\ell-t'} \sum_{t=t'}^{\ell} \binom{\ell}{t} = p^{\frac{\ell+1}{2}} (1-p)^{\frac{\ell-1}{2}} \sum_{t=t'}^{\ell} \binom{\ell}{t}$$

$$\leq p^{\frac{\ell+1}{2}} (1-p)^{\frac{\ell-1}{2}} \cdot 2^{\ell} = p \cdot \big(p(1-p)\big)^{\frac{\ell-1}{2}} \cdot 2^{\ell}$$

נתבונן בפונקציה $p(1-p)$:



אנחנו יודעים ש- $0 \leq p \leq \frac{1}{4}$ ולכן המקסימום של הפונק' הזאת מתקבל עבור $p = \frac{1}{4}$. כלומר

$$p(1-p) \leq \frac{1}{4} \cdot \frac{3}{4} = \frac{3}{16}$$

לכן:

$$p \cdot \big(p(1-p)\big)^{\frac{\ell-1}{2}} \cdot 2^{\ell} \leq \frac{1}{4} \cdot \left(\frac{3}{16}\right)^{-\frac{1}{2}} \cdot \left(\frac{3}{16}\right)^{\frac{\ell}{2}} \cdot 2^{\ell} \leq \left(\frac{3}{16}\right)^{\frac{\ell}{2}} \cdot 2^{\ell} = \left(\frac{3}{16} \cdot 4\right)^{\frac{\ell}{2}} = \left(\frac{3}{4}\right)^{\frac{\ell}{2}} \leq 2^{-0.2\ell}$$

אפנדיקס – הוכחת הלמה של שוורץ-זיפל

<u>תזכורת ללמה:</u> יהי $p(x_1,\dots,x_n)$ פולינום שאינו זהותית אפס ב- n משתנים שדרגתו $d \geq$ ויהי m מספר טבעי. תהי $S \subseteq \mathbb{R}$ בגודל $|S| = m$. אז מספר השורשים של $p(x_1,\dots,x_n)$ בקבוצה S^n הוא לכל היותר $d \cdot m^{n-1}$.

הוכחה באינדוקציה על מספר המשתנים n.

<u>בסיס:</u> $n = 1$
צריך להוכיח מספר השורשים הוא לכל היותר $d \cdot m^0 = d$. נובע ממשפט באלגברה לגבי מספר השורשים של פולינום במשתנה אחד שאינו זהותית אפס.

<u>צעד:</u> נתון p פוילנום ב n משתנים. נרשום את p בצורה הבאה:

$$p(x_1,\dots,x_n) = \sum_{i=0}^{d} p_i(x_1,\dots,x_{n-1}) \cdot x_n^i$$

כלומר כתבנו את p כפולינום ב x_n שכל מקדם הוא פולינום ב $x_1, x_2, \dots, x_{n-1}$.

דוגמה: אם $p = x_1 + x_1x_2 + 3x_1^5x_2 + x_1^2x_2^2$
אז נקבל

$$p = 0 \cdot x_2^6 + 0 \cdot x_2^5 + 0 \cdot x_2^4 + 0 \cdot x_2^3 + (x_1^2) \cdot x_2^2 + (x_1 + 3x_1^5) \cdot x_2 + (x_1) \cdot x_2^0$$

נסמן ב t את האינדקס המקסימלי כך ש- $p_t(x_1,\dots,x_{n-1})$ אינו זהותית אפס.

מהי דרגת p_t ?

אנחנו יודעים שהדרגה של $p_t(x_1,\dots,x_{n-1}) \cdot x_n^t$ היא לכל היותר d
ולכן הדרגה של p_t היא לכל היותר $d - t$.

p_t הוא פולינום ב *n-1* משתנים ולכן לפי הנחת האינדוקציה מספר השורשים שלו הוא לכל היותר $(d-t) \cdot m^{n-2}$.

עכשיו אנחנו רוצים לספור כמה שורשים יכולים להיות ל p.

נחלק את השורשים $x_1,\dots,x_n$ של p לשתי קבוצות זרות:

(1) שורשים כך ש- $p_t(x_1,\dots,x_{n-1}) = 0$.
- ל p_t יש לכל היותר $(d-t) \cdot m^{n-2}$ שורשים, וכלך שורש כזה אפשר להרחיב ע"י לכל היותר m אפשרויות לשורש של p.
- לכן סה"כ מספר השורשים מקבוצה (1) הוא לכל היותר $(d-t) \cdot m^{n-1}$

(2) שורשים כך ש- $p_t(x_1,\dots,x_{n-1}) \neq 0$.
- נקבע $x_1,\dots,x_{n-1}$ כך ש- $p_t(x_1,\dots,x_{n-1}) \neq 0$.
- אחרי הצבת $x_1,\dots,x_{n-1}$ בפולינום p נשאר עם פולינום ב- x_n שדרגתו היא t ולכן יש לו לכל היותר t שורשים.
- יש m^{n-1} אפשרויות ל $x_1,\dots,x_{n-1}$ ולכל אפשרות כנ"ל יש לכל היותר t אפשרויות להרחיב לשורש של p.
- סה"כ יש לכל היותר $t \cdot m^{n-1}$ שורשים בקבוצה השניה.

לכן סך כל מספר השורשים הוא לכל היותר $(d-t) \cdot m^{n-1} + t \cdot m^{n-1} = d \cdot m^{n-1}$

מ.ש.ל.

אפנדיקס – לפולינום מדרגה d במשתנה 1 יש $\geq d$ שורשים

(כמובן בהנחה שהפולינום לא זהותית אפס...)

הוכחה באינדוקציה על הדרגה *d*.

<u>בסיס *(d=1)*:</u> פולינום מדרגה 0 הוא קבוע, למשל *p(x)=7* ולכן יש לו 0 שורשים

<u>צעד:</u> יהי *p(x)* פולינום מדרגה *d* ונניח ש *a* הוא שורש, כלומר *p(a)=0*. אז אפשר לרשום
$$p(x) = (x-a)q(x)$$
עבור איזשהו פולינום q מדרגה d-1, שלפי ה.א. יש לו לכל היותר d-1 שורשים.
לכן ל p יש לכל היותר d שורשים בסה"כ (השורשים של q והשורש a).

מ.ש.ל.