בס"ד

# סיכום סיבוכיות (ללא הוכחות) – מיכאל שחר

## מחלקות ומושגים בסיסיים

### בעיית חיפוש

כל בעיית חיפוש למעשה ניתנת לתיאור על ידי יחס $R \subseteq \{0,1\}^* \times \{0,1\}^*$

יחס $R$ ייקרא **חסום פולינומיאלית** אם קיים פולינום p כך שעבור כל זוג $(x,y) \in R$ מתקיים $|y| \leq p(|x|)$.

### המחלקה PF

$$PF = \left\{ R \middle| \begin{matrix} R \text{ is polynimal bounded}, \exists A \text{ polynomial, and } A(x) \text{ return } y \text{ such that} \\ (x,y) \in R \text{ or } \perp \text{ if no such } y \text{ exist} \end{matrix} \right\}$$

ומוגדר גם אוסף הפתרונות האפשריים עבור x:

$$R(x) = \{y | (x,y) \epsilon R\}$$

### המחלקה PC

$$PC = \{R | R \text{ is polynimal bounded}, \exists A \text{ polynomial, and } A(x,y) = 1 \Leftrightarrow (x,y) \in R\}$$

### המחלקה P

$$P = \{S \mid \text{there is determenistic poly algorithm } A_S \text{ such that: } A_S(x) = 1 \Leftrightarrow x \in S\}$$

### המחלקה NP

$$\text{NP} = \{S \mid \text{there is a "proof system from type NP" for the problem } S\}$$

#### מערכת הוכחה מסוג NP עבור בעיה S

היא זוג (V,P) כאשר V "מוודא", אלגוריתם פולינומי דטרמיניסטי, ו-P פולינום כך שמתקיימות הדרישות הבאות:

1) **שלמות**: טענות חוקיות ניתנות להוכחה.
$x \in S \Longrightarrow \exists y \; |y| < p(|x|) \; \text{ such that } \; V(x,y) = 1$
2) **נאותות**: טענות לא חוקיות לא ניתנות להוכחה. $x \notin S \Longrightarrow \forall y \;\; V(x,y) = 0$

### co-NP

$$co - NP = \{\{0,1\}^* \backslash L \mid L \in NP\}$$

ובדומה עם P.

לדוגמא, עבור $SAT \in NP$ אוסף הנוסחאות הספיקות, $\overline{SAT} \in co - NP$ – אוסף הנוסחאות שאינן ספיקות.

בעיות הכרעה ניתנות לתיאור בעזרת קבוצות

$$S = \{x \mid x \text{ has property } \pi\}$$

### טענות שהוכחו בהרצאה

1) $NP = P \Leftrightarrow PC \subseteq PF$
2) $PF \nsubseteq PC, \quad \exists R \in PF \backslash PC$
3) $L \in NP \Rightarrow R_L = \{(x,y) \mid V(x,y) = 1\} \in PC\} \mid R \epsilon PC \Rightarrow S_R = \{x \mid \exists y: (x,y) \epsilon R\}$

## רדוקציות ומחלקות נוספות

### מכונת טיורינג בעלת גישת אורקל

נאמר כי מכונה M היא מכונת טיורינג בעלת גישת אורקל לפונקציה f וסמן $M_f$ אם M מ"ט רגילה ובנוסף יכולה לבצע קריאה לf, וכך להכריע האם $x \in A$, בעלות של צעד בודד

### רדוקציית קוק

רדוקציית קוק מA לB הינה מ"ט פולינומית הפותרת את A על ידי גישת אורקל לB.

מסמנים $A \leq_T^p B$ או $A \in P^B$.

### רדוקציית קארפ פולינומית: many to one

מקרה פרטי של רדוקציית קוק היא רדוקציית קארפ. תהיינה A וB בעיות הכרעה. נאמר שקיימת רדוקציית קארפ מA לB ונסמן $A \leq_m^p B$ אם קיימת פונקציה $f$ הניתנת לחישוב בזמן פולינומי ומתקיים $f(x) \in B \Leftrightarrow x \in A$

רדוקציית קארפ סגורה ב*P*: אם מתקיים $A \leq_m^p B$ וגם $B \in P$ אזי $A \in P$

היא סגורה גם ב*NP*.

### רדוקציה עצמית

רדוקצייה עצמית היא רדוקציית קוק מ-R לבעיית ההכרעה המתאימה לה $S_R$. כלומר בהינתן קלט x ואלגוריתם A המחזיר האם קיים או לא קיים פתרון ל-x, ניתן ליצור אלגוריתם M המוצא את הפתרון y, אם קיים, תוך שימוש ב-A/עם גישת אורקל ל-$S_R$, בזמן פולינומי (עד כדי זמן הריצה של A).

<u>הדגמה:</u>

בעיות לדוגמא ב-*PC*:

$$Clique = \{(<G,k>, C): |C| \geq k, C \text{ is a clique in } G\}$$
$$IS = \{(<G,k>, IS):$$
$$|IS| \geq k, IS \text{ an independent set (has no direct edge between to edges) in } G\}$$

ובעיות ההכרעה המתאימות הן:

$$S_{Clique} = \{<G,k>: \exists C, (<G,k>, C) \in Clique\}$$

$$S_{IS} = \{<G,k>: \exists IS, (<G,k>, IS) \in IS\}$$

## NP hard

תהיי S בעיית הכרעה. S היא NP-קשה אם מתקיים $\forall S' \in NP \quad S' \leq_m^p S$

## NP complete

תהיי S בעיית הכרעה. S היא NP-שלמה אם מתקיים:

1) $S \in NP$
2) S היא NP-קשה

## השערות וטענות מההרצאה

השערה 1: $P \neq NP$.

השערה 2: $NP \neq co - NP$.

השערה 3: $P \subsetneq NP \ \cap Co - NP$

השערה 4: NP אינו סגור לרדוקציית קוק. (ז"א אם קיימת רדוקציית קוק מ-'L ל-L וכן $L \in NP$, אזי לא ניתן להסיק $L' \in NP$).

- השערה 2 גוררת את השערה 1.
- $R_u$ שתוגדר כדלהלן היא *NP*-שלמה.

$$R_u = \{< M, x, 1^t >, y\}$$
$$| \, M \; is \; Turing \; machine, M \; accepts \; (x, y) \; within \; t \; steps, and \; |y| < t\}$$

- *SAT* היא *NP*-שלמה (קוק-לוין).
- לא תמיד קיימת רדוקציית קארפ בין $L \epsilon NP$ ל-$\bar{L} \epsilon co - NP$.
- עבור *L* תמיד קיימת רדוקציית קוק מ*L* למשלימה שלה.
- עבור *L* שאינה טריוויאלית (אינה ריקה ואינה $\Sigma^*$), תמיד קיימת רדוקציית קארפ למשלימתה.
- יהי $R \in PC$ כך ש$S_R$ היא *NP*-שלמה אזי *R* ניתנת לרדוקציה עצמית.
- קיום של שפה שהיא גם *NP* שלמה וגם ב*P* גורר: *P=NP*.
- משפט לדנר: אם $P \neq NP$ אזי קיימת *S* כך ש $S \in NP$ אזי $S \notin P$ וכן $S \notin NPC$.
- $P = co - P$.
- $P \subseteq NP \cap Co - NP$
- אם $NP \cap Co - NP$ מכיל שפות שהן *NP* קשות אזי *NP=Co-NP*

# ההיררכיה הפולינומיאלית באמצעות כמתים

## הסיגמא

נאמר כי $A \in \Sigma_k$ אם קיים מוודא פולינומי v ופולינום ()p כך שלכל x מתקיים

$$\exists y_1 \forall y_2 \exists y_3 \ldots . Q_k y_k \colon |y_i| < p(|x|), v(x, y_1, y_2, \ldots, y_k) = 1 \iff x \in A$$

כאשר $Q_k = \exists$ אם k אי-זוגי ו-$Q_k = \forall$ אם k זוגי.

## הפאי

נאמר כי $A \in \Pi_k$ אם קיים מוודא פולינומי v ופולינום ()p כך שלכל x מתקיים

$$\Pi_k = co - \Sigma_k = \forall y_1 \exists y_2 \forall y_3 \ldots . Q_k y_k \colon |y_i| < p(|x|), v(x, y_1, y_2, \ldots, y_k) = 1 \iff x \in A$$

כאשר $Q_k = \forall$ אם k אי-זוגי ו-$Q_k = \exists$ אם k זוגי.

### ההיררכיה כאיחוד

ההיררכיה הפולינומית היא המחלקה $PH$, היא מחלקה שמכלילה את NP ואת co-NP. והיא למעשה איחוד של כל הסיגמות או הפאיים:

$$PH = \bigcup_{k=0}^{\infty} \Sigma_k = \bigcup_{k=0}^{\infty} \Pi_k$$

### אבחנות

$$\Sigma_0 = P, \qquad \Sigma_1 = NP, \ \ \Pi_0 = P, \qquad \Pi_1 = co - Np$$

$$\Sigma_k \subseteq \Sigma_{k+1} \quad \Pi_k \subseteq \Pi_{k+1} \quad \Sigma_k \subseteq \Pi_{k+1} \quad \Pi_k \subseteq \Sigma_{k+1}$$

### טענות

1) $S \in \Sigma_{k+1} \Leftrightarrow$ קיים פולינום p ובעיה $S' \in \Pi_k$ כך ש
$S = \{x \mid \exists y, |y| < p(|x|), (x, y) \in S'\}$
2) PH סגורה לרדוקציית קוק.
3) עבור $k \geq 1$ אם $\Pi_k \subseteq \Sigma_k$ אזי $\Sigma_k = \Sigma_{k+1}$ (ואז יש לשים לב למשפט הבא)
4) יהי $k \in \mathbb{N}$ אם $\Sigma_k = \Sigma_{k+1}$ אזי ההיררכיה קורסת לרמה הk: $PH = \Sigma_k$ .
5) מסקנה מטענה 4: $PH = P \Leftrightarrow P = NP$
6) יהי $S \epsilon NP$. תהי $S'$ כך שקיימת רדוקציית קוק מS ל-$S'$, אזי $S' \in \Sigma_2$

## ההיררכיה הפולינומיאלית באמצעות אורקלים

### מכונת טיורינג ל"ד עם גישת אורקל

עבור אורקל או פונקציה $f: \{0,1\}^* \longrightarrow \{0,1\}$ (בעיית הכרעה) ומ"ט ל"ד M וקלט x $M^f(x) = 1$ אם קיים מסלול מקבל של M עבור הקלט x תוך אפשרות גישת אורקל ל-f (תשובת האורקל תמיד נכונה)

### המחלקה של מכונות ל"ד עם גישת אורקל

$NP^f$ מוגדרת להיות המחלקה של בעיות ההכרעה שקיימת עבורן מ"ט ל"ד פולינומית בעלת גישת אורקל ל-f המכריעה אותן.

עבור C שהיא מחלקה כלשהי של בעיות הכרעה אנחנו מגדירים: $\cup_{f \in c} NP^f = NP^C$ (עובד אותו דבר עם P)

למשל, $\mathrm{NP}^{NP}$ היא מחלקת בעיות ההכרעה שניתן להכריע בעזרת מ"ט ל"ד פולינומית בעלת גישת אורקל לפונקציה או בעייה כלשהי בNP.

### המשפט המרכזי בנושא:

לכל $k \geq 0$ מתקיים $\quad \Sigma_{k+1} = NP^{\Sigma_k}$

### אבחנה:

$$\mathrm{NP}^{\Sigma_k} = \mathrm{NP}^{\Pi_k}$$

## חישוב לא יוניפורמי, P\Poly

בחישוב יוניפורמי, קיים <u>אלגוריתם אחד לכל אורך קלט.</u>

### מעגל לוגי

מעגל לוגי הוא גרף מכוון, בו ישנם קודקודים מ-3 סוגים: קלט; שער לוגי מהסוג: AND, OR, NOT; פלט. מעגל מסוים יכול לטפל אך ורק בקלטים באורך <u>ספציפי</u>, ולכן נעסוק <u>במשפחות של מעגלים</u>.
גודל המעגל הוא מספר הקשתות שלו ומסומן להיות |C|.

משפחה של מעגלים היא קבוצה אינסופית של מעגלים $\{C_n\}_{n=1}^{\infty}$ . אומרים שמשפחה של מעגלים מחשבת פונקציה $f:\{0,1\}^* \longrightarrow \{0,1\}^*$ אם לכל קלט x $C_{|x|}(x) = f(x)$.

## שני מודלים לא יוניפורמיים

### הגדרה לפי מודל 1

בעיה A ניתנת לפתרון ע"י משפחה של מעגלים $\{C_n\}_{n=1}^{\infty}$ בגודל פולינומי אם קיים פולינום P() כך ש: $x \in A \Leftrightarrow C_{|x|}(x) = 1$. וכן מתקיים שלכל אורך של $x$ $|C_{|x|}| \leq p(|x|)$ (אורך המעגל חסום פולינומית).

### הגדרה לפי מודל 2 (המודל המרכזי)

נאמר כי פונקציה $f:\{0,1\}^* \longrightarrow \{0,1\}$ (בעיית הכרעה) שייכת למחלקה $P/_{l}$ עבור $l$ פונקצייה כלשהי אם קיימת מ"ט פולינומית דטרמיניסטית A וסדרה אינסופית של מחרוזות עצה $\{a_n\}_{n=1}^{\infty}$ כך שמתקיים: לכל $x\epsilon\{0,1\}^*$ מתקיים $f(x) = 1 \Leftrightarrow A(x, a_{|x|}) = 1$ וגם לכל $n$ $|a_n| \leq l(n)$.
למשל, $P/_{1}$ מתאר שפות שניתנות להכרעה בעזרת מ"ט שמקבלות עצה באורך של ביט אחד לכל אורך קלט.

### P\Poly

$$P/_{poly} = \bigcup_{l \text{ } is \text{ } polynomial} P/_{l}$$

כלומר קיום הגדרה של מודל 2 כך שאורך העצה פולינומי באורך הקלט.

### אבחנות

1) $P = P/_{0} \subsetneq P/_{1} \subseteq P/_{Poly}$
2) המחלקה $P/_{1}$ מכילה שפות שאינן כריעות.

### טענות

1) המודלים שקולים, כלומר: קבוצה A שייכת ל-P\Poly אמ"מ A ניתנת לפתרון ע"י משפחת מעגלים בגודל פולינומי.
2) אם $NP \subseteq P/_{poly}$ אזי $\mathrm{PH} = \Sigma_2$
3) אם $NP \nsubseteq P/_{poly}$ אזי $P \neq NP$

# סיבוכיות מקום

## מודל המכונה עליה נעבוד

מ"ט עם שלושה סרטים: קלט פלט ועבודה - הקלט לקריאה בלבד ותנועה דו כיוונית. הפלט לכתיבה בלבד ותנועה חד כיוונית. העבודה לכתיבה וקריאה ולתנועה דו כיוונית וסיבוכיות המקום נמדדת עפ"י השטח המנוצל בסרט זה.

## סיבוכיות מקום

נאמר כי בעיה מסוימת שייכת ל $\boldsymbol{DSPACE}(\boldsymbol{s}(\boldsymbol{n}))$ כאשר s היא פונקציה כלשהי, אם בהינתן קלט באורך n ניתן להכריע את הבעיה ע"י מ"ט ד"ט במודל הנ"ל וגישה לכל היותר s(n) תאי זיכרון מתוך סרט העבודה.

$\boldsymbol{DTIME}(s(n))$ זוהי מחלקת השפות הניתנות להכרעה ע"י מ"ט דט' המשתמשת בזמן $S(n) \geq$ עבור קלט באורך *n*.

## קשר בין זמן למקום

$$DTIME(s(n)) \subseteq DSPACE(s(n))$$

$$\mathrm{DSPACE}(s(n)) \subseteq DTIME(n \cdot 2^{O(s(n))})$$

עבור $s(n) \geq \log n$ ניתן להשמיט את ה*n* שלפני האקספוננט.

## המחלקה L

$$\mathrm{L} = \bigcup_{c} DSPACE(c \cdot \log n)$$

## סיבוכיות מקום ל"ד, חישוב ל"ד במקום לוגריתמי

אנחנו נעבוד במודל ה-On-line [זה שמחליט במקום על הבחירה ולא מקבל עד (מודל ה-Off-line)] ההבדל בין המודלים הוא עד כדי לוג (האונליין צורך יותר זיכרון).

נאמר כי בעיה מסוימת שייכת ל $\boldsymbol{NSPACE}(\boldsymbol{s}(\boldsymbol{n}))$ עבור פונקציה s כלשהי, אם בהינתן קלט לבעיה באורך n, ניתן להכריע את הבעיה ע"י מ"ט ל"ד במודל ה-online, ע"י שימוש בזיכרון מתוך סרט העבודה החסום ע"י s(n).

## המחלקה NL - המחלקה הל"ד המקבילה ל-L

$$NL = \bigcup_{c} NSPACE(c \cdot \log n)$$

## רדוקציית log-space

רדוקציית log-space מA לB היא פונקציה f(x) החשיבה בזיכרון log(|x|) כך שמתקיים

$$f(x) \in B \Leftrightarrow x \in A$$

והיא מהווה מקרה פרטי של רדוקציית קארפ. כמו כן הרדוקצייה סגורה בNL. (בדוגמא שלנו אם B בNL אזי A בNL)

## NL שלמות

שפה היא NL שלמה אם $A \in NL$ וגם קיימת רדוקציית log-space מכל שפה אחרת מNL לA.

להלן תיאור של בעיה שלמה ב-NL:

$\boldsymbol{St-conn} = \{(G,s,t) \mid G \text{ is directed graph, there is a path from } s \text{ to } t\} \in NLC$

## משפט סאביץ' המוכלל

$$NSPACE(s(n)) \subseteq DSPACE\left(\left(s(n)\right)^2\right)$$

(המשפט המקורי הוא לגבי $s(n) = O(\log n)$)

## ניפוח

נגדיר ניפוח. תהי $\boldsymbol{A \epsilon NSPACE(s(n))}$. הניפוח של A ייקרא 'A כך ש:

$$A' = \{x \cdot 1 \cdot 0^{2^{s(|x|)}} \mid x \epsilon A\}$$

מתקיים $\left|x \cdot 1 \cdot 0^{2^{s(|x|)}}\right| = |x| + 1 + 2^{s(|x|)}$

## משפט אימרמן

$$\mathrm{NL} = co-NL$$

<u>נגדיר</u> את הבעיה $Total-Reach(G,s)$ ובקיצור $TR(G,s)$ להיות מס' הקודקודים אליהם קיים מסלול בגרף G היוצא מ-s.

## חשיבות ב-NL

עבור פונקציה $f:\{0,1\}^* \to \{0,1\}^*$ שאינה בינארית, כמו $TR(G,s)$, נאמר ש-f חשיבה ב-NL אם מתקיימים התנאים הבאים:

1. קיימת מכונה ל"ד M המחזירה עבור קלט $x$ או את $f(x)$ או $\perp$ הרצה בזיכרון לוגריתמי.
2. קיימת סדרת בחירות אקראיות של M הגורמת ל-M להחזיר $f(x)$.

## סיבוכיות מקום פולינומית

$$PSPACE = \bigcup_{k=1}^{\infty} DSPACE(n^k)$$

$$NPSPACE = \bigcup_{k=1}^{\infty} NSPACE(n^k)$$

## EXP

$$\boldsymbol{EXP} = \cup_{\boldsymbol{c=1}}^{\infty} \ (\boldsymbol{2^{n^c}})$$

## PSPACE שלמה

בעיה A היא PSPACE שלמה אם:

1. $A \epsilon PSPACE$.
2. לכל $B \epsilon PSPACE$ קיימת רדוקציית קארפ מB לA.

דוגמא לבעיה כזו היא QBF:

$\boldsymbol{QBF} = \{\varphi \mid \varphi \text{ is a quantified } (\text{עם כמתים}) \text{boolean formula that returns true}\}$

**השערה:** $\boldsymbol{P \not\subseteq L}$.

### טענות ואבחנות

1) אם $A \subseteq B$ אזי, $NP^A \subseteq NP^B$ (וכן עבור כל בסיס). בדומה, אם $A \subseteq B$ אזי $A^{NP} \subseteq B^{NP}$.
2) $L \subseteq NL \subseteq P$ ולכן $L^{NL} \subseteq NL^{NL}$.
3) $DSPACE(s(n)) \subseteq NSPACE(s(n))$
4) $\mathrm{N}TIME\big(t(n)\big) \subseteq NSPACE\big(t(n)\big)$
5) קיימת רדוקציית log-space מ-$A\epsilon NL$ ל-St-conn.
6) אם $TR(G,s)\ \epsilon\ NL$ אזי $\overline{St-conn}(G,s,t)\ \epsilon\ NL$.
7) $TR(G,s)\ \epsilon\ NL$.
8) $NSPACE(s(n)) \subseteq DSPACE(s(n)^2)$ ולכן $\mathrm{PSPACE} = \mathrm{NSPACE}$.
9) $PH \subseteq PSPACE \subseteq EXP$

# אלגוריתמים הסתברותיים

## מ"ט הסתברותית במודל הon line

מ"ט **הסתברותית** היא מ"ט <u>לא דטרמיניסטית</u> בעלת היכולת להטיל מטבע אחיד הפועלת באופן הבא: כל פעם שהמכונה מגיעה לפיצול בו המעבר אינו מוגדר באופן יחיד, המכונה מטילה מטבע, ובסיכוי חצי מבצעת מעבר ראשון ובסיכוי חצי מבצעת מעבר שני.

בשונה ממ"ט ל"ד כללית המקבלת קלט אם קיים מסלול מקבל עבור קלט זה, מ"ט הסתברותית מקבלת קלט אם קיימת "הסתברות גבוהה" להגיע למצב מקבל.

נאמר כי תוצאת החישוב של מ"ט הסתברותית M על קלט x,  M(x), היא משתנה מקרי (בסיכוי חצי מחזיר 1/0).
קיים מודל Off-line שקול בו המ"ט M שלעיל מתוארת ע"י 'M <u>דטרמינסטית</u>, המקבלת כקלט זוג $(x,r)$ כאשר x הוא קלט מקורי ל-M ו-r היא סדרה של הטלות מטבע ו-$M'(x,r)$ מחזירה את תוצאת ריצת M על x עם r. עבור r שנבחר באקראי, $M'(x,r)$ הוא משתנה מקרי המתפלג כמו M(x).
המכונות עליהן נדבר הן פולינומיות.

## מכונות טיורינג הסתברותיות בעלות טעות חד-צדדית

### RP

$\mathrm{A} \in \mathrm{RP}$ אם קיימת מ"ט הסתברותית פולינומית M המקיימת

$$\forall x \in A\ [\Pr[M(x,r) = 1]] \geq \frac{1}{2}$$

$$\forall x \notin A\ [\Pr[M(x,r) = 0]] = 1$$

### Co-RP

$\mathrm{A} \in co\mathrm{RP}$ אם קיימת מ"ט הסתברותית פולינומית M המקיימת

$$\forall x \in A\ [\Pr[M(x,r) = 1]] = 1$$

$$\forall x \notin A\ [\Pr[M(x,r) = 0]] \geq \frac{1}{2}$$

## RP1

אם קיימת מ"ט הסתברותית פולינומית $M$ ופולינום $P$ כך ש: $L \in RP1$

$$\forall x \in A\ [\Pr[M(x,r)=1]] \geq \frac{1}{p(|x|)}$$

$$\forall x \notin A\ [\Pr[M(x,r)=0]] = 1$$

## RP2

אם קיימת מ"ט הסתברותית פולינומית $M$ ופולינום $q$ כך ש: $L \in RP2$

$$\forall x \in A\ [\Pr[M(x,r)=1]] \geq 1-\frac{1}{2^{q(|x|)}}$$

$$\forall x \notin A\ [\Pr[M(x,r)=0]] = 1$$

## BPP – מכונת טיורינג הסתברותית עם טעות דו-צדדית

$A \in BPP$ (Bounded Error Probibilistic Poly) אם קיימת מ"ט הסתברותית פולינומית M המקיימת

$$\Pr[M(x,r)=\chi_A(x)] \geq \frac{2}{3}$$

כאשר $\chi_A(x)$ האינדיקטור של A, כלומר:

$$\chi_A(x) = \begin{cases} 1 & x \in A \\ 0 & x \notin A \end{cases}$$

## הערות וטענות

- תהי M מ"ט הסתברותית להכרעת A אשר על כל קלט x מחזירה תשובה נכונה בהסתברות 1. אזי קיימת M' דטרמיניסטית המכריעה את A בעלת זמן ריצה זהה לזה של A.
- <u>מאוד חשוב:</u> **אמפליפיקציה** – יהי $A \in RP$. לכן קיימת מ"ט הסתברותית חד-צדדית M שמכריעה את A. נבצע p(x) ריצות של המכונה $M$ ואם אחת מהריצות החזירה 1 נחזיר 1 אחרת נחזיר 0.

  מתקיים: קיימת מ"ט הסתברותית פולינומית $M$ ופולינום $p$ כך ש:

$$\forall x \in A\ [\Pr[M(x,r)=1]] \geq 1-\frac{1}{2^{p(|x|)}}$$

$$\forall x \notin A\ [\Pr[M(x,r)=0]] = 1$$

- $1-\frac{1}{2^{p(|x|)}}$ זה המינימום, אפשר גם $1-\frac{1}{p(|x|)}$, למשל.
- <u>חשוב:</u> אמפליפיקציה עבור BPP, מסומן גם $BPP_1$ - תהי $A \epsilon BPP$. אזי קיימת מ"ט הסתברותית דו-צדדית $M'$ שמכריעה את $A$. נבצע $p(x)$ ריצות של $M'$ ונחזיר את תשובת רוב הריצות. מתקיים: לכל פולינום $p(\cdot)$ ישנה מ"ט $M^*$ הסתברותית העוצרת בזמן פולינומי המקיימת

$$\forall \text{x}: \Pr_r[M^*(x,r)=\chi_A(x)] \geq 1-\frac{1}{2^{p(|x|)}}$$

- חסם צ'רנוב: יהיו $X_1 \dots X_n$ משתנים מקריים בלתי תלויים שווי התפלגות המקבלים ערכים ב-$\{0,1\}$ ותהי $\mu$ התוחלת של כל אחד מהם. אזי עבור כל $\varepsilon > 0$:

$$\Pr[\frac{\sum_{i=1}^{k} X_i}{k} \geq \mu + \varepsilon] < e^{-2\varepsilon^2 k}$$

1. $RP = RP1 = RP2$
2. $RP, CoRP \subseteq BPP$
3. $BPP \subseteq PSPACE \subseteq EXP$
4. $P \subseteq RP \subseteq NP$
5. BPP vs NP is an open question
6. $BPP = coBPP$
7. $\mathrm{BPP} \subseteq \mathrm{P/Poly}$
8. $\mathrm{BPP} \subseteq \Sigma_2 \cap \pi_2$

# בעיות ספירה

## הפונקציה הסופרת

עבור $\mathrm{R} \subseteq \{0,1\}^* \times \{0,1\}^*$ נגדיר $f_R: \{0,1\}^* \to \mathbb{N}$ באופן הבא: $f_R(x) = |\{y | (x, y) \in R\}|$

כלומר בהינתן x הפונקציה מחשבת כמה y מתאימים לx הזה תחת יחס R.

## המחלקה #P

$$\#\mathrm{P} = \{f_R | R \in PC\}$$

כל פונקציות הספירה כך שניתן לוודא אם x,y בR בזמן פולינומי כלומר R יחס ב-PC.

## גרסת ההכרעה של #P

תהי $\boldsymbol{f} \in \#\boldsymbol{P}$, נגדיר בעיית הכרעה מתאימה:

$$\mathrm{S}_f = \{(x, N) | f_R(x) > N\}$$

ישנה רדוקצייה דו כיוונית מ#P לבעיית ההכרעה שלה. כלומר בהינתן פתרון ל$\mathrm{S}_f$ ניתן למצוא את $f_R(x)$ והפוך.

## #P complete

פונקציה f היא #P שלמה אם מקיימת שf ב#P וגם עבור כל $g \in \#P$ קיימת רדוקצייה פולינומית מ-g ל-f.

## רדוקצייה פארסמונית – משמרת עדים

יהיו יחסים $R, R' \in PC$ ותהינה בעיות ההכרעה המתאימות להם: $S_R, S_{R'}$. תהי $g$ רדוקציית קארפ מ $S_R$ ל$S_{R'}$ כך שמתקיים $g(x) \in S_{R'} \Leftrightarrow x \in S_R$

נאמר ש$g$ היא רדוקצייה פרסמונית יחסית לR וR' אם מתקיים $|\mathrm{R}(x)| = |R'(g(x))|$ כלומר כמות הy של בעיית הספירה נשמרת - אם נפעיל את פונקציית הספירה של *R* על הקלט *x* ואת פונקציית הספירה של *R'* על הפלט *g(x)* נקבל את אותו המספר.

## קירוב של f

$f: \{0,1\}^* \to N$ , $\delta \in [0,1]$ , $k \in (1, \infty)$

תהי $\Pi$ מ"ט פולינומית הסתברותית פולינומית המחזירה מספר. יהי $\mathrm{R} \in PC$ ופונקציה סופרת מתאימה $f_R$. נאמר כי $\Pi$ מקרבת $(\delta, k)$ את $f_R$ אם

$$\Pr\left[\frac{f_R(x)}{k} \le \Pi(x) \le k * f_R(x)\right] \ge 1 - \delta$$

## משפחה של פונקציות Hash

$$H = \{h \mid h: \{0,1\}^l \to \{0,1\}^m$$

תכונות נדרשות:

1. $h \in H$ ניתנת לייצוג בגודל $P(|x|) \ge$.
2. בהינתן y, $h(y)$ חושב בזמן פולינומי ב-$|y|$.
3. ניתן להגריל פונקציה אקראית $h \in H$ בזמן פולינומי ב-$|x|$.
4. ל-h יש את תכונת המסננת האקראית:
   לכל $S \subseteq \{0,1\}^l$ יתקיים

$$\Pr\left[(1-\varepsilon)\frac{|S|}{2^l} < \left|\{y \in S \mid h(y) = 0^m\}\right| < \quad (1-\varepsilon)\frac{|S|}{2^i}\right] \ge 1 - \frac{2^i}{\varepsilon^2 |S|}$$

ε אומר כמה קרוב אני רוצה להיות לאמת. אם $\varepsilon \approx 0$ אני באמת עצמה. ככל ש-$\varepsilon$ יותר גדול, אני מאפשר טעות יותר קטנה, אבל אז אני פחות מדויק. ככל ש-$\varepsilon$ יותר קטן, אני יותר מדויק אבל ההסתברות לטעות גדלה.

### הגדרה:

$$S_{R,H}^* = \{(x,h,i) \mid \exists y \in R(x) \wedge h(y) = \ 0^i\} \ \in NP$$

### טענות

1) $NP \subseteq P^{\#P}$
2) קיימת רדוקציית קוק מ-NP ל-#P - תהי $A \epsilon NP$:
   $$f_{R_A(x)} > 0 \Leftrightarrow x \epsilon A$$
3) $BPP \subseteq P^{\#P}$
4) קיימת רדוקציית קוק מ-BPP ל-#P. תהי $A \in BPP$. $M_A$ מכונת ה-BPP של A.
   נגדיר יחס:
   $$R_A = \{(x,r) | M(x,r) = 1, |r| \le p(|x|)\}$$
   $$f_{R_A(x)} \ge \frac{2}{3} \cdot 2^{p(|x|)} \Leftrightarrow x \epsilon A$$
5) $PH \subseteq P^{\#P}$
6) קיימת רדוקציה פולינומית מ-f ל-$S_f$ ולהיפך.
7) יהיו $f \in \#P$ ויהי $R_f \in PC$ היחס הנספר על ידי f. אם לכל $R' \in PC$ מתקיים שקיימת רדוקציה פרסמונית מ$R'$ ל$R_f$ אזי f היא #P שלמה.
8) #SAT היא #P שלמה
9) ישנו $R \in PC$ כך ש-$f_R$ היא $\#P$ שלמה אבל $S_R$ (בעיית ההכרעה) היא ב-P.
   דוגמא: הבעיה של הזיווג המושלם היא ב-P ובעיית הספירה המתאימה לה היא #P שלמה.
10) לכל $i \le 1$ קיימת משפחה של פונקציות hash $H_l^i$:
   $$h \epsilon H_l^i \quad h: \{0,1\}^l \to \{0,1\}^i \quad 1 \le i \le l$$
   בעלות ארבעת התכונות הבאות הנ"ל.

11) עבור כל $R \in PC$ קיים אלגוריתם הסתברותי פולינומי בעל גישת אורקל ל-NP הנותן $(16, \frac{1}{3})$ קירוב ל-$f_R$.

12) אם לכל $f \in \#P$ קיים $\Pi$ מ"ט פולינומית הסתברותית פולינומית מקרבת $\left(\frac{1}{3}, 10\right)$ אזי $NP \subseteq BPP$ (וזה משהו שלא מצפים שיקרה).