תרגיל בית PRG

- שאלה תיאורטית: האם קיים RAC^0 שאינו בתוך LE? הסבר.

- **הגדרה:** $LERAC^0$ הוא אוסף כל השפות L עבורן קיים מעגל C_n (לכל n) ומספר $m(n)$ פולינומי ב-n, כך ש:

  $x \in \{0,1\}^n$, $y \in \{0,1\}^{m(n)}$ משתנים

  $|C_n|$: גודל המעגל $= n$

$$\forall x \in \{0,1\}^n \quad x \in L \Rightarrow \Pr_y\left(C(x,y)=1\right) \geq \frac{2}{3}$$

$$x \notin L \Rightarrow \Pr_y\left(C(x,y)=1\right) \leq \frac{1}{3}$$

- **הגדרה:** PRG הוא $G_m : \{0,1\}^{s(m)} \to \{0,1\}^m$ כך ש:

  קיים מעגל p ו-ε כך ש

  לכל $m \in \mathbb{N}$ מעגל C_m,

  עבור m כלשהו, $p=p(m)$ ו-$s=s(m)$

  מתקיים

$$\forall m \quad \left| \Pr_{y \in U_{s(m)}}\left(C_m(G_m(y))=1\right) - \Pr_{y \in U_m}\left(C_m(y)=1\right) \right| \leq \varepsilon = \varepsilon(m)$$

שיעור נושא שמרכז:

קיים פתרון מקורב

ג' $G: \{0,1\}^{t(m)} \to \{0,1\}^m$ שבהינתן $\varepsilon = \frac{1}{m^3}$ וגם

$t(m) = O(\log m)^{c_p+2}$ עבור

כך שלכל מכונה M בזמן p

$$\text{Space}\left(O(t(m)) + \log(m)\right)$$

מסקנה: $RAC^0 \subseteq \bigcup_c DSpace(\log^c n)$

הוכחה: יהי $L \in RAC^0$

כלומר יש מעגל $M(x,y)$ כך ש- $x \in \{0,1\}^n$, $y \in \{0,1\}^h$

לפי הגדרה $|M| = w = poly(n)$ והעומק p קבוע.

נזכיר: $M(x, y_0)$ על y_0 מחרוזת $(0,1)^h$

$y_0 \in G(\{0,1\}^z)$ כך ש-

(סכום $\cdot$ מספר מחרוזות y שעבורן M מקבל x קטן מ- $\frac{1}{9}$)

$$\left| \Pr_{y \in G(\{0,1\}^z)} [M(x,y)=1] - \Pr_{y \in \{0,1\}^h} [M(x,y)=1] \right| \leq \frac{1}{9}$$

לכל $x \in \{0,1\}^n$ קבוע.

ולכן, $M_x(y) = M(x,y)$

M_x ניתן לייצוג ע"י מעגל AC^0 עומק p.

גודל w.

$$\Pr_{y \in \{0,1\}^h} [M_x(y)=1] - \Pr_{y \in G(\{0,1\}^z)} [M_x(y)=1] \leq \frac{1}{9}$$

$$= \sum_{y \in \{0,1\}^h} M_x(y) \cdot p_s(y) - \sum_{y \in G(\{0,1\}^z)} M_x(y) \cdot p_s(y)$$

$$= \sum_{y \in \{0,1\}^h} (M_x(y) - \exp(w^{-1})) \cdot p_s(y) - \sum_{y \in G(\{0,1\}^z)} M_x(y) \cdot p_s(y)$$

משפט הרחבה: לכל שדה F וכל הרחבה K של F, לכל $\sigma \in \mathrm{Aut}(F)$ קיימת הרחבה L של K ו-$\tau \in \mathrm{Aut}(L)$ כך ש-$\tau|_F = \sigma$.

הגדרה: תהי K הרחבה של F. נאמר ש-K היא הרחבה **נורמלית** של F אם כל פולינום אי-פריק ב-$F[x]$ שיש לו שורש ב-K מתפרק לגורמים לינאריים ב-$K[x]$.

משפט: תהי K הרחבה של F. התנאים הבאים שקולים:

1. K היא הרחבה נורמלית של F.
2. K היא שדה הפיצול של קבוצה כלשהי של פולינומים ב-$F[x]$.
3. K היא שדה הפיצול של פולינום כלשהו ב-$F[x]$.
4. כל $\sigma \in \mathrm{Aut}(K/F)$ מקבעת את K, כלומר $\sigma(K) = K$.

הוכחה:

$(1) \Rightarrow (2)$: נבחר לכל $\alpha \in K$ את הפולינום המינימלי $p_\alpha(x) \in F[x]$. מכיוון ש-K נורמלית, כל p_α מתפרק ב-K. נסמן $S = \{p_\alpha : \alpha \in K\}$. אז K נוצרת מעל F על ידי השורשים של פולינומים ב-S, ולכן K היא שדה הפיצול של S.

$(2) \Rightarrow (3)$: אם K היא שדה הפיצול של $S \subseteq F[x]$, נסמן $f = \prod_{p \in S} p$. אז $f \in F[x]$ ו-K היא שדה הפיצול של f, שכן K נוצרת מעל F על ידי השורשים של f.

$(3) \Rightarrow (4)$: תהי K שדה הפיצול של $f \in F[x]$, ויהיו $\alpha_1, \ldots, \alpha_n$ השורשים של f ב-K. יהי $\sigma \in \mathrm{Aut}(K/F)$. אז σ מעתיקה שורשים לשורשים, כלומר $\sigma(\alpha_i) \in \{\alpha_1, \ldots, \alpha_n\}$ לכל i. מכיוון ש-σ חח"ע ו-$\{\alpha_1, \ldots, \alpha_n\}$ סופית, σ מפתה את הקבוצה הזו על עצמה, ולכן $\sigma(K) = K$.

$(4) \Rightarrow (1)$: תהי $p \in F[x]$ אי-פריק שיש לו שורש $\alpha \in K$. יהי L שדה הפיצול של p מעל K, ויהי $\beta \in L$ שורש נוסף של p. קיים איזומורפיזם $\sigma : F(\alpha) \to F(\beta)$ כך ש-$\sigma|_F = \mathrm{id}_F$ ו-$\sigma(\alpha) = \beta$. לפי משפט ההרחבה, σ ניתנת להרחבה ל-$\tau \in \mathrm{Aut}(L/F)$. מכיוון ש-$K$ מקובעת על ידי כל $\tau \in \mathrm{Aut}(L/F)$, נקבל $\beta \in K$. לכן כל שורש של p ב-L שייך ל-K, ולכן p מתפרק ב-K.

הגדרה: תהי K הרחבה של F. נאמר ש-K היא הרחבה **ספרבילית** של F אם לכל $\alpha \in K$, הפולינום המינימלי $p_\alpha \in F[x]$ הוא ספרבילי, כלומר אין לו שורשים כפולים.

משפט: תהי K הרחבה סופית של F. התנאים הבאים שקולים:

1. K היא הרחבה ספרבילית של F.
2. K היא שדה הפיצול של פולינום ספרבילי ב-$F[x]$.
3. $|\mathrm{Aut}(K/F)| = [K : F]$.

הוכחה:

$(1) \Rightarrow (2)$: נבחר $\alpha_1, \ldots, \alpha_n$ בסיס של K מעל F. אז $K = F(\alpha_1, \ldots, \alpha_n)$. נסמן $f = p_{\alpha_1} \cdots p_{\alpha_n}$. אז f ספרבילי, ו-K היא שדה הפיצול של f.

$(2) \Rightarrow (3)$: נוכיח באינדוקציה על $[K : F]$. אם $[K : F] = 1$ אז $K = F$ ו-$|\mathrm{Aut}(K/F)| = 1$. נניח שהטענה נכונה לכל הרחבה של דרגה קטנה מ-$[K : F]$. יהי $\alpha \in K \setminus F$, ויהי p_α הפולינום המינימלי שלו. מכיוון ש-K היא שדה הפיצול של פולינום ספרבילי, p_α מתפרק ב-K ויש לו $\deg p_\alpha$ שורשים שונים. לכל שורש β של p_α קיים איזומורפיזם $\sigma : F(\alpha) \to F(\beta)$ כך ש-$\sigma|_F = \mathrm{id}_F$ ו-$\sigma(\alpha) = \beta$. לפי משפט ההרחבה, σ ניתנת להרחבה ל-$\tau \in \mathrm{Aut}(K/F)$. מכיוון ש-$K$ היא שדה הפיצול של f מעל $F(\alpha)$, ו-$[F(\alpha) : F] = \deg p_\alpha$, נקבל $|\mathrm{Aut}(K/F)| = [K : F]$.

$(3) \Rightarrow (1)$: נניח בשלילה ש-K אינה ספרבילית מעל F. אז קיים $\alpha \in K$ כך ש-p_α אי-ספרבילי. נסמן $n = \deg p_\alpha$. אז p_α יש פחות מ-n שורשים שונים ב-K, ולכן $|\mathrm{Aut}(K/F)| < [F(\alpha) : F] = n$. מצד שני, $[K : F] = [K : F(\alpha)] \cdot [F(\alpha) : F] \geq n$, בסתירה.

הגדרה: תהי K הרחבה של F. נאמר ש-K היא הרחבה **גלואה** של F אם היא נורמלית וספרבילית. במקרה זה נסמן $\mathrm{Gal}(K/F) = \mathrm{Aut}(K/F)$ ונקרא לזו **חבורת גלואה** של K מעל F.

משפט: תהי K הרחבה סופית של F. התנאים הבאים שקולים:

1. K היא הרחבה גלואה של F.
2. K היא שדה הפיצול של פולינום ספרבילי ב-$F[x]$.
3. $|\mathrm{Aut}(K/F)| = [K : F]$.
4. $K^{\mathrm{Aut}(K/F)} = F$.

הוכחה:

$(1) \Leftrightarrow (2)$: נובע מהמשפטים הקודמים.

$(1) \Leftrightarrow (3)$: נובע מהמשפטים הקודמים.

$(3) \Rightarrow (4)$: נסמן $G = \mathrm{Aut}(K/F)$ ו-$L = K^G$. אז K היא הרחבה גלואה של L, ולכן $|\mathrm{Aut}(K/L)| = [K : L]$. מכיוון ש-$G = \mathrm{Aut}(K/L)$, נקבל $|G| = [K : L]$. מצד שני, $[K : F] = [K : L] \cdot [L : F]$, ולכן $[L : F] = 1$, כלומר $L = F$.

$(4) \Rightarrow (3)$: נסמן $G = \mathrm{Aut}(K/F)$ ו-$L = K^G$. אז K היא הרחבה גלואה של L, ולכן $|\mathrm{Aut}(K/L)| = [K : L]$. מכיוון ש-$G = \mathrm{Aut}(K/L)$, נקבל $|G| = [K : L]$. מצד שני, $[K : F] = [K : L] \cdot [L : F]$, ולכן $[L : F] = 1$, כלומר $L = F$.

משפט: תהי K הרחבה גלואה של F, ותהי $G = \mathrm{Gal}(K/F)$. אז יש התאמה חח"ע ועל בין תתי-החבורות של G לבין השדות הביניים של K מעל F, המוגדרת על ידי $H \mapsto K^H$. ההתאמה הפוכה להכלה, כלומר $H_1 \subseteq H_2$ אם ורק אם $K^{H_2} \subseteq K^{H_1}$.

הוכחה:

ההתאמה חח"ע: נניח $K^{H_1} = K^{H_2}$. אז K היא הרחבה גלואה של K^{H_1}, ולכן $|\mathrm{Aut}(K/K^{H_1})| = [K : K^{H_1}]$. מכיוון ש-$H_1 = \mathrm{Aut}(K/K^{H_1})$, נקבל $|H_1| = [K : K^{H_1}]$. באופן דומה, $|H_2| = [K : K^{H_2}]$. מכיוון ש-$K^{H_1} = K^{H_2}$, נקבל $|H_1| = |H_2|$. מכיוון ש-$H_1 \subseteq H_2$, נקבל $H_1 = H_2$.

ההתאמה על: תהי L שדה ביניים של K מעל F. אז K היא הרחבה גלואה של L, ולכן $|\mathrm{Aut}(K/L)| = [K : L]$. מכיוון ש-$\mathrm{Aut}(K/L) \subseteq G$, נקבל $|\mathrm{Aut}(K/L)| \leq |G|$. מצד שני, $[K : F] = [K : L] \cdot [L : F]$, ולכן $[K : L] \leq [K : F]$. לכן $|\mathrm{Aut}(K/L)| \leq [K : F]$. מכיוון ש-$K$ היא הרחבה גלואה של F, נקבל $|G| = [K : F]$. לכן $|\mathrm{Aut}(K/L)| \leq |G|$. מכיוון ש-$\mathrm{Aut}(K/L) \subseteq G$, נקבל $\mathrm{Aut}(K/L) = G$. לכן $L = K^G$.

ההתאמה הפוכה להכלה: נניח $H_1 \subseteq H_2$. אז $K^{H_2} \subseteq K^{H_1}$, שכן כל איבר של K^{H_2} מקובע על ידי כל איבר של H_2, ובפרט על ידי כל איבר של H_1. להפך, נניח $K^{H_2} \subseteq K^{H_1}$. אז K היא הרחבה גלואה של K^{H_2}, ולכן $|\mathrm{Aut}(K/K^{H_2})| = [K : K^{H_2}]$. מכיוון ש-$H_2 = \mathrm{Aut}(K/K^{H_2})$, נקבל $|H_2| = [K : K^{H_2}]$. באופן דומה, $|H_1| = [K : K^{H_1}]$. מכיוון ש-$K^{H_2} \subseteq K^{H_1}$, נקבל $|H_2| \geq |H_1|$. מכיוון ש-$H_1 \subseteq H_2$, נקבל $H_1 = H_2$.

משפט: תהי K הרחבה גלואה של F, ותהי $G = \mathrm{Gal}(K/F)$. תהי L שדה ביניים של K מעל F, ותהי $H = \mathrm{Gal}(K/L)$. אז L היא הרחבה נורמלית של F אם ורק אם H היא תת-חבורה נורמלית של G. במקרה זה, $\mathrm{Gal}(L/F) \cong G/H$.

הוכחה:

נניח ש-L היא הרחבה נורמלית של F. יהי $\sigma \in G$ ויהי $\tau \in H$. אז $\tau(\alpha) = \alpha$ לכל $\alpha \in L$. נחשב את $\sigma\tau\sigma^{-1}(\alpha)$. מכיוון ש-$\sigma(\alpha) \in L$ (כי L נורמלית), נקבל $\tau(\sigma(\alpha)) = \sigma(\alpha)$. לכן $\sigma\tau\sigma^{-1}(\alpha) = \alpha$. מכיוון ש-$\alpha \in L$ שרירותי, נקבל $\sigma\tau\sigma^{-1} \in H$. לכן H היא תת-חבורה נורמלית של G.

להפך, נניח ש-H היא תת-חבורה נורמלית של G. יהי $\alpha \in L$ ויהי β שורש נוסף של p_α. קיים איזומורפיזם $\sigma : F(\alpha) \to F(\beta)$ כך ש-$\sigma|_F = \mathrm{id}_F$ ו-$\sigma(\alpha) = \beta$. לפי משפט ההרחבה, σ ניתנת להרחבה ל-$\tau \in G$. יהי $\gamma \in H$. אז $\gamma(\alpha) = \alpha$. נחשב את $\gamma(\beta)$. מכיוון ש-H נורמלית ב-G, קיים $\delta \in H$ כך ש-$\gamma\tau = \tau\delta$. לכן $\gamma(\beta) = \gamma(\tau(\alpha)) = \tau(\delta(\alpha)) = \tau(\alpha) = \beta$. מכיוון ש-$\gamma \in H$ שרירותי, נקבל $\beta \in L$. לכן כל שורש של p_α ב-K שייך ל-L, ולכן p_α מתפרק ב-L.

נניח ש-L היא הרחבה נורמלית של F. נגדיר $\varphi : G \to \mathrm{Aut}(L/F)$ על ידי $\varphi(\sigma) = \sigma|_L$. אז φ הומומורפיזם, שכן $\varphi(\sigma\tau) = (\sigma\tau)|_L = \sigma|_L \circ \tau|_L = \varphi(\sigma)\varphi(\tau)$. הגרעין של φ הוא $\{\sigma \in G : \sigma|_L = \mathrm{id}_L\} = H$. מכיוון ש-$L$ היא הרחבה נורמלית של F, φ על. לכן $\mathrm{Gal}(L/F) \cong G/H$.

כלומר: ההסתברות שפונקציה "קשה" כלשהי תיראה כזו שכמעט כל

$\Pr[f_n = \text{Parity}(x)] \leq \frac{1}{2} + 2^{-(\frac{1}{\log n})n}$ עבור

אלו שבהן n קטן מספיק

כאשר (Hastad): כל מעגל $\{C_n\}$ מעמיק p בגודל $2^{(\frac{1}{\log n})^{d-1}}$

ובכך את קבוצת השפות בזמן פולינומי $\leq AM$

יוצא שלמרות, הקבוצה של שפות $\text{Parity} \notin AC^0$

ולכן מספיק $p_1, \ldots$ פולינום כלשהו: Parity בגודל $2^{(\log n)^{d-1}}$

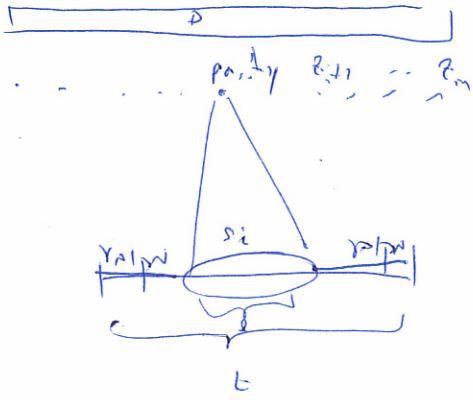
בהסתברות גבוהה: פולינום $\exists$ כזה ש Parity בגודל $2^{(\frac{1}{\log n})^2}$.

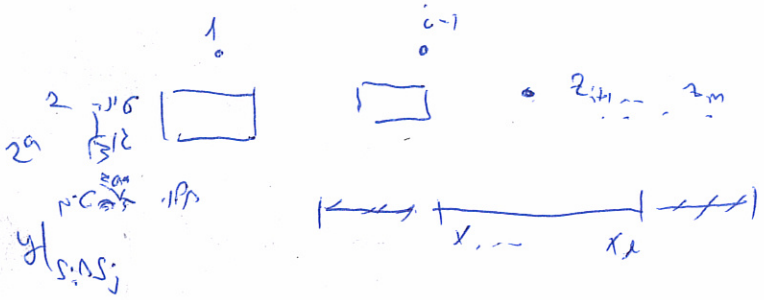
כלומר יש מעגל C שמחשב Parity בגודל פולינומי p

$(\log n)^2$.

כלומר: Parity נמצאת גם ב AC^0.

הוכחה משפט





(7)

משפט: $BPP = P$ אם ורק אם לכל קבוצת שפות $L \in BPP$ מתקיים:

- לכל L ב-BPP קיים $k \in \mathbb{N}$ כך ש-$L \in DTime(2^{n^k})$

- לכל L ב-BPP קיים $k \in \mathbb{N}$ כך ש-$L \in DTime(n^k)$

- לכל L ב-BPP קיים $k \in \mathbb{N}$ כך ש-$L \in DTime(n^k)$ עבור אינסוף n-ים.

- $BPP \subseteq \bigcap_{\varepsilon > 0} DTime(2^{n^\varepsilon})$

- $BPP \subseteq DTime(2^{(\log n)^c})$ לכל $c > 0$

הגדרה: קבוצת שפות C נקראת *סגורה* תחת יחס $\leq_m$ אם לכל A, B מתקיים:

$$(B \in C \wedge A \leq_m B) \Rightarrow A \in C$$

משפט: $(C, \leq_m)$

- לכל C קיים $L \in C$ שהוא $\leq_m$-קשה עבור C.

- לכל C קיים $L \in C$ שהוא $\leq_m$-שלם עבור C.

- לכל C קיים $L \in C$ שהוא $\leq_m$-קשה עבור C אך $L \notin C$.

- לכל C קיים $L \in C$ שהוא $\leq_m$-שלם עבור C אך $L \notin C$.

תזכורת -

אם $L \in PSPACE$ אז קיים אלגוריתם M שפותר את L בסיבוכיות מקום worst-case $s(n)$ כך ש- $s(n) = 2^{O(n)}$.

אם $L \in PSPACE$ אז קיים אלגוריתם M שפותר את L בסיבוכיות מקום ממוצע $s(n)$ כך ש- $s(n) = 2^{O(n)}$.

$PSPACE$ ו EXP.

נגדיר f בעיה שקשה ב $PSPACE$ בסיבוכיות מקום worst-case

$f \in PSPACE$

נניח ש f ניתנת לחישוב ע"י אלגוריתם M בסיבוכיות מקום worst-case

$space(2^n) = 2^{O(n)}$

נגדיר את $\overline{f}$ שניתנת לחישוב ב $2^{O(n)}$ ← $|x| = n$

נראה כי $\overline{f}$ קשה ב EXP.

---

hardness amplification

contra-positive: אם f קשה אז $\overline{f}$ קשה

worst-case to A_{vg}-case reduction

$\overline{f} \in PSPACE$ אם $f \in PSPACE$

$\overline{f} \notin EXP$ אם $f \notin EXP$

המכונות על סדר מקבילי.

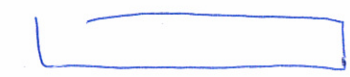
משפט: אם ל- $L \in E$ קשה [illegible] (worst-case)

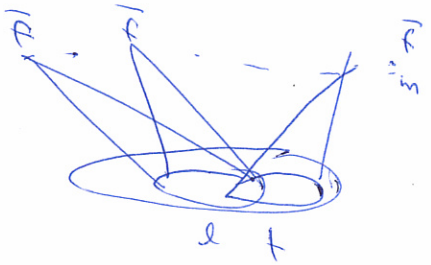
למעגלים בגודל $2^{\epsilon n}$

אז BPP=P

Trevisan ext
NW PRG

NW
Worst-case





Trevisan:

$|x| \geq i^4$ $N_M(x) \geq k$ $x \in f$

f 'informationtheoretic' (אי אפשר לנחש את f)

ECC (אי אפשר לנחש אם f או g)