

**גודל מעגל בוליאני:** יהיו  $n, m \in \mathbb{N}$  ויהי  $C$  מעגל בוליאני בעל  $n$  חוטים וכן  $m$  קלטים אזי  $\text{Size}(C) = n + m$ .

**עומק מעגל בוליאני:** יהי  $C$  מעגל בוליאני אזי  $\text{depth}(C)$  הינו אורך המסלול המקסימלי מקלט לפלט.

**הגדרה:** יהי  $n \in \mathbb{N}_{\geq 3}$  אזי  $\vee_n : \{0, 1\}^n \rightarrow \{0, 1\}$  המוגדרת  $\vee_n(x) = \bigvee_{i=1}^n x_i$ .

**הגדרה:** יהי  $n \in \mathbb{N}_{\geq 3}$  אזי  $\wedge_n : \{0, 1\}^n \rightarrow \{0, 1\}$  המוגדרת  $\wedge_n(x) = \bigwedge_{i=1}^n x_i$ .

**מעגל בוליאני בעל fan-in לא מוגבל:** מעגל בוליאני מעל בסיס הפונקציות הבוליאניות  $\{\wedge, \vee, \neg\}$   $(\bigcup_{n \in \mathbb{N}} \{\wedge_n\}) \cup (\bigcup_{n \in \mathbb{N}} \{\vee_n\})$  הערה: אלא אם נאמר אחרת מעגל בוליאני הוא בעל fan-in מוגבל.

**טענה:** תהא  $f : \{0, 1\}^n \rightarrow \{0, 1\}$  אזי קיים מעגל בוליאני  $C$  בעל fan-in לא מוגבל המחשב את  $f$  בגודל  $\mathcal{O}(n \cdot 2^n)$  ובעומק 2.

**טענה:** תהא  $f : \{0, 1\}^n \rightarrow \{0, 1\}$  אזי קיים מעגל בוליאני  $C$  המחשב את  $f$  בגודל  $\mathcal{O}(n \cdot 2^n)$  ובעומק  $n + \log_2(n)$ .

**מסקנה:** תהא  $L$  שפה אזי קיימת משפחת מעגלים  $\mathcal{C}$  מגודל  $\mathcal{O}(n \cdot 2^n)$  ומעומק  $n + \log(n)$  המחשבת את  $L$ .

**מסקנה:** יהי  $n \in \mathbb{N}$  אזי קיימת  $f : \{0, 1\}^n \rightarrow \{0, 1\}$  עבורה לכל מעגל בוליאני  $C$  המחשב אותה מתקיים  $\text{Size}(C) \geq \frac{2^n}{2n}$ .

**הגודל של פונקציה בוליאנית:** יהי  $n \in \mathbb{N}$  ותהא  $f : \{0, 1\}^n \rightarrow \{0, 1\}$  אזי  $\text{Size}(f) = \min \{\text{Size}(C) \mid C \text{ מחשבת את } f\}$ .

**טענה:** יהי  $n \in \mathbb{N}$  ותהא  $f : \{0, 1\}^n \rightarrow \{0, 1\}$  אזי  $\text{Size}(f) \leq 15 \cdot (2^n - 1)$ .

**טענה:** יהי  $n \in \mathbb{N}$  ותהא  $f : \{0, 1\}^n \rightarrow \{0, 1\}$  אזי  $\text{Size}(f) = \mathcal{O}\left(\frac{2^n}{n}\right)$ .

**מסקנה שאנון:** יהי  $n \in \mathbb{N}$  אזי  $\max \{\text{Size}(f) \mid f : \{0, 1\}^n \rightarrow \{0, 1\}\} = \Theta\left(\frac{2^n}{n}\right)$ .

**משפט:** קיים  $C \in \mathbb{R}_+$  עבורו לכל  $n \in \mathbb{N}$  ולכל  $S : \mathbb{N} \rightarrow \mathbb{N}$  המקיימת  $n \leq S < C \cdot \frac{2^n}{n}$  קיימת  $f : \{0, 1\}^n \rightarrow \{0, 1\}$  באשר  $f$  חשיבה על ידי מעגל מגודל  $S(n) + 10n$  וכן  $f$  לא חשיבה על ידי מעגל מגודל  $S(n)$ .

**הגדרה:** תהא  $S : \mathbb{N} \rightarrow \mathbb{N}$  אזי  $L$  חשיבה על ידי משפחת מעגלים מגודל לכל היותר  $S(n)$   $\text{Size}(S(n)) = \{L \subseteq \{0, 1\}^* \mid S(n) \text{ חשיבה על ידי מעגל מגודל לכל היותר } S(n)\}$ .

**מסקנה:**  $\text{Size}(2^n) = \mathcal{P}(\{0, 1\}^*)$ .

**מסקנה:** תהא  $S : \mathbb{N} \rightarrow \mathbb{N}$  עבורה  $n \leq S(n) \leq \frac{2^n}{n}$  אזי  $\text{Size}(S(n)) \subsetneq \text{Size}(S(n) + 10n)$ .

**הגדרה:** יהי  $k \in \mathbb{N}$  אזי  $\text{Size}(\mathcal{O}(n^k)) = \bigcup_{c \in \mathbb{N}} \text{Size}(c \cdot n^k)$ .

**הגדרה Polynomial Size Circuits:**  $\text{Size}(\text{poly}) = \bigcup_{c \in \mathbb{N}} \text{Size}(n^c)$ .

**הגדרה:** תהא  $S : \mathbb{N} \rightarrow \mathbb{N}$  ותהא  $L$  שפה עבורה קבוצת מעגלים  $\{C_n \mid n \in \mathbb{N}\}$  המקיימת

• לכל  $n \in \mathbb{N}$  מתקיים  $\text{Size}(C_n) = S(n)$ .

• לכל  $x \in \{0, 1\}^*$  אם  $x \in L$  אז  $\exists w. C_{|x|}(x, w) = 1$ .

• לכל  $x \in \{0, 1\}^*$  אם  $x \notin L$  אז  $\forall w. C_{|x|}(x, w) = 0$ .

אזי  $L \in \text{NSize}(S(n))$ .

**הגדרה Nondeterministic Polynomial Size Circuits:**  $\text{NSize}(\text{poly}) = \bigcup_{c \in \mathbb{N}} \text{NSize}(n^c)$ .

**הגדרה Non Uniform Alternating Class:** תהיינה  $s, d : \mathbb{N} \rightarrow \mathbb{N}$  אזי

$\text{nu-AC}(s, d) = \left\{ L \subseteq \{0, 1\}^* \mid \begin{array}{l} L(C) = L \\ \text{Size}(C_n) \leq s(n) \\ \text{depth}(C_n) \leq d(n) \end{array} \right\}$  קיימת משפחת מעגלים  $C$  בעלת fan-in לא מוגבל עבורה

**הגדרה:** יהי  $k \in \mathbb{N}$  אזי  $\text{nu-AC}^k = \bigcup_{c \in \mathbb{N}} \text{nu-AC}(n^c, \log^k(n))$ .

**הגדרה Non Uniform Nick's Class:** תהיינה  $s, d : \mathbb{N} \rightarrow \mathbb{N}$  אזי

$\text{nu-NC}(s, d) = \left\{ L \subseteq \{0, 1\}^* \mid \begin{array}{l} L(C) = L \\ \text{Size}(C_n) \leq s(n) \\ \text{depth}(C_n) \leq d(n) \end{array} \right\}$  קיימת משפחת מעגלים  $C$  עבורה

**הגדרה:** יהי  $k \in \mathbb{N}$  אזי  $\text{nu-NC}^k = \bigcup_{c \in \mathbb{N}} \text{nu-NC}(n^c, \log^k(n))$ .

**מסקנה:** תהיינה  $s, d : \mathbb{N} \rightarrow \mathbb{N}$  אזי  $\text{nu-NC}(s, d) \subseteq \text{nu-AC}(s, d)$ .

**טענה:** יהי  $k \in \mathbb{N}$  אזי  $\text{nu-AC}^k \subseteq \text{nu-NC}^{k+1}$ .

**מסקנה:**  $\text{nu-NC}^0 \subsetneq \text{nu-AC}^0$ .

**פונקציית זוגיות:** יהי  $n \in \mathbb{N}_+$  אזי  $\text{parity} : \{0, 1\}^n \rightarrow \{0, 1\}$  המוגדרת  $\text{parity}(x) = \bigoplus_{i=1}^n x_i$ .

**טענה:** קיים מעגל  $C$  המחשב את  $\text{parity}_n$  מגודל  $\mathcal{O}(n)$  ועומק  $\mathcal{O}(\log(n))$ .

**מסקנה:**  $\text{parity} \in \text{nu-NC}^1$ .

**פולינום מולטי-לינארי (מ"ל):** יהי  $n \in \mathbb{N}_+$  אזי  $p \in \mathbb{R}[x_1 \dots x_n]$  בעל דרגה 1.

**פולינום מחשב פונקציה בוליאנית:** תהא  $f : \{0, 1\}^n \rightarrow \{0, 1\}$  אזי  $p \in \mathbb{R}[x_1 \dots x_n]$  מ"ל עבורו  $f(x) = p(x)$  לכל  $x \in \{0, 1\}^n$ .

**טענה:** תהא  $f : \{0, 1\}^n \rightarrow \{0, 1\}$  אזי קיים פולינום מ"ל יחיד המחשב את  $f$ .

**סימון:** תהא  $f : \{0, 1\}^n \rightarrow \{0, 1\}$  ויהי  $p \in \mathbb{R}[x_1 \dots x_n]$  מ"ל המחשב את  $f$  אזי  $\deg(f) = \deg(p)$ .

**מסקנה:** יהי  $n \in \mathbb{N}$  אזי  $\deg(\vee_n) = n$ .

**טענה:** יהי  $n \in \mathbb{N}$  אזי  $\deg(\text{parity}_n) = n$ .

**פולינום מחשב פונקציה בוליאנית בממוצע עם שגיאה  $\varepsilon$ :** יהי  $\varepsilon > 0$  ותהא  $f : \{0, 1\}^n \rightarrow \{0, 1\}$  אזי  $p \in \mathbb{R}[x_1 \dots x_n]$  מ"ל עבורו  $\mathbb{P}_{x \leftarrow \{0, 1\}^n} (p(x) = f(x)) \geq 1 - \varepsilon$ .

**טענה:** הפולינום 1 מחשב את  $\vee_n$  בממוצע עם שגיאה  $\frac{1}{3}$ .

**התפלגות משפחת פולינומים מחשבת פונקציה בוליאנית עם שגיאה  $\varepsilon$ :** יהי  $\varepsilon > 0$  ותהא  $f : \{0, 1\}^n \rightarrow \{0, 1\}$  אזי קבוצת פולינומים מ"ל  $P \subseteq \mathbb{R}[x_1 \dots x_n]$  עבורה לכל  $x \in \{0, 1\}^n$  מתקיים  $\mathbb{P}_{p \leftarrow P} (p(x) = f(x)) \geq 1 - \varepsilon$ .

**טענה:** יהי  $\varepsilon > 0$  ותהא  $f : \{0, 1\}^n \rightarrow \{0, 1\}$  אזי קיים  $p \in P$  המחשב בממוצע את  $f$  עם שגיאה  $\varepsilon$ .

**סימון:** יהי  $(\Omega, \mathbb{P})$  מרחב הסתברות אזי  $(x \leftarrow \Omega) : \Omega \rightarrow \Omega$  הינו מ"מ באשר  $\mathbb{P}((x \leftarrow \Omega) = \omega) = \mathbb{P}(\omega)$ .

**הערה:** תהא  $A$  קבוצה סופית אזי  $x \leftarrow A$  הינו המ"מ כאשר  $A$  עם ההתפלגות האחידה.

**סימון:** יהי  $\varepsilon > 0$  ותהא  $S_{j,k} \leftarrow \mathcal{P}([n])$  לכל  $k \in \{0 \dots \log(n)\}$  ולכל  $j \in [\log(\frac{1}{\varepsilon})]$  אזי  $R_V(x) = 1 - \prod_{k,j} (1 - \sum_{i \in S_{j,k}} x_i)$  **למה:** יהי  $x \in \{0, 1\}^n$  עבורו  $\vee_n(x) = 0$  אזי  $R_V(x) = 0$  לכל  $S_{j,k} \leftarrow \mathcal{P}([n])$ .

**למה:** יהי  $x \in \{0, 1\}^n$  ותהינה  $S_{j,k} \leftarrow \mathcal{P}([n])$  עבורן קיימים  $j, k$  המקיימים  $|S_{j,k} \cap \{i \mid x_i = 1\}| = 1$  אזי  $R_V(x) = 1$  וכן  $\vee_n(x) = 1$ .

**למה:** יהי  $k \in \mathbb{N}$  ויהי  $x \in \{0, 1\}^n$  עבורו  $|\{i \mid x_i = 1\}| \leq 2^k$  אזי  $\mathbb{P}_{S \leftarrow \mathcal{P}([n])} (|S \cap I| = 1) \geq \frac{1}{2^e}$ .

**טענה:** יהי  $\varepsilon > 0$  אזי קיימת קבוצת פולינומים מ"ל  $P \subseteq \mathbb{R}[x_1 \dots x_n]$  מדרגה  $\mathcal{O}(\log(n) \cdot \log(\frac{1}{\varepsilon}))$  שמחשבת את  $\vee_n$  עם שגיאה  $\varepsilon$ .

**טענה:** תהא  $f : \{0, 1\}^n \rightarrow \{0, 1\}$  חשיבה על ידי מעגל בוליאני מגודל  $s(n)$  ועומק  $d(n)$  אזי לכל  $\varepsilon > 0$  קיימת קבוצת פולינומים מ"ל  $P \subseteq \mathbb{R}[x_1 \dots x_n]$  מדרגה  $\mathcal{O}\left(\left(\log(n) \cdot \log\left(\frac{s(n)}{\varepsilon}\right)\right)^{d(n)}\right)$  המחשבת את  $f$  עם שגיאה  $\varepsilon$ .

**מסקנה:** תהא  $f : \{0, 1\}^n \rightarrow \{0, 1\}$  חשיבה על ידי מעגל בוליאני מגודל  $s(n)$  ועומק  $d(n)$  אזי לכל  $\varepsilon > 0$  קיים פולינום מ"ל  $p \in \mathbb{R}[x_1 \dots x_n]$  מדרגה  $\mathcal{O}\left(\left(\log(n) \cdot \log\left(\frac{s(n)}{\varepsilon}\right)\right)^{d(n)}\right)$  המחשב את  $f$  בממוצע עם שגיאה  $\varepsilon$ .

**למה:** יהי  $\delta > 0$  ויהי  $p \in \mathbb{R}[x_1 \dots x_n]$  מ"ל המחשב את  $\text{parity}_n$  בממוצע עם שגיאה  $\frac{1}{2} + \delta$  אזי  $\deg(p) = \Omega(\delta \sqrt{n})$ .

**טענה:** יהי  $\varepsilon > 0$  ויהי  $p \in \mathbb{R}[x_1 \dots x_n]$  מ"ל המחשב את  $\text{parity}_n$  בממוצע עם שגיאה  $\varepsilon$  אזי  $\deg(p) = \Omega(\sqrt{n})$ .

**מסקנה:** יהי  $C$  מעגל המחשב את  $\text{parity}_n$  בעל fan-in לא מוגבל ועומק  $d(n)$  אזי  $\text{Size}(C) \geq 2^{\Omega\left(n^{\frac{1}{4 \cdot d(n)}}\right)}$ .

**משפט:**  $\text{parity} \notin \text{nu-AC}^0$ .

**מסקנה:**  $\text{nu-AC}^0 \subsetneq \text{nu-NC}^1$ .

**הגדרה:** יהי  $n \in \mathbb{N}_+$  אזי  $\text{BinAdd}_n : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}^{n+1}$  המוגדרת  $\text{BinAdd}_n(x, y) = x + y$ .

**טענה:** יהי  $n \in \mathbb{N}_+$  אזי  $\text{BinAdd}_n \in \text{nu-AC}^0$ .

**הגדרה:** יהי  $n \in \mathbb{N}_+$  אזי  $\text{IteratedBinAdd}_n : \{0, 1\}^n \rightarrow \{0, 1\}^{2n}$  המוגדרת  $\text{IteratedBinAdd}_n(x_1 \dots x_n) = \sum_{i=1}^n x_i$ .

**טענה:**  $\text{IteratedBinAdd} \in \text{nu-AC}^1$ .

**הגדרה:** יהי  $n \in \mathbb{N}_+$  אזי  $\text{BinMult}_n : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}^{2n}$  המוגדרת  $\text{BinMult}_n(x, y) = x \cdot y$ .

**טענה:**  $\text{BinMult} \in \text{nu-AC}^1$ .

**טענה:**  $\text{BinMult} \notin \text{nu-AC}^0$ .

**חתך מקסימלי:** יהי  $G$  גרף אזי חתך  $(A, B)$  עבורו  $|E(A, B)| \geq |E(C, D)|$  לכל חתך  $(C, D)$ .

**סימון:** יהי  $G$  גרף ויהי  $(A, B)$  חתך מקסימלי אזי  $\text{maxCut}(G) = |E(A, B)|$ .

**למה:** יהי  $G$  גרף אזי  $\mathbb{E}_{\text{חתך } (A, B)} [|E(A, B)|] = \frac{|E(G)|}{2}$ .

**טענה:** יהי  $G$  גרף אזי קיים חתך  $(A, B)$  עבורו  $|E(A, B)| \geq \frac{|E(G)|}{2}$ .

**אלגוריתם חיפוש אלים למציאת חתך גדול:** תהא  $E$  קבוצה יהי  $n \in \mathbb{N}$  ותהא  $\{v_1, \dots, v_n\}$  קבוצה אזי

**function** BruteForceBigCut( $E, \{v_1 \dots v_n\}$ ):

```

     $S \in \mathcal{P}(\{v_1 \dots v_n\})$ 
    for  $r \in \{0, 1\}^n$  do
         $S \leftarrow \{v_i \mid r_i = 1\}$ 
        if  $|E(S, \bar{S})| \geq \frac{|E|}{2}$  then return  $S$ 
    end
```

**טענה:** תהא  $E$  קבוצה יהי  $n \in \mathbb{N}$  ותהא  $\{v_1, \dots, v_n\}$  קבוצה אזי BruteForceBigCut בעלת סיבוכיות זמן ריצה  $\Omega(2^n)$ .  
**טענה:** קיימת מ"ט אקראית  $M_{\text{supp}}$  עבורה לכל  $n \in \mathbb{N}$  ולכל  $r \leftarrow \{0, 1\}^{\log(n)+1}$  מתקיים כי  $M_{\text{supp}}(1^n; r)$  מחזירה מ"מ  $X_1 \dots X_n : [0, 1] \rightarrow \{0, 1\}$  עבורם

- $X_1 \dots X_n$  ב"ת בזוגות.
- $\mathbb{P}(X_i = 1) = \frac{1}{2}$  לכל  $i \in [n]$ .
- $M_{\text{supp}}$  רצה בזמן  $\text{poly}(n)$ .

**טענה:** יהי  $p \in \mathbb{P}$  ולכל  $c, d \in \mathbb{F}$  נגדיר מ"מ  $X_{c,d} : \mathbb{F} \rightarrow \mathbb{F}$  כך  $X_{c,d}(\alpha) = c\alpha + d$  אזי  $\{X_{c,d}\}_{c,d \in \mathbb{F}}$  ב"ת בזוגות וכן  $X_{c,d} \sim \text{Uni}(\mathbb{F})$  לכל  $c, d \in \mathbb{F}$ .

**סימון:** יהי  $n \in \mathbb{N}$  יהי  $r \in \{0, 1\}^{\log(n)+1}$  ותהא  $\{v_1 \dots v_n\}$  קבוצה אזי  $S_{\text{supp}} = \{v_i \mid M_{\text{supp}}(1^n; r)_i = 1\}$ .  
**טענה:** יהי  $G$  גרף באשר  $V = \{v_1 \dots v_n\}$  אזי  $\mathbb{E}_{r \leftarrow \{0, 1\}^{\log(n)+1}} [|E(S_{\text{supp}}, \overline{S_{\text{supp}}})|] = \frac{|E|}{2}$ .  
**אלגוריתם בעל משתנים מקריים למציאת חתך גדול:** תהא  $E$  קבוצה יהי  $n \in \mathbb{N}$  ותהא  $\{v_1, \dots, v_n\}$  קבוצה אזי

```
function IndVarBigCut( $E, \{v_1 \dots v_n\}$ ):
   $S \in \mathcal{P}(\{v_1 \dots v_n\})$ 
  for  $r \in \{0, 1\}^{\log(n)+1}$  do
     $X \leftarrow M_{\text{supp}}(1^n; r)$ 
     $S \leftarrow \{v_i \mid X_i = 1\}$ 
    if  $|E(S, \overline{S})| \geq \frac{|E|}{2}$  then return  $S$ 
  end
```

**טענה:** תהא  $E$  קבוצה יהי  $n \in \mathbb{N}$  ותהא  $\{v_1, \dots, v_n\}$  קבוצה אזי IndVarBigCut בעלת סיבוכיות זמן ריצה  $\text{poly}(n)$ .  
**סימון:** תהא  $E$  קבוצה יהי  $n \in \mathbb{N}$  ותהא  $\{v_1, \dots, v_n\}$  קבוצה ויהי  $r \in \{0, 1\}^n$  אזי  $S_r = \{v_i \mid r_i = 1\}$ .  
**אלגוריתם למציאת חתך גדול עם תוחלת מותנית:** תהא  $E$  קבוצה יהי  $n \in \mathbb{N}$  ותהא  $\{v_1, \dots, v_n\}$  קבוצה אזי

```
function CEBigCut( $E, \{v_1 \dots v_n\}$ ):
   $a \in \bigcup_{i=0}^n \{0, 1\}^i$ 
   $a \leftarrow \epsilon$ 
  for  $i \in [1 \dots n]$  do
     $c_0 \leftarrow \mathbb{E}_{r \leftarrow \{0, 1\}^n} [|E(S_r, \overline{S_r})| \mid (r_1 = a_1), \dots, (r_{i-1} = a_{i-1}), (r_i = 0)]$ 
     $c_1 \leftarrow \mathbb{E}_{r \leftarrow \{0, 1\}^n} [|E(S_r, \overline{S_r})| \mid (r_1 = a_1), \dots, (r_{i-1} = a_{i-1}), (r_i = 1)]$ 
     $a_i \leftarrow \arg \max_{\ell \in \{0, 1\}} (c_\ell)$ 
  end
  return  $S_a$ 
```

**טענה:** תהא  $E$  קבוצה יהי  $n \in \mathbb{N}$  ותהא  $\{v_1, \dots, v_n\}$  קבוצה אזי לכל  $i \in [n]$  באיטרציה ה- $i$  של CEBigCut מתקיים  $\mathbb{E}_{r \leftarrow \{0, 1\}^n} [|E(S_r, \overline{S_r})| \mid (r_1 = a_1), \dots, (r_{i-1} = a_{i-1})] = |\{(v_i, v_j) \in E \mid (i, j \leq k) \wedge (a_i \neq a_j)\}| + \frac{1}{2} |\{(v_i, v_j) \in E \mid (i > k) \vee (j > k)\}|$ .  
**מסקנה:** תהא  $E$  קבוצה יהי  $n \in \mathbb{N}$  ותהא  $\{v_1, \dots, v_n\}$  קבוצה אזי CEBigCut בעלת סיבוכיות זמן ריצה  $\text{poly}(n)$ .

**טענה:** תהא  $E$  קבוצה יהי  $n \in \mathbb{N}$  ותהא  $\{v_1, \dots, v_n\}$  קבוצה אזי לכל  $i \in [n]$  באיטרציה ה- $i$  של CEBigCut מתקיים  $\mathbb{E}_{r \leftarrow \{0, 1\}^n} [|E(S_r, \overline{S_r})| \mid (r_1 = a_1), \dots, (r_{i-1} = a_{i-1})] \geq \frac{|E|}{2}$ .  
**מסקנה:** תהא  $E$  קבוצה יהי  $n \in \mathbb{N}$  ותהא  $\{v_1, \dots, v_n\}$  קבוצה אזי  $E(\text{CEBigCut}, \overline{\text{CEBigCut}}) \geq \frac{|E|}{2}$ .

**טענה:** יהי  $n \in \mathbb{N}$  יהי  $k \geq 2 \log_2(2n)$  אזי קיימת צביעת קשתות  $f$  של  $K_n$  בשני צבעים עבורה לא קיים תת-גרף  $K_k$  מונוכרומטי.  
**מספר הפסוקיות המסופקות:** תהא  $\varphi \in \text{CNF}$  באשר  $\varphi = \bigwedge_{i=1}^m C_i$  בעלת  $n$  משתנים ותהא  $\alpha \in \{0, 1\}^n$  השמה אזי  $\text{CL}(\varphi, \alpha) = |\{i \in [m] \mid \alpha(C_i) = \text{True}\}|$ .

**יחס הפסוקיות המסופקות:** תהא  $\varphi \in \text{CNF}$  באשר  $\varphi = \bigwedge_{i=1}^m C_i$  אזי  $\text{RCL}(\varphi, \alpha) = \frac{1}{m} \cdot \text{Cl}(\varphi, \alpha)$ .  
**הגדרה:** יהי  $k \in \mathbb{N}_+$  נגדיר  $k\text{CNF} : \text{CNF} \rightarrow \mathbb{N}$  כך  $\max k\text{SAT}(\varphi) = \max \left\{ \text{RCL}(\varphi, \alpha) \mid \alpha \in \{0, 1\}^{|\text{FV}(\varphi)|} \right\}$ .  
**טענה:** תהא  $\varphi \in 3\text{CNF}$  בעלת  $m$  פסוקיות אזי  $\max 3\text{SAT}(\varphi) \geq \frac{7}{8} m$ .

**הגדרה Exactly  $k\text{CNF}$ :** יהי  $k \in \mathbb{N}_+$  אזי  $\text{EkSAT} = \{\langle \varphi \rangle \mid (\langle \varphi \rangle \in k\text{SAT}) \wedge (|\text{FV}(C)| = k \text{ מתקיים } C)\}$ .  
**הגדרה:** יהי  $k \in \mathbb{N}_+$  נגדיר  $\text{EkSAT} : \text{EkSAT} \rightarrow \mathbb{N}$  כך  $\max \text{EkSAT}(\varphi) = \max \left\{ \text{RCL}(\varphi, \alpha) \mid \alpha \in \{0, 1\}^{|\text{FV}(\varphi)|} \right\}$ .

**סימון:** תהא  $M$  מ"ט  $k$ -סרטית ותהא  $c_1 \$ c_2 \$ \dots \$ c_k$  קונפיגורציה אזי  $c_i = (c_1 \$ c_2 \$ \dots \$ c_k)^i$ .

**סימון:** תהא  $x \in \Sigma^*$  ותהא  $A \subseteq \Sigma^*$  אזי  $x \setminus A$  הינה המחרוזת  $x$  ללא אברי  $A$ .

**מכונת טיורינג בעלת סיבוכיות מקום:** תהא  $S : \mathbb{N} \rightarrow \mathbb{N}$  אזי מ"ט תלת-סרטית  $M$  עבורה לכל קונפיגורציות  $c_0 \dots c_n$  באשר  $c_0 = q_0 x$  וכן  $c_{i-1}$  עוברת ל- $c_i$  לכל  $i \in [n]$  מתקיים

- סרט לקריאה בלבד: לכל  $i \in [n]$  מתקיים  $c_i^1 = x \setminus Q$ .
- סרט חסום במקום: לכל  $i \in [n]$  מתקיים  $|c_{i-1}^2| \leq S(n) + 1$ .
- סרט לכתובה חד-פעמית: לכל  $i \in [n]$  ולכל  $j \in [|c_{i-1}^3|]$  מתקיים  $(c_{i-1}^3 \setminus Q)_j = (c_i^3 \setminus Q)_j$ .

**חסם עליון למקום ריצה של מכונת טיורינג:** תהא  $S : \mathbb{N} \rightarrow \mathbb{N}$  ותהא  $M$  מ"ט בעלת סיבוכיות מקום  $S$  אזי  $S$ .

**הערה:** נקרא למכונת טיורינג בעלת סיבוכיות מקום מכונת טיורינג.

**הגדרה Deterministic Space:** תהא  $S : \mathbb{N} \rightarrow \mathbb{N}$  אזי  $\{M \mid M \text{ מ"ט שרצה במקום } \mathcal{O}(S(n)) \mid L(M)\} = \text{DSpace}(S(n))$ .

**הגדרה Polynomial Space:**  $\text{PSPACE} = \bigcup_{c \in \mathbb{N}} \text{DSpace}(n^c)$ .

**הגדרה Logarithmic Space:**  $\text{LOG} = \text{DSpace}(\log(n))$ .

**סימון:**  $\text{LOG} = \text{LOGSPACE} = \text{LSPACE} = \text{L}$ .

**טענה:**  $\text{DSpace}(1) = \text{DSpace}(\log(\log(n))) = \{L \mid L \text{ רגולרית}\}$ .

**טענה:** תהא  $T$  חשיבה בזמן אזי  $\text{DTime}(T(n)) \subseteq \text{DSpace}(T(n))$ .

**טענה:**  $\mathcal{NP} \subseteq \text{PSPACE}$ .

**טענה:** תהא  $S : \mathbb{N} \rightarrow \mathbb{N}$  באשר  $S \geq \log$  אזי  $\text{DSpace}(S(n)) \subseteq \text{DTime}(2^{\mathcal{O}(S(n))})$ .

**מסקנה:**  $\text{LOG} \subseteq \mathcal{P}$ .

**מסקנה:**  $\text{PSPACE} \subseteq \text{EXP}$ .

**פונקציה חשיבה במקום:** פונקציה  $S : \mathbb{N} \rightarrow \mathbb{N}$  עבורה קיימת מ"ט  $M$  המקיימת לכל  $n \in \mathbb{N}$  כי  $M$  על הקלט  $1^n$  מחשבת את  $(S(n))_2$  במקום  $\mathcal{O}(S(n))$ .

**משפט היררכיית המקום:** תהא  $S : \mathbb{N} \rightarrow \mathbb{N}$  חשיבה במקום ותהא  $t(n) = o(S(n))$  אזי  $\text{DSpace}(t(n)) \subsetneq \text{DSpace}(S(n))$ .

**מסקנה:**  $\text{LOG} \subsetneq \text{PSPACE}$ .

**מסקנה:** לפחות אחד מהבאים נכון

•  $\text{LOG} \subsetneq \mathcal{P}$

•  $\mathcal{P} \subsetneq \text{PSPACE}$

**השערה:**  $\text{LOG} \subsetneq \mathcal{P}$  השערה פתוחה

**השערה:**  $\mathcal{P} \subsetneq \text{PSPACE}$  השערה פתוחה

**פונקציה חשיבה במקום  $S$ :** תהא  $D \subseteq \Sigma$  אזי  $f : D \rightarrow (\Gamma \setminus \{\perp\})^*$  עבורה קיימת מ"ט  $M$  בעלת סיבוכיות מקום  $S(n)$  המחשבת את  $f$ .

**רדוקציית מיפוי במקום לוגריתמי:** יהיו  $\Delta, \Sigma$  אלפביטים באשר  $\Sigma \subseteq \Delta$  תהא  $A \subseteq \Sigma^*$  שפה ותהא  $B \subseteq \Delta^*$  שפה אזי רדוקציית מיפוי  $f$  מ- $A$  ל- $B$  חשיבה במקום לוגריתמי.

**סימון:** יהיו  $\Delta, \Sigma$  אלפביטים באשר  $\Sigma \subseteq \Delta$  תהא  $A \subseteq \Sigma^*$  שפה ותהא  $B \subseteq \Delta^*$  שפה ותהא  $f : \Sigma^* \rightarrow \Delta^*$  רדוקציית מיפוי במקום לוגריתמי אזי  $A \leq_{\text{Log}} B$ .

**טענה:** תהיינה  $A, B$  שפות עבורן  $A \leq_{\text{Log}} B$  אזי  $A \leq_p B$ .

**שפה קשה ביחס למחלקה:** תהא  $\mathcal{C}$  קבוצה של שפות אזי שפה  $\mathcal{L}$  עבורה לכל שפה  $L \in \mathcal{C}$  מתקיים  $L \leq_{\text{Log}} \mathcal{L}$ .

**שפה שלמה ביחס למחלקה:** תהא  $\mathcal{C}$  קבוצה של שפות אזי שפה  $\mathcal{L} \in \mathcal{C}$  באשר  $\mathcal{L}$  הינה  $\mathcal{C}$ -קשה.

**טענה:** תהא  $f$  חשיבה במקום  $S : \mathbb{N} \rightarrow \mathbb{N}$  תהא  $g$  חשיבה במקום  $R : \mathbb{N} \rightarrow \mathbb{N}$  ותהא  $m : \mathbb{N} \rightarrow \mathbb{N}$  עבורה לכל  $n \in \mathbb{N}$  ולכל  $x \in \Sigma^n$  מתקיים  $|f(x)| \leq m(n)$  אזי  $g \circ f$  חשיבה במקום  $\mathcal{O}(S(n) + \log(m(n)) + R(m(n)))$ .

**מסקנה:** תהא  $S : \mathbb{N} \rightarrow \mathbb{N}$  חשיבה במקום תהא  $f$  חשיבה במקום  $S$  תהא  $g$  חשיבה במקום  $R : \mathbb{N} \rightarrow \mathbb{N}$  ותהא  $m : \mathbb{N} \rightarrow \mathbb{N}$  עבורה לכל  $n \in \mathbb{N}$  ולכל  $x \in \Sigma^n$  מתקיים  $|f(x)| \leq m(n)$  אזי  $g \circ f$  חשיבה במקום  $\mathcal{O}(S(n) + R(m(n)))$ .

**טענה:** תהיינה  $A, B$  שפות באשר  $B \in \text{LOG}$  וכן  $A \leq_L B$  אזי  $A \in \text{LOG}$ .

**מסקנה:** תהיינה  $A, B, C$  שפות באשר  $A \leq_{\text{Log}} B$  וכן  $B \leq_{\text{Log}} C$  אזי  $A \leq_{\text{Log}} C$ .

**טענה:** תהא  $A \in \text{LOG}$  באשר  $A$  הינה  $\mathcal{P}$ -שלמה אזי  $\mathcal{P} = \text{LOG}$ .

**הגדרה Circuit Value Problem:**  $\text{CVAL} = \{\langle C, x \rangle \mid (C \text{ מעגל בוליאני}) \wedge (C(x) = 1)\}$ .

**למה קוק-לוין:** תהא  $M$  מ"ט רצה בזמן פולינומי אזי קיימת פונקציה חשיבה  $f$  במקום לוגריתמי עבורה  $f(1^n) = \langle C_{M,n} \rangle$  כאשר  $C_{M,n}$  מעגל עבורו לכל  $z \in \{0, 1\}^n$  מתקיים  $(C_{M,n}(z) = 1) \iff (M(z) \text{ מקבלת})$ .  
**טענה:** CVAL הינה  $\mathcal{P}$ -שלמה.

**נוסחה מכומתת לחלוטין:** תהא  $\varphi$  נוסחה כאשר  $\text{FV}(\varphi) = \{x_1 \dots x_n\}$  ויהיו  $Q_1 \dots Q_n \in \{\forall, \exists\}$  כמתים אזי  $Q_1 x_1 \dots Q_n x_n (\varphi)$ .  
**הגדרה True Quantified Boolean Formula Problem:**  $\text{TQBF} = \{\langle \varphi \rangle \mid \varphi \text{ נוסחה מכומתת לחלוטין וספיקה}\}$ .  
**טענה:** CVAL  $\in$  PSPACE.

**טענה:** TQBF הינה PSPACE-שלמה.  
**מילה בעלת ייצוג:** יהי  $k \in \mathbb{N}$  אזי  $x \in \Sigma^n$  עבורה קיימת מ"ט  $M$  המקיימת  $| \langle M \rangle | = k$  וכן  $M(i) = x_i$  לכל  $i \in [n]$ .  
**מעגל מיוצג על ידי מעגל:** יהי  $C$  מעגל בגודל  $s$  אזי מעגל  $A$  המקבל  $\log(s)$  ביטים עבורו קיימת  $f: V(C) \rightarrow [s]$  הפיכה המקיימת  $i \in [s] \implies A(i) = \langle f(i), \text{adj}^-(f(i)), \text{adj}^+(f(i)) \rangle$ .  
**סימון:** יהי  $C$  מעגל ויהי  $A$  מעגל המייצג את  $C$  אזי  $C = [A]$ .

**הגדרה Succinct Circuit Value Problem:**  $\text{Succ-CVAL} = \{\langle A, x \rangle \mid (A \text{ מעגל המייצג מעגל}) \wedge (\langle [A], x \rangle \in \text{CVAL})\}$ .  
**טענה:** Succ-CVAL  $\in$  EXP.  
**טענה:** Succ-CVAL הינה EXP-שלמה.

**מטריצה מיוצגת על ידי מעגל:** תהא  $A \in M_n(\mathbb{Z}_2)$  אזי מעגל  $C$  המקיים  $C(i, j) = (A)_{i,j}$  לכל  $i, j \in [n]$ .  
**סימון:** תהא  $A \in M_n(\mathbb{Z}_2)$  ויהי  $C$  מעגל המייצג את  $A$  אזי  $A = [C]$ .  
**הגדרה:**  $\text{Succ-BoolMatPower} = \left\{ \langle \langle C \rangle, n, t, i, j \rangle \mid (C \text{ מעגל המייצג מטריצה מסדר } n) \wedge \left( ([C]^t)_{i,j} = 1 \right) \right\}$ .  
**טענה:** Succ-BoolMatPower הינה PSPACE-שלמה.

**הגדרה Circuit Satisfiability Problem:**  $\text{CSAT} = \{\langle C \rangle \mid C \text{ מעגל ספיק}\}$ .  
**טענה:** CSAT הינה  $\mathcal{NP}$ -שלמה.

**הגדרה:**  $\text{Succ-CSAT} = \{\langle A \rangle \mid (A \text{ מעגל המייצג מעגל}) \wedge (\langle [A] \rangle \in \text{CSAT})\}$ .  
**טענה:** Succ-CSAT הינה  $\mathcal{NEXP}$ -שלמה.

**סדרת מעגלים Log-יוניפורמית:** משפחת מעגלים  $C$  עבורה קיימת מ"ט  $M$  באשר  $M$  רצה במקום  $\mathcal{O}(\log(n))$  וכן  $M(1^n) = \langle C_n \rangle$  לכל  $n \in \mathbb{N}$ .

**הגדרה Uniform Alternating Class:** תהיינה  $s, d: \mathbb{N} \rightarrow \mathbb{N}$  אזי  $\text{u-AC}(s, d) = \left\{ L \subseteq \{0, 1\}^* \mid \begin{array}{l} L(C) = L \\ \text{Size}(C_n) \leq s(n) \\ \text{depth}(C_n) \leq d(n) \end{array} \right\}$  קיימת משפחת מעגלים יוניפורמית  $C$  בעלת fan-in לא מוגבל עבורה.  
**הגדרה:**  $\text{u-AC}^k = \bigcup_{c \in \mathbb{N}} \text{u-AC}(n^c, \log^k(n))$  יהי  $k \in \mathbb{N}$  אזי.

**הגדרה Uniform Nick's Class:** תהיינה  $s, d: \mathbb{N} \rightarrow \mathbb{N}$  אזי  $\text{u-NC}(s, d) = \left\{ L \subseteq \{0, 1\}^* \mid \begin{array}{l} L(C) = L \\ \text{Size}(C_n) \leq s(n) \\ \text{depth}(C_n) \leq d(n) \end{array} \right\}$  קיימת משפחת מעגלים יוניפורמית  $C$  עבורה.  
**הגדרה:**  $\text{u-NC}^k = \bigcup_{c \in \mathbb{N}} \text{u-NC}(n^c, \log^k(n))$  יהי  $k \in \mathbb{N}$  אזי.

**סימון:** יהי  $k \in \mathbb{N}$  אזי  $\text{AC}^k = \text{u-AC}^k$ .

**סימון:** יהי  $k \in \mathbb{N}$  אזי  $\text{NC}^k = \text{u-NC}^k$ .

**מסקנה:** יהי  $k \in \mathbb{N}$  אזי  $\text{NC}^k \subseteq \text{AC}^k$ .

**טענה:** יהי  $k \in \mathbb{N}$  אזי  $\text{AC}^k \subseteq \text{NC}^{k+1}$ .

**הגדרה:**  $\text{AC} = \bigcup_{k=0}^{\infty} \text{AC}^k$ .

**הגדרה:**  $\text{NC} = \bigcup_{k=0}^{\infty} \text{NC}^k$ .

**מסקנה:**  $\text{AC} = \text{NC}$ .

**טענה:**  $\text{LOG} \subseteq \text{AC}^1$ .

**טענה:** יהי  $k \in \mathbb{N}$  אזי  $\text{NC}^k \subseteq \text{DSpace}\left(\mathcal{O}\left(\log^k(n)\right)\right)$ .

**טענה:** תהא  $S: \mathbb{N} \rightarrow \mathbb{N}$  יהי  $M$  מ"ט רץ בזמן  $S$  יהי  $x \in \Sigma^*$  ותהא  $G$  מטריצה המייצגת את עץ הקונפיגורציות אזי  $M(x)$  מקבלת  $\iff \left( (I + G)^{S(|x|)}_{x,y} \geq 1 \right)$  באשר  $y$  קונפיגורציה במצב מקבל.

**השערה:** קיימת מ"ט  $M$  הרצה בזמן פולינומי ובזיכרון  $\mathcal{O}(n)$  עבורה לכל מטריצה  $A$  המייצגת גרף מכון בעל  $n$  קודקודים ולכל קודקודים  $s, t$  מתקיים  $(M(\langle A, s, t \rangle) \text{ מקבלת}) \iff (s, t \text{ קיים מסלול מ- } s \text{ ל- } t)$ . השערה פתוחה

**מכונת טיורינג עם עצה:** תהא  $T : \mathbb{N} \rightarrow \mathbb{N}$  חשיבה בזמן תהא  $a : \mathbb{N} \rightarrow \mathbb{N}$  ותהא  $L$  שפה עבורה קיימת  $\{\alpha_n\}_{n \in \mathbb{N}}$  המקיימת  $| \alpha_n | \leq a(n)$  וקיימת מ"ט  $M$  עם זמן ריצה  $T$  המקיימת  $(x \in L) \iff (M(x, \alpha_{|x|}) = 1)$  אזי  $L \in \text{DTime}(T(n))/a(n)$ .  
**הגדרה Polynomial Time with Advice:** תהא  $a : \mathbb{N} \rightarrow \mathbb{N}$  אזי  $\mathcal{P}/a(n) = \bigcup_{k \in \mathbb{N}} \text{DTime}(n^k)/a(n)$ .  
**טענה:** קיימת שפה לא כריעה  $L$  המקיימת  $L \in \mathcal{P}/1$ .

**הגדרה:**  $\mathcal{P}/\text{poly} = \bigcup_{\ell \in \mathbb{N}} \mathcal{P}/n^\ell$

**טענה:**  $\mathcal{P}/\text{poly} = \text{Size}(\text{poly})$

**מכונת טיורינג לא דטרמיניסטית עם עצה:** תהא  $T : \mathbb{N} \rightarrow \mathbb{N}$  חשיבה בזמן תהא  $a : \mathbb{N} \rightarrow \mathbb{N}$  ותהא  $L$  שפה עבורה קיימת  $\{\alpha_n\}_{n \in \mathbb{N}}$  המקיימת  $| \alpha_n | \leq a(n)$  וקיימת מ"ט לא דטרמיניסטית  $M$  עם זמן ריצה  $T$  המקיימת  $(x \in L) \iff (M(x, \alpha_{|x|}) = 1)$  אזי  $L \in \text{NTIME}(T(n))/a(n)$ .

**הגדרה Nondeterministic Polynomial Time with Advice:** תהא  $a : \mathbb{N} \rightarrow \mathbb{N}$  אזי  $\mathcal{NP}/a(n) = \bigcup_{k \in \mathbb{N}} \text{NTIME}(n^k)/a(n)$

**הגדרה:**  $\mathcal{NP}/\text{poly} = \bigcup_{\ell \in \mathbb{N}} \mathcal{NP}/n^\ell$

**טענה:** תהא  $F : 3\text{CNF} \rightarrow \{0, 1\}^* \cup \{\perp\}$  באשר  $F(\varphi)$  השמה מספקת עבור  $\varphi$   $\iff (F(\varphi) \in \{0, 1\}^*)$  אזי  $F \in \mathcal{P}^{\text{SAT}}$ .  
**טענה:** אם קיים  $k \in \mathbb{N}$  עבורו  $\text{SAT} \in \mathcal{P}/\lfloor k \cdot \log(n) \rfloor$  אזי  $\text{SAT} \in \mathcal{P}$ .

**הגדרה Linear Programming:**  $\text{LIN-PROG} = \{ \langle A, b \rangle \mid (A \in M_{m \times n}(\mathbb{R})) \wedge (b \in \mathbb{R}^m) \wedge (\exists x \in \mathbb{R}^n. Ax \leq b) \}$

**טענה:**  $\text{LIN-PROG}$  הינה  $\mathcal{P}$ -קשה.

**מודל מקבילי (PRAM/Parallel RAM):** יהי  $(k, \Pi)$  מודל RAM ויהי  $p \in \mathbb{N}$  אזי  $(p, k, \Pi)$ .

**מספר המעבדים במודל PRAM:** יהי  $(p, k, \Pi)$  מודל PRAM אזי  $p$ .

**קונפיגורציה במודל PRAM:** יהי  $(p, k, \Pi)$  מודל PRAM ותהא  $(T, R, \text{PC})$  קונפיגורציה של מודל ה-RAM  $(k, \Pi)$  אזי  $(T, R, \text{PC})$ .

**קונפיגורציה עוברת במודל PRAM:** יהי  $(k, \Pi)$  מודל RAM ותהא  $(T, R, \text{PC})$  קונפיגורציה אזי קונפיגורציה  $(T', R', \text{PC}')$  באשר

$$\bullet \text{PC}' = \text{PC} + 1$$

**קיימים**  $i_1 \dots i_p \in [k]$  עבורם לכל  $j \in [k] \setminus \{i_1 \dots i_p\}$  מתקיים  $R'_j = R_j$  וכן קיימים  $\pi_1 \dots \pi_p \in \Pi \cup \{\text{Id}\}$  עבורם לכל

$$R'_{i_\ell} = \pi_{i_\ell}(R_{i_\ell}) \quad \ell \in [p]$$

**קיימים**  $i_1 \dots i_p \in \mathbb{N}$  עבורם לכל  $j \in \mathbb{N} \setminus \{i_1 \dots i_p\}$  מתקיים  $T'(j) = T(j)$  וכן קיימים  $\pi_1 \dots \pi_p \in \Pi \cup \{\text{Id}\}$  עבורם לכל

$$T'(\ell) = \pi(T(\ell)) \quad \ell \in [p]$$

**אלגוריתם במודל PRAM:** יהי  $(p, k, \Pi)$  מודל PRAM אזי פונקציה  $\delta$  מקונפיגורציות לקונפיגורציות עבורה לכל קונפיגורציה  $C$  מתקיים  $C$  עוברת ל- $\delta(C)$ .

**סימון:** יהי  $(p, k, \Pi)$  מודל PRAM ויהי  $x \in \mathbb{N}$  נגדיר  $T : \mathbb{N} \rightarrow \mathbb{N}$  כך  $T(n) = \begin{cases} x & n=0 \\ 0 & \text{else} \end{cases}$  אזי  $\text{Start}_x = (T, \{0\}, 0)$

**סימון:** יהי  $(p, k, \Pi)$  מודל PRAM יהי  $A$  אלגוריתם ויהי  $x \in \mathbb{N}$  אזי  $A_{\text{stop}} = \min \{n \in \mathbb{N} \mid A^{(n+1)}(\text{Start}_x) = A^{(n)}(\text{Start}_x)\}$  אזי  $(A^{(i)}(\text{Start}_x))_{i=1}^{A_{\text{stop}}}$

**זמן ריצה במודל PRAM:** יהי  $(p, k, \Pi)$  מודל PRAM יהי  $A$  אלגוריתם ויהי  $x \in \mathbb{N}$  אזי  $\text{Time}(A, x) = (A^{(A_{\text{stop}})}(\text{Start}_x))_3$

**עבודה במודל PRAM:** יהי  $(p, k, \Pi)$  מודל PRAM יהי  $A$  אלגוריתם ויהי  $x \in \mathbb{N}$  אזי  $\text{Work}(A, x) = p \cdot \text{Time}(A, x)$

**טענה:** תהא  $L \in \text{NC}^k$  ויהי  $n \in \mathbb{N}$  אזי  $L \cap \Sigma^n$  ניתנת לחישוב במודל PRAM בעל  $\text{poly}(n)$  מעבדים בזמן  $\mathcal{O}(\log^k(n))$

**טענה:** תהא  $L$  שפה באשר  $L \cap \Sigma^n$  ניתנת לחישוב במודל PRAM בעל  $\text{poly}(n)$  מעבדים בזמן  $\mathcal{O}(\log^k(n))$  לכל  $n \in \mathbb{N}$  אזי  $L \in \text{NC}^k$ .  
**השערה:** קיים מודל PRAM וקיים אלגוריתם  $A$  הפותר את CVAL בזמן  $\text{polylog}(n)$  ובעבודה  $\text{poly}(n)$ . השערה פתוחה

**השערה:**  $\mathcal{P} = \text{NC}$ . השערה פתוחה

**טענה:**  $\text{APSP} \in \text{NC}$

**מכונת טיורינג בעלת אורקל:** תהא  $\mathcal{O} \subseteq \{0, 1\}^*$  תהא  $Q \neq \emptyset$  קבוצה סופית ויהיו  $q_{\text{query}}, q_{\text{yes}}, q_{\text{no}} \in Q$  אזי מ"ט דו-סרטית  $M^\mathcal{O}$  באשר  $(M^\mathcal{O})_1 = Q$  המקיימת

**סרט שאילתה:** לכל קונפיגורציות  $c_0, c_1$  של  $M^\mathcal{O}$  באשר  $c_0$  עוברת ל- $c_1$  וכן  $c_0 \cap Q = \{q_{\text{query}}\}$  מתקיים

- אם  $c_0^2 \setminus Q \in \mathcal{O}$  אזי  $c_0^2 \cap Q = \{q_{\text{yes}}\}$

- אם  $c_0^2 \setminus Q \notin \mathcal{O}$  אזי  $c_0^2 \cap Q = \{q_{\text{no}}\}$

**הערה:** תהא  $\mathcal{O} \subseteq \{0, 1\}^*$  אזי מכאן והלאה  $M^\mathcal{O}$  תסמן מ"ט עם אורקל  $\mathcal{O}$ .

**הגדרה:** תהא  $\mathcal{O} \subseteq \{0, 1\}^*$  ותהא  $T : \mathbb{N} \rightarrow \mathbb{N}$  חשיבה בזמן אזי  $M^\mathcal{O}$  מ"ט הרצה בזמן  $\{L(M) \mid T(n)\}$   $\text{DTime}^\mathcal{O}(T(n))$

**הגדרה:** תהא  $\mathcal{O} \subseteq \{0, 1\}^*$  ותהא  $T : \mathbb{N} \rightarrow \mathbb{N}$  חשיבה במקום אזי  $M^\mathcal{O}$  מ"ט הרצה במקום  $\{L(M) \mid T(n)\}$   $\text{DSpace}^\mathcal{O}(T(n))$

**הגדרה:** תהא  $\mathcal{O} \subseteq \{0, 1\}^*$  אזי  $\mathcal{P}^\mathcal{O} = \bigcup_{c=0}^\infty \text{DTime}^\mathcal{O}(n^c)$



**הגדרה:** תהא  $\mathcal{O} \subseteq \{0, 1\}^*$  אזי  $\text{PSPACE}^{\mathcal{O}} = \bigcup_{c=0}^{\infty} \text{DSpace}^{\mathcal{O}}(n^c)$ .

**הגדרה:** תהא  $\mathcal{O} \subseteq \{0, 1\}^*$  ותהא  $L$  שפה עבודה קיימת מ"ט  $M^{\mathcal{O}}$  שרצה בזמן  $\text{poly}(n)$  באשר לכל  $x \in \Sigma$  מתקיים  $(x \in L) \iff$

$$L \in \mathcal{NP}^{\mathcal{O}} \iff (\exists y \in \Sigma^{\text{poly}(|x|)} . M(x, y) = 1)$$

**הגדרה:** תהיינה  $\mathcal{A}, \mathcal{B}$  משפחות של שפות אזי  $\mathcal{A}^{\mathcal{B}} = \bigcup_{L \in \mathcal{B}} \mathcal{A}^L$ .

**טענה:**  $\mathcal{NP}^{\text{PSPACE}} = \text{PSPACE}$

**מסקנה:**  $\mathcal{NP}^{\text{PSPACE}} = \mathcal{P}^{\text{PSPACE}}$

**טענה:** קיימת  $\mathcal{O} \subseteq \{0, 1\}^*$  עבורה  $\mathcal{NP}^{\mathcal{O}} \neq \mathcal{P}^{\mathcal{O}}$

**טענה משפט היררכיית הזמן עם אורקל:** תהא  $\mathcal{O} \subseteq \{0, 1\}^*$  תהא  $T : \mathbb{N} \rightarrow \mathbb{N}$  חשיבה בזמן ותהא  $t(n) = o\left(\frac{T(n)}{\log(T(n))}\right)$  אזי  $\text{DTime}^{\mathcal{O}}(t(n)) \subsetneq \text{DTime}^{\mathcal{O}}(T(n))$ .

**טענה משפט היררכיית הזמן עם אורקל:** תהא  $\mathcal{O} \subseteq \{0, 1\}^*$  תהא  $S : \mathbb{N} \rightarrow \mathbb{N}$  חשיבה במקום ותהא  $t(n) = o(S(n))$  אזי  $\text{DSpace}^{\mathcal{O}}(t(n)) \subsetneq \text{DSpace}^{\mathcal{O}}(T(n))$ .

**ריפוד של שפה:** תהא  $T : \mathbb{N} \rightarrow \mathbb{N}$  תהא  $L \in \text{DTime}(T(n))$  ותהא  $f$  חח"ע חשיבה בזמן באשר לכל  $n \in \mathbb{N}$   $f(n) \geq n$  אזי  $L_{\text{pad}}^f = \{x \mid |1^{f(|x|)-|x|-1}| \mid x \in L\}$

**טענה:** תהא  $T : \mathbb{N} \rightarrow \mathbb{N}$  תהא  $L \in \text{DTime}(T(n))$  ותהא  $f : \mathbb{N} \rightarrow \mathbb{N}$  אזי  $L_{\text{pad}}^f \in \text{DTime}(\text{poly}(n) + T(f^{-1}(n)))$

**מסקנה:**  $\mathcal{P}^{\text{EXP}} \neq \text{EXP}^{\text{EXP}}$

**טענה:**  $\mathcal{P}^{\text{EXP}} = \mathcal{NP}^{\text{EXP}}$

**הגדרה:**  $2\text{EXP} = \bigcup_{c=0}^{\infty} \text{DTime}(2^{2^{n^c}})$

**טענה:**  $\text{EXP}^{\text{EXP}} = 2\text{EXP}$

**טענה:** אם  $\mathcal{P} = \mathcal{NP}$  אזי  $\text{EXP} = \mathcal{NEXP}$

**הגדרה:**  $\text{E} = \bigcup_{k=0}^{\infty} \text{DTime}(2^{kn})$

**טענה:**  $\text{E} \neq \text{EXP}$

**טענה:**  $\text{E} \neq \text{PSPACE}$

**טענה:** תהא  $\mathcal{C}$  מחלקת שפות ותהא  $L$  שפה  $\mathcal{C}$ -שלמה אזי  $\mathcal{P}^{\mathcal{C}} = \mathcal{P}^L$

**טענה:**  $\mathcal{NP}^{\text{TQBF}} = \text{PSPACE}^{\text{TQBF}}$

**טענה:**  $\text{EXP} \neq \text{DSpace}(\mathcal{O}(2^n))$

**טענה:**  $\text{PSPACE}^{\text{PSPACE}} \neq \text{EXP}^{\text{PSPACE}}$

**טענה:**  $\mathcal{P}^{\text{HALT}} \neq \text{EXP}^{\text{HALT}}$

**הגדרה NP Error Zero:** תהא  $L$  שפה עבודה קיימת מטל"ד  $M$  עם זמן ריצה פולינומי המקיימת

• לכל  $x \in L$  מתקיים  $M(x) \in \{1, \text{quit}\}$

• לכל  $x \notin L$  מתקיים  $M(x) \in \{0, \text{quit}\}$

• לכל  $x \in \{0, 1\}^*$  קיים מסלול חישוב עבורו  $M(x) \neq \text{quit}$

אזי  $L \in \mathcal{ZNP}$

**טענה:**  $\mathcal{ZNP} = \mathcal{NP} \cap \text{coNP}$

**טענה:**  $\mathcal{P}^{\mathcal{ZNP}} = \mathcal{ZNP}$

**טענה:**  $\mathcal{NP}^{\mathcal{ZNP}} = \mathcal{NP}$

**הגדרה Bounded-error Probabilistic:** תהא  $T : \mathbb{N} \rightarrow \mathbb{N}$  חשיבה בזמן תהיינה  $s, c : \mathbb{N} \rightarrow [0, 1]$  ותהא שפה  $\mathcal{L}$  עבודה קיימת מ"ט

אקראית  $M$  עם זמן ריצה  $T$  המקיימת כי החל ממקום מסויים  $n \in \mathbb{N}$  מתקיים

• לכל  $x \in \mathcal{L} \cap \Sigma^n$  מתקיים  $\mathbb{P}_{r \leftarrow \{0, 1\}^{T(n)}}(M(x; r)) \geq c(n)$  (מקבלת)

• לכל  $x \notin \mathcal{L} \cap \Sigma^n$  מתקיים  $\mathbb{P}_{r \leftarrow \{0, 1\}^{T(n)}}(M(x; r)) \leq s(n)$  (מקבלת)

אזי  $\mathcal{L} \in \text{BP-Time}_{[s, c]}(T(n))$

**הגדרה Bounded-error Probabilistic Polynomial-time:** תהיינה  $s, c : \mathbb{N} \rightarrow [0, 1]$  אזי  $\mathcal{BPP}_{[s, c]} = \text{BP-Time}_{[s, c]}(\text{poly}(n))$

**טענה:**  $\bigcup_{\alpha: \mathbb{N} \rightarrow (0, 1]} \text{BPP}_{[0, \alpha]} = \mathcal{NP}$

**סימון:**  $\text{BPP} = \text{BPP}_{[\frac{1}{3}, \frac{2}{3}]}$

**הגדרה Randomized Polynomial-time:** תהא  $c : \mathbb{N} \rightarrow [0, 1]$  אזי  $\mathcal{RP}_{[c]} = \text{BPP}_{[0, c]}$

**סימון:**  $\mathcal{RP} = \text{BPP}_{[0, \frac{1}{2}]}$

**משלים של מחלקת שפות:** תהא  $\mathcal{C}$  מחלקת שפות אזי  $\text{co}\mathcal{C} = \{\bar{L} \mid L \in \mathcal{C}\}$ .

**טענה:**  $\text{coRP} = \text{BPP}_{[\frac{1}{2}, 1]}$ .

**טענה:** תהיינה  $\mathcal{C}_1, \mathcal{C}_2$  מחלקות שפות באשר  $\mathcal{C}_1 \subseteq \mathcal{C}_2$  אזי  $\text{co}\mathcal{C}_1 \subseteq \text{co}\mathcal{C}_2$ .

**בעיית הזיווג המושלם:**  $\text{PM} = \{\langle G \rangle \mid (G \text{ גרף דו-צדדי}) \wedge (G \text{ מושלם ב-} G)\}$ .

**טענה:**  $\text{PM} \in \mathcal{P}$ .

**פרמנטה של מטריצה:** תהא  $A \in M_n(\mathbb{F})$  אזי  $\text{perm}(A) = \sum_{\sigma \in S_n} \prod_{i=1}^n (A)_{i, \sigma(i)}$ .

**טענה:** יהי  $G$  גרף דו-צדדי ותהא  $A$  מטריצת השכנויות של  $G$  אזי  $\text{perm}(A) = \# \{G\text{-זיווגים מושלמים ב-} G\}$ .

**טענה:**  $\text{det} \in \text{NC}^2$ .

**אלגוריתם אקראי לקיום זיווג מושלם:** יהי  $G$  גרף דו-צדדי ויהי  $X \in M_n(\mathbb{N})$  באשר  $(X)_{i,j} \sim \text{Uni}([10n])$  לכל  $(i, j) \in [n]^2$  אזי

**function** IsPerfectMatching( $G, X$ ):

```

   $A \in M_n(\mathbb{N})$ 
   $A \leftarrow 0$ 
  for  $(i, j) \in E(G)$  do
     $(A)_{i,j} \leftarrow (X)_{i,j}$ 
  end
  return  $\mathbb{1}[\text{det}(A) \neq 0]$ 

```

**טענה:** יהי  $G$  גרף דו-צדדי אזי

• אם  $\langle G \rangle \notin \text{PM}$  אז  $\mathbb{P}_X(\text{IsPerfectMatching}(G, X) = 0) = 1$ .

• אם  $\langle G \rangle \in \text{PM}$  אז  $\mathbb{P}_X(\text{IsPerfectMatching}(G, X) = 0) \leq \frac{1}{10}$ .

**מודל RAM מקבילי הסתברותי (PPRAM/Probabilistic Parallel RAM):** יהי  $(p, k, \Pi)$  מודל PRAM אזי  $(p, k, \Pi)$ .

**קונפיגורציה במודל PPRAM:** יהי  $(p, k, \Pi)$  מודל PPRAM ותהא  $(T, R, \text{PC})$  קונפיגורציה כמודל PRAM ויהי  $X \in \{0, 1\}^*$  אזי  $(T, R, \text{PC}, X)$ .

**אקראיות בקונפיגורציה:** יהי  $(p, k, \Pi)$  מודל PPRAM ותהא  $(T, R, \text{PC}, X)$  קונפיגורציה אזי  $X$ .

**הערה:** את כל הפעולות ממודל PRAM נכליל בצורה הטבעית עבור PPRAM.

**טענה:** קיים מודל PPRAM המחשב את IsPerfectMatching בזמן  $\mathcal{O}(\log^2(n))$  ובעבודה  $\text{poly}(n)$ .

**מעגל אריתמטי:** יהי  $\mathbb{F}$  שדה אזי נוסחה מעל הבסיס  $\{+, *, -\}$ .

**הגדרה Polynomial Identity Testing Problem:**  $\text{PIT} = \{\langle \mathbb{F}, C \rangle \mid (\mathbb{F} \text{ שדה}) \wedge (C \text{ מעגל אריתמטי מעל } \mathbb{F} \text{ המייצג את פולינום ה-} 0^{\text{th}})\}$ .

**הערה:** בבעיית PIT נרצה שבפולינום שהמעגל מייצג כל המקדמים יהיו 0 זהותית.

**טענה:**  $\text{PIT} \in \text{coRP}$ .

**השערה:**  $\text{PIT} \in \mathcal{P}$ . השערה פתוחה

**טענה:** יהי  $\delta > 0$  ותהא  $L \in \mathcal{RP}$  ותהא  $V$  מ"ט העדה לכך באשר  $V$  מטילה  $m$  מטבעות אזי קיימת מ"ט  $M$  המטילה  $m \cdot \log(\frac{1}{\delta})$ .

מטבעות הרצה בזמן  $\text{Time}(V) \cdot \log(\frac{1}{\delta})$  אשר עדה להיות  $L \in \mathcal{RP}_{[\delta]}$ .

**טענה אמפליפיקציה חד-צדדית:** תהא  $L \in \mathcal{RP}$  אזי לכל  $c \in \mathbb{N}_+$  מתקיים  $L \in \mathcal{RP}_{[1-2^{-nc}]}$ .

**טענה אמפליפיקציה דו-צדדית:** תהא  $L \in \text{BPP}$  אזי לכל  $c \in \mathbb{N}_+$  מתקיים  $L \in \text{BPP}_{[2^{-nc}, 1-2^{-nc}]}$ .

**משפט צ'רנוף:** יהי  $p \in (0, 1)$  ויהיו  $Y_1 \dots Y_n \sim \text{Ber}(p)$  ב"ת אזי  $\mathbb{P}(|\sum_{i=1}^n Y_i - pn| \geq \alpha \cdot pn) \leq 2^{-\Omega(\alpha^2 \cdot pn)}$ .

**טענה:** יהי  $p \in [0, 1]$  ויהיו  $c, d \in \mathbb{N}$  אזי  $\text{BPP}_{[p, p+\frac{1}{nc}]} = \text{BPP}_{[2^{-nd}, 1-2^{-nd}]}$ .

**הגדרה:** תהא  $L$  שפה עבורה קיים  $k \in \mathbb{N}$  וקיימת מ"ט אקראית  $M$  המקיימת

• זמן פולינומי בממוצע: לכל  $x \in \{0, 1\}^*$  מתקיים  $\mathbb{E}_r(\text{Time}(M(x; r))) = \mathcal{O}(|x|^k)$ .

• נכונות: לכל  $x \in \{0, 1\}^*$  מתקיים  $x \in L \iff (x \text{ לכל } r \text{ אם } M(x; r) \text{ עוצרת אז } 1)$ .

אזי  $L \in \mathcal{ZPP}_1$ .

**טענה:**  $\mathcal{ZPP}_1 = \mathcal{RP} \cap \text{coRP}$ .

**הגדרה:** תהא  $L$  שפה עבורה קיימת מ"ט אקראית  $M$  המחזירה  $\{\text{Accept}, \text{Reject}, \text{Quit}\}$  עם זמן ריצה פולינומי המקיימת

• לכל  $x \in \{0, 1\}^*$  מתקיים  $\mathbb{P}_r(M(x; r) = \text{Quit}) \leq \frac{1}{2}$ .

• נכונות: לכל  $x \in \{0, 1\}^*$  ולכל  $r$  באשר  $M(x; r) \neq \text{Quit}$  מתקיים  $x \in L \iff (M(x; r) = 1)$ .



אזי  $L \in \mathcal{ZPP}_2$

**טענה:**  $\mathcal{ZPP}_1 = \mathcal{ZPP}_2$

**הגדרה**  $\mathcal{ZPP} = \mathcal{ZPP}_1$ : **Zero-error Probabilistic Polynomial-time**

**איזומורפיזם בין גרפים:** יהיו  $G, K$  גרפים אזי זיווג  $\pi : V(G) \rightarrow V(K)$  המקיים  $(u, v) \in E(G) \iff (\pi(u), \pi(v)) \in E(K)$

לכל  $u, v \in V(G)$

**סימון:** יהיו  $G, K$  גרפים איזומורפיים אזי  $G \cong K$

**הגדרה** **Tree Isomorphism Problem**:  $\text{Tree-ISO} = \{\langle T, S \rangle \mid (T, S) \text{ עצים} \wedge (T \cong S)\}$

**הגדרה** **Rooted Tree Isomorphism Problem**:  $\text{RTree-ISO} = \{\langle T, S \rangle \mid (T, S) \text{ עצים בעלי שורש} \wedge (T \cong S)\}$

**סימון:** יהי  $T$  עץ ויהי  $v \in V(T)$  אזי  $T_v = T[\text{child}(v)]$

**פולינום אופייני של עץ בעל שורש:** יהי  $T$  עץ בעל שורש  $r$  אזי  $p_T \in \mathbb{R}[x_0, \dots, x_{\text{depth}(T)}]$  המוגדרת כך

• אם  $T = (\{r\}, \emptyset)$  אזי  $p_T(x) = x$

• אחרת  $p_T(x_0, \dots, x_{\text{depth}(T)}) = \prod_{(r,v) \in E} (x_{\text{depth}(T)} - p_{T_v})$

**טענה:** יהיו  $T, S$  עצים בעלי שורש אזי  $(T \cong S) \iff (p_T = p_S)$

**אלגוריתם לבעיית איזומורפיזם העצים בעלי שורש:** יהיו  $T, S$  עצים בעלי שורש ותהא  $A \in \mathbb{N}^{\text{depth}(T)}$  באשר  $A_i \sim \text{Uni}([2 \cdot |V(T)|])$

ב"ת לכל  $i \in [\text{depth}(T)]$  אזי

**function** **IsTreeIsomorphic**( $T, S, A$ ):

```
if (depth(T) ≠ depth(S)) ∨ (|V(T)| ≠ |V(S)|) then
  return False
return 1[p_T(A_0, ..., A_{depth(T)}) = p_S(A_0, ..., A_{depth(T)})]
```

**טענה:**  $\text{RTree-ISO} \in \text{coRP}$

**מסקנה:**  $\text{Tree-ISO} \in \text{coRP}$

**מסקנה:** קיים אלגוריתם  $A$  ב- $\text{coRP}$  המחשב איזומורפיזם בין עצים.

**טענה:** אם  $\text{SAT} \in \mathcal{BPP}$  אזי  $\text{SAT} \in \mathcal{RP}$

**אלגוריתם** **Schöning**: תהא  $\varphi \in 3\text{CNF}$  באשר  $\text{FV}(\varphi) = \{x_1 \dots x_m\}$  וכן  $\varphi = \bigwedge_{i=1}^k C_i$  ותהא  $\alpha \sim \text{Uni}(\{0, 1\}^m)$  אזי

**function** **Schöning'sAlgorithm**( $\varphi, \alpha$ ):

```
for i ∈ [m] do
  if φ(α) = True then return True
  C ← arg min{n ∈ [m] | C_i(α) = False}
  ℓ ← FV(C)
  j ← n ∈ [m]. ℓ = x_n
  α_j = 1 - α_j
end
return False
```

**טענה:** תהא  $\varphi \in 3\text{CNF}$  באשר  $\varphi$  אי-ספיקה אזי  $\text{Schöning'sAlgorithm}(\varphi, \alpha) = \text{False}$  לכל  $\alpha \in \{0, 1\}^m$

**מרחק המינג:** יהי  $m \in \mathbb{N}_+$  ותהינה  $\alpha, \beta \in \{0, 1\}^m$  אזי  $d(\alpha, \beta) = |\{i \in [m] \mid \alpha_i \neq \beta_i\}|$

**סימון:** יהי  $m \in \mathbb{N}_+$  ותהינה  $\alpha, \beta \in \{0, 1\}^m$  אזי  $\Delta(\alpha, \beta) = d(\alpha, \beta)$

**טענה:** תהא  $\varphi \in 3\text{CNF}$  באשר  $\text{FV}(\varphi) = \{x_1 \dots x_m\}$  וכן  $\varphi$  ספיקה אזי  $\mathbb{P}_\alpha(\text{Schöning'sAlgorithm}(\varphi, \alpha) = \text{True}) \geq \frac{1}{2} \cdot \left(\frac{1}{3}\right)^{\frac{m}{2}}$

**טענה:** תהא  $\varphi \in 3\text{CNF}$  באשר  $\text{FV}(\varphi) = \{x_1 \dots x_m\}$  וכן  $\varphi$  ספיקה אזי  $\mathbb{P}_\alpha(\text{Schöning'sAlgorithm}(\varphi, \alpha) = \text{True}) \geq \left(\frac{2}{3}\right)^m$

**מסקנה:** תהא  $\varphi \in 3\text{CNF}$  באשר  $\text{FV}(\varphi) = \{x_1 \dots x_m\}$  וכן  $\varphi$  ספיקה אזי  $\mathbb{P}_{\alpha_1 \dots \alpha_{\left(\frac{3}{2}\right)^m}}(\exists i \in \left[\left(\frac{3}{2}\right)^m\right]. \text{Schöning'sAlgorithm}(\varphi, \alpha_i) = \text{True}) \geq \frac{1}{2}$

**מסקנה:**  $3\text{SAT} \in \mathcal{BP}\text{-Time}_{[0, \frac{1}{2}]}(\text{poly}(m) \cdot \left(\frac{3}{2}\right)^m)$

**טענה:**  $\mathcal{BPP} \subseteq \text{PSPACE}$

**טענה:**  $\mathcal{BPP} = \text{coBPP}$

**השערה:**  $\mathcal{RP} = \mathcal{NP}$  השערה פתוחה

**טענה:**  $\mathcal{NP} = \mathcal{RP}$  אזי  $\mathcal{NP} \subseteq \mathcal{BPP}$

**טענה:**  $\mathcal{NP} = \mathcal{RP}$  אזי  $\text{co}\mathcal{NP} \subseteq \mathcal{BPP}$

**טענה:**  $\mathcal{NP} = \mathcal{BPP}_{[0, \frac{1}{2\pi}]}$

**השערה:**  $\mathcal{BPP} \not\subseteq \mathcal{NP}$ . השערה פתוחה

**השערה:**  $\mathcal{NP} \subseteq \mathcal{BPP}$ . השערה פתוחה

**פרוטוקול תקשורת:** יהי  $t \in \mathbb{N}_+$  תהייה  $A, B : \{0, 1\}^* \times \{0, 1\}^* \rightarrow \{0, 1\}^*$  ויהי  $\text{Ret} \in \{A, B\}$  אזי  $(t, A, B, \text{Ret})$ .

**משתתפים בפרוטוקול תקשורת:** יהי  $\Pi$  פרוטוקול תקשורת אזי  $\{A, B\}$ .

**הרצת פרוטוקול תקשורת:** יהי  $(t, A, B, \text{Ret})$  פרוטוקול תקשורת ויהיו  $x, y \in \{0, 1\}^*$  אזי  $b_1 \dots b_t \in \{0, 1\}^*$  וכן  $\text{ANS} \in \{0, 1\}$  המקיימים

• לכל  $i \in \{2 \dots t\}$  אם  $i \% 2 = 1$  אז  $b_i = A(x, b_1 \dots b_{i-1})$

• לכל  $i \in \{2 \dots t\}$  אם  $i \% 2 = 0$  אז  $b_i = B(y, b_1 \dots b_{i-1})$

• אם  $\text{Ret} = A$  אז  $\text{ANS} = A(x, b_1 \dots b_t)$  אחרת  $\text{ANS} = B(y, b_1 \dots b_t)$ .

**סיבוב בפרוטוקול תקשורת:** יהי  $\Pi$  פרוטוקול תקשורת אזי  $b_i$  באשר  $i \in [t]$ .

**מספר הסיבובים בפרוטוקול תקשורת:** יהי  $(t, A, B, \text{Ret})$  פרוטוקול תקשורת אזי  $t$ .

**סימון:** יהי  $\Pi$  פרוטוקול תקשורת ויהיו  $x, y \in \{0, 1\}^*$  אזי  $\Pi(x, y) = \text{ANS}$ .

**פרוטוקול תקשורת מחשב פונקציה:** יהי  $n \in \mathbb{N}_+$  ותהא  $f : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$  אזי פרוטוקול תקשורת  $\Pi$  עבורו מתקיים  $\Pi(x, y) = f(x, y)$  לכל  $x, y \in \{0, 1\}^n$ .

**עלות תקשורת של פרוטוקול תקשורת:** יהי  $\Pi$  פרוטוקול תקשורת אזי  $\mathcal{C}(\Pi) = \max_{x, y \in \{0, 1\}^n} \sum_{i=1}^t |b_i(x, y)|$ .

**סיבוכיות תקשורת:** יהי  $n \in \mathbb{N}_+$  ותהא  $f : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$  אזי  $\mathcal{D}(f) = \min \{\mathcal{C}(\Pi) \mid f \text{ פרוטוקול המחשב את } f\}$ .

**טענה:** תהא  $f : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$  אזי  $\mathcal{D}(f) \leq n$ .

**הגדרה:** יהי  $n \in \mathbb{N}_+$  אזי  $\text{EQ}_n : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$  המוגדרת  $\text{EQ}_n(x, y) = \mathbb{1}[x = y]$ .

**המטריצה המייצג של פונקציה בוליאנית:** תהא  $f : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$  אזי  $M_f \in M_n(\mathbb{Z}_2)$  המוגדרת  $(M_f)_{i,j} = f(i, j)$  לכל  $i, j \in [n]$ .

**מלבן קומבינטורי:** תהייה  $S, T \subseteq \{0, 1\}^n$  אזי  $S \times T$ .

**מלבן קומבינטורי מונוכרומטי:** תהא  $f : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$  אזי מלבן קומבינטורי  $R$  עבורו  $\left| \left\{ (M_f)_{i,j} \mid (i, j) \in R \right\} \right| = 1$ .

**טענה:** תהא  $f : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$  אזי קיימת חלוקה של  $\{0, 1\}^n \times \{0, 1\}^n$  ל- $2^{\mathcal{D}(f)}$  מלבנים מונוכרומטיים.

**מסקנה:** תהא  $f : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$  אזי  $\text{rank}(M_f) \leq 2^{\mathcal{D}(f)}$ .

**מסקנה:** יהי  $n \in \mathbb{N}_+$  אזי  $\mathcal{D}(\text{EQ}_n) = n$ .

**פרוטוקול תקשורת בעל מטבעות פרטיים מחשב פונקציה:** יהי  $n \in \mathbb{N}_+$  ותהא  $f : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$  ויהי  $\varepsilon \in [0, 1]$  אזי פרוטוקול תקשורת  $\Pi$  עבורו מתקיים  $\mathbb{P}_{r_1, r_2}(\Pi((x; r_1), (y; r_2)) = f(x, y)) \geq 1 - \varepsilon$  לכל  $x, y \in \{0, 1\}^n$ .

**הגדרה:** יהי  $n \in \mathbb{N}_+$  אזי נגדיר פרוטוקול תקשורת בעל מטבעות פרטיים  $\Pi_{\text{REQ}}[n]$  כך

• בהינתן  $x, y \in \{0, 1\}^n$

• מגרילה  $A \in \{1, \dots, n^4\}$  ראשוני ושולחת את  $p$  ואת  $p \bmod x$ .

• עונה  $B \in \{1, \dots, n^4\}$  ואת  $y \bmod p$  ואת  $x \bmod p$ .

**טענה:** יהי  $n \in \mathbb{N}_+$  אזי  $\Pi_{\text{REQ}}[n]$  מחשבת את  $\text{EQ}_n$  בהסתברות  $\frac{1}{n^2}$  ובעלות  $8 \log(n)$ .

**פרוטוקול תקשורת בעל מטבעות פומביים מחשב פונקציה:** יהי  $n \in \mathbb{N}_+$  ותהא  $f : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$  ויהי  $\varepsilon \in [0, 1]$  אזי פרוטוקול תקשורת  $\Pi$  עבורו מתקיים  $\mathbb{P}_r(\Pi((x; r), (y; r)) = f(x, y)) \geq 1 - \varepsilon$  לכל  $x, y \in \{0, 1\}^n$ .

**קידוד לינארי:** יהי  $\mathbb{F}$  שדה ויהיו  $n, k, d \in \mathbb{N}_+$  אזי  $C : \mathbb{F}^k \rightarrow \mathbb{F}^n$  המקיימת

• לינאריות: לכל  $\alpha, \beta \in \mathbb{F}$  ולכל  $a, b \in \mathbb{F}^k$  מתקיים  $C(\alpha a + \beta b) = \alpha \cdot C(a) + \beta \cdot C(b)$ .

• מרחק: לכל  $a, b \in \mathbb{F}^k$  באשר  $a \neq b$  מתקיים  $\Delta(C(x), C(y)) \geq d$ .

**מימד של קידוד לינארי:** יהי  $\mathbb{F}$  שדה יהיו  $n, k, d \in \mathbb{N}_+$  ויהי  $C : \mathbb{F}^k \rightarrow \mathbb{F}^n$  קוד לינארי אזי  $k$ .

**מרחק של קידוד לינארי:** יהי  $\mathbb{F}$  שדה יהיו  $n, k, d \in \mathbb{N}_+$  ויהי  $C : \mathbb{F}^k \rightarrow \mathbb{F}^n$  קוד לינארי אזי  $d$ .

**טענה:** יהי  $\mathbb{F}$  שדה יהיו  $n, k, d \in \mathbb{N}_+$  ותהא  $C : \mathbb{F}^k \rightarrow \mathbb{F}^n$  אזי  $C$  קוד לינארי  $\iff (\text{Im}(C) \text{ תמ"ו של } \mathbb{F}^n) \wedge (\text{Im}(C) \text{ לכל } x, y \in \text{Im}(C))$ .

באשר  $x \neq y$  מתקיים  $\Delta(x, y) \geq d$ .

**הגדרה:** יהי  $\mathbb{F}$  שדה יהיו  $n, k, d \in \mathbb{N}_+$  ויהי  $C : \mathbb{F}^k \rightarrow \mathbb{F}^n$  קוד לינארי אזי  $C$  הינו  $[n, k, d]_{\mathbb{F}}$ .

**הגדרה:** יהי  $\mathbb{F}$  שדה יהי  $k \in \mathbb{N}_+$  יהי  $n \leq |\mathbb{F}|$  ויהי  $a \in \mathbb{F}^k$  אזי  $p_a \in \mathbb{F}[x]$  המוגדר  $p_a(x) = \sum_{i=0}^{k-1} a_{i+1}x^i$

**הגדרה קידוד ריד-סולומון:** יהי  $\mathbb{F}$  שדה יהי  $k \in \mathbb{N}_+$  יהי  $n \leq |\mathbb{F}|$  ויהיו  $f_1 \dots f_n \in \mathbb{F}$  אזי  $C : \mathbb{F}^k \rightarrow \mathbb{F}^n$  המוגדרת  $C(a) = (p_a(f_1) \dots p_a(f_n))$

**טענה:** יהי  $\mathbb{F}$  שדה יהי  $k \in \mathbb{N}_+$  יהי  $n \leq |\mathbb{F}|$  ויהיו  $f_1 \dots f_n \in \mathbb{F}$  אזי קידוד ריד-סולומון הינו  $[n, k, n-k]_{|\mathbb{F}|}$

**הגדרה:** יהיו  $n, m \in \mathbb{N}_+$  יהי  $\mathbb{F}$  שדה באשר  $|\mathbb{F}| = m$  ויהי  $C : \mathbb{F}^n \rightarrow \mathbb{F}^m$  קידוד ריד-סולומון אזי נגדיר פרוטוקול תקשורת בעל מטבעות פרטיים  $\Pi_{\text{req}}[n, m]$  כך

•  $A$  מגרילה  $i \in \{1, \dots, m\}$  ושולחת את  $i$  ואת  $(C(x))_i$

•  $B$  עונה  $[(C(x))_i = (C(y))_i]$  1.

**טענה:** יהי  $n \in \mathbb{N}_+$  אזי  $\Pi_{\text{req}}[n, m]$  מחשבת את  $\text{EQ}_n$  בהסתברות  $\frac{n}{m}$  ובעלות  $2 \log(m)$

**סימון:** תהיינה  $V, W$  קבוצות יהי  $D \in \mathbb{N}_+$  תהא  $C : V \times [D] \rightarrow W$  ותהא  $A \subseteq V$  אזי  $\Gamma(A) = \{C(a, i) \mid (a \in A) \wedge (i \in [D])\}$

**הגדרה Disperser:** יהי  $\varepsilon > 0$  יהי  $k \in \mathbb{N}_+$  תהיינה  $V, W$  קבוצות ויהי  $D \in \mathbb{N}_+$  אזי  $C : V \times [D] \rightarrow W$  עברה לכל  $A \subseteq V$  באשר  $|\Gamma(A)| \geq (1 - \varepsilon) |W|$  מתקיים  $2^k \leq |A|$

**טענה:** יהי  $\varepsilon > 0$  ויהיו  $k, t, m, D \in \mathbb{N}_+$  באשר  $2^m \leq \frac{D \cdot 2^k}{2 \ln(\frac{\varepsilon}{2})}$  וכן  $D > \frac{2 \cdot \ln(e \cdot \frac{2^t}{2^k})}{\varepsilon}$  אזי קיים  $C : \{0, 1\}^t \times [D] \rightarrow \{0, 1\}^m$  אשר הינו disperser  $(k, \varepsilon)$

**טענה:** יהי  $\delta > 0$  תהא  $L \in \mathcal{RP}$  ותהא  $V$  מ"ט העדה לכך באשר  $V$  מטילה  $m$  מטבעות אזי קיימת מ"ט  $M$  המטילה  $m + \log(\frac{1}{\delta})$  מטבעות הרצה בזמן  $\text{Time}(V) \cdot \mathcal{O}(\log(\frac{1}{\delta}))$  אשר עדה להיות  $L \in \mathcal{RP}_{[\delta]}$

**מקור:** יהי  $n \in \mathbb{N}$  אזי מ"מ  $Y$  מעל  $\{0, 1\}^n$

**k-מקור:** יהיו  $n, k \in \mathbb{N}$  באשר  $k \leq n$  אזי מקור  $Y$  מעל  $\{0, 1\}^n$  המקיים  $\mathbb{P}(Y = y) \leq 2^{-k}$  לכל  $y \in \{0, 1\}^n$

**מקור שטוח:** יהי  $n \in \mathbb{N}$  ותהא  $S \subseteq \{0, 1\}^n$  אזי מקור  $Y$  המקיים  $\mathbb{P}(Y = s) = \mathbb{P}(Y = x)$  לכל  $x, s \in S$

**מרחק סטטיסטי:** תהא  $\Omega$  קבוצה סופית ויהיו  $X, Y$  מ"מ מעל  $\Omega$  אזי  $\|X - Y\| = \frac{1}{2} \sum_{s \in \Omega} |\mathbb{P}(X = s) - \mathbb{P}(Y = s)|$

**טענה:** תהא  $\Omega$  קבוצה סופית ויהיו  $X, Y$  מ"מ מעל  $\Omega$  אזי  $\|X - Y\| = \max_{S \subseteq \Omega} |\mathbb{P}(X \in S) - \mathbb{P}(Y \in S)|$

**הגדרה Extractor:** יהיו  $n, k, d, m \in \mathbb{N}$  באשר  $k \leq n$  ויהי  $\varepsilon > 0$  אזי  $f : \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m$  עברה לכל k-מקור  $Y$  מעל  $\{0, 1\}^n$  מתקיים  $\left\| f(Y, \text{Uni}(\{0, 1\}^d)) - \text{Uni}(\{0, 1\}^m) \right\| < \varepsilon$

**משפט:** יהיו  $n, k \in \mathbb{N}$  באשר  $k \leq n$  ויהי  $\varepsilon > 0$  אזי קיים  $f : \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m$  אשר הינו extractor  $(k, \varepsilon)$  באשר

•  $m = k + d - 2 \log(\frac{1}{\varepsilon}) - \mathcal{O}(1)$

•  $d = \log(n - k) + 2 \log(\frac{1}{\varepsilon}) + \mathcal{O}(1)$

**טענה:** יהיו  $n, k \in \mathbb{N}$  באשר  $k \leq n - 1$  ויהי  $\varepsilon \in (0, \frac{1}{2})$  אזי  $f : \{0, 1\}^n \rightarrow \{0, 1\}$  אינו extractor  $(k, \varepsilon)$

**טענה:** תהא  $L \in \mathcal{BPP}$  אזי קיימת מ"ט הסתברותית  $M$  המשתמשת ב- $t$  ביטי אקראיות אשר עדה להיות  $L \in \mathcal{BPP}_{[2^{-\frac{2}{3}t}, 1 - 2^{-\frac{2}{3}t}]}$

**טענה:** יהיו  $n, k, d, m \in \mathbb{N}$  באשר  $k \leq n$  ויהי  $\varepsilon > 0$  ותהא  $f : \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m$  באשר  $f$  הינה extractor  $(k, \varepsilon)$  אזי  $f$  הינה disperser  $(k, \varepsilon)$

**טענה:** תהא  $L \in \mathcal{RP}$  אזי קיימת מ"ט הסתברותית  $M$  המשתמשת ב- $t$  ביטי אקראיות אשר עדה להיות  $L \in \mathcal{RP}_{[2^{-\frac{2}{3}t}]}$

**בעיית הבטחה:** תהיינה  $N, Y \subseteq \{0, 1\}^*$  באשר  $N \cap Y = \emptyset$  אזי  $(Y, N)$

**אלגוריתם פותר בעיית הבטחה:** תהא  $(Y, N)$  בעיית הבטחה ותהא  $\mathcal{C}$  מחלקה אזי אלגוריתם  $A : N \cup Y \rightarrow \{0, 1\}$  באשר  $A$  עדה להיות  $Y \in \mathcal{C}$

**הערה:** תהא  $L \subseteq \{0, 1\}^*$  אזי  $L \mapsto (L, \bar{L})$  הינו שיכון לבעיית הבטחה.

**הגדרה:** תהא  $\mathcal{C}$  מחלקה אזי  $\{\text{קיים אלגוריתם } A \text{ הפותר את בעיית ההבטחה וכן } A \text{ עד להיות } (Y, N) \mid (Y, N) \in \mathcal{C}\}$  Promise- $\mathcal{C}$

**אלגוריתם קירוב בעיה מקסימלית:** יהי  $c \geq 1$  תהא  $X$  קבוצה ותהא  $f : X \rightarrow \mathbb{R}$  אזי אלגוריתם  $A : X \rightarrow \mathbb{R}$  המקיים

$$\max_{x \in X} \frac{f(x)}{c} \leq A(x) \leq \max_{x \in X} f(x)$$

**אלגוריתם קירוב בעיה מינימלית:** יהי  $c \geq 1$  תהא  $X$  קבוצה ותהא  $f : X \rightarrow \mathbb{R}$  אזי אלגוריתם  $A : X \rightarrow \mathbb{R}$  המקיים

$$\min_{x \in X} f(x) \leq A(x) \leq c \cdot \min_{x \in X} f(x)$$

**הגדרה Min Gap Problem:** יהיו  $a, b \in \mathbb{R}$  תהא  $X$  קבוצה ותהא  $f : X \rightarrow \mathcal{P}(\mathbb{R})$  אזי  $\text{GAP}_{[a, b]} \min f = (\text{Yes}, \text{No})$  באשר

$$\text{Yes} = \{\langle x \rangle \mid (x \in X) \wedge (f(x) \leq a)\}$$

$$\text{No} = \{\langle x \rangle \mid (x \in X) \wedge (f(x) > b)\}$$

**הגדרה Max Gap Problem:** יהיו  $a, b \in \mathbb{R}$  תהא  $X$  קבוצה ותהא  $f : X \rightarrow \mathcal{P}(\mathbb{R})$  אזי  $\text{GAP}_{[a, b]} \max f = (\text{Yes}, \text{No})$  באשר

$$\bullet \text{ Yes} = \{\langle x \rangle \mid (x \in X) \wedge (f(x) \geq b)\}$$

$$\bullet \text{ No} = \{\langle x \rangle \mid (x \in X) \wedge (f(x) < a)\}$$

**הערה:** אם  $f$  הינה פונקציית  $\min, \max$  בצורה טבעית אזי  $\text{GAP}_{[a,b]} f$  הינה בעיית המרווח המתאימה.

**הגדרה Cover Vertex Min:** נגדיר  $\text{minVC} : \{G \mid \text{גרף } G\} \rightarrow \mathbb{N}$  כך  $\text{minVC}(G) = \min \{|A| \mid A \text{ כיסוי צמתים}\}$ .

**טענה:** יהי  $c \geq 1$  תהא  $X$  קבוצה תהא  $f : X \rightarrow \mathbb{R}$  ויהי  $A$  אלגוריתם פולינומי  $c$ -קירוב ל- $\text{min } f(X)$  אזי  $\text{GAP}_{[k,ck]} f \in \text{Promise-}\mathcal{P}$  לכל  $k \in \mathbb{N}$ .

**טענה:** קיים אלגוריתם פולינומי 2-קירוב לבעיית  $\text{minVC}$ .

**הגדרה Programming Linear Integer:**  $\text{INT-LIN-PROG} = \{\langle A, b \rangle \mid (A \in M_{m \times n}(\mathbb{R})) \wedge (b \in \mathbb{R}^m) \wedge (\exists x \in \mathbb{N}^n. Ax \leq b)\}$

**טענה:**  $\text{INT-LIN-PROG}$  הינה  $\mathcal{NP}$ -קשה.

**טענה:** יהי  $G$  גרף אזי הבעיה  $\text{minVC}(G)$  הינה

$$\begin{array}{ll} \min & C^T w \\ \text{s.t.} & w_v + w_u \geq 1, \forall (v, u) \in E \\ & w_v \in \{0, 1\}, \forall v \in V \end{array}$$

**אלגוריתם קירוב לבעיית הכיסוי המינימלי בעזרת תכנות לינארי:** יהי  $G$  גרף אזי

**function**  $\text{Approx-minVC}(G)$ :

$$\left| \begin{array}{l} w \leftarrow \text{solve} \left( \begin{array}{ll} \min & C^T w \\ \text{s.t.} & w_v + w_u \geq 1, \forall (v, u) \in E \\ & w_v \in [0, 1], \forall v \in V \end{array} \right) \\ \text{return } \{v \in V \mid w_v \geq \frac{1}{2}\} \end{array} \right|$$

**טענה:** יהי  $G$  גרף אזי  $\text{Approx-minVC}(G)$  הינו כיסוי צמתים.

**טענה:** יהי  $G$  גרף אזי  $\text{Approx-minVC}$  בעל זמן ריצה פולינומי.

**טענה:** יהי  $G$  גרף אזי  $\text{minVC}(G) \leq |\text{Approx-minVC}(G)| \leq 2 \cdot \text{minVC}(G)$

**טענה:** יהי  $G$  גרף אזי הבעיה  $\text{maxCut}(G)$  הינה

$$\begin{array}{ll} \max & \sum_{(u,v) \in E} \frac{1 - x_u x_v}{2} \\ \text{s.t.} & x_v \in \{-1, 1\}, \forall v \in V \end{array}$$

**הגדרה:** יהי  $G$  גרף אזי נגדיר את  $\text{maxCutExt}_1$  כך

$$\begin{array}{ll} \max & \sum_{(u,v) \in E} \frac{1 - x_u \cdot x_v}{2} \\ \text{s.t.} & x_v \in \mathbb{R}^n, \forall v \in V \\ & x_v \cdot x_v = 1, \forall v \in V \end{array}$$

**טענה:** יהי  $n \in \mathbb{N}_+$  יהיו  $v_1 \dots v_n \in \mathbb{S}^{n-1}$  ונגדיר  $A \in M_n(\mathbb{R})$  כך  $A = \begin{pmatrix} - & v_1 & - \\ & \vdots & \\ - & v_n & - \end{pmatrix}$  אזי  $AA^T$  מוגדרת חיובית.

**טענה:** יהי  $n \in \mathbb{N}_+$  אזי  $\{A \in M_n(\mathbb{R}) \mid A \text{ מוגדרת חיובית}\}$  קמורה.

**הגדרה:** יהי  $G$  גרף אזי נגדיר את  $\text{maxCutExt}_2$  כך

$$\begin{aligned} \max \quad & \sum_{(u,v) \in E} \frac{1 - (B)_{u,v}}{2} \\ \text{s.t.} \quad & B \in M_n(\mathbb{R}) \\ & (B)_{v,v} = 1, \forall v \in V \\ & (B)_{v,u} = (B)_{u,v}, \forall v, u \in V \end{aligned}$$

**טענה:** קיים אלגוריתם הפותר את  $\max\text{CutExt}_2$  בזמן פולינומי.

**טענה:** יהי  $G$  גרף אזי  $\max\text{CutExt}_1(G) = \max\text{CutExt}_2(G)$ .

**סימון:** יהי  $G$  גרף אזי  $\max\text{CutExt}(G) = \max\text{CutExt}_1(G)$ .

**טענה:** יהי  $G$  גרף אזי  $\max\text{Cut}(G) \leq |\max\text{CutExt}(G)| \leq \frac{1}{0.878} \max\text{Cut}(G)$ .

**פונקציית מרחק על גרף:** יהי  $G$  גרף לא מכוון אזי  $d : V^2 \rightarrow \mathbb{N}$  עבורה

• סימטריות: לכל  $u, v \in V$  מתקיים  $d(u, v) = d(v, u)$ .

• חיוביות ממש: לכל  $u \in V$  מתקיים  $d(u, u) = 0$ .

• אי-שיוויון המשולש: לכל  $u, v, w \in V$  מתקיים  $d(u, v) \leq d(u, w) + d(w, v)$ .

**סימון:** יהי  $G$  גרף תהא  $d$  פונקציית מרחק תהא  $S \subseteq V$  ותהא  $u \in V$  אזי  $d(u, S) = \min_{v \in V} d(u, v)$ .

**סימון:** יהי  $G$  גרף תהא  $d$  פונקציית מרחק ותהא  $S \subseteq V$  אזי  $r(S) = \max_{u \in V} d(u, S)$ .

**הגדרה  $k$ -Center Problem:** יהי  $k \in \mathbb{N}_+$  נגדיר  $\min\text{Center} : \{(G, d, k) \mid (G \text{ גרף}) \wedge (d \text{ מרחק}) \wedge (k \in \mathbb{N})\} \rightarrow \mathbb{N}$  כך

$\min\text{Center}(G, d, k) = \min \{r(S) \mid S \in \mathcal{P}_k(V)\}$ .

**אלגוריתם קירוב למציאת  $k$ -מרכז:** יהי  $k \in \mathbb{N}_+$  יהי  $G$  גרף ויהי  $d$  מרחק אזי

```
function ApproxCenter( $G, d, k$ ):
     $v \leftarrow V$ 
     $S \leftarrow \{v\}$ 
    while  $|S| < k$  do
         $v \leftarrow \arg \max \{d(u, S) \mid u \in V\}$ 
         $S \leftarrow S \cup \{v\}$ 
    end
    return  $S$ 
```

**טענה:** יהי  $k \in \mathbb{N}_+$  יהי  $G$  גרף ויהי  $d$  מרחק אזי  $\text{ApproxCenter}$  בעלת זמן ריצה פולינומי.

**טענה:** יהי  $k \in \mathbb{N}_+$  יהי  $G$  גרף ויהי  $d$  מרחק אזי  $\min\text{Center}(G) \leq |\text{ApproxCenter}(G, d, k)| \leq 2 \cdot \min\text{Center}(G)$ .

**הגדרה Dominating Set:**  $\text{DS} = \{(G, k) \mid \exists S \in \mathcal{P}_k(V). \forall v \in V. ((\text{adj}(v) \cup \{v\}) \cap S \neq \emptyset)\}$ .

**טענה:**  $\text{DS}$  הינה  $\mathcal{NP}$ -שלמה.

**טענה:** יהי  $c < 2$  אם קיים אלגוריתם פולינומי  $A$  אשר מהווה  $c$ -קירוב לבעיית  $\min\text{Center}$  אזי  $\mathcal{P} = \mathcal{NP}$ .

**רדוקציה פולינומית משמרת מרווח בין בעיות הבטחה:** יהיו  $(Y, N), (Y', N')$  בעיות הבטחה עבורן קיימת מ"ט פולינומית  $M$  המקיימת

• לכל  $x \in \{0, 1\}^*$  אם  $x \in Y$  אז  $M(x) \in Y'$ .

• לכל  $x \in \{0, 1\}^*$  אם  $x \in N$  אז  $M(x) \in N'$ .

אז  $(Y, N) \leq_p (Y', N')$ .

**בעיית הבטחה  $\mathcal{NP}$ -Promise-קשה:** בעיית הבטחה  $\Pi$  עבורה לכל  $L \in \mathcal{NP}$  מתקיים  $L \leq_p \Pi$ .

**טענה:** תהא  $\Pi$  בעיית הבטחה אזי  $(\Pi \text{ הינה } \mathcal{NP}\text{-Promise-קשה}) \iff (3\text{SAT} \leq_{\text{LOG}} \Pi)$ .

**בעיית קירוב  $\mathcal{NP}$ -קשה:** יהי  $c \geq 1$  ותהא  $f : X \rightarrow \mathbb{R}$  עבורה לכל  $A$  אשר  $c$ -מקרב את  $f$  מתקיים  $\text{SAT} \in \mathcal{P}^A$  אזי בעיית ה- $c$ -קירוב של  $f$ .

**טענה:** תהא  $X$  קבוצה תהא  $f : X \rightarrow \mathbb{R}$  ויהיו  $a, b \in \mathbb{R}$  באשר  $\text{GAP}_{[a,b]} f$  הינה  $\mathcal{NP}$ -Promise-קשה אזי בעיית ה- $\frac{b}{a}$  קירוב של  $f$  הינה

$\mathcal{NP}$ -קשה.

**מסקנה:**  $\min\text{Center}_{[1,2]}$  הינה  $\mathcal{NP}$ -Promise-קשה.

**הגדרה Max Clique:** נגדיר  $\maxClique : \{G \mid \text{גרף } G\} \rightarrow \mathbb{N}$  כך  $\maxClique(G) = \max \left\{ \frac{|K|}{|V|} \mid (K \text{ קליקה}) \wedge (K \text{ תת-גרף של } G) \right\}$ .

**הגדרה Max Independent Set:** נגדיר  $\maxIS : \{G \mid \text{גרף } G\} \rightarrow \mathbb{N}$  כך  $\maxIS(G) = \max \left\{ \frac{|I|}{|V|} \mid (I \subseteq V) \wedge (I \text{ בלתי תלויה}) \right\}$ .

**טענה:** יהיו  $a, b \in (0, 1)$  באשר  $a < b$  אזי  $\text{GAP}_{[a,b]} \maxClique \leq_p \text{GAP}_{[a,b]} \maxIS$ .

**טענה:** יהיו  $a, b \in (0, 1)$  באשר  $a < b$  אזי  $\text{GAP}_{[a,b]} \maxIS \leq_p \text{GAP}_{[1-b, 1-a]} \minVC$ .

**טענה:** יהיו  $a, b \in (0, 1)$  באשר  $a < b$  אזי  $\text{GAP}_{[a,b]} \max 3SAT \leq_p \text{GAP}_{[\frac{a}{3}, \frac{b}{3}]} \maxClique$ .

**הערה:** משמעות  $a, b \in (0, 1)$  היא אחוזים ביחס לטווח התוצאות האפשריות.

**הגדרה:** יהי  $b \in \mathbb{N}_+$  אזי  $3CNF(b) = \{\varphi \in 3SAT \mid b \text{ הוא לכל היותר } x \text{ מספר המופעים של } x \text{ ב-}\varphi\}$ .

**הגדרה:** יהי  $b \in \mathbb{N}_+$  אזי  $3SAT(b) = \{\langle \varphi \rangle \mid (\varphi \in 3CNF(b)) \wedge (\varphi \text{ ספיק})\}$ .

**טענה:**  $3SAT(3)$  הינה  $\mathcal{NP}$ -קשה.

**הגדרה:** יהי  $b \in \mathbb{N}_+$  אזי נגדיר  $\max 3SAT(b) : 3CNF(b) \rightarrow \mathbb{N}$  כך  $\max 3SAT(b)(\varphi) = \max 3SAT(\varphi)$ .

**טענה:** יהי  $d \in \mathbb{N}$  באשר  $\frac{1}{2} \leq e^2 d \cdot \left(\frac{1}{2}\right)^{d-2} \leq \frac{1}{2}$  אזי קיימת סדרת גרפים מכוונים  $\{G_k \mid k \in \mathbb{N}_+\}$  באשר  $G_n$  גרף על  $n$  קודקודים וכן  $\deg(v) \leq d$  לכל  $n \in \mathbb{N}$  ולכל  $v \in G_n$  עבודה לכל  $n \in \mathbb{N}$  ולכל  $A \subseteq V(G_n)$  באשר  $|A| \leq \frac{|V(G_n)|}{2}$  מתקיים  $|E(A, \overline{A})| \geq |A|$ .

**טענה:** יהי  $d \in \mathbb{N}$  באשר  $\frac{1}{2} \leq e^2 d \cdot \left(\frac{1}{2}\right)^{d-2} \leq \frac{1}{2}$  אזי  $\text{GAP}_{[0.9, 1]} \max 3SAT \leq \text{GAP}_{[1 - \frac{1}{10(12d+1)}, 1]} \max 3SAT(4d+1)$ .

**הגדרה Three-variable Linear Equation:**  $3LIN = \left\{ (A, v) \in M_{m \times n}(\mathbb{Z}_2) \times \mathbb{Z}_2^m \mid \forall i \in [m]. \sum_{j=1}^n \mathbf{1}[(A)_{i,j} = 1] \leq 3 \right\}$ .

**יחס המשוואת המסופקות:** יהיו  $m, n \in \mathbb{N}$  תהא  $A \in M_{m \times n}(\mathbb{Z}_2)$  תהא  $b \in \mathbb{Z}_2^m$  ותהא  $x \in \mathbb{Z}_2^n$  אזי  $\text{RTE}(A, v, x) = \frac{1}{m} |\{i \in [m] \mid R_i(A) \cdot x = v_i\}|$ .

**הגדרה:** נגדיר  $\max 3LIN : 3LIN \rightarrow \mathbb{N}$  כך  $\max 3LIN(A, v) = \max \left\{ \text{RTE}(A, v, x) \mid x \in \mathbb{Z}_2^{\text{rows}(A)} \right\}$ .

**טענה:** יהיו  $a, b \in [0, 1]$  אזי  $\text{GAP}_{[a,b]} \max 3SAT \leq_{\text{LOG}} \text{GAP}_{[\frac{a}{4}, \frac{b}{4}]} \max 3LIN$ .

**טענה:** יהיו  $a, b \in [0, 1]$  אזי  $\text{GAP}_{[a,b]} \max 3SAT \leq_{\text{LOG}} \text{GAP}_{[\frac{6+a}{10}, \frac{6+b}{10}]} \max 2SAT$ .

**טענה:** יהיו  $a, b \in [0, 1]$  אזי  $\text{GAP}_{[a,b]} \max 3LIN \leq_{\text{LOG}} \text{GAP}_{[\frac{a}{4}, \frac{b}{4}]} \maxIS$ .

**מספר הצביעה:** יהי  $G$  גרף אזי קיימת צביעה חוקית של  $G$  ב- $k$  צבעים  $\chi(G) = \min \{k \in \mathbb{N}_+ \mid \dots\}$ .

**טענה:** אם  $\mathcal{P} \neq \mathcal{NP}$  אז  $\text{GAP}_{[2, \sqrt{|V|}]} \chi$  אינה  $\mathcal{NP}$ -קשה.

**טענה:** יהי  $\varepsilon > 0$  אזי  $\text{GAP}_{[\frac{7}{8}-\varepsilon, \frac{7}{8}+\varepsilon]} \max E3SAT \in \text{Promise-}\mathcal{P}$ .

**הגדרה:** יהי  $d \in \mathbb{N}$  אזי  $\text{GraphDegree}_d = \{G \mid (\text{גרף } G) \wedge (\forall v \in V. \deg(V) \leq d)\}$ .

**הגדרה:** יהי  $d \in \mathbb{N}$  נגדיר  $\maxIS(d) : \text{GraphDegree}_d \rightarrow \mathbb{N}$  כך  $\maxIS(d)(G) = \maxIS(G)$ .

**טענה:** אם  $\mathcal{P} \neq \mathcal{NP}$  אז לכל  $a, b \in (0, 1)$  באשר  $a < b$  מתקיים  $\text{GAP}_{[a,b]} \maxIS(2)$  אינה  $\mathcal{NP}$ -קשה.

**טענה:** קיימים  $a, b \in (0, 1)$  באשר  $a < b$  וקיים  $D \in \mathbb{N}$  עבורם  $\text{GAP}_{[a,b]} \maxIS(D)$  הינה  $\mathcal{NP}$ -קשה.

**הגדרה Problem Circuit Minimal:**  $\text{MinCircuit} = \{\langle C \rangle \mid (C \text{ מעגל}) \wedge (|D| \geq |C| \text{ אז } C(x) = D(x) \text{ אם } D \text{ מעגל } D)\}$ .

**טענה:**  $\text{MinCircuit} \in \text{PSPACE}$ .

**סימון:** יהי  $k \in \mathbb{N}$  יהי  $A$  אלגוריתם ויהי  $x$  אזי  $\text{Alt}_k^{\exists}(M, x) = Q_1 w_1 \dots Q_k w_k (A(x, w_1 \dots w_k))$  באשר  $Q_i = \exists$  לכל  $i \in \mathbb{N}_{\text{odd}}$  וכן  $Q_i = \forall$  לכל  $i \in \mathbb{N}_{\text{even}}$ .

**הגדרה:** יהי  $k \in \mathbb{N}$  ותהא  $L$  שפה עבורה קיימת מ"ט פולינומית  $M$  המקיים כי  $(x \in L) \iff \text{Alt}_k^{\exists}(M, x)$  אזי  $L \in \Sigma_k$ .

**סימון:** יהי  $k \in \mathbb{N}$  יהי  $A$  אלגוריתם ויהי  $x$  אזי  $\text{Alt}_k^{\forall}(M, x) = Q_1 w_1 \dots Q_k w_k (A(x, w_1 \dots w_k))$  באשר  $Q_i = \forall$  לכל  $i \in \mathbb{N}_{\text{odd}}$  וכן  $Q_i = \exists$  לכל  $i \in \mathbb{N}_{\text{even}}$ .

**הגדרה:** יהי  $k \in \mathbb{N}$  ותהא  $L$  שפה עבורה קיימת מ"ט פולינומית  $M$  המקיים כי  $(x \in L) \iff \text{Alt}_k^{\forall}(M, x)$  אזי  $L \in \Pi_k$ .

**טענה:** יהי  $k \in \mathbb{N}$  אזי  $\Pi_k = \text{co}\Sigma_k$ .

**טענה:**  $\mathcal{P} = \Sigma_0 = \Pi_0$ .

**טענה:**  $\text{co}\mathcal{NP} = \Pi_1$  וכן  $\mathcal{NP} = \Sigma_1$ .

**טענה:**  $\text{MinCircuit} \in \Pi_2$ .

**טענה:**  $\text{TQBF} \in \Sigma_{\text{poly}}$ .

**טענה:** יהי  $k \in \mathbb{N}$  אזי  $\Sigma_k \subseteq \Sigma_{k+1}$  וכן  $\Pi_k \subseteq \Pi_{k+1}$  וכן  $\Sigma_k \subseteq \Pi_{k+1}$  וכן  $\Pi_k \subseteq \Sigma_{k+1}$ .

**הגדרה Polynomial Hierarchy:**  $\mathcal{PH} = \bigcup_{k \in \mathbb{N}} \Sigma_k$ .

**טענה:**  $\mathcal{PH} \subseteq \text{PSPACE}$ .

**טענה:** יהי  $k \in \mathbb{N}$  אזי  $\Sigma_{k+1} = \mathcal{NP}^{\Sigma_k}$ .



**הגדרה:** יהי  $k \in \mathbb{N}$  אזי  $\text{TQBF}_k^{\exists} = \{ \langle \varphi \rangle \mid (\varphi = \text{Alt}_k^{\exists}(\psi, \varepsilon) \text{ עבורה } \psi \text{ נוסחה קיימת נוסחה } \varphi) \wedge (\varphi \text{ ספיקה}) \}$

**טענה:** יהי  $k \in \mathbb{N}$  אזי  $\Sigma_k = \{ L \mid L \leq_{\text{Log}} \text{TQBF}_k^{\exists} \}$

**טענה:** יהי  $\ell \in \mathbb{N}_+$  אם  $\Sigma_\ell = \Pi_\ell$  אז  $\mathcal{PH} = \Sigma_\ell$

**הגדרה:**  $\text{ExactClique} = \{ \langle G, k \rangle \mid \text{maxClique}(G) = k \}$

**טענה:**  $\text{ExactClique} \in \Sigma_2 \cap \Pi_2$

**למה:** יהי  $k \in \mathbb{N}$  אזי  $\Sigma_4 \not\subseteq \text{Size}(\mathcal{O}(n^k))$

**משפט קאנאן:** יהי  $k \in \mathbb{N}$  אזי  $\Sigma_2 \not\subseteq \text{Size}(\mathcal{O}(n^k))$

**הגדרה Isomorphism Graph:**  $\text{GISO} = \{ \langle G, H \rangle \mid (G, H) \text{ עצים} \wedge (G \cong H) \}$

**הגדרה Isomorphism Non Graph:**  $\text{GNISO} = \overline{\text{GISO}}$

**טענה:**  $\text{GISO} \in \mathcal{NP}$

**השערה:**  $\text{GISO} \in \mathcal{P}$  השערה פתוחה

**טענה:**  $\text{PSPACE} = \text{coPSPACE}$

**טענה:**  $\mathcal{PH} = \text{coPH}$

**פרוטוקול אינטרקטיבי:** תהייה  $P, V : \{0, 1\}^* \rightarrow \{0, 1\}^*$  ויהי  $k \in \mathbb{N}_+$  אזי  $(P, V)$

**מוכיח בפרוטוקול אינטרקטיבי:** יהי  $(P, V)$  פרוטוקול אינטרקטיבי אזי  $P$

**מוודא בפרוטוקול אינטרקטיבי:** יהי  $(P, V)$  פרוטוקול אינטרקטיבי אזי  $V$

**מספר הסיבובים בפרוטוקול אינטרקטיבי:** יהי  $k \in \mathbb{N}_+$  ויהי  $(P, V)$  פרוטוקול אינטרקטיבי אזי  $k$

**הרצת פרוטוקול אינטרקטיבי:** יהי  $(P, V)$  פרוטוקול אינטרקטיבי יהי  $x \in \{0, 1\}^n$  ויהיו  $y_1 \dots y_k \in \{0, 1\}^m$  אזי

$a_1 \dots a_k \in \{0, 1\}^\ell$  וכן  $\text{ANS} \in \{0, 1\}$  המקיימים

• לכל  $i \in [t]$  מתקיים  $a_i = P(x, V(y_1 \dots y_{i-1}))$

•  $\text{ANS} = V(x, y_1 \dots y_k, a_1 \dots a_t)$

**הערה:** אלא אם נאמר אחרת  $y_1 \dots y_k \in \{0, 1\}^{\text{poly}(|x|)}$  וכן  $P : \{0, 1\}^* \rightarrow \{0, 1\}^{\text{poly}(|x|)}$

**הגדרה Deterministic Proof System:** יהי  $k \in \mathbb{N}$  ותהא  $L$  שפה עבורה קיימת מ"ט  $V$  פולינומית המקיימת לכל  $x \in \{0, 1\}^*$  קיימים

$y_1 \dots y_k \in \{0, 1\}^{\text{poly}(|x|)}$  המקיימים

• אם  $x \in L$  אז קיימת  $P$  עבורה  $(P, V)(x) = 1$

• אם  $x \notin L$  אז לכל  $P$  מתקיים  $(P, V)(x) = 0$

אזי  $L \in \text{dIP}(k)$

**הגדרה:**  $\text{dIP} = \text{dIP}(\text{poly}(n))$

**משפט:**  $\text{dIP} = \mathcal{NP}$

**פרוטוקול אינטרקטיבי הסתברותי:** תהא  $P : \{0, 1\}^* \rightarrow \{0, 1\}^*$  ותהא  $V$  מ"ט הסתברותית ויהי  $k \in \mathbb{N}_+$  אזי הפרוטוקול האינטרקטיבי

$(P, V)$

**פרוטוקול אינטרקטיבי בעל מטבעות פרטיים:** פרוטוקול אינטרקטיבי הסתברותי  $(P, V)$  באשר  $(y_1 \dots y_{i-1}) \neq V(y_1 \dots y_{i-1})$  לכל

$i \in [k]$

**פרוטוקול אינטרקטיבי בעל מטבעות פומביים:** פרוטוקול אינטרקטיבי הסתברותי  $(P, V)$  באשר  $(y_1 \dots y_{i-1}) = V(y_1 \dots y_{i-1})$  לכל

$i \in [k]$

**הערה:** מכאן פרוטוקול אינטרקטיבי יתייחס להסתברותי ואם לא נאמר אחרת אז בעל מטבעות פומביים.

**ערך של פרוטוקול אינטרקטיבי:** יהי  $\Pi$  פרוטוקול אינטרקטיבי ויהי  $x \in \{0, 1\}^n$  אזי  $\text{Val}(\Pi, x) = \mathbb{P}_{y_1 \dots y_k}(\Pi(x) = 1)$

**ערך של מוודא:** יהי  $V$  מוודא בפרוטוקול אינטרקטיבי אזי  $\text{Val}(V, x) = \max_P \text{Val}((P, V), x)$

**הגדרה Interactive Proof:** יהי  $k \in \mathbb{N}$  תהייה  $s, c : \mathbb{N} \rightarrow [0, 1]$  ותהא  $L$  שפה עבורה קיים מוודא  $V$  בפרוטוקול אינטרקטיבי בעל

מפתחות פרטיים ו- $k$  סיבוכים המקיים

• לכל  $x \in L$  אם  $x \in \{0, 1\}^*$  אז  $\text{Val}(V, x) \geq c(|x|)$

• לכל  $x \notin L$  אם  $x \in \{0, 1\}^*$  אז  $\text{Val}(V, x) \leq s(|x|)$

אזי  $L \in \text{IP}_{[s, c]}(k)$

**הגדרה:** תהייה  $s, c : \mathbb{N} \rightarrow [0, 1]$  אזי  $\text{IP}_{[s, c]} = \text{IP}_{[s, c]}(\text{poly}(n))$

**הגדרה:** יהי  $n \in \mathbb{N}_+$  אזי נגדיר פרוטוקול אינטרקטיבי בעל מטבעות פרטיים  $\Pi_{\text{GNISO}}^{\text{priv}}[n]$  כך

- בהינתן קלט  $(G_1, G_2)$  באשר  $G_1, G_2$  גרפים על  $n$  קודקודים.
- $V$  מגרילה  $\sigma \in S_n$  וכן  $b \in \{1, 2\}$  ושולחת את  $\sigma(G_b)$ .
- $P$  שולח  $c \in \{1, 2\}$ .
- $V$  עונה  $\mathbb{1}[b = c]$ .

**טענה:** יהי  $n \in \mathbb{N}_+$  והיו  $G_1, G_2$  גרפים איזומורפיים על  $n$  קודקודים אזי  $\mathbb{P}(\Pi_{\text{GNISO}}^{\text{priv}}[n](G_1, G_2) = 1) = \frac{1}{2}$ .

**טענה:** יהי  $n \in \mathbb{N}_+$  והיו  $G_1, G_2$  גרפים לא איזומורפיים על  $n$  קודקודים אזי  $\mathbb{P}(\Pi_{\text{GNISO}}^{\text{priv}}[n](G_1, G_2) = 1) = 0$ .

**מסקנה:**  $\text{GNISO} \in \text{IP}_{[0, \frac{1}{2}]}$ .

**הגדרה:** יהי  $n \in \mathbb{N}_+$  יהי  $\ell \in \mathbb{N}$  באשר  $4n! \leq 2^\ell < 8n!$  ונגדיר  $\mathcal{H} = \{h : \{0, 1\}^{n^2} \rightarrow \{0, 1\}^\ell \mid \exists a, b \in \mathbb{F}_{2^{n^2}}. h = ax + b\}$  אזי

נגדיר פרוטוקול אינטרקטיבי  $\Pi_{\text{GNISO}}^{\text{pub}}[n]$  כך

- בהינתן קלט  $(G_1, G_2)$  באשר  $G_1, G_2$  גרפים על  $n$  קודקודים.
- $V$  מגריל  $h \in \mathcal{H}$  וכן  $z \in \{0, 1\}^\ell$  ושולח את  $(h, z)$ .
- $P$  שולח גרף  $G$  וכן  $\sigma \in S_n$  וכן  $b \in \{1, 2\}$ .
- $V$  עונה  $\mathbb{1}[(h(G) = z) \wedge (\sigma(G_b) = G)]$ .

**טענה:** יהי  $n \in \mathbb{N}_+$  והיו  $G_1, G_2$  גרפים איזומורפיים על  $n$  קודקודים אזי  $\mathbb{P}(\Pi_{\text{GNISO}}^{\text{pub}}[n](G_1, G_2) = 1) \leq \frac{n!}{2^\ell}$ .

**טענה:** יהי  $n \in \mathbb{N}_+$  והיו  $G_1, G_2$  גרפים לא איזומורפיים על  $n$  קודקודים אזי  $\mathbb{P}_r(\Pi_{\text{GNISO}}^{\text{pub}}[n](G_1, G_2) = 1) \geq 1.5 \cdot \frac{n!}{2^\ell}$ .

**הגדרה Arthur Merlin:** יהי  $k \in \mathbb{N}$  תהינה  $s, c : \mathbb{N} \rightarrow [0, 1]$  ותהא  $L$  שפה עבורה קיים מוודא  $V$  בפרוטוקול אינטרקטיבי בעל  $k$  סיבובים המקיים

- לכל  $x \in \{0, 1\}^*$  אם  $x \in L$  אז  $\text{Val}(V, x) \geq c(|x|)$
- לכל  $x \in \{0, 1\}^*$  אם  $x \notin L$  אז  $\text{Val}(V, x) \leq s(|x|)$

אזי  $L \in \text{AM}_{[s, c]}(k)$ .

**הגדרה Merlin Arthur:** יהי  $k \in \mathbb{N}$  תהינה  $s, c : \mathbb{N} \rightarrow [0, 1]$  ותהא  $L$  שפה עבורה קיים מוודא  $V$  בפרוטוקול אינטרקטיבי בעל  $k$  סיבובים המקיים

- לכל  $x \in \{0, 1\}^*$  אם  $x \in L$  אז  $\text{Val}(V, x \mid y_1 = \varepsilon) \geq c(|x|)$
- לכל  $x \in \{0, 1\}^*$  אם  $x \notin L$  אז  $\text{Val}(V, x \mid y_1 = \varepsilon) \leq s(|x|)$

אזי  $L \in \text{MA}_{[s, c]}(k)$ .

**הגדרה:** יהי  $k \in \mathbb{N}$  אזי  $\text{AM}(k) = \text{AM}_{[\frac{1}{3}, \frac{2}{3}]}(k)$ .

**הגדרה:** תהינה  $s, c : \mathbb{N} \rightarrow [0, 1]$  אזי  $\text{AM}_{[s, c]} = \text{AM}_{[s, c]}(2)$ .

**הגדרה:**  $\text{AM} = \text{AM}(2)$ .

**מסקנה:**  $\text{GNISO} \in \text{AM}$ .

**הגדרה:** יהי  $k \in \mathbb{N}$  אזי  $\text{MA}(k) = \text{MA}_{[\frac{1}{3}, \frac{2}{3}]}(k)$ .

**הגדרה:** תהינה  $s, c : \mathbb{N} \rightarrow [0, 1]$  אזי  $\text{MA}_{[s, c]} = \text{MA}_{[s, c]}(2)$ .

**הגדרה:**  $\text{MA} = \text{MA}(2)$ .

**השערה:**  $\text{GNISO} \in \text{MA}$  השערה פתוחה

**משפט:** תהינה  $s, c : \mathbb{N} \rightarrow [0, 1]$  אזי  $\text{IP}_{[s, c]} = \text{AM}_{[s, c]}(\text{poly}(n))$ .

**הגדרה:**  $\text{IP} = \text{IP}_{[\frac{1}{3}, \frac{2}{3}]}$ .

**טענה:** יהי  $\mathbb{F}$  שדה ותהא  $A \in M_n(\mathbb{F})$  אזי  $\text{perm}(A) = \sum_{i=1}^n (A)_{i,1} \cdot \text{perm}(A_{i,1})$ .

**מטריצה פולינומית:** יהי  $\mathbb{F}$  שדה והיו  $n, m \in \mathbb{N}_+$  אזי  $M_{n \times m}(\mathbb{F}[x])$ .

**דרגה של מטריצה פולינומית:** תהא  $D \in M_{n \times m}(\mathbb{F}[x])$  אזי  $\deg(D) = \max \left\{ \deg \left( (D)_{i,j} \right) \mid (i \in [n]) \wedge (j \in [m]) \right\}$ .

**טענה:** יהי  $n \in \mathbb{N}$  יהי  $p > 2^{n^2}$  ותהא  $A \in M_n(\mathbb{F}_p)$  אזי קיימת  $D \in M_{n-1}(\mathbb{F}_p[x])$  באשר  $\deg(D) \leq n-1$  המקיימת

$$D(i) = A_{i,1} \text{ לכל } i \in [n]$$

**סימון:** יהי  $n \in \mathbb{N}$  יהי  $p > 2^{n^2}$  ותהא  $A \in M_n(\mathbb{F}_p)$  ותהא  $D \in M_{n-1}(\mathbb{F}_p[x])$  באשר  $\deg(D) \leq n-1$  וכן  $D(i) = A_{i,1}$  לכל

$$D_A = D \text{ אזי } i \in [n]$$

**הגדרה:** יהי  $n \in \mathbb{N}$  והי  $2^{n^2} < p < 2^{n^2+1}$  ראשוני אזי נגדיר פרוטוקול אינטרקטיבי  $\Pi_{\text{perm}}[n]$  כך

- בהינתן קלט  $k \in \mathbb{F}_p$  וכן  $A \in M_n(\mathbb{F}_p)$
- לכל  $i \in [n-3]$

-  $P$  שולח פולינום  $g_i \in \mathbb{F}_q[x]$  באשר  $\deg(g_i) \leq (n-i)^2$ .

-  $V$  מגריל  $y_i \in \mathbb{F}_q$  ושולח אותו.

•  $P$  שולח פולינום  $g_{n-2} \in \mathbb{F}_q[x]$  באשר  $\deg(g_i) \leq 4$ .

•  $V$  מחשב  $B_1 = D_A(y_1)$ .

• לכל  $i \in \{2, \dots, n-3\}$  מחשב את  $B_i = D_{B_{i-1}}(y_i)$ .

• לכל  $i \in [n-1]$  מחשב את  $t_i = \mathbb{1} \left[ g_i(y_i) = \sum_{i=1}^n (B_i)_{i,1} \cdot g_{i+1}(i) \right]$ .

•  $V$  עונה  $\mathbb{1} \left[ \left( k = \sum_{i=1}^n (A)_{i,1} \cdot g_1(i) \right) \wedge \left( \bigwedge_{i=1}^{n-1} t_i \right) \wedge (g_{n-2} = \text{perm}(D_{B_{n-3}})) \right]$ .

**טענה:** יהי  $k \in \mathbb{F}_p$  ותהא  $A \in M_n(\mathbb{F}_p)$  באשר  $\text{perm}(A) = k$  אזי  $\mathbb{P}(\text{Val}_M(\Pi_{\text{perm}}[n], (A, k)) = 1) = 1$ .

**טענה:** יהי  $k \in \mathbb{F}_p$  ותהא  $A \in M_n(\mathbb{F}_p)$  באשר  $\text{perm}(A) \neq k$  אזי  $\mathbb{P}(\text{Val}_M(\Pi_{\text{perm}}[n], (A, k)) = 1) \leq \frac{1}{3}$ .

**מסקנה:** תהא  $p: \mathbb{N} \rightarrow \mathbb{N}$  באשר  $2^{n^2} < p(n) < 2^{n^2+1}$  וכן  $p(n) \in \mathbb{P}$  לכל  $n \in \mathbb{N}$  אזי  $\text{perm}_{\mathbb{F}_{p(n)}} \in \text{IP}$ .

**הערה:** משמעות  $\exists$  היא קיים עד, משמעות  $\forall$  היא לכל עד, משמעות  $\$$  היא באופן הסתברותי.

**הערה:** בהגדרות מלרע  $M, x, w, r$  פולינומיים, משמע  $\mathcal{P}$ .

**הגדרה:**  $\exists \mathcal{P} = \{L \mid \exists M. (x \in L) \iff (\exists w. M(x, w) = 1)\}$ .

**טענה:**  $\exists \mathcal{P} = \mathcal{NP}$ .

**הגדרה:**  $\forall \mathcal{P} = \{L \mid \exists M. (x \in L) \iff (\forall w. M(x, w) = 1)\}$ .

**טענה:**  $\forall \mathcal{P} = \text{coNP}$ .

**הגדרה:**  $\$_{[s,c]} \mathcal{P} = \left\{ L \mid \exists M. \begin{cases} (x \in L) \implies (\mathbb{P}_r(M(x, r) = 1) \geq c) \\ (x \notin L) \implies (\mathbb{P}_r(M(x, r) = 1) \leq s) \end{cases} \right\}$ .

**הגדרה:**  $\exists \$_{[s,c]} \mathcal{P} = \left\{ L \mid \exists M. \begin{cases} (x \in L) \implies (\exists w. \mathbb{P}_r(M(x, w, r) = 1) \geq c) \\ (x \notin L) \implies (\forall w. \mathbb{P}_r(M(x, w, r) = 1) \leq s) \end{cases} \right\}$ .

**טענה:**  $\exists \$_{[s,c]} \mathcal{P} = \text{MA}_{[s,c]}$ .

**הגדרה:**  $\$_{[s,c]} \exists \mathcal{P} = \left\{ L \mid \exists M. \begin{cases} (x \in L) \implies (\mathbb{P}_r(\exists w. M(x, w) = 1) \geq c) \\ (x \notin L) \implies (\mathbb{P}_r(\exists w. M(x, w) = 1) \leq s) \end{cases} \right\}$ .

**טענה:**  $\$_{[s,c]} \exists \mathcal{P} = \text{AM}_{[s,c]}$ .

**הערה:** ניתן להמשיך בצורה רקורסיבית זו על מנת להגדיר רצף קומבינציות בכל אורך של הכמתים.

**סימון:** יהי  $k \in \mathbb{N}$  אזי  $\underbrace{\text{MAMA} \dots}_k = \text{MA}(k)$ .

**טענה:** יהי  $k \in \mathbb{N}$  אזי  $\underbrace{\exists \exists \exists \dots}_k \mathcal{P} = \underbrace{\text{MAMA} \dots}_k$ .

**סימון:** יהי  $k \in \mathbb{N}$  אזי  $\underbrace{\text{AMAM} \dots}_k = \text{AM}(k)$ .

**טענה:** יהי  $k \in \mathbb{N}$  אזי  $\underbrace{\exists \exists \exists \dots}_k \mathcal{P} = \underbrace{\text{AMAM} \dots}_k$ .

**טענה:** יהי  $k \in \mathbb{N}$  אזי  $\underbrace{\exists \forall \exists \dots}_k \mathcal{P} = \Sigma_k$ .

**טענה:** יהי  $k \in \mathbb{N}$  אזי  $\underbrace{\forall \exists \forall \dots}_k \mathcal{P} = \Pi_k$ .

**הערה:**  $\underbrace{\exists \exists \exists \dots}_{\text{poly}(n)} \mathcal{P} = \text{IP}$ .

**הערה:**  $\underbrace{\exists \forall \exists \dots}_{\text{poly}(n)} \mathcal{P} = \text{PSPACE}$ .

**פרוטוקול אינטרקטיבי מרובה משתתפים:** יהיו  $m, k \in \mathbb{N}_+$  ותהינה  $P_1 \dots P_m, V: \{0, 1\}^* \rightarrow \{0, 1\}^*$  אזי  $(P_1, \dots, P_m, V)$ .

**הרצת פרוטוקול אינטרקטיבי מרובה משתתפים:** יהי  $(P_1, \dots, P_m, V)$  פרוטוקול אינטרקטיבי מרובה משתתפים יהי  $x \in \{0, 1\}^n$  יהי

אזי  $y \in M_{m \times k}(\{0, 1\}^\ell)$  וכן  $a \in M_{m \times k}$  ו- $\text{ANS} \in \{0, 1\}$  המקיימים

• לכל  $\eta \in [m]$  ולכל  $i \in [t]$  מתקיים  $(a)_{\eta,i} = P_\eta \left( x, V \left( (y)_{\eta,1}, \dots, (y)_{\eta,i-1} \right) \right)$ .

•  $\text{ANS} = V \left( x, (y)_{1,1}, \dots, (y)_{m,k}, (a)_{1,1}, \dots, (a)_{m,k} \right)$ .

**ערך של מוודא:** יהי  $V$  מוודא בפרוטוקול אינטרקטיבי מרובה משתתפים אזי  $\text{Val}(V, x) = \max_{P_1 \dots P_m} \text{Val}((P_1 \dots P_m, V), x)$ .

**הגדרה Proofs Interactive Multi-prover:** יהיו  $k, m \in \mathbb{N}_+$  תהינה  $s, c: \mathbb{N} \rightarrow [0, 1]$  ותהא  $L$  שפה עבורה קיים מוודא  $V$  בפרוטוקול

אינטרקטיבי בעל מפתחות פרטיים ו- $m$  משתתפים ו- $k$  סיבוכים המקיים

• לכל  $x \in \{0, 1\}^*$  אם  $x \in L$  אז  $\text{Val}(V, x) \geq c(|x|)$ .

• לכל  $x \in \{0, 1\}^*$  אם  $x \notin L$  אז  $\text{Val}(V, x) \leq s(|x|)$ .

אזי  $L \in \text{MIP}_{[s,c]}(m, k)$

**טענה:** יהי  $k \in \mathbb{N}_+$  ותהייה  $s, c : \mathbb{N} \rightarrow [0, 1]$  אזי  $\text{MIP}_{[s,c]}(1, k) = \text{IP}_{[s,c]}(k)$

**הגדרה:** יהיו  $m, k \in \mathbb{N}_+$  אזי  $\text{MIP}_{[\frac{1}{3}, \frac{2}{3}]}(m, k) = \text{MIP}(m, k)$

**משפט:**  $\text{MIP}(2, 2) = \mathcal{NEXP}$

**הגדרה:** יהיו  $n, q \in \mathbb{N}$  באשר  $q > 2^n$  אזי  $P_{x_i}(x_1 \dots x_n) = x_i$  המוגדר  $P_{x_i} \in \mathbb{F}_q[x_1 \dots x_n]$

**הגדרה:** יהיו  $n, q \in \mathbb{N}$  באשר  $q > 2^n$  אזי  $P_{\neg a}(x_1 \dots x_n) = 1 - P_a$  המוגדר  $P_{\neg a} \in \mathbb{F}_q[x_1 \dots x_n]$

**הגדרה:** יהיו  $n, q \in \mathbb{N}$  באשר  $q > 2^n$  אזי  $P_{a \vee b}(x_1 \dots x_n) = P_a + P_b - P_a P_b$  המוגדר  $P_{a \vee b} \in \mathbb{F}_q[x_1 \dots x_n]$

**הגדרה:** יהיו  $n, q \in \mathbb{N}$  באשר  $q > 2^n$  אזי  $P_{a \wedge b}(x_1 \dots x_n) = P_a \cdot P_b$  המוגדר  $P_{a \wedge b} \in \mathbb{F}_q[x_1 \dots x_n]$

**טענה:** יהי  $n \in \mathbb{N}$  והי  $\varphi \in 3\text{CNF}$  באשר  $\text{FV}(\varphi) = \{x_1 \dots x_n\}$  אזי  $P_\varphi(a) = \varphi(a)$  לכל  $a \in \{0, 1\}^n$

**טענה:** יהי  $n \in \mathbb{N}$  והי  $\varphi \in 3\text{CNF}$  באשר  $\text{FV}(\varphi) = \{x_1 \dots x_n\}$  אזי  $\varphi$  אינה ספיקה  $\iff (\sum_{a \in \{0, 1\}^n} P_\varphi(a) = 0)$

**הגדרה:** יהיו  $n, m, k, q \in \mathbb{N}_+$  באשר  $q > 2^n$  וכן  $k \in \{0 \dots 2^n\}$  נגדיר פרוטוקול אינטרקטיבי  $\Pi_{3\text{SAT}}$  כך

• בהינתן קלט  $\varphi \in 3\text{CNF}$  באשר  $\text{FV}(\varphi) = \{x_1 \dots x_n\}$  וכן  $\varphi = \bigwedge_{i=1}^m C_i$

• לכל  $i \in [n]$

-  $P$  שולח פולינום  $A_i \in \mathbb{F}_q[x]$  באשר  $\deg(A_i) \leq 3m$

-  $V$  מגדיל  $y_i \in \mathbb{F}_q$  ושולח אותו.

•  $P$  שולח  $A_{n+1} \in \mathbb{F}_q$

•  $V$  עונה  $\mathbb{1}[(A_1(0) + A_1(1) = k) \wedge (\forall i \in [n-1]. A_{i+1}(0) + A_{i+1}(1) = A_i(y_i)) \wedge (A_{n+1} = P_\varphi(y_1 \dots y_n))]$

**מוכיח הוגן:** תהא  $L \in \text{IP}$  והי  $(P, V)$  פרוטוקול אינטרקטיבי אשר עד להיות  $\text{val}(V, x) \geq c(|x|)$  לכל  $x \in \{0, 1\}^*$  אזי  $P$

**משפט שמיר:** קיים פרוטוקול אינטרקטיבי  $(P, V)$  בעל מוכיח הוגן ל- $\text{TQBF}$  באשר  $P$  רצה ב- $\text{PSPACE}$

**משפט:** אם  $\text{PSPACE} \subseteq \mathcal{P}/\text{poly}$  אז  $\text{PSPACE} = \text{AM}$

**השערה:**  $\text{PSPACE} \not\subseteq \mathcal{P}/\text{poly}$ . השערה פתוחה

**השערה:**  $\text{PSPACE} \neq \text{AM}$ . השערה פתוחה

**טענה:**  $\text{IP} \subseteq \text{PSPACE}$

**מסקנה:**  $\text{IP} = \text{PSPACE}$

**משפט אדלמן:**  $\mathcal{BPP} \subseteq \mathcal{P}/\text{poly}$

**השערה:**  $\mathcal{BPP} \neq \text{EXP}$ . השערה פתוחה

**טענה:**  $\text{AM} \subseteq \mathcal{N}^{\mathcal{P}/\text{poly}}$

**טענה:**  $\text{AM} \subseteq \text{NSize}(\text{poly})$

**למה:** אם  $\mathcal{NP} = \text{coNP}$  אז  $\Sigma_2 = \mathcal{NP}$

**הגדרה  $\text{Solver SAT Correct}$ :** יהיו  $n, m \in \mathbb{N}$  אזי  $\{\langle C \rangle \mid (C' \text{ מעגל בגודל } n \text{ על } m \text{ קלטים}) \wedge (3\text{SAT את } C')\}$

**טענה:**  $\text{CorrectSATSolver} \in \Pi_2$

**מסקנה:**  $\text{CorrectSATSolver} \in \Pi_1$

**משפט קארפ-ליפטון:** אם  $\mathcal{NP} \subseteq \mathcal{P}/\text{poly}$  אז  $\Sigma_2 = \Pi_2$

**משפט סיפסר:**  $\mathcal{BPP} \subseteq \Sigma_2$

**מסקנה:**  $\mathcal{BPP} \subseteq \Sigma_2 \cap \Pi_2$

**טענה:**  $\mathcal{BPP} \subseteq \mathcal{RP}^{\text{SAT}}$

**טענה:**  $\mathcal{BPP} \subseteq \mathcal{ZPP}^{\text{SAT}}$

**טענה אמפליפיקציה:** יהי  $c \in \mathbb{N}$  אזי  $\text{MA} = \text{MA}_{[2^{-n^c}, 1-2^{-n^c}]}$

**טענה אמפליפיקציה:** יהי  $c \in \mathbb{N}$  אזי  $\text{AM} = \text{AM}_{[2^{-n^c}, 1-2^{-n^c}]}$

**משפט:**  $\text{MA} = \text{MA}_{[\frac{1}{2}, 1]}$

**טענה:**  $\text{MA} \subseteq \text{AM}$

**השערה:**  $\text{MA} = \text{AM}$ . השערה פתוחה

**טענה:**  $\text{AM} \subseteq \Pi_2$

**טענה:**  $\text{MA} \subseteq \Sigma_2$

**טענה:**  $\mathcal{BPP} \subseteq \text{MA}$

**מסקנה:** יהי  $k \in \mathbb{N}_+$  אזי  $\text{AM}(k) \subseteq \text{AM}$

**טענה:** אם  $\text{GISO}$  הינה  $\mathcal{NP}$ -קשה אז  $\mathcal{PH} = \Sigma_2$

**טענה:** תהינה  $s, c : \mathbb{N} \rightarrow [0, 1]$  אזי  $\text{IP}_{[s,c]} \subseteq \text{IP}_{[s,1]}$

**למה:**  $\text{MAM}_{[\frac{1}{2},1]} = \text{AM}_{[\frac{1}{2},1]}$

**משפט:**  $\text{AM} = \text{AM}_{[\frac{1}{2},1]}$

**טענה:**  $\text{AM}_{[0,\frac{1}{2}]} = \mathcal{NP}$

**טענה:**  $\text{AM}_{[0,\frac{1}{2}]} = \text{MA}_{[0,\frac{1}{2}]}$

**הגדרה:** יהי  $\Sigma$  אלפבית תהינה  $r, q : \mathbb{N} \rightarrow \mathbb{N}$  תהינה  $s, c : \mathbb{N} \rightarrow [0, 1]$  ויהי  $n \in \mathbb{N}$  אזי נגדיר פרוטוקול אינטרקטיבי כך  $\Pi_{\text{PCP}}(\Sigma, s, c, r, q)[n]$

• בהינתן קלט  $x \in \{0, 1\}^n$

•  $P$  שולח מחרוזת  $w \in \Sigma^m$  באשר  $m \leq 2^{r(n)} \cdot q(n)$

•  $V$  מגריל  $y \in \{0, 1\}^{r(n)}$  ומחשב  $i \in [m]^{q(n)}$

•  $V$  עונה  $(x, y, w_{i_1} \dots w_{i_{q(n)}})$

**הגדרה Probabilistically Checkable Proof:** יהי  $\Sigma$  אלפבית תהינה  $r, q : \mathbb{N} \rightarrow \mathbb{N}$  תהינה  $s, c : \mathbb{N} \rightarrow [0, 1]$  ותהא  $L$  שפה עבורה קיים

מוודא  $V$  בפרוטוקול האינטרקטיבי  $\Pi_{\text{PCP}}(\Sigma, s, c, r, q)$  המקיים

• לכל  $x \in \{0, 1\}^*$  אם  $x \in L$  אז  $\text{Val}(V, x \mid y_1 = \varepsilon) \geq c(|x|)$

• לכל  $x \in \{0, 1\}^*$  אם  $x \notin L$  אז  $\text{Val}(V, x \mid y_1 = \varepsilon) \leq s(|x|)$

אזי  $L \in \text{PCP}_{[s,c]}(r(n), q(n))_{\Sigma}$

**הערה:** במחלקה  $\text{PCP}$  המוכיח לא חייב להיות פולינומי וכן ההודעות לא חייבות להיות פולינומיות.

**הגדרה:** תהינה  $r, q : \mathbb{N} \rightarrow \mathbb{N}$  ותהינה  $s, c : \mathbb{N} \rightarrow [0, 1]$  אזי  $\text{PCP}_{[s,c]}(r(n), q(n)) = \text{PCP}_{[s,c]}(r(n), q(n))_{\{0,1\}}$

**טענה:**  $3\text{SAT} \in \text{PCP}_{[1-\frac{1}{n},1]}(\log(n), 3)$

**משוואה ריבועית:** יהי  $n \in \mathbb{N}$  ויהי  $A \in M_{n \times n}(\mathbb{Z}_2)$  אזי  $\text{Quad}_{\alpha} : \mathbb{Z}_2^n \rightarrow \mathbb{Z}$  המוגדרת  $\text{Quad}_{\alpha}(x) = \sum_{i=1}^n \sum_{j=1}^n (A)_{i,j} \cdot x_i x_j$

**מכפלת וקטורים טנזורית:** יהיו  $n, m \in \mathbb{N}$  יהי  $u \in \mathbb{Z}_2^n$  ויהי  $v \in \mathbb{Z}_2^m$  אזי  $u \otimes v \in \mathbb{Z}_2^{n \cdot m}$  המוגדר  $(u \otimes v)_{i,j} = u_i \cdot v_j$

**מערכת משוואות ריבועיות:**  $\text{QuadEQ} = \{ \langle A, b \rangle \mid (A \in M_{m \times n \times n}(\mathbb{Z}_2)) \wedge (b \in \mathbb{Z}_2^m) \wedge (\exists x \in \mathbb{Z}_2^n. \forall k \in [m]. \text{Quad}_{A_k}(x) = b_k) \}$

**טענה:**  $\text{QuadEQ}$  הינה  $\mathcal{NP}$ -שלמה.

**טענה:**  $\text{QuadEQ} = \{ \langle B, b \rangle \mid (B \in M_{m \times n^2}(\mathbb{Z}_2)) \wedge (b \in \mathbb{Z}_2^m) \wedge (\exists u \in \{0, 1\}^n. B \cdot (u \otimes u) = b) \}$

**קוד הדמרד:** יהי  $n \in \mathbb{N}$  אזי  $\text{HAD} : \{0, 1\}^n \rightarrow \{0, 1\}^{2^n}$  המוגדר  $(\text{HAD}(x))_i = \langle x, (i)_2 \rangle$

**טענה:** יהי  $n \in \mathbb{N}$  אזי קוד הדמרד הינו קידוד לינארי  $[2^n, n, 2^{n-1}]_2$

**הגדרה:** יהי  $m \in \mathbb{N}_+$  ותהינה  $\alpha, \beta \in \{0, 1\}^m$  אזי  $\text{Ag}(\alpha, \beta) = |\{i \in [m] \mid \alpha_i = \beta_i\}|$

**משפט:** אם קיימת  $z : \{0, 1\}^n \rightarrow \{0, 1\}$  וקיים  $\rho \in [\frac{1}{2}, 1)$  עבורם  $\mathbb{P}_{x,y}(z(x) + z(y) = z(x+y)) \geq \rho$  אז קיימת  $u \in \{0, 1\}^n$

עבורה  $\text{Ag}(z, \text{HAD}(u)) \geq \rho \cdot 2^n$

**משפט:**  $\mathcal{NP} \subseteq \text{PCP}_{[0.9,1]}(\mathcal{O}(n^2), \mathcal{O}(1))$

**משפט ה-PCP:** קיים  $\gamma < 1$  עבורו  $\mathcal{NP} = \text{PCP}_{[\gamma,1]}(\mathcal{O}(\log(n)), 3)$

**טענה:** יהי  $\varepsilon > 0$  אזי  $\text{max E3SAT}_{[\frac{7}{8}+\varepsilon,1]} \text{GAP}$  הינה  $\mathcal{NP}$ -Promise-קשה.

**טענה:** יהי  $\Sigma$  אלפבית ותהינה  $s, c : \mathbb{N} \rightarrow [0, 1]$  אזי  $\text{PCP}_{[s,c]}(0, 0)_{\Sigma} = \mathcal{P}$

**טענה:** יהי  $\Sigma$  אלפבית אזי  $\text{PCP}_{[\frac{1}{3},\frac{2}{3}]}(\text{poly}(n), 0)_{\Sigma} = \mathcal{BPP}$

**טענה:** יהי  $\Sigma$  אלפבית ותהינה  $s, c : \mathbb{N} \rightarrow [0, 1]$  אזי  $\text{PCP}_{[s,c]}(\log(n), 0)_{\Sigma} = \mathcal{P}$

**טענה:** יהי  $\Sigma$  אלפבית ותהינה  $s, c : \mathbb{N} \rightarrow [0, 1]$  אזי  $\text{PCP}_{[s,c]}(0, \text{poly}(n))_{\Sigma} = \mathcal{NP}$

**טענה:** תהינה  $s, c : \mathbb{N} \rightarrow [0, 1]$  אזי  $\text{PCP}_{[s,c]}(0, \text{poly}(n)) = \mathcal{NP}$

**טענה:** תהינה  $s, c : \mathbb{N} \rightarrow [0, 1]$  אזי  $\text{PCP}_{[s,c]}(\log \log(n), \mathcal{O}(1)) = \mathcal{P}$

**טענה:** תהינה  $s, c : \mathbb{N} \rightarrow [0, 1]$  אזי  $\text{PCP}_{[s,c]}(\mathcal{O}(\log(n)), 1) = \mathcal{P}$

**טענה:** תהינה  $s, c : \mathbb{N} \rightarrow [0, 1]$  אזי  $\text{PCP}_{[s,c]}(\mathcal{O}(\log(n)), 1)_{\{1, \dots, n^c\}} = \mathcal{P}$

**טענה:** תהינה  $s, c : \mathbb{N} \rightarrow [0, 1]$  אזי  $\text{PCP}_{[s,c]}(\mathcal{O}(\log(n)), 1)_{\{1, \dots, 2^{n^c}\}} = \mathcal{NP}$

**טענה:** תהינה  $r, q : \mathbb{N} \rightarrow \mathbb{N}$  ותהינה  $s, c : \mathbb{N} \rightarrow [0, 1]$  אזי  $\text{PCP}_{[s,c]}(r(n), q(n)) \subseteq \text{NTime}(\text{poly}(n, 2^{r(n)} \cdot q(n)))$

**מסקנה:** תהינה  $s, c : \mathbb{N} \rightarrow [0, 1]$  אזי  $\text{PCP}_{[s,c]}(\mathcal{O}(\log(n)), \mathcal{O}(1)) = \mathcal{NP}$

**מסקנה:** תהיינה  $s, c : \mathbb{N} \rightarrow [0, 1]$  אזי  $\text{PCP}_{[s,c]}(\text{poly}(n), \text{poly}(n)) = \mathcal{NEXP}$ .

**טענה:** יהי  $\Sigma$  אלפבית ותהיינה  $s, t : \mathbb{N} \rightarrow [0, 1]$  אזי  $\text{PCP}_{[s,1]}(r(n), q(n))_{\Sigma} \subseteq \text{PCP}_{[s^t,1]}(r(n) \cdot t(n), q(n) \cdot t(n))_{\Sigma}$ .

**טענה:** יהי  $\Sigma$  אלפבית אזי  $\text{PSPACE} \subseteq \text{PCP}_{[\frac{1}{3}, \frac{2}{3}]}(\text{poly}(n), \text{poly}(n))_{\Sigma}$ .

**הייפר גרף:** יהי  $q \in \mathbb{N}$  תהא  $V$  קבוצה ותהא  $E \subseteq \mathcal{P}_{\leq q}(V)$  אזי  $(q, V, E)$ .

**הגדרה:** יהי  $\Sigma$  אלפבית ויהי  $q \in \mathbb{N}_+$  אזי  $q\text{-GraphConstraint}_{\Sigma} = \{(G, f) \mid (G \text{ הייפר גרף}) \wedge (\forall e \in E. f(e) : \Sigma^{|e|} \rightarrow \{0, 1\})\}$ .

**הגדרה:** יהי  $\Sigma$  אלפבית ויהי  $q \in \mathbb{N}_+$  אזי  $\max q\text{-CSP}_{\Sigma} : q\text{-GraphConstraint}_{\Sigma} \rightarrow \mathbb{N}$ .

$\max q\text{-CSP}_{\Sigma}(G, f) = \max_{\sigma: V \rightarrow \Sigma} \mathbb{P}_{e \in E}(f_e(\sigma|_e) = 1)$

**הגדרה  $q\text{-Constraint Satisfiability Problem}$ :** יהי  $\Sigma$  אלפבית יהי  $q \in \mathbb{N}_+$  ותהיינה  $s, c : \mathbb{N} \rightarrow [0, 1]$  אזי

$q\text{-CSP}_{s,c,\Sigma} = \text{GAP}_{[s,c]} \max q\text{-CSP}_{\Sigma}$

**טענה:** יהי  $\Sigma$  אלפבית תהיינה  $r, q : \mathbb{N} \rightarrow \mathbb{N}$  ותהא  $s, c : \mathbb{N} \rightarrow [0, 1]$  אזי  $L \in \text{PCP}_{[s,c]}(\mathcal{O}(\log(n)), q(n))_{\Sigma}$

$L \leq_p q\text{-CSP}_{[s,c],\Sigma}$

**משפט:** קיים  $\gamma < 1$  עבורו  $3\text{-CSP}_{[\gamma,1],\{0,1\}}$  הינה  $\mathcal{NP}$ -Promise-קשה.

**סימון:** יהי  $\gamma < 1$  באשר  $3\text{-CSP}_{[\gamma,1],\{0,1\}}$  הינה  $\mathcal{NP}$ -Promise-קשה אזי  $\gamma_{\text{hard}} = \gamma$ .

**מסקנה:**  $\max 3\text{SAT}_{[\gamma_{\text{hard}},1]}$  הינה  $\mathcal{NP}$ -Promise-קשה.

**מסקנה:**  $\max \text{Clique}_{[\frac{\gamma_{\text{hard}}}{3}, \frac{1}{3}]}$  הינה  $\mathcal{NP}$ -Promise-קשה.

**מסקנה:** בעיית ה- $\left(\frac{1}{\gamma_{\text{hard}}}\right)$ -קירוב של  $\max \text{Clique}$  הינה  $\mathcal{NP}$ -קשה.

**מסקנה:**  $\max \text{IS}_{[\frac{\gamma_{\text{hard}}}{3}, \frac{1}{3}]}$  הינה  $\mathcal{NP}$ -Promise-קשה.

**מסקנה:**  $\min \text{VC}_{[\frac{2}{3}, 1 - \frac{\gamma_{\text{hard}}}{3}]}$  הינה  $\mathcal{NP}$ -Promise-קשה.

**מסקנה:** בעיית ה- $\left(\frac{3 - \gamma_{\text{hard}}}{2}\right)$ -קירוב של  $\min \text{VC}$  הינה  $\mathcal{NP}$ -קשה.

**טענה:**  $\mathcal{NP} = \text{PCP}_{[\frac{1}{2},1]}(\mathcal{O}(\log(n)), \mathcal{O}(1))$ .

**טענה:**  $\mathcal{NP} \subseteq \text{PCP}_{[2^{-n},1]}(\mathcal{O}(n \log(n)), \mathcal{O}(n))$ .

**טענה:**  $\text{PCP}_{[\frac{1}{n},1]}(\mathcal{O}(\log(n)), \mathcal{O}(\log(n))) \leq_p \text{GAP}_{[\frac{1}{n},1]} \max \text{Clique}$ .

**טענה:**  $\mathcal{NP} = \text{PCP}_{[\frac{1}{n},1]}(\mathcal{O}(\log(n)), \mathcal{O}(\log(n)))$ .

**מסקנה:** קיים  $\alpha > 0$  עבורו בעיית ה- $n^{\alpha}$ -קירוב של  $\max \text{Clique}$  הינה  $\mathcal{NP}$ -קשה.

**מסקנה:** יהי  $\varepsilon > 0$  אזי  $\text{GAP}_{[n^{\varepsilon}, n^{1-\varepsilon}]} \max \text{Clique}$  הינה  $\mathcal{NP}$ -Promise-קשה.