

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 $\text{Size}(C) \geq \frac{2^n}{2^n}$.

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 $S(n)$ $\text{Size}(S(n)) = \{L \subseteq \{0, 1\}^* \mid S(n) \text{ חשיבה על ידי } L\}$.

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

הגדרה Non Uniform Alternating Class: תהייה $s, d : \mathbb{N} \rightarrow \mathbb{N}$ 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: תהייה $s, d : \mathbb{N} \rightarrow \mathbb{N}$ 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: תהייה $s, d : \mathbb{N} \rightarrow \mathbb{N}$ 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 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 ε : 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 ε : 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 $\varepsilon > 0$ תהא $f : \{0, 1\}^n \rightarrow \{0, 1\}$ ותהא $P \subseteq \mathbb{R}[x_1 \dots x_n]$ מ"ל המחשבת את f עם שגיאה ε אזי קיים $p \in P$ המחשב בממוצע את f עם שגיאה ε .

סימון: יהי (Ω, \mathbb{P}) מרחב הסתברות אזי $\Omega \rightarrow \Omega : (x \leftarrow \Omega) = \mathbb{P}(\omega) = \mathbb{P}((x \leftarrow \Omega) = \omega)$ 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 $j \in [c \log(\frac{1}{\varepsilon})]$ 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 $\mathbb{P}_{S \leftarrow \mathcal{P}([n])}(|S \cap I| = 1) \geq \frac{1}{2^k}$.

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 ε .

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 ε .

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 ε .

למה: יהי $\delta > 0$ ויהי $p \in \mathbb{R}[x_1 \dots x_n]$ מ"ל המחשב את 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 parity_n בממוצע עם שגיאה ε אזי $\deg(p) = \Omega(\sqrt{n})$.

מסקנה: יהי C מעגל המחשב את 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 $\text{IteratedBinAdd}_n : (\{0, 1\}^n)^n \rightarrow \{0, 1\}^{2^n}$ 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 $\text{BinMult}_n : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}^{2^n}$ 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 $|E(C, D)| \geq |E(A, B)|$ לכל חתך (C, D) .

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

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 $|E(A, B)| \geq \frac{|E(G)|}{2}$.

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

```
function SlowBigCut( $E, \{v_1 \dots v_n\}$ ):
     $S \in \mathcal{P}(\{v_1 \dots v_n\})$ 
    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 SlowBigCut בעלת סיבוכיות זמן ריצה $\Omega(2^n)$.

טענה: קיימת מ"ט אקראית M_{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

$X_1 \dots X_n : [\log(n) + 1] \rightarrow \{0, 1\}$ עבורם

• $X_1 \dots X_n$ ב"ת בזוגות.

• $\mathbb{P}(X_i = 1) = \frac{1}{2}$ לכל $i \in [n]$.

• M_{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 $\mathbb{E}_{r \leftarrow \{0,1\}^{\log(n)+1}} [|E(S_{\text{supp}}, \overline{S_{\text{supp}}})|] = \frac{|E|}{2}$.
מסקנה אלגוריתם מהיר למציאת חתך גדול: תהא E קבוצה יהי $n \in \mathbb{N}$ ותהא $\{v_1, \dots, v_n\}$ קבוצה אזי

```
function FastBigCut( $E, \{v_1 \dots v_n\}$ ):
   $S \in \mathcal{P}(\{v_1 \dots v_n\})$ 
  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 FastBigCut 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.
טענה: תהא $\varphi \in 3\text{CNF}$ בעלת m פסוקיות ו- n משתנים אזי קיימת השמה $\alpha \in \{0, 1\}^n$ המספקת $\frac{7}{8} \cdot m$ פסוקיות.
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 המחזורות 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 לכתיבה 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 $\{M \mid \text{מ"ט שרצה במקום } \mathcal{O}(S(n)) \mid L(M)\}$ $\text{DSpace}(S(n))$.
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 $\text{DSpace}(S(n)) \subseteq \text{DTime}(2^{O(S(n))})$.

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 Δ, Σ אלפבייטים 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 Δ, Σ אלפבייטים 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 $f(1^n) = \langle C_{M,n} \rangle$ באשר $C_{M,n}(z) = 1 \iff (M(z) \text{ מקבלת})$.

טענה: CVAL הינה \mathcal{P} -שלמה.

נוסחה מכומתת לחלוטין: תהא φ נוסחה באשר $\text{FV}(\varphi) = \{x_1 \dots x_n\}$ 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: $\text{CVAL} \in \text{PSPACE}$.

טענה: TQBF הינה PSPACE -שלמה.

מילה בעלת ייצוג: יהי $k \in \mathbb{N}$ אזי $x \in \Sigma^n$ עבורה קיימת מ"ט M המקיימת $|M| = k$ 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

$i \in [s] \text{ לכל } A(i) = (f(i), \text{adj}^-(f(i)), \text{adj}^+(f(i)))$

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: $\text{Succ-CVAL} \in \text{EXP}$.

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 \mathcal{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: יהי $k \in \mathbb{N}$ אזי $\text{u-AC}^k = \bigcup_{c \in \mathbb{N}} \text{u-AC}(n^c, \log^k(n))$

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

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 $x \in S^*$ ותהא G מטריצה המייצגת את עץ הקונפיגורציות אזי $M(x)$ מקבלת $\langle (I + G)^{S(|x|)} \rangle_{x, y} \geq 1$ באשר y קונפיגורציה במצב מקבל.

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

מכונת טיורינג עם עצצה: 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 $(M(x, \alpha_{|x|}) = 1) \iff (x \in L)$ 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: $\mathcal{P}/\text{poly} = \text{Size}(\text{poly})$

טענה: תהא $F : 3\text{CNF} \rightarrow \{0, 1\}^* \cup \{\perp\}$ באשר $(F(\varphi))$ השמה מספקת עבור φ $\iff (F(\varphi) \in \{0, 1\}^*)$ 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: LIN-PROG הינה \mathcal{P} -קשה.

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

מספר המעבדים במודל PRAM: יהי (p, k, Π) מודל PRAM אזי p

קונפיגורציה במודל PRAM: יהי (p, k, Π) מודל PRAM ותהא (T, R, PC) קונפיגורציה של מודל ה-RAM (k, Π) אזי (T, R, PC)

קונפיגורציה עוברת במודל PRAM: יהי (k, Π) מודל RAM ותהא (T, R, PC) קונפיגורציה אזי קונפיגורציה (T', R', 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 $\ell \in [p]$ מתקיים $R'_{i_\ell} = \pi_{i_\ell}(R_{i_\ell})$.
- 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 $\ell \in [p]$ מתקיים $T'(\ell) = \pi(T(\ell))$.

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

- סימון:** יהי (p, k, Π) 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, Π) מודל PRAM יהי A אלגוריתם ויהי $x \in \mathbb{N}$ אזי $A_{\text{stop}} = \min \{n \in \mathbb{N} \mid A^{(n+1)}(\text{Start}_x) = A^{(n)}(\text{Start}_x)\}$.
- ריצה של מודל PRAM:** יהי (p, k, Π) מודל PRAM יהי A אלגוריתם ויהי $n \in \mathbb{N}$ אזי $(A^{(i)}(\text{Start}_x))_{i=1}^{A_{\text{stop}}}$.
- זמן ריצה במודל PRAM:** יהי (p, k, Π) 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, Π) 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:** $\text{P} = \text{NC}$. *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

$$- \text{ אם } c_1 \cap Q = \{q_{\text{yes}}\} \text{ אזי } c_0^2 \setminus Q \in \mathcal{O}$$

$$- \text{ אם } c_1 \cap Q = \{q_{\text{no}}\} \text{ אזי } c_0^2 \setminus Q \notin \mathcal{O}$$

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 $\{M^{\mathcal{O}} \mid \text{מ"ט הרצה בזמן } T(n)\}$ $\text{DTime}^{\mathcal{O}}(T(n)) = \{L(M) \mid T(n) \text{ חשיבה בזמן } T(n)\}$.
- הגדרה:** תהא $\mathcal{O} \subseteq \{0, 1\}^*$ ותהא $T : \mathbb{N} \rightarrow \mathbb{N}$ חשיבה במקום אזי $\{M^{\mathcal{O}} \mid \text{מ"ט הרצה במקום } T(n)\}$ $\text{DSpace}^{\mathcal{O}}(T(n)) = \{L(M) \mid T(n) \text{ חשיבה במקום } T(n)\}$.
- 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 עבורה קיימת מ"ט $M^{\mathcal{O}}$ שרצה בזמן $\text{poly}(n)$ באשר לכל $x \in \Sigma$ מתקיים $(x \in L) \iff (\exists y \in \Sigma^{\text{poly}(|x|)} \cdot M(x, y) = 1)$ אזי $L \in \mathcal{NP}^{\mathcal{O}}$.
- הגדרה:** תהיינה \mathcal{A}, \mathcal{B} משפחות של שפות אזי $\mathcal{A}^{\mathcal{B}} = \bigcup_{L \in \mathcal{B}} \mathcal{A}^L$.

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

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

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

טענה משפט היררכיית הזמן עם אורקל: תהא $\mathcal{O} \subseteq \{0, 1\}^*$ ותהא $T : \mathbb{N} \rightarrow \mathbb{N}$ 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 $\mathcal{O} \subseteq \{0, 1\}^*$ ותהא $S : \mathbb{N} \rightarrow \mathbb{N}$ 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 $T : \mathbb{N} \rightarrow \mathbb{N}$ ותהא $L \in \text{DTime}(T(n))$ ותהא f חח"ע חשיבה בזמן באשר $f(n) \geq n$ לכל $n \in \mathbb{N}$ אזי

$$L_{\text{pad}}^f = \{x \mid 1^{f(|x|)-|x|-1} \mid x \in L\}$$

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

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

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

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

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

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

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

טענה: $E \neq EXP$

טענה: $E \neq PSPACE$

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

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

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

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

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

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 תהינה $s, c: \mathbb{N} \rightarrow [0, 1]$ 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 $M(x; r)$)

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

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

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

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

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

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

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

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

טענה: $\text{co}\mathcal{RP} = \mathcal{BPP}_{[\frac{1}{2}, 1]}$

טענה: תהינה $\mathcal{C}_1, \mathcal{C}_2$ 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: $\text{PM} = \{\langle G \rangle \mid (G \text{ גרף דו-צדדי}) \wedge (G \text{ מושלם ב-})\}$

טענה: $\text{PM} \in \mathcal{P}$

פרמננטה 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 $\{\langle G \rangle \mid \text{perm}(A) \neq 0\}$ 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 $(X)_{i,j} \sim \text{Uni}([10n])$ ב"ת 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, Π) מודל PRAM אזי (p, k, Π) .

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

אקראיות בקונפיגורציה: יהי (p, k, Π) מודל PPRAM ותהא (T, R, 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: $\{C' \mid C' \text{ מעגל אריתמטי מעל } \mathbb{F} \text{ המייצג את פולינום ה-} 0 \wedge (\mathbb{F}, C') \in \text{PIT}\}$.

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 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 $L \in \mathcal{BPP}$ אזי לכל $c \in \mathbb{N}_+$ מתקיים $L \in \mathcal{BPP}_{[2^{-nc}, 1-2^{-nc}]}$.

משפט צ'רנוף: יהי $p \in (0, 1)$ ויהיו $Y_1 \dots Y_n \sim \text{Ber}(p)$ 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 $\mathcal{BPP}_{[p, p + \frac{1}{n^c}]} = \mathcal{BPP}_{[2^{-n^d}, 1-2^{-n^d}]}$.

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: $\{\langle T, S \rangle \mid (T, S) \text{ עצים} \wedge (T \cong S)\}$.

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

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( $T$ )  $\neq$  depth( $S$ ))  $\vee$  ( $|V(T)| \neq |V(S)|$ ) then
        | return False
    return  $\mathbb{1}[p_T(A_0, \dots, A_{\text{depth}(T)}) = p_S(A_0, \dots, A_{\text{depth}(T)})]$ 

```

טענה: $\text{RTree-IS} \in \text{coRP}$

מסקנה: $\text{Tree-IS} \in \text{coRP}$

מסקנה: קיים אלגוריתם A ב- 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

טענה: תהא $\varphi \in 3\text{CNF}$ באשר φ 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 $d(\alpha, \beta) = |\{i \in [m] \mid \alpha_i \neq \beta_i\}|$.

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

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

מסקנה: תהא $\varphi \in 3\text{CNF}$ באשר $\text{FV}(\varphi) = \{x_1 \dots x_m\}$ וכן φ ספיקה אזי

$\mathbb{P}_{\alpha_1 \dots \alpha_m}(\text{Schöning'sAlgorithm}(\varphi, \alpha_i) = \text{True}) \geq \frac{1}{2} \quad (\exists i \in [(\frac{3}{2})^m])$.

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


```

function Schöning'sAlgorithm( $\varphi, \alpha$ ):
  for  $i \in [m]$  do
    if  $\varphi(\alpha) = \text{True}$  then return True
     $C \leftarrow \arg \min\{n \in [m] \mid C_i(\alpha) = \text{False}\}$ 
     $\ell \leftarrow \text{FV}(C)$ 
     $j \leftarrow \iota n \in [m]. \ell = x_n$ 
     $\alpha_j = 1 - \alpha_j$ 
  end
  return False

```

טענה: $BPP \subseteq PSPACE$

טענה: $BPP = coBPP$

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

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

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

טענה: $\mathcal{NP} = BPP_{[0, \frac{1}{2^n}]}$

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

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

פרוטוקול תקשורת: יהי $t \in \mathbb{N}_+$ תהיינה $S_1 \dots S_{t+1} : \{0, 1\}^* \rightarrow \{A, B\}$ ויהי $C_1 \dots C_t : \{A, B\} \times \{0, 1\}^* \rightarrow \{0, 1\}^*$ ותהא

$R : \{A, B\} \times \{0, 1\}^* \rightarrow \{0, 1\}$ אזי $((S_1, C_1) \dots (S_t, C_t), (S_{t+1}, R))$

סיבוב בפרוטוקול תקשורת: יהי $((S_1, C_1) \dots (S_t, C_t), (S_{t+1}, R))$ פרוטוקול תקשורת אזי (S_i, C_i) באשר $i \in [t]$

מספר הסיבובים בפרוטוקול תקשורת: יהי $((S_1, C_1) \dots (S_t, C_t), (S_{t+1}, R))$ פרוטוקול תקשורת אזי t

הרצת פרוטוקול תקשורת: יהי $((S_1, C_1) \dots (S_t, C_t), (S_{t+1}, R))$ פרוטוקול תקשורת ויהיו $x_A, x_B \in \{0, 1\}^*$ אזי $b_1 \dots b_{t+1} \in \{0, 1\}^*$ המקיימים

$b_1 = C_1(S_1(\varepsilon), x_{S_1(\varepsilon)})$ •

$b_i = C_i(S_i(b_1 \dots b_{i-1}), x_{S_i(b_1 \dots b_{i-1})}, b_1 \dots b_{i-1})$ •

$b_{t+1} = R(S_{t+1}(b_1 \dots b_t), x_{S_{t+1}(b_1 \dots b_t)}, b_1 \dots b_t)$ •

הערה: מעתה והלאה נסמן $(b_1 \dots b_{t+1})$ עבור הרצה של פרוטוקול וכן נסמן $b_i(x_A, x_B)$ עבור ההרצה על x_A, x_B

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

עלות תקשורת של פרוטוקול: יהי Π פרוטוקול 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 Π פרוטוקול המחשב את f $\mathcal{D}(f) = \min\{\mathcal{C}(\Pi) \mid f \text{ מחשב את } \Pi\}$

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 $EQ_n : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$ המוגדרת $EQ_n(x, y) = \mathbb{1}[x = y]$

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: תהיינה $S, T \subseteq \{0, 1\}^n$ אזי $S \times T$

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

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 $n = \mathcal{D}(EQ_n)$