גודל מעגל בוליאני: יהיו $n,m\in\mathbb{N}$ ויהי C מעגל בוליאני בעל n חוטים וכן m קלטים אזי $\text{Size}\left(C\right)=n+m$.
עומק מעגל בוליאני: יהי C מעגל בוליאני אזי $\text{depth}\left(C\right)$ הינו אורך המסלול המקסימלי מקלט לפלט.
הגדרה: יהי $n\in\mathbb{N}_{\ge3}$ אזי $\vee_n:\{0,1\}^n\to\{0,1\}$ המוגדרת $\vee_n\left(x\right)=\bigvee_{i=1}^n x_i$.
הגדרה: יהי $n\in\mathbb{N}_{\ge3}$ אזי $\wedge_n:\{0,1\}^n\to\{0,1\}$ המוגדרת $\wedge_n\left(x\right)=\bigwedge_{i=1}^n x_i$.
מעגל בוליאני בעל fan-in לא מוגבל: מעגל בוליאני מעל בסיס הפונקציות הבוליאניות $\{\wedge,\vee,\neg\}\cup\left(\bigcup_{n\in\mathbb{N}}\{\vee_n\}\right)\cup\left(\bigcup_{n\in\mathbb{N}}\{\wedge_n\}\right)$.
הערה: אלא אם נאמר אחרת מעגל בוליאני הוא בעל fan-in מוגבל.
טענה: תהא $f:\{0,1\}^n\to\{0,1\}$ אזי קיים מעגל בוליאני C בעל fan-in לא מוגבל המחשב את f בגודל $\mathcal{O}\left(n\cdot2^n\right)$ ובעומק 2.
טענה: תהא $f:\{0,1\}^n\to\{0,1\}$ אזי קיים מעגל בוליאני C המחשב את f בגודל $\mathcal{O}\left(n\cdot2^n\right)$ ובעומק $n+\log_2\left(n\right)$.
מסקנה: תהא L שפה אזי קיימת משפחת מעגלים $\mathcal{C}$ מגודל $\mathcal{O}\left(n\cdot2^n\right)$ ומעומק $n+\log\left(n\right)$ המחשבת את L.
מסקנה: יהי $n\in\mathbb{N}$ אזי קיימת $f:\{0,1\}^n\to\{0,1\}$ עבורה לכל מעגל בוליאני C המחשב אותה מתקיים $\text{Size}\left(C\right)\ge\frac{2^n}{2n}$.
הגודל של פונקציה בוליאנית: יהי $n\in\mathbb{N}$ ותהא $f:\{0,1\}^n\to\{0,1\}$ אזי $\text{Size}\left(f\right)=\min\left\{\text{Size}\left(C\right)\mid\left(\text{מעגל }C\right)\wedge\left(f\text{ מחשבת את }C\right)\right\}$.
טענה: יהי $n\in\mathbb{N}$ ותהא $f:\{0,1\}^n\to\{0,1\}$ אזי $\text{Size}\left(f\right)\le15\cdot\left(2^n-1\right)$.
טענה: יהי $n\in\mathbb{N}$ ותהא $f:\{0,1\}^n\to\{0,1\}$ אזי $\text{Size}\left(f\right)=\mathcal{O}\left(\frac{2^n}{n}\right)$.
מסקנה שאנון: יהי $n\in\mathbb{N}$ אזי $\max\left\{\text{Size}\left(f\right)\mid f:\{0,1\}^n\to\{0,1\}\right\}=\Theta\left(\frac{2^n}{n}\right)$.
משפט: קיים $C\in\mathbb{R}_+$ עבורו לכל $n\in\mathbb{N}$ ולכל $S:\mathbb{N}\to\mathbb{N}$ המקיימת $n\le S<C\cdot\frac{2^n}{n}$ קיימת $f:\{0,1\}^n\to\{0,1\}$ באשר f חשיבה על ידי מעגל מגודל $S\left(n\right)+10n$ וכן f לא חשיבה על ידי מעגל מגודל $S\left(n\right)$.
הגדרה: תהא $S:\mathbb{N}\to\mathbb{N}$ אזי $\text{Size}\left(S\left(n\right)\right)=\left\{L\subseteq\{0,1\}^*\mid S\left(n\right)\text{ חשיבה על ידי משפחת מעגלים מגודל לכל היותר } L\right\}$.
מסקנה: $\text{Size}\left(2^n\right)=\mathcal{P}\left(\{0,1\}^*\right)$.
מסקנה: תהא $S:\mathbb{N}\to\mathbb{N}$ עבורה $n\le S\left(n\right)\le\frac{2^n}{n}$ אזי $\text{Size}\left(S\left(n\right)\right)\subsetneq\text{Size}\left(S\left(n\right)+10n\right)$.
הגדרה: $\text{Size}\left(\text{poly}\right)=\bigcup_{c\in\mathbb{N}}\text{Size}\left(n^c\right)$.
הגדרה Non Uniform Alternating Class: תהיינה $s,d:\mathbb{N}\to\mathbb{N}$ אזי
$$\text{nu-AC}\left(s,d\right)=\left\{L\subseteq\{0,1\}^*\;\middle|\;\begin{smallmatrix}L(C)=L\\ \text{Size}(C_n)\le s(n)\\ \text{depth}(C_n)\le d(n)\end{smallmatrix}\text{ קיימת משפחת מעגלים } C \text{ בעלת fan-in לא מוגבל עבורה}\right\}.$$
הגדרה: יהי $k\in\mathbb{N}$ אזי $\text{nu-AC}^k=\bigcup_{c\in\mathbb{N}}\text{nu-AC}\left(n^c,\log^k\left(n\right)\right)$.
הגדרה Non Uniform Nick's Class: תהיינה $s,d:\mathbb{N}\to\mathbb{N}$ אזי
$$\text{nu-NC}\left(s,d\right)=\left\{L\subseteq\{0,1\}^*\;\middle|\;\begin{smallmatrix}L(C)=L\\ \text{Size}(C_n)\le s(n)\\ \text{depth}(C_n)\le d(n)\end{smallmatrix}\text{ קיימת משפחת מעגלים } C \text{ עבורה}\right\}.$$
הגדרה: יהי $k\in\mathbb{N}$ אזי $\text{nu-NC}^k=\bigcup_{c\in\mathbb{N}}\text{nu-NC}\left(n^c,\log^k\left(n\right)\right)$.
מסקנה: תהיינה $s,d:\mathbb{N}\to\mathbb{N}$ אזי $\text{nu-NC}\left(s,d\right)\subseteq\text{nu-AC}\left(s,d\right)$.
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 $\text{parity}:\{0,1\}^n\to\{0,1\}$ המוגדרת $\text{parity}\left(x\right)=\bigoplus_{i=1}^n x_i$.
טענה: קיים מעגל C המחשב את parity_n מגודל $\mathcal{O}\left(n\right)$ ועומק $\mathcal{O}\left(\log\left(n\right)\right)$.
מסקנה: $\text{parity}\in\text{nu-NC}^1$.
פולינום מולטי־לינארי (מ״ל): יהי $n\in\mathbb{N}_+$ אזי $p\in\mathbb{R}\left[x_1\ldots x_n\right]$ בעל דרגה 1.
פולינום מחשב פונקציה בוליאנית: תהא $f:\{0,1\}^n\to\{0,1\}$ אזי $p\in\mathbb{R}\left[x_1\ldots x_n\right]$ מ״ל עבורו $f\left(x\right)=p\left(x\right)$ לכל $x\in\{0,1\}^n$.
טענה: תהא $f:\{0,1\}^n\to\{0,1\}$ אזי קיים פולינום מ״ל יחיד המחשב את f.
סימון: תהא $f:\{0,1\}^n\to\{0,1\}$ ויהי $p\in\mathbb{R}\left[x_1\ldots x_n\right]$ מ״ל המחשב את f אזי $\deg\left(f\right)=\deg\left(p\right)$.
מסקנה: יהי $n\in\mathbb{N}$ אזי $\deg\left(\vee_n\right)=n$.
טענה: יהי $n\in\mathbb{N}$ אזי $\deg\left(\text{parity}_n\right)=n$.
פולינום מחשב פונקציה בוליאנית בממוצע עם שגיאה ε: יהי $\varepsilon>0$ ותהא $f:\{0,1\}^n\to\{0,1\}$ אזי $p\in\mathbb{R}\left[x_1\ldots x_n\right]$ מ״ל עבורו $\mathbb{P}_{x\leftarrow\{0,1\}^n}\left(p\left(x\right)=f\left(x\right)\right)\ge1-\varepsilon$.
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 $f:\{0,1\}^n\to\{0,1\}$ אזי קבוצת פולינומים מ״ל $P\subseteq\mathbb{R}\left[x_1\ldots x_n\right]$ עבורה לכל $x\in\{0,1\}^n$ מתקיים $\mathbb{P}_{p\leftarrow P}\left(p\left(x\right)=f\left(x\right)\right)\ge1-\varepsilon$.

טענה: יהי $\varepsilon > 0$ תהא $f : \{0,1\}^n \to \{0,1\}$ 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 $(\Omega, \mathbb{P})$ מרחב הסתברות אזי $(x \leftarrow \Omega) : \Omega \to \Omega$ הינו מ"מ באשר $\mathbb{P}((x \leftarrow \Omega) = \omega) = \mathbb{P}(\omega)$.

הערה: תהא A קבוצה סופית אזי $A \leftarrow x$ 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 $j \in \left[c \log\left(\frac{1}{\varepsilon}\right)\right]$ אזי $R_\vee(x) = 1 - \prod_{k,j}\left(1 - \sum_{i \in S_{j,k}} x_i\right)$.

למה: יהי $x \in \{0,1\}^n$ עבורו $\vee_n(x) = 0$ אזי $R_\vee(x) = 0$ לכל $S_{j,k} \leftarrow \mathcal{P}([n])$.

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

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

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

טענה: תהא $f : \{0,1\}^n \to \{0,1\}$ 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 $f : \{0,1\}^n \to \{0,1\}$ 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 $\text{Size}(C) \ge 2^{\Omega\left(n^{\frac{1}{4 \cdot d(n)}}\right)}$.

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 $\text{BinAdd}_n = \left\{\langle x,y,z\rangle \mid (x,y \in \{0,1\}^n) \wedge \left(z \in \{0,1\}^{n+1}\right) \wedge (x+y=z)\right\}$.

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

הגדרה: יהי $n \in \mathbb{N}_+$ אזי $\text{IteratedBinAdd}_n = \left\{\langle x_1 \dots x_n, z\rangle \mid (x_1 \dots x_n \in \{0,1\}^n) \wedge \left(z \in \{0,1\}^{2n}\right) \wedge \left(\sum_{i=1}^n x_i = z\right)\right\}$.

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

הגדרה: יהי $n \in \mathbb{N}_+$ אזי $\text{BinMult}_n = \left\{\langle x,y,z\rangle \mid (x,y \in \{0,1\}^n) \wedge \left(z \in \{0,1\}^{2n}\right) \wedge (x \cdot y = z)\right\}$.

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 $|E(A,B)| \ge |E(C,D)|$ 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 $E(A,B) \ge \frac{|E(G)|}{2}$.

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 ... v_n}):
    S ∈ P({v_1 ... v_n})
    for r ∈ {0,1}^n do
        S ← {v_i | r_i = 1}
        if |E(S, S̄)| ≥ |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 $X_1 \dots X_n : [\log(n)+1] \to \{0,1\}$ 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 $X_{c,d} : \mathbb{F} \to \mathbb{F}$ 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 $\mathbb{E}_{r \leftarrow \{0,1\}^{\log(n)+1}}\left[\left|E\left(S_{\text{supp}}, \overline{S_{\text{supp}}}\right)\right|\right] = \frac{|E|}{2}$.

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 $n \in \mathbb{N}$ תהא $\{v_1, \dots, v_n\}$ 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**
  - $c_0 \leftarrow \mathbb{E}_{r \leftarrow \{0,1\}^n}\left[\left|E\left(S_r, \overline{S_r}\right)\right| \mid (r_1 = a_1), \dots, (r_{i-1} = a_{i-1}), (r_i = 0)\right]$
  - $c_1 \leftarrow \mathbb{E}_{r \leftarrow \{0,1\}^n}\left[\left|E\left(S_r, \overline{S_r}\right)\right| \mid (r_1 = a_1), \dots, (r_{i-1} = a_{i-1}), (r_i = 1)\right]$
  - $a_i \leftarrow \arg\max_{\ell \in \{0,1\}}(c_\ell)$
- **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
$\mathbb{E}_{r \leftarrow \{0,1\}^n}\left[\left|E\left(S_r, \overline{S_r}\right)\right| \mid (r_1 = a_1), \dots, (r_{i-1} = a_{i-1})\right] = |\{(v_i, v_j) \in E \mid (i,j \leq k) \wedge (a_i \neq a_j)\}| + \frac{1}{2}|\{(v_i, v_j) \in E \mid (i > k) \vee (j > k)\}|$.

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 $\mathbb{E}_{r \leftarrow \{0,1\}^n}\left[\left|E\left(S_r, \overline{S_r}\right)\right| \mid (r_1 = a_1), \dots, (r_{i-1} = a_{i-1})\right] \geq \frac{|E|}{2}$.

מסקנה: תהא E קבוצה יהי $n \in \mathbb{N}$ ותהא $\{v_1, \dots, v_n\}$ קבוצה אזי $E\left(\text{CEBigCut}, \overline{\text{CEBigCut}}\right) \geq \frac{|E|}{2}$.

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 $(c_1\$c_2\$\dots\$c_k)^i = c_i$.

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

מכונת טיורינג בעלת סיבוכיות מקום: תהא $S : \mathbb{N} \to \mathbb{N}$ 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 $c_i^1 = x \backslash Q$.
- סרט חסום במקום: לכל $i \in [n]$ מתקיים $\left|c_{i-1}^2\right| \leq S(n) + 1$.
- סרט לכתיבה חד־פעמית: לכל $i \in [n]$ ולכל $j \in \left[\left|c_{i-1}^3\right|\right]$ מתקיים $\left(c_{i-1}^3 \backslash Q\right)_j = \left(c_i^3 \backslash Q\right)_j$.

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

הערה: נקרא למכונת טיורינג בעלת סיבוכיות מקום מכונת טיורינג.

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

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: $\mathrm{DSpace}\left(1\right)=\mathrm{DSpace}\left(\log\left(\log\left(n\right)\right)\right)=\left\{ L\mid\text{רגולרית }L\right\}$.

טענה: תהא T חשיבה בזמן אזי $\mathrm{DTime}\left(T\left(n\right)\right)\subseteq\mathrm{DSpace}\left(T\left(n\right)\right)$.

טענה: $\mathcal{NP}\subseteq\mathrm{PSPACE}$.

טענה: תהא $S:\mathbb{N}\to\mathbb{N}$ באשר $S\ge\log$ אזי $\mathrm{DSpace}\left(S\left(n\right)\right)\subseteq\mathrm{DTime}\left(2^{\mathcal{O}\left(S\left(n\right)\right)}\right)$.

מסקנה: $\mathrm{LOG}\subseteq\mathcal{P}$.

מסקנה: $\mathrm{PSPACE}\subseteq\mathrm{EXP}$.

פונקציה חשיבה במקום: פונקציה $S:\mathbb{N}\to\mathbb{N}$ עבורה קיימת מ"ט M המקיימת לכל $n\in\mathbb{N}$ כי M על הקלט 1^{n} מחשבת את $\left(S\left(n\right)\right)_{2}$ במקום $\mathcal{O}\left(S\left(n\right)\right)$.

משפט היררכיית המקום: תהא $S:\mathbb{N}\to\mathbb{N}$ חשיבה במקום ותהא $t\left(n\right)=o\left(S\left(n\right)\right)$ אזי $\mathrm{DSpace}\left(t\left(n\right)\right)\subsetneq\mathrm{DSpace}\left(T\left(n\right)\right)$.

מסקנה: $\mathrm{LOG}\subsetneq\mathrm{PSPACE}$.

מסקנה: לפחות אחד מהבאים נכון

- $\mathrm{LOG}\subsetneq\mathcal{P}$.
- $\mathcal{P}\subsetneq\mathrm{PSPACE}$.

השערה: $\mathrm{LOG}\subsetneq\mathcal{P}$. השערה פתוחה

השערה: $\mathcal{P}\subsetneq\mathrm{PSPACE}$. השערה פתוחה

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

רדוקציית מיפוי במקום לוגריתמי: יהיו Σ,Δ אלפבייתים 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 Σ,Δ אלפבייתים באשר $\Sigma\subseteq\Delta$ תהא $A\subseteq\Sigma^{*}$ שפה תהא $B\subseteq\Delta^{*}$ שפה ותהא $f:\Sigma^{*}\to\Delta^{*}$ רדוקציית מיפוי במקום לוגריתמי אזי $A\le_{\mathrm{Log}}B$.

טענה: תהיינה A,B שפות עבורן $A\le_{\mathrm{Log}}B$ אזי $A\le_{p}B$.

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

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

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

טענה: תהיינה A,B שפות באשר $B\in\mathrm{LOG}$ וכן $A\le_{L}B$ אזי $A\in\mathrm{LOG}$.

מסקנה: תהיינה A,B,C שפות באשר $B\le_{\mathrm{Log}}A$ וכן $B\le_{\mathrm{Log}}C$ אזי $A\le_{\mathrm{Log}}C$.

טענה: תהא $A\in\mathrm{LOG}$ באשר A הינה $\mathcal{P}$־שלמה אזי $\mathcal{P}=\mathrm{LOG}$.

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

למה קוק־לוין: תהא M מ"ט רצה בזמן פולינומי אזי קיימת פונקציה חשיבה f במקום לוגריתמי עבורה $f\left(1^{n}\right)=\left\langle C_{M,n}\right\rangle$ באשר $C_{M,n}$ מעגל עבורו לכל $z\in\left\{ 0,1\right\} ^{n}$ מתקיים $\left(M\left(z\right)\text{ מקבלת}\right)\Longleftrightarrow\left(C_{M,n}\left(z\right)=1\right)$.

טענה: CVAL הינה $\mathcal{P}$־שלמה.

נוסחה מכומתת לחלוטין: תהא φ נוסחה באשר $\mathrm{FV}\left(\varphi\right)=\left\{ x_{1}\ldots x_{n}\right\}$ ויהיו $Q_{1}\ldots Q_{n}\in\left\{ \forall,\exists\right\}$ כמתים אזי $Q_{1}x_{1}\ldots Q_{n}x_{n}\left(\varphi\right)$.

הגדרה True Quantified Boolean Formula Problem: $\mathrm{TQBF}=\left\{ \left\langle \varphi\right\rangle \mid\text{נוסחה מכומתת לחלוטין וספיקה }\varphi\right\}$.

טענה: $\mathrm{CVAL}\in\mathrm{PSPACE}$.

טענה: TQBF הינה PSPACE־שלמה.

מילה בעלת ייצוג: יהי $k\in\mathbb{N}$ אזי $x\in\Sigma^{n}$ עבורה קיימת מ"ט M המקיימת $\left|\left\langle M\right\rangle \right|=k$ וכן $M\left(i\right)=x_{i}$ לכל $i\in\left[n\right]$.

מעגל מיוצג על ידי מעגל: יהי C מעגל בגודל s אזי מעגל A המקבל $\log\left(s\right)$ ביטים עבורו קיימת $f:V\left(C\right)\to\left[s\right]$ הפיכה המקיימת $A\left(i\right)=\left\langle f\left(i\right),\mathrm{adj}^{-}\left(f\left(i\right)\right),\mathrm{adj}^{+}\left(f\left(i\right)\right)\right\rangle$ לכל $i\in\left[s\right]$.

סימון: יהי C מעגל ויהי A מעגל המייצג את C אזי $C=\left[A\right]$.

הגדרה Succinct Circuit Value Problem: $\mathrm{Succ\text{-}CVAL}=\left\{ \left\langle A,x\right\rangle \mid\left(\text{מעגל המייצג מעגל }A\right)\wedge\left(\left\langle \left[A\right],x\right\rangle \in\mathrm{CVAL}\right)\right\}$.

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

טענה: Succ-CVAL הינה EXP־שלמה.

מטריצה מיוצגת על ידי מעגל: תהא $A\in M_n\left(\mathbb{Z}_2\right)$ אזי מעגל C המקיים $C\left(i,j\right)=\left(A\right)_{i,j}$ לכל $i,j\in\left[n\right]$.

סימון: תהא $A\in M_n\left(\mathbb{Z}_2\right)$ ויהי C מעגל המייצג את A אזי $A=\left[C\right]$.

הגדרה: $\text{Succ-BoolMatPower}=\left\{\left\langle \left\langle C\right\rangle ,n,t,i,j\right\rangle \mid \left(C\text{ מעגל המייצג מטריצה מסדר }n\right)\wedge\left(\left(\left[C\right]^{t}\right)_{i,j}=1\right)\right\}$.

טענה: Succ-BoolMatPower הינה PSPACE־שלמה.

הגדרה Circut Satisfiability Problem: $\text{CSAT}=\left\{\left\langle C\right\rangle \mid C\text{ מעגל ספיק}\right\}$.

טענה: CSAT הינה $\mathcal{NP}$־שלמה.

הגדרה: $\text{Succ-CSAT}=\left\{\left\langle A\right\rangle \mid \left(A\text{ מעגל המייצג מעגל}\right)\wedge\left(\left\langle \left[A\right]\right\rangle \in\text{CSAT}\right)\right\}$.

טענה: Succ-CSAT הינה $\mathcal{NEXP}$־שלמה.

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

הגדרה Uniform Alternating Class: תהיינה $s,d:\mathbb{N}\to\mathbb{N}$ אזי
$\text{u-AC}\left(s,d\right)=\left\{L\subseteq\left\{0,1\right\}^{*}\;\middle|\;\text{קיימת משפחת מעגלים יוניפורמית }C\text{ בעלת fan-in לא מוגבל עבורה }\begin{smallmatrix}L(C)=L\\ \text{Size}(C_n)\le s(n)\\ \text{depth}(C_n)\le d(n)\end{smallmatrix}\right\}$.

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

הגדרה Uniform Nick's Class: תהיינה $s,d:\mathbb{N}\to\mathbb{N}$ אזי
$\text{u-NC}\left(s,d\right)=\left\{L\subseteq\left\{0,1\right\}^{*}\;\middle|\;\text{קיימת משפחת מעגלים יוניפורמית }C\text{ עבורה }\begin{smallmatrix}L(C)=L\\ \text{Size}(C_n)\le s(n)\\ \text{depth}(C_n)\le d(n)\end{smallmatrix}\right\}$.

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

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 $\text{NC}^{k}\subseteq\text{DSpace}\left(\mathcal{O}\left(\log^{k}\left(n\right)\right)\right)$.

טענה: תהא $S:\mathbb{N}\to\mathbb{N}$ יהי M מ"ט רץ בזמן S יהי $x\in\Sigma^{*}$ ותהא G מטריצה המייצגת את עץ הקונפיגורציות אזי $\left(M\left(x\right)\right.$ מקבלת$\left.\right)\Longleftrightarrow\left(\left(\left(I+G\right)^{S\left(\left|x\right|\right)}\right)_{x,y}\geq1\right)$ באשר y קונפיגורציה במצב מקבל.

הערה: קיימת מ"ט M הרצה בזמן פולינומי ובזיכרון $o\left(n\right)$ עבורה לכל מטריצה A המייצגת גרף מכוון בעל n קודקודים ולכל קודקודים s,t מתקיים $\left(M\left(\left\langle A,s,t\right\rangle \right)\right.$ מקבלת$\left.\right)\Longleftrightarrow\left(\right.$קיים מסלול מ־$s$ ל־$t\left.\right)$. השערה פתוחה

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

הגדרה Polynomial Time with Advice: תהא $a:\mathbb{N}\to\mathbb{N}$ אזי ${}^{\mathcal{P}}/_{a\left(n\right)}=\bigcup_{k\in\mathbb{N}}{}^{\text{DTime}\left(n^{k}\right)}/_{a\left(n\right)}$.

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: ${}^{\mathcal{P}}/_{\text{poly}}=\text{Size}\left(\text{poly}\right)$.

טענה: תהא $F:3\text{CNF}\to\left\{0,1\right\}^{*}\cup\left\{\bot\right\}$ באשר $\left(F\left(\varphi\right)\text{ השמה מספקת עבור }\varphi\right)\iff\left(F\left(\varphi\right)\in\left\{0,1\right\}^{*}\right)$ אזי $F\in\mathcal{P}^{\text{SAT}}$.

טענה: אם קיים $k\in\mathbb{N}$ עבורו $\text{SAT}\in{}^{\mathcal{P}}/_{\left\lfloor k\cdot\log\left(n\right)\right\rfloor}$ אזי $\text{SAT}\in\mathcal{P}$.

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

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

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

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

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

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

- $.\mathrm{PC}' = \mathrm{PC}+1$
- 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 $\pi_1 \dots \pi_p \in \Pi \cup \{\mathrm{Id}\}$ 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 $\pi_1 \dots \pi_p \in \Pi \cup \{\mathrm{Id}\}$ 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 $T : \mathbb{N} \to \mathbb{N}$ כך $T(n) = \left\{\begin{smallmatrix} x & n=0 \\ 0 & \text{else}\end{smallmatrix}\right.$ אזי $.\mathrm{Start}_x = (T, \{0\}, 0)$

סימון: יהי (p,k,Π) מודל PRAM יהי A אלגוריתם ויהי $x \in \mathbb{N}$ אזי $.A_{\text{stop}} = \min\left\{n \in \mathbb{N} \mid A^{(n+1)}(\mathrm{Start}_x) = A^{(n)}(\mathrm{Start}_x)\right\}$

ריצה של מודל PRAM: יהי (p,k,Π) מודל PRAM יהי A אלגוריתם ויהי $n \in \mathbb{N}$ אזי $.\left(A^{(i)}(\mathrm{Start}_x)\right)_{i=1}^{A_{\text{stop}}}$

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

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

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

טענה: תהא L שפה באשר $L \cap \Sigma^n$ ניתנת לחישוב במודל PRAM בעל $\mathrm{poly}(n)$ מעבדים בזמן $\mathcal{O}\left(\log^k(n)\right)$ לכל $n \in \mathbb{N}$ אזי $.L \in \mathsf{NC}^k$

השערה: קיים מודל PRAM וקיים אלגוריתם A הפותר את CVAL בזמן $\mathrm{polylog}(n)$ ובעבודה $.\mathrm{poly}(n)$ השערה פתוחה

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

טענה: $.\mathrm{APSP} \in \mathsf{NC}$

מכונת טיורינג בעלת אורקל: תהא $\mathcal{O} \subseteq \{0,1\}^*$ תהא $Q \neq \varnothing$ קבוצה סופית ויהיו $q_{\text{query}}, q_{\text{yes}}, q_{\text{no}} \in Q$ אזי מ"ט דו־סרטית $M^{\mathcal{O}}$ באשר $\left(M^{\mathcal{O}}\right)_1 = Q$ 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 $c_0^2 \backslash Q \in \mathcal{O}$ אזי $.c_1 \cap Q = \{q_{\text{yes}}\}$
  - אם $c_0^2 \backslash Q \notin \mathcal{O}$ אזי $.c_1 \cap Q = \{q_{\text{no}}\}$

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 $T : \mathbb{N} \to \mathbb{N}$ חשיבה בזמן אזי $.\mathrm{DTime}^{\mathcal{O}}(T(n)) = \left\{L(M) \mid T(n) \text{ מ"ט הרצה בזמן } M^{\mathcal{O}}\right\}$

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

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

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

הגדרה: תהא $\mathcal{O} \subseteq \{0,1\}^*$ ותהא L שפה עבורה קיימת מ"ט $M^{\mathcal{O}}$ שרצה בזמן $\mathrm{poly}(n)$ באשר לכל $x \in \Sigma$ מתקיים $(x \in L) \Longleftrightarrow \left(\exists y \in \Sigma^{\mathrm{poly}(|x|)}.M(x,y) = 1\right)$ אזי $.L \in \mathcal{NP}^{\mathcal{O}}$

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

טענה: $.\mathcal{NP}^{\mathrm{PSPACE}} = \mathrm{PSPACE}$

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

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 $T : \mathbb{N} \to \mathbb{N}$ חשיבה בזמן ותהא $t(n) = o\left(\frac{T(n)}{\log(T(n))}\right)$ אזי $.\mathrm{DTime}^{\mathcal{O}}(t(n)) \subsetneq \mathrm{DTime}^{\mathcal{O}}(T(n))$

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

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

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

מסקנה: $.\mathcal{P}^{\mathrm{EXP}} \neq \mathrm{EXP}^{\mathrm{EXP}}$

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

הגדרה: $.2\mathrm{EXP} = \bigcup_{c=0}^{\infty} \mathrm{DTime}\left(2^{2^{n^c}}\right)$

טענה: $.\mathrm{EXP}^{\mathrm{EXP}} = 2\mathrm{EXP}$

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

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

טענה: $\mathrm{E}\neq\mathrm{EXP}$.

טענה: $\mathrm{E}\neq\mathrm{PSPACE}$.

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

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

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

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

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

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

- לכל $x\in L$ מתקיים $M\left(x\right)\in\{1,\mathrm{quit}\}$.
- לכל $x\notin L$ מתקיים $M\left(x\right)\in\{0,\mathrm{quit}\}$.
- לכל $x\in\{0,1\}^{*}$ קיים מסלול חישוב עבורו $M\left(x\right)\neq\mathrm{quit}$.

אזי $L\in\mathcal{ZNP}$.

טענה: $\mathcal{ZNP}=\mathcal{NP}\cap\mathrm{co}\mathcal{NP}$.

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

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

הגדרה Bounded-error Probabilistic: תהא $T:\mathbb{N}\to\mathbb{N}$ חשיבה בזמן תהיינה $s,c:\mathbb{N}\to[0,1]$ ותהא שפה $\mathcal{L}$ עבורה 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 $\mathbb{P}_{r\leftarrow\{0,1\}^{T(n)}}\left(M\left(x;r\right)\text{ מקבלת}\right)\geq c\left(n\right)$.
- לכל $x\notin\mathcal{L}\cap\Sigma^{n}$ מתקיים $\mathbb{P}_{r\leftarrow\{0,1\}^{T(n)}}\left(M\left(x;r\right)\text{ מקבלת}\right)\leq s\left(n\right)$.

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

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

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

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

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

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

משלים של מחלקת שפות: תהא $\mathcal{C}$ מחלקת שפות אזי $\mathrm{co}\mathcal{C}=\left\{\overline{L}\mid L\in\mathcal{C}\right\}$.

טענה: $\mathrm{co}\mathcal{RP}=\mathcal{BPP}_{\left[\frac{1}{2},1\right]}$.

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

בעיית הזיווג המושלם: $\mathrm{PM}=\left\{\langle G\rangle\mid\left(G\text{ גרף דו־צדדי}\right)\wedge\left(G\text{-קיים זיווג מושלם ב}\right)\right\}$.

טענה: $\mathrm{PM}\in\mathcal{P}$.

פרמננטה של מטריצה: תהא $A\in M_{n}\left(\mathbb{F}\right)$ אזי $\mathrm{perm}\left(A\right)=\sum_{\sigma\in S_{n}}\prod_{i=1}^{n}\left(A\right)_{i,\sigma(i)}$.

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

טענה: $\det\in\mathsf{NC}^{2}$.

אלגוריתם אקראי לקיום זיווג מושלם: יהי G גרף דו־צדדי ויהי $X\in M_{n}\left(\mathbb{N}\right)$ באשר $\left(X\right)_{i,j}\sim\mathrm{Uni}\left(\left[10n\right]\right)$ ב"ת לכל $\left(i,j\right)\in\left[n\right]^{2}$ אזי

```
function IsPerfectMatching(G, X):
    A ∈ M_n(ℕ)
    A ← 0
    for (i, j) ∈ E(G) do
        (A)_{i,j} ← (X)_{i,j}
    end
    return 𝟙[det(A) ≠ 0]
```

טענה: יהי G גרף דו־צדדי אזי

- אם $\langle G\rangle\notin\mathrm{PM}$ אז $\mathbb{P}_{X}\left(\mathrm{IsPerfectMatching}\left(G,X\right)=0\right)=1$.

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

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 $\mathcal{O}\left(\log^2(n)\right)$ ובעבודה $\text{poly}(n)$.

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

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

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

טענה: $\text{PIT}\in\text{co}\mathcal{RP}$.

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

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

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

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

טענה: יהי $p\in[0,1)$ ויהיו $c,d\in\mathbb{N}$ אזי $\mathcal{BPP}_{\left[p,p+\frac{1}{n^c}\right]}=\mathcal{BPP}_{\left[2^{-n^d},1-2^{-n^d}\right]}$.

איזומורפיזם בין גרפים: יהיו G,K גרפים אזי זיווג $\pi:V(G)\to V(K)$ המקיים $(u,v)\in E(G)\Longleftrightarrow(\pi(u),\pi(v))\in E(K)$ לכל $u,v\in V(G)$.

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

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

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

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

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

- אם $T=(\{r\},\varnothing)$ אזי $p_T(x)=x$.
- אחרת $p_T\left(x_0,\ldots,x_{\text{depth}(T)}\right)=\prod_{(r,v)\in E}\left(x_{\text{depth}(T)}-p_{T_v}\right)$.

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

אלגוריתם לבעיית איזומורפיזם העצים בעלי שורש: יהיו T,S עצים בעלי שורש ותהא $A\in\mathbb{N}^{\text{depth}(T)}$ באשר $A_i\sim\text{Uni}\left([2\cdot|V(T)|]\right)$ 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: $\text{RTree-IS}\in\text{co}\mathcal{RP}$.

מסקנה: $\text{Tree-IS}\in\text{co}\mathcal{RP}$.

מסקנה: קיים אלגוריתם A ב־$\text{co}\mathcal{RP}$ המחשב איזומורפיזם בין עצים.

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

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

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

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

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

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

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

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

```
function Schöning'sAlgorithm(φ, α):
    for i ∈ [m] do
        if φ(α) = True then return True
        C ← arg min{n ∈ [m] | C_i(α) = False}
        ℓ ← FV(C)
        j ← ιn ∈ [m].ℓ = x_n
        α_j = 1 − α_j
    end
    return False
```

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

טענה: $\mathcal{BPP} = \text{co}\mathcal{BPP}$.

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

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

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