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 $n\in\mathbb{N}_{\geq3}$ אזי $\vee_{n}:\left\{ 0,1\right\} ^{n}\to\left\{ 0,1\right\}$ המוגדרת $\vee_{n}\left(x\right)=\bigvee_{i=1}^{n}x_{i}$.

הגדרה: יהי $n\in\mathbb{N}_{\geq3}$ אזי $\wedge_{n}:\left\{ 0,1\right\} ^{n}\to\left\{ 0,1\right\}$ 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 $\left\{ \wedge,\vee,\neg\right\} \cup\left(\bigcup_{n\in\mathbb{N}}\left\{ \vee_{n}\right\} \right)\cup\left(\bigcup_{n\in\mathbb{N}}\left\{ \wedge_{n}\right\} \right)$.

הערה: אלא אם נאמר אחרת מעגל בוליאני הוא בעל fan-in מוגבל.

טענה: תהא $f:\left\{ 0,1\right\} ^{n}\to\left\{ 0,1\right\}$ 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 $f:\left\{ 0,1\right\} ^{n}\to\left\{ 0,1\right\}$ 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 $f:\left\{ 0,1\right\} ^{n}\to\left\{ 0,1\right\}$ עבורה לכל מעגל בוליאני C המחשב אותה מתקיים $\text{Size}\left(C\right)\geq\frac{2^{n}}{2n}$.

הגודל של פונקציה בוליאנית: יהי $n\in\mathbb{N}$ ותהא $f:\left\{ 0,1\right\} ^{n}\to\left\{ 0,1\right\}$ 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 $f:\left\{ 0,1\right\} ^{n}\to\left\{ 0,1\right\}$ אזי $\text{Size}\left(f\right)\leq15\cdot\left(2^{n}-1\right)$.

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

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

משפט: קיים $C\in\mathbb{R}_{+}$ עבורו לכל $n\in\mathbb{N}$ ולכל $S:\mathbb{N}\to\mathbb{N}$ המקיימת $n\leq S<C\cdot\frac{2^{n}}{n}$ קיימת $f:\left\{ 0,1\right\} ^{n}\to\left\{ 0,1\right\}$ 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 $\text{Size}\left(S\left(n\right)\right)=\left\{ L\subseteq\left\{ 0,1\right\} ^{*}\mid S\left(n\right)\text{ חשיבה על ידי משפחת מעגלים מגודל לכל היותר }L\right\}$.

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

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

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

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

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

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

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

מסקנה אלגוריתם איטי למציאת חתך גדול: תהא E קבוצה יהי $n\in\mathbb{N}$ ותהא $\left\{ v_{1},\ldots,v_{n}\right\}$ 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 $\left\{ v_{1},\ldots,v_{n}\right\}$ קבוצה אזי SlowBigCut בעלת סיבוכיות זמן ריצה $\Omega\left(2^{n}\right)$.

טענה: קיימת מ"ט אקראית M_{supp} עבורה לכל $n\in\mathbb{N}$ ולכל $r\leftarrow\left\{ 0,1\right\} ^{\log\left(n\right)+1}$ מתקיים כי $M_{\text{supp}}\left(1^{n};r\right)$ מחזירה מ"מ $X_{1}\ldots X_{n}:\left[\log\left(n\right)+1\right]\to\left\{ 0,1\right\}$ עבורם

- $X_{1}\ldots X_{n}$ ב"ת בזוגות.
- $\mathbb{P}\left(X_{i}=1\right)=\frac{1}{2}$ לכל $i\in\left[n\right]$.
- M_{supp} רצה בזמן $\text{poly}\left(n\right)$.

סימון: יהי $n\in\mathbb{N}$ יהי $r\in\left\{ 0,1\right\} ^{\log\left(n\right)+1}$ ותהא $\left\{ v_{1}\ldots v_{n}\right\}$ קבוצה אזי $S_{\text{supp}}=\left\{ v_{i}\mid M_{\text{supp}}\left(1^{n};r\right)_{i}=1\right\}$.

טענה: יהי G גרף באשר $V=\left\{ v_{1}\ldots v_{n}\right\}$ אזי $\mathbb{E}_{r\leftarrow\left\{ 0,1\right\} ^{\log\left(n\right)+1}}\left[\left|E\left(S_{\text{supp}},\overline{S_{\text{supp}}}\right)\right|\right]=\frac{\left|E\right|}{2}$.

מסקנה אלגוריתם מהיר למציאת חתך גדול: תהא E קבוצה יהי $n\in\mathbb{N}$ ותהא $\left\{ v_{1},\ldots,v_{n}\right\}$ קבוצה אזי

```
function FastBigCut(E, {v_1 ... v_n}):
    S ∈ P({v_1 ... v_n})
    for r ∈ {0,1}^{log(n)+1} do
        X ← M_supp(1^n; r)
        S ← {v_i | X_i = 1}
        if |E(S, S̄)| ≥ |E|/2 then return S
    end
```

טענה: תהא E קבוצה יהי $n \in \mathbb{N}$ ותהא $\{v_1, \ldots, v_n\}$ קבוצה אזי FastBigCut בעלת סיבוכיות זמן ריצה $\text{poly}(n)$.

סימון: תהא E קבוצה יהי $n \in \mathbb{N}$ תהא $\{v_1, \ldots, v_n\}$ 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 $\{v_1, \ldots, v_n\}$ קבוצה אזי

```
function CEBigCut(E, {v_1 ... v_n}):
    a ∈ ⋃_{i=0}^{n} {0,1}^i
    a ← ϵ
    for i ∈ [1 ... , n] do
        c_0 ← E_{r←{0,1}^n} [ |E(S_r, S̄_r)| | (r_1 = a_1), ..., (r_{i-1} = a_{i-1}), (r_i = 0) ]
        c_1 ← E_{r←{0,1}^n} [ |E(S_r, S̄_r)| | (r_1 = a_1), ..., (r_{i-1} = a_{i-1}), (r_i = 1) ]
        a_i ← arg max_{ℓ∈{0,1}} (c_ℓ)
    end
    return S_a
```

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

מסקנה: תהא E קבוצה יהי $n \in \mathbb{N}$ ותהא $\{v_1, \ldots, v_n\}$ קבוצה אזי CEBigCut בעלת סיבוכיות זמן ריצה $\text{poly}(n)$.

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

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

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

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

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

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

מסקנה: תהיינה $s,d : \mathbb{N} \to \mathbb{N}$ 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 $\text{parity} : \{0,1\}^n \to \{0,1\}$ 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 $p \in \mathbb{R}[x_1 \ldots x_n]$ בעל דרגה 1.

פולינום מחשב פונקציה בוליאנית: תהא $f : \{0,1\}^n \to \{0,1\}$ אזי $p \in \mathbb{R}[x_1 \ldots x_n]$ מ"ל עבורו $f(x) = p(x)$ 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 $p \in \mathbb{R}[x_1 \ldots x_n]$ 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 $f : \{0,1\}^n \to \{0,1\}$ 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 $f : \{0,1\}^n \to \{0,1\}$ 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 $f : \{0,1\}^n \to \{0,1\}$ 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 $x \leftarrow A$ 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 $j \in \left[c \log\left(\frac{1}{\varepsilon}\right)\right]$ 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 $2^{k-1} \leq |\{i \mid x_i = 1\}| \leq 2^k$ אזי $\mathbb{P}_{S \leftarrow \mathcal{P}([n])}(|S \cap I| = 1) \geq \frac{1}{2e}$.

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 $\text{Size}(C) \geq 2^{\Omega\left(n^{\frac{1}{4 \cdot d(n)}}\right)}$.

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

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

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

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

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

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

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

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

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 $(S(n))_2$ במקום $\mathcal{O}(S(n))$.

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

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 $f:D\to(\Gamma\backslash\{\sqcup\})^*$ עבורה קיימת מ"ט M בעלת סיבוכיות מקום $S(n)$ המחשבת את f.

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

טענה: תהיינה A,B שפות עבורן $A\le_{\text{Log}}B$ 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 $L\le_{\text{Log}}\mathcal{L}$.

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 $S:\mathbb{N}\to\mathbb{N}$ 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 $|f(x)|\le m(n)$ אזי $g\circ f$ חשיבה במקום $\mathcal{O}(S(n)+\log(m(n))+R(m(n)))$.

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 $|f(x)|\le m(n)$ אזי $g\circ f$ חשיבה במקום $\mathcal{O}(S(n)+R(m(n)))$.

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

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

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

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

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 $C_{M,n}$ מעגל עבורו לכל $z\in\{0,1\}^n$ מתקיים $(M(z)\text{ מקבלת})\Longleftrightarrow(C_{M,n}(z)=1)$.

טענה: CVAL הינה $\mathcal{P}$־שלמה.

נוסחה מכומתת לחלוטין: תהא φ נוסחה באשר $\text{FV}(\varphi)=\{x_1\ldots x_n\}$ ויהיו $Q_1\ldots Q_n\in\{\forall,\exists\}$ כמתים אזי $Q_1x_1\ldots Q_nx_n(\varphi)$.

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

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 $|\langle M\rangle|=k$ 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 $f:V(C)\to[s]$ הפיכה המקיימת $A(i)=\langle f(i),\text{adj}^-(f(i)),\text{adj}^+(f(i))\rangle$ לכל $i\in[s]$.

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

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

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

טענה: succ-CVAL הינה EXP־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 $s,d:\mathbb{N}\to\mathbb{N}$ אזי
$\text{u-AC}(s,d)=\left\{L\subseteq\{0,1\}^*\;\middle|\;\substack{L(C)=L\\ \text{Size}(C_n)\le s(n)\\ \text{depth}(C_n)\le d(n)}\text{ קיימת משפחת מעגלים יוניפורמית }C\text{ בעלת fan-in לא מוגבל עבורה}\right\}$.

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

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

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 $\mathsf{AC}^{k}=\text{u-AC}^{k}$.

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

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

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

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

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

מסקנה: $\mathsf{AC}=\mathsf{NC}$.

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

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

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 ($M\left(x\right)$ מקבלת)$\Longleftrightarrow$($\left(\left(I+G\right)^{S\left(\left|x\right|\right)}\right)_{x,y}\ge1$ באשר y קונפיגורציה במצב מקבל).

השערה: 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 ($M\left(\left\langle A,s,t\right\rangle \right)$ מקבלת)$\Longleftrightarrow$(קיים מסלול מ־s ל־t). השערה פתוחה

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

- $\text{PC}'=\text{PC}+1$.
- קיימים $i_{1}\ldots i_{p}\in\left[k\right]$ עבורם לכל $j\in\left[k\right]\backslash\left\{ i_{1}\ldots i_{p}\right\}$ מתקיים $R_{j}'=R_{j}$ וכן קיימים $\pi_{1}\ldots\pi_{p}\in\Pi\cup\left\{ \text{Id}\right\}$ עבורם לכל $\ell\in\left[p\right]$ מתקיים $R_{i_{\ell}}'=\pi_{i_{\ell}}\left(R_{i_{\ell}}\right)$.
- קיימים $i_{1}\ldots i_{p}\in\mathbb{N}$ עבורם לכל $j\in\mathbb{N}\backslash\left\{ i_{1}\ldots i_{p}\right\}$ מתקיים $T'\left(j\right)=T\left(j\right)$ וכן קיימים $\pi_{1}\ldots\pi_{p}\in\Pi\cup\left\{ \text{Id}\right\}$ עבורם לכל $\ell\in\left[p\right]$ מתקיים $T'\left(\ell\right)=\pi\left(T\left(\ell\right)\right)$.

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

סימון: יהי $\left(p,k,\Pi\right)$ מודל PRAM ויהי $x\in\mathbb{N}$ נגדיר $T:\mathbb{N}\to\mathbb{N}$ כך $T\left(n\right)=\left\{ {\scriptstyle \begin{array}{cc} x & n=0\\ 0 & \text{else} \end{array}}\right.$ אזי $\text{Start}_{x}=\left(T,\left\{ 0\right\} ,0\right)$.

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

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

זמן ריצה במודל PRAM: יהי $\left(p,k,\Pi\right)$ מודל PRAM יהי A אלגוריתם ויהי $x\in\mathbb{N}$ אזי $\text{Time}\left(A,x\right)=\left(A^{\left(A_{\text{stop}}\right)}\left(\text{Start}_{x}\right)\right)_{3}$.

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

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

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

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

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

טענה: $\text{APSP}\in\mathsf{NC}$.

מכונת טיורינג בעלת אורקל: תהא $\mathcal{O}\subseteq\left\{ 0,1\right\} ^{*}$ 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 $c_{0}\cap Q=\left\{ q_{\text{query}}\right\}$ מתקיים
  - אם $c_{0}^{2}\backslash Q\in\mathcal{O}$ אזי $c_{1}\cap Q=\left\{ q_{\text{yes}}\right\}$.
  - אם $c_{0}^{2}\backslash Q\notin\mathcal{O}$ אזי $c_{1}\cap Q=\left\{ q_{\text{no}}\right\}$.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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 $\text{co}\mathcal{C} = \left\{\overline{L} \mid L \in \mathcal{C}\right\}$.

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

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

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

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 $\text{perm}(A) = \#\{\text{זיווגים מושלמים ב־} G\}$.

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 $\left(X\right)_{i,j}\sim\text{Uni}\left(\left[10n\right]\right)$ 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 $\left\langle G\right\rangle \notin\text{PM}$ אז $\mathbb{P}_{X}\left(\text{IsPerfectMatching}\left(G,X\right)=0\right)=1$.
- אם $\left\langle G\right\rangle \in\text{PM}$ 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 $\left(p,k,\Pi\right)$ מודל PRAM אזי $\left(p,k,\Pi\right)$.

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

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

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

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

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

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

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 $L\in\mathcal{RP}_{\left[1-2^{-n^{c}}\right]}$.

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

משפט צ'רנוף: יהי $p\in\left(0,1\right)$ ויהיו $Y_{1}\ldots Y_{n}\sim\text{Ber}\left(p\right)$ ב"ת אזי $\mathbb{P}\left(\left|\sum_{i=1}^{n}Y_{i}-pn\right|\ge\alpha\cdot pn\right)\le2^{-\Omega\left(\alpha^{2}\cdot pn\right)}$.

טענה: יהי $p\in\left[0,1\right)$ 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 $\pi:V\left(G\right)\to V\left(K\right)$ המקיים $\left(u,v\right)\in E\left(G\right)\iff\left(\pi\left(u\right),\pi\left(v\right)\right)\in E\left(K\right)$ לכל $u,v\in V\left(G\right)$.

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

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

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

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

פולינום אופייני של עץ בעל שורש: יהי T עץ בעל שורש r אזי $p_{T}\in\mathbb{R}\left[x_{0},\ldots,x_{\text{depth}\left(T\right)}\right]$ המוגדרת כך
- אם $T=\left(\left\{ r\right\} ,\varnothing\right)$ אזי $p_{T}\left(x\right)=x$.
- אחרת $p_{T}\left(x_{0},\ldots,x_{\text{depth}\left(T\right)}\right)=\prod_{\left(r,v\right)\in E}\left(x_{\text{depth}\left(T\right)}-p_{T_{v}}\right)$.

טענה: יהיו T,S עצים בעלי שורש אזי $\left(T\cong S\right)\iff\left(p_{T}=p_{S}\right)$.

אלגוריתם לבעיית איזומורפיזם העצים בעלי שורש: יהיו T,S עצים בעלי שורש ותהא $A\in\mathbb{N}^{\text{depth}\left(T\right)}$ באשר $A_{i}\sim\text{Uni}\left(\left[2\cdot\left|V\left(T\right)\right|\right]\right)$ ב"ת לכל $i\in\left[\text{depth}\left(T\right)\right]$ 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 $\varphi \in 3\text{CNF}$ 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

```
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: 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 $m \in \mathbb{N}_+$ ותהיינה $\alpha, \beta \in \{0,1\}^m$ אזי $d(\alpha, \beta) = |\{i \in [m] \mid \alpha_i \neq \beta_i\}|$.

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

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

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

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