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

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

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
$$\text{nu-NC}\left(s,d\right)=\left\{ L\subseteq\left\{ 0,1\right\} ^{*}\;\middle|\;\begin{array}{c}L(C)=L\\\text{Size}(C_{n})\leq s(n)\\\text{depth}(C_{n})\leq d(n)\end{array}\text{ קיימת משפחת מעגלים } C \text{ עבורה}\right\} .$$

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 $\text{parity}:\left\{ 0,1\right\} ^{n}\to\left\{ 0,1\right\}$ 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 $f:\left\{ 0,1\right\} ^{n}\to\left\{ 0,1\right\}$ אזי $p\in\mathbb{R}\left[x_{1}\ldots x_{n}\right]$ מ"ל עבורו $f\left(x\right)=p\left(x\right)$ לכל $x\in\left\{ 0,1\right\} ^{n}$.

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

סימון: תהא $f:\left\{ 0,1\right\} ^{n}\to\left\{ 0,1\right\}$ 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 $f:\left\{ 0,1\right\} ^{n}\to\left\{ 0,1\right\}$ אזי $p\in\mathbb{R}\left[x_{1}\ldots x_{n}\right]$ מ"ל עבורו $\mathbb{P}_{x\leftarrow\left\{ 0,1\right\} ^{n}}\left(p\left(x\right)=f\left(x\right)\right)\geq1-\varepsilon$.

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 $f:\left\{ 0,1\right\} ^{n}\to\left\{ 0,1\right\}$ אזי קבוצת פולינומים מ"ל $P\subseteq\mathbb{R}\left[x_{1}\ldots x_{n}\right]$ עבורה לכל $x\in\left\{ 0,1\right\} ^{n}$ מתקיים $\mathbb{P}_{p\leftarrow P}\left(p\left(x\right)=f\left(x\right)\right)\geq1-\varepsilon$.

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

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

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

טענה: יהי $n\in\mathbb{N}$ יהי $k\ge 2\log_2(2n)$ 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 $c_0=q_0x$ 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 $\left|c_{i-1}^2\right|\le S(n)+1$.
- 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: $\text{DSpace}\left(1\right)=\text{DSpace}\left(\log\left(\log\left(n\right)\right)\right)=\left\{ L\mid\right.$ רגולרית $\left.L\right\}$.

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

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

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

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 $\left(S\left(n\right)\right)_{2}$ 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 $\text{DSpace}\left(t\left(n\right)\right)\subsetneq\text{DSpace}\left(T\left(n\right)\right)$.

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

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

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 $S:\mathbb{N}\to\mathbb{N}$ 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 $\left|f\left(x\right)\right|\leq m\left(n\right)$ 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 $\left|f\left(x\right)\right|\leq m\left(n\right)$ 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 $B\in\text{LOG}$ 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: $\text{CVAL}=\left\{ \left\langle C,x\right\rangle \mid\left(\right.\right.$ מעגל בוליאני $\left.C\right)\wedge\left.\left(C\left(x\right)=1\right)\right\}$.

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 ($M\left(z\right)$ מקבלת)$\Longleftrightarrow$($C_{M,n}\left(z\right)=1$).

טענה: CVAL הינה $\mathcal{P}$־שלמה.

נוסחה מכומתת לחלוטין: תהא φ נוסחה באשר $\text{FV}\left(\varphi\right)=\left\{ x_{1}\ldots x_{n}\right\}$ 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: $\text{TQBF}=\left\{ \left\langle \varphi\right\rangle \mid\right.$ φ נוסחה מכומתת לחלוטין וספיקה$\left.\right\}$.

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 $\left|\left\langle M\right\rangle \right|=k$ 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 $A\left(i\right)=\left\langle f\left(i\right),\text{adj}^{-}\left(f\left(i\right)\right),\text{adj}^{+}\left(f\left(i\right)\right)\right\rangle$ 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: $\text{Succ-CVAL}=\left\{ \left\langle A,x\right\rangle \mid\left(\right.\right.$ מעגל המייצג מעגל $\left.A\right)\wedge\left.\left(\left\langle \left[A\right],x\right\rangle \in\text{CVAL}\right)\right\}$.

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

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 Circuit 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 $\text{u-AC}\left(s,d\right)=\left\{ L\subseteq\left\{ 0,1\right\} ^{*}\mid\text{קיימת משפחת מעגלים יוניפורמית }C\text{ בעלת fan-in לא מוגבל עבורה }\begin{smallmatrix}L(C)=L\\ \text{Size}(C_{n})\le s(n)\\ \text{depth}(C_{n})\le d(n)\end{smallmatrix}\right\}$.

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 $\text{u-NC}\left(s,d\right)=\left\{ L\subseteq\left\{ 0,1\right\} ^{*}\mid\text{קיימת משפחת מעגלים יוניפורמית }C\text{ עבורה }\begin{smallmatrix}L(C)=L\\ \text{Size}(C_{n})\le s(n)\\ \text{depth}(C_{n})\le d(n)\end{smallmatrix}\right\}$.

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 $M\left(x\right)$ אזי ($M\left(x\right)$ מקבלת)$\iff$($\left(\left(I+G\right)^{S\left(\left|x\right|\right)}\right)_{x,y}\ge1$ 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)$\iff$(קיים מסלול מ־s ל־t). 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 $\left|\alpha_{n}\right|\le a\left(n\right)$ 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 $F:\text{3CNF}\to\left\{ 0,1\right\} ^{*}\cup\left\{ \bot\right\}$ באשר ($F\left(\varphi\right)$ השמה מספקת עבור φ) $\iff\left(F\left(\varphi\right)\in\left\{ 0,1\right\} ^{*}\right)$ 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: $\text{LIN-PROG}=\left\{ \left\langle A,b\right\rangle \mid\left(A\in M_{m\times n}\left(\mathbb{R}\right)\right)\wedge\left(b\in\mathbb{R}^{m}\right)\wedge\left(\exists x\in\mathbb{R}^{n}.Ax\le b\right)\right\}$.

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

- $\text{PC}' = \text{PC} + 1$.
- קיימים $i_1 \ldots i_p \in [k]$ עבורם לכל $j \in [k] \setminus \{i_1 \ldots i_p\}$ מתקיים $R'_j = R_j$ וכן קיימים $\pi_1 \ldots \pi_p \in \Pi \cup \{\text{Id}\}$ עבורם לכל $\ell \in [p]$ מתקיים $R'_{i_\ell} = \pi_{i_\ell}(R_{i_\ell})$.
- קיימים $i_1 \ldots i_p \in \mathbb{N}$ עבורם לכל $j \in \mathbb{N} \setminus \{i_1 \ldots i_p\}$ מתקיים $T'(j) = T(j)$ וכן קיימים $\pi_1 \ldots \pi_p \in \Pi \cup \{\text{Id}\}$ 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 $T : \mathbb{N} \to \mathbb{N}$ כך $T(n) = \{\begin{smallmatrix} x & n=0 \\ 0 & \text{else} \end{smallmatrix}$ אזי $\text{Start}_x = (T, \{0\}, 0)$.

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

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

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

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

טענה: תהא L שפה באשר $L \cap \Sigma^n$ ניתנת לחישוב במודל PRAM בעל $\text{poly}(n)$ 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 $\text{polylog}(n)$ ובעבודה $\text{poly}(n)$. השערה פתוחה

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

טענה: $\text{APSP} \in \mathsf{NC}$.

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 $c_0^2 \setminus Q \in \mathcal{O}$ אזי $c_1 \cap Q = \{q_{\text{yes}}\}$.
  - אם $c_0^2 \setminus Q \notin \mathcal{O}$ 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 $\text{DTime}^{\mathcal{O}}(T(n)) = \left\{L(M) \mid T(n) \text{ מ״ט הרצה בזמן } M^{\mathcal{O}}\right\}$.

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

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

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

טענה: $E\ne\text{EXP}$.

טענה: $E\ne\text{PSPACE}$.

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

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

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

טענה: $\text{PSPACE}^{\text{PSPACE}}\ne\text{EXP}^{\text{PSPACE}}$.

טענה: $\mathcal{P}^{\text{HALT}}\ne\text{EXP}^{\text{HALT}}$.

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

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

אזי $L\in\mathcal{ZNP}$.

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

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 $s,c:\mathbb{N}\to\left[0,1\right]$ 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 $\mathbb{P}_{r\leftarrow\left\{ 0,1\right\}^{T\left(n\right)}}\left(\text{מקבלת }M\left(x;r\right)\right)\ge c\left(n\right)$.
- לכל $x\notin\mathcal{L}\cap\Sigma^{n}$ מתקיים $\mathbb{P}_{r\leftarrow\left\{ 0,1\right\}^{T\left(n\right)}}\left(\text{מקבלת }M\left(x;r\right)\right)\le s\left(n\right)$.

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

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

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

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

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

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

טענה: $\text{PM}\in\mathcal{P}$.

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

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

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 $\left(X\right)_{i,j}\sim\text{Uni}\left(\left[10n\right]\right)$ 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 $\langle G\rangle \in \text{PM}$ אז $\mathbb{P}_X\left(\text{IsPerfectMatching}\left(G, X\right)=0\right) \leq \frac{1}{10}$.

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

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

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 $\pi:V\left(G\right)\to V\left(K\right)$ המקיים $(u,v)\in E\left(G\right) \iff \left(\pi\left(u\right),\pi\left(v\right)\right)\in E\left(K\right)$ לכל $u,v\in V\left(G\right)$.

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

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

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

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

- אם $T=\left(\{r\},\varnothing\right)$ אזי $p_T\left(x\right)=x$.
- 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 $(p_T=p_S)\iff(T\cong S)$.

אלגוריתם לבעיית איזומורפיזם העצים בעלי שורש: יהיו T,S עצים בעלי שורש ותהא $A\in\mathbb{N}^{\text{depth}(T)}$ באשר $A_i\sim\text{Uni}\left(\left[2\cdot\left|V\left(T\right)\right|\right]\right)$ 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 $\varphi\in3\text{CNF}$ באשר $\text{FV}\left(\varphi\right)=\{x_1\ldots x_m\}$ וכן $\varphi=\bigwedge_{i=1}^k C_i$ ותהא $\alpha\sim\text{Uni}\left(\{0,1\}^m\right)$ אזי

טענה: תהא $\varphi\in3\text{CNF}$ באשר φ אי־ספיקה אזי $\text{Schöning'sAlgorithm}\left(\varphi,\alpha\right)=\text{False}$ לכל $\alpha\in\{0,1\}^m$.

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

טענה: תהא $\varphi\in3\text{CNF}$ באשר $\text{FV}\left(\varphi\right)=\{x_1\ldots x_m\}$ וכן φ ספיקה אזי $\mathbb{P}_\alpha\left(\text{Schöning'sAlgorithm}\left(\varphi,\alpha\right)=\text{True}\right)\geq\frac{1}{2}\cdot\left(\frac{1}{3}\right)^{\frac{m}{2}}$.

טענה: תהא $\varphi\in3\text{CNF}$ באשר $\text{FV}\left(\varphi\right)=\{x_1\ldots x_m\}$ וכן φ ספיקה אזי $\mathbb{P}_\alpha\left(\text{Schöning'sAlgorithm}\left(\varphi,\alpha\right)=\text{True}\right)\geq\left(\frac{2}{3}\right)^m$.

מסקנה: תהא $\varphi\in3\text{CNF}$ באשר $\text{FV}\left(\varphi\right)=\{x_1\ldots x_m\}$ וכן φ ספיקה אזי
$\mathbb{P}_{\alpha_1\ldots\alpha_{\left(\frac{3}{2}\right)^m}}\left(\exists i\in\left[\left(\frac{3}{2}\right)^m\right].\text{Schöning'sAlgorithm}\left(\varphi,\alpha_i\right)=\text{True}\right)\geq\frac{1}{2}$.

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

function `Schöning'sAlgorithm`(φ, α):
  for $i \in [m]$ **do**
    if $\varphi(\alpha) =$ 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: $\mathcal{BPP} \subseteq \text{PSPACE}$.

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 $\mathcal{NP} = \mathcal{RP}$.