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 $\text{Size}\left(f\right)=\min\left\{\text{Size}\left(C\right)\mid\left(f\text{ מחשבת את }C\right)\wedge\left(\text{מעגל }C\right)\right\}$.

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
$$\text{nu-AC}\left(s,d\right)=\left\{L\subseteq\left\{0,1\right\}^{*}\;\middle|\;\begin{matrix}L(C)=L\\ \text{Size}(C_{n})\leq s(n)\\ \text{depth}(C_{n})\leq d(n)\end{matrix}\text{ קיימת משפחת מעגלים }C\text{ בעלת fan-in לא מוגבל עבורה}\right\}.$$

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

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 $\text{BinAdd}_n:\{0,1\}^n\times\{0,1\}^n\to\{0,1\}^{n+1}$ המוגדרת $\text{BinAdd}_n(x,y)=x+y$.

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

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

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

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

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

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

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

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

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

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

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

function BruteForceBigCut$(E,\{v_1\dots v_n\})$:
  $S\in\mathcal{P}(\{v_1\dots v_n\})$
  for $r\in\{0,1\}^n$ **do**
    $S\leftarrow\{v_i\mid r_i=1\}$
    if $|E(S,\overline{S})|\ge\frac{|E|}{2}$ **then return** S
  end

טענה: תהא E קבוצה יהי $n\in\mathbb{N}$ ותהא $\{v_1,\dots,v_n\}$ קבוצה אזי BruteForceBigCut בעלת סיבוכיות זמן ריצה $\Omega(2^n)$.

טענה: קיימת מ"ט אקראית M_{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 $X_{c,d}\left(\alpha\right)=c\alpha+d$ אזי $\left\{X_{c,d}\right\}_{c,d\in\mathbb{F}}$ ב״ת בזוגות וכן $X_{c,d}\sim\text{Uni}\left(\mathbb{F}\right)$ 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 $S_{\text{supp}}=\left\{v_i\mid M_{\text{supp}}\left(1^n;r\right)_i=1\right\}$.

טענה: יהי G גרף באשר $V=\{v_1\dots v_n\}$ אזי $\mathbb{E}_{r\leftarrow\{0,1\}^{\log(n)+1}}\left[\left|E\left(S_{\text{supp}},\overline{S_{\text{supp}}}\right)\right|\right]=\frac{|E|}{2}$.

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

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

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

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

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

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

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 $k\geq2\log_2\left(2n\right)$ אזי קיימת צביעת קשתות f של K_n בשני צבעים עבורה לא קיים תת־גרף K_k מונוכרומטי.

מספר הפסוקיות המסופקות: תהא $\varphi\in3\text{SAT}$ באשר $\varphi=\bigwedge_{i=1}^mC_i$ בעלת n משתנים ותהא $\alpha\in\{0,1\}^n$ השמה אזי $\text{Cl}\left(\varphi,\alpha\right)=\left|\left\{i\in[m]\mid\alpha\left(C_i\right)=\text{True}\right\}\right|$.

הגדרה Max 3SAT: נגדיר $\text{max3SAT}:3\text{CNF}\to\mathbb{N}$ כך $\text{max3SAT}\left(\varphi\right)=\max\left\{\text{Cl}\left(\varphi,\alpha\right)\mid\alpha\in\{0,1\}^{|\text{FV}(\varphi)|}\right\}$.

טענה: תהא $\varphi\in3\text{CNF}$ בעלת m פסוקיות אזי $\text{max3SAT}\left(\varphi\right)\geq\frac{7}{8}\cdot m$.

סימון: תהא M מ״ט k־סרטית ותהא $c_1\$c_2\$\dots\$c_k$ קונפיגורציה אזי $\left(c_1\$c_2\$\dots\$c_k\right)^i=c_i$.

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 $\left|c_{i-1}^2\right|\leq S\left(n\right)+1$.
- 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 $\text{DSpace}\left(S\left(n\right)\right)=\left\{L\left(M\right)\mid\mathcal{O}\left(S\left(n\right)\right)\text{ מ״ט שרצה במקום }M\right\}$.

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

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

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

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

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 $S\ge\log$ 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 אלפבייתים באשר $\Delta\subseteq\Sigma$ תהא $A\subseteq\Sigma^{*}$ שפה ותהא $B\subseteq\Delta^{*}$ שפה $f:\Sigma^{*}\to\Delta^{*}$ 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 $\left|f\left(x\right)\right|\le m\left(n\right)$ 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 $B\in\text{LOG}$ 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: $\text{CVAL}=\left\{ \left\langle C,x\right\rangle \mid\left(\text{מעגל בוליאני } C\right)\wedge\left(C\left(x\right)=1\right)\right\}$.

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

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: $\text{TQBF}=\left\{ \left\langle \varphi\right\rangle \mid\text{נוסחה מכומתת לחלוטין וספיקה } \varphi\right\}$.

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 $C=[A]$.

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.

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

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

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

טענה: Succ-BoolMatPower הינה PSPACE־שלמה.

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

טענה: CSAT הינה $\mathcal{NP}$־שלמה.

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

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

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

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

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

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

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

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

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 ($M(x)$ מקבלת)$\iff\left(\left((I+G)^{S(|x|)}\right)_{x,y}\ge 1\right)$ באשר y קונפיגורציה במצב מקבל.

השערה: קיימת מ"ט M הרצה בזמן פולינומי ובזיכרון $o(n)$ עבורה לכל מטריצה A המייצגת גרף מכוון בעל n קודקודים ולכל קודקודים s,t מתקיים ($M(\langle A,s,t\rangle)$ 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 $\{\alpha_n\}_{n\in\mathbb{N}}$ המקיימת $|\alpha_n|\le a(n)$ וקיימת מ"ט M עם זמן ריצה T המקיימת $\left(M\left(x,\alpha_{|x|}\right)=1\right)\iff(x\in L)$ אזי $L\in{}^{\text{DTime}(T(n))}/_{a(n)}$.

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

טענה: קיימת שפה לא כריעה L המקיימת $L\in{}^{\mathcal{P}}/_{1}$.

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

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

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

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

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

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

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

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

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

קונפיגורציה עוברת במודל PRAM: יהי (k,Π) מודל RAM ותהא (T,R,PC) קונפיגורציה אזי קונפיגורציה (T',R',PC') באשר

- $\text{PC}'=\text{PC}+1$.
- 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 $T(n)=\left\{\begin{smallmatrix} x & n=0\\ 0 & \text{else}\end{smallmatrix}\right.$ 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 $c_0^2\backslash Q\in\mathcal{O}$ 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 $\text{DTime}^{\mathcal{O}}(T(n))=\left\{L(M)\mid T(n)\text{ מ"ט הרצה בזמן } M^{\mathcal{O}}\right\}$.

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

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

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

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

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

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

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

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

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 $\mathcal{BPP}_{[s,c]}=\mathcal{BP}\text{-Time}_{[s,c]}\left(\text{poly}\left(n\right)\right)$.

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

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 $A\in M_n\left(\mathbb{F}\right)$ אזי $\text{perm}\left(A\right)=\sum_{\sigma\in S_n}\prod_{i=1}^{n}\left(A\right)_{i,\sigma(i)}$.

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

טענה: $\det\in\text{NC}^2$.

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 $(i,j)\in[n]^2$ אזי

טענה: יהי G גרף דו־צדדי אזי

- אם $\langle G\rangle\notin\text{PM}$ 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).

```
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]
```

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

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

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 $\mathbb{P}\left(\left|\sum_{i=1}^n Y_i-pn\right|\geq\alpha\cdot pn\right)\leq 2^{-\Omega(\alpha^2\cdot pn)}$.

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

הגדרה: תהא L שפה עבורה קיים $k\in\mathbb{N}$ וקיימת מ"ט אקראית M המקיימת
- זמן פולינומי בממוצע: לכל $x\in\{0,1\}^*$ מתקיים $\mathbb{E}_r\left(\text{Time}\left(M\left(x;r\right)\right)\right)=\mathcal{O}\left(|x|^k\right)$.
- נכונות: לכל $x\in\{0,1\}^*$ מתקיים $(x\in L)\Longleftrightarrow$(לכל r אם $M(x;r)$ עוצרת אז $M(x;r)=1$).

אזי $L\in\mathcal{ZPP}_1$.

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

הגדרה: תהא L שפה עבורה קיימת מ"ט אקראית M המחזירה $\{\text{Accept},\text{Reject},\text{Quit}\}$ עם זמן ריצה פולינומי המקיימת
- לכל $x\in\{0,1\}^*$ מתקיים $\mathbb{P}_r\left(M\left(x;r\right)=\text{Quit}\right)\leq\frac{1}{2}$.
- נכונות: לכל $x\in\{0,1\}^*$ ולכל r באשר $M(x;r)\neq\text{Quit}$ מתקיים $(x\in L)\Longleftrightarrow(M(x;r)=1)$.

אזי $L\in\mathcal{ZPP}_2$.

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

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

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

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

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

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 $A_i\sim\text{Uni}\left(\left[2\cdot|V(T)|\right]\right)$ ב"ת לכל $i\in[\text{depth}(T)]$ אזי

טענה: $\text{RTree-ISO}\in\text{co}\mathcal{RP}$.

```
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))]
```

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

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 $\alpha \sim \text{Uni}(\{0,1\}^m)$ 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 $d(\alpha, \beta) = |\{i \in [m] \mid \alpha_i \neq \beta_i\}|$.

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

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

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

מסקנה: תהא $\varphi \in 3\text{CNF}$ באשר $\text{FV}(\varphi) = \{x_1 \ldots x_m\}$ 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: $3\text{SAT} \in \mathcal{BP}\text{-Time}_{\left[0, \frac{1}{2}\right]}\left(\text{poly}(m) \cdot \left(\frac{3}{2}\right)^m\right)$.

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

טענה: $\mathcal{NP} = \mathcal{BPP}_{\left[0, \frac{1}{2^n}\right]}$.

השערה: $\mathcal{BPP} \nsubseteq \mathcal{NP}$. השערה פתוחה

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

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

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

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

- לכל $i \in \{2 \ldots t\}$ אם $i\%2 = 1$ אז $b_i = A(x, b_1 \ldots b_{i-1})$.
- לכל $i \in \{2 \ldots t\}$ אם $i\%2 = 0$ אז $b_i = B(y, b_1 \ldots b_{i-1})$.
- אם $\text{Ret} = A$ אז $\text{ANS} = A(x, b_1 \ldots b_t)$ אחרת $\text{ANS} = B(y, b_1 \ldots b_t)$.

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

מספר הסיבובים בפרוטוקול תקשורת: יהי (t, A, B, Ret) פרוטוקול תקשורת אזי t.

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

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

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

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

טענה: תהא $f:\{0,1\}^{n}\times\{0,1\}^{n}\to\{0,1\}$ אזי $\mathcal{D}\left(f\right)\le n$.

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

המטריצה המייצג של פונקציה בוליאנית: תהא $f:\{0,1\}^{n}\times\{0,1\}^{n}\to\{0,1\}$ אזי $M_{f}\in M_{n}\left(\mathbb{Z}_{2}\right)$ המוגדרת $\left(M_{f}\right)_{i,j}=f\left(i,j\right)$ לכל $i,j\in\left[n\right]$.

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

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

טענה: תהא $f:\{0,1\}^{n}\times\{0,1\}^{n}\to\{0,1\}$ אזי קיימת חלוקה של $\{0,1\}^{n}\times\{0,1\}^{n}$ ל־$2^{\mathcal{D}\left(f\right)}$ מלבנים מונוכרומטיים.

מסקנה: תהא $f:\{0,1\}^{n}\times\{0,1\}^{n}\to\{0,1\}$ אזי $\text{rank}\left(M_{f}\right)\le2^{\mathcal{D}\left(f\right)}$.

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

פרוטוקול תקשורת בעל מטבעות פרטיים מחשב פונקציה: יהי $n\in\mathbb{N}_{+}$ תהא $f:\{0,1\}^{n}\times\{0,1\}^{n}\to\{0,1\}$ ויהי $\varepsilon\in\left[0,1\right]$ אזי פרוטוקול תקשורת Π עבורו מתקיים $\mathbb{P}_{r_{1},r_{2}}\left(\Pi\left(\left(x;r_{1}\right),\left(y;r_{2}\right)\right)=f\left(x,y\right)\right)\ge1-\varepsilon$ לכל $x,y\in\{0,1\}^{n}$.

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

- בהינתן $x,y\in\{0,1\}^{n}$.
- A מגרילה $p\in\left\{1,\ldots,n^{4}\right\}$ ראשוני ושולחת את p ואת $x\mod p$.
- B עונה $\mathbb{1}\left[x\mod p=y\mod p\right]$.

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

פרוטוקול תקשורת בעל מטבעות פומביים מחשב פונקציה: יהי $n\in\mathbb{N}_{+}$ ותהא $f:\{0,1\}^{n}\times\{0,1\}^{n}\to\{0,1\}$ ויהי $\varepsilon\in\left[0,1\right]$ אזי פרוטוקול תקשורת Π עבורו מתקיים $\mathbb{P}_{r}\left(\Pi\left(\left(x;r\right),\left(y;r\right)\right)=f\left(x,y\right)\right)\ge1-\varepsilon$ לכל $x,y\in\{0,1\}^{n}$.

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

- לינאריות: לכל $\alpha,\beta\in\mathbb{F}$ ולכל $a,b\in\mathbb{F}^{k}$ מתקיים $C\left(\alpha a+\beta b\right)=\alpha\cdot C\left(a\right)+\beta\cdot C\left(b\right)$.
- מרחק: לכל $a,b\in\mathbb{F}^{k}$ באשר $a\ne b$ מתקיים $\Delta\left(C\left(x\right),C\left(y\right)\right)\ge d$.

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

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

טענה: יהי $\mathbb{F}$ שדה יהיו $n,k,d\in\mathbb{N}_{+}$ ותהא $C:\mathbb{F}^{k}\to\mathbb{F}^{n}$ אזי (C קוד לינארי)$\Longleftrightarrow$($\text{Im}\left(C\right)$ תמ"ו של $\mathbb{F}^{n}$)$\wedge$(לכל $x,y\in\text{Im}\left(C\right)$ באשר $x\ne y$ מתקיים $\Delta\left(x,y\right)\ge d$).

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

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

הגדרה קידוד ריד־סולומון: יהי $\mathbb{F}$ שדה יהי $k\in\mathbb{N}_{+}$ יהי $n\le\left|\mathbb{F}\right|$ ויהיו $f_{1}\ldots f_{n}\in\mathbb{F}$ אזי $C:\mathbb{F}^{k}\to\mathbb{F}^{n}$ המוגדרת $C\left(a\right)=\left(p_{a}\left(f_{1}\right)\ldots p_{a}\left(f_{n}\right)\right)$.

טענה: יהי $\mathbb{F}$ שדה יהי $k\in\mathbb{N}_{+}$ יהי $n\le\left|\mathbb{F}\right|$ ויהיו $f_{1}\ldots f_{n}\in\mathbb{F}$ אזי קידוד ריד־סולומון הינו $\left[n,k,n-k\right]_{\left|\mathbb{F}\right|}$.

הגדרה: יהיו $n,m\in\mathbb{N}_{+}$ יהי $\mathbb{F}$ שדה באשר $\left|\mathbb{F}\right|=m$ ויהי $C:\mathbb{F}^{n}\to\mathbb{F}^{m}$ קידוד ריד־סולומון אזי נגדיר פרוטוקול תקשורת בעל מטבעות פרטיים $\Pi_{r\text{EQ}}\left[n,m\right]$ כך

- A מגרילה $i\in\{1,\ldots,m\}$ ושולחת את i ואת $\left(C\left(x\right)\right)_{i}$.
- B עונה $\mathbb{1}\left[\left(C\left(x\right)\right)_{i}=\left(C\left(y\right)\right)_{i}\right]$.

טענה: יהי $n\in\mathbb{N}_{+}$ אזי $\Pi_{r\text{EQ}}\left[n,m\right]$ מחשבת את EQ_{n} בהסתברות $\frac{n}{m}$ ובעלות $2\log\left(m\right)$.

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

מפזר: יהי $\varepsilon>0$ יהי $k\in\mathbb{N}_{+}$ תהיינה V,W קבוצות ויהי $D\in\mathbb{N}_{+}$ אזי $C:V\times\left[D\right]\to W$ עבורה לכל $A\subseteq V$ באשר $2^{k}\le\left|A\right|$ מתקיים $\left|\Gamma\left(A\right)\right|\ge\left(1-\varepsilon\right)\left|W\right|$.

טענה: יהי $\varepsilon>0$ ויהיו $k,t,m,D\in\mathbb{N}_{+}$ באשר $2^{m}\le\frac{D\cdot2^{k}}{2\ln\left(\frac{e}{\varepsilon}\right)}$ וכן $D>\frac{2\cdot\ln\left(e\cdot\frac{2^{t}}{2^{k}}\right)}{\varepsilon}$ אזי קיים $C:\{0,1\}^{t}\times\left[D\right]\to\{0,1\}^{m}$ מפזר־$\left(k,\varepsilon\right)$.

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

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

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

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

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

אלגוריתם קירוב בעיה מקסימלית: יהי $c \geq 1$ תהא X קבוצה ותהא $f : X \to \mathbb{R}$ אזי אלגוריתם $A : X \to \mathbb{R}$ המקיים $\frac{\max f(X)}{c} \leq A(x) \leq \max f(X)$ לכל $x \in X$.

אלגוריתם קירוב בעיה מינימלית: יהי $c \geq 1$ תהא X קבוצה ותהא $f : X \to \mathbb{R}$ אזי אלגוריתם $A : X \to \mathbb{R}$ המקיים $\min f(X) \leq A(x) \leq c \cdot \min f(X)$ לכל $x \in X$.

הגדרה Min Gap Problem: יהיו $a, b \in \mathbb{R}$ תהא X קבוצה ותהא $f : X \to \mathcal{P}(\mathbb{R})$ אזי $\text{GAP}_{[a,b]} \min f = (\text{Yes}, \text{No})$ באשר
- $\text{Yes} = \{\langle x \rangle \mid (x \in X) \wedge (f(x) \leq a)\}$.
- $\text{No} = \{\langle x \rangle \mid (x \in X) \wedge (f(x) > b)\}$.

הגדרה Max Gap Problem: יהיו $a, b \in \mathbb{R}$ תהא X קבוצה ותהא $f : X \to \mathcal{P}(\mathbb{R})$ אזי $\text{GAP}_{[a,b]} \max f = (\text{Yes}, \text{No})$ באשר
- $\text{Yes} = \{\langle x \rangle \mid (x \in X) \wedge (f(x) \geq b)\}$.
- $\text{No} = \{\langle x \rangle \mid (x \in X) \wedge (f(x) < a)\}$.

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

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

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

טענה: קיים אלגוריתם פולינומי 2-קירוב לבעייה minVC.

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

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

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

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

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

```
function Approx-minVC(G):
    w ← solve( min C^T w
               s.t. w_v + w_u ≥ 1   ,∀(v,u) ∈ E
                    w_v ∈ [0,1]     ,∀v ∈ V )
    return {v ∈ V | w_v ≥ 1/2}
```

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

טענה: יהי G גרף אזי Approx-minVC בעל זמן ריצה פולינומי.

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

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

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

הגדרה: יהי G גרף אזי נגדיר את maxCutExt_1 כך

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

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

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

הגדרה: יהי G גרף אזי נגדיר את maxCutExt_2 כך

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

טענה: קיים אלגוריתם הפותר את maxCutExt_2 בזמן פולינומי.

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

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

טענה: יהי G גרף אזי $\text{maxCut}(G) \le |\text{maxCutExt}(G)| \le \frac{1}{0.878}\text{maxCut}(G)$.

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

- סימטריות: לכל $u,v \in V$ מתקיים $d(u,v) = d(v,u)$.
- חיוביות ממש: לכל $u \in V$ מתקיים $d(u,u) = 0$.
- אי־שיוויון המשולש: לכל $u,v,w \in V$ מתקיים $d(u,v) \le d(u,w) + d(w,v)$.

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

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

הגדרה k-Center Problem: יהי $k \in \mathbb{N}_+$ נגדיר $\text{minCenter} : \{(G,d,k) \mid (\text{גרף } G) \wedge (\text{מרחק } d) \wedge (k \in \mathbb{N})\} \to \mathbb{N}$ כך $\text{minCenter}(G,d,k) = \min\{r(S) \mid S \in \mathcal{P}_k(V)\}$.

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

```
function ApproxCenter(G, d, k):
    v ← V
    S ← {v}
    while |S| < k do
        v ← arg max{d(u, S) | u ∈ V}
        S ← S ∪ {v}
    end
    return S
```

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

טענה: יהי $k\in\mathbb{N}_+$ יהי G גרף ויהי d מרחק אזי $\text{minCenter}\left(G\right)\le\left|\text{ApproxCenter}\left(G,d,k\right)\right|\le2\cdot\text{minCenter}\left(G\right)$.

הגדרה Dominating Set: $\text{DS}=\left\{\langle G,k\rangle\mid\exists S\in\mathcal{P}_k\left(V\right).\forall v\in V.\left(\left(\text{adj}\left(v\right)\cup\left\{v\right\}\right)\cap S\ne\varnothing\right)\right\}$.

טענה: DS הינה $\mathcal{NP}$־שלמה.

טענה: יהי $c<2$ אם קיים אלגוריתם פולינומי A אשר מהווה c־קירוב לבעיית minCenter אזי $\mathcal{P}=\mathcal{NP}$.

רדוקציה פולינומית משמרת מרווח בין בעיות הבטחה: יהיו $\left(Y,N\right),\left(Y',N'\right)$ בעיות הבטחה עבורן קיימת מ"ט פולינומית M המקיימת
- לכל $x\in\left\{0,1\right\}^*$ אם $x\in Y$ אז $M\left(x\right)\in Y'$.
- לכל $x\in\left\{0,1\right\}^*$ אם $x\in N$ אז $M\left(x\right)\in N'$.

אזי $\left(Y,N\right)\le_p\left(Y',N'\right)$.

בעיית הבטחה $\mathcal{NP}$-Promise־קשה: בעיית הבטחה Π עבורה לכל $L\in\mathcal{NP}$ מתקיים $L\le_p\Pi$.

טענה: תהא X קבוצה תהא $f:X\to\mathbb{R}$ ויהיו $a,b\in\mathbb{R}$ אם $\mathcal{P}\ne\mathcal{NP}$ וכן $\text{GAP}_{[a,b]}f$ הינה $\mathcal{NP}$-Promise־קשה אז לכל $c<\frac{b}{a}$ לא קיים אלגוריתם c־קירוב פולינומי ל־f.

מסקנה: $\text{GAP}_{[1,2]}\text{minCenter}$ הינה $\mathcal{NP}$-Promise־קשה.

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

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

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

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

טענה: יהיו $a,b\in\left(0,1\right)$ באשר $a<b$ אזי $\text{GAP}_{[a,b]}\text{max3SAT}\le_p\text{GAP}_{\left[\frac{a}{3},\frac{b}{3}\right]}\text{maxClique}$.

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

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

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

סימון: יהי $k\in\mathbb{N}$ יהי A אלגוריתם ויהי x אזי $\text{Alt}_k^{\exists}\left(M,x\right)=Q_1w_1\ldots Q_kw_k\left(A\left(x,w_1\ldots w_k\right)\right)$ באשר $Q_i=\exists$ לכל $i\in\mathbb{N}_{\text{odd}}$ וכן $Q_i=\forall$ לכל $i\in\mathbb{N}_{\text{even}}$.

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

סימון: יהי $k\in\mathbb{N}$ יהי A אלגוריתם ויהי x אזי $\text{Alt}_k^{\forall}\left(M,x\right)=Q_1w_1\ldots Q_kw_k\left(A\left(x,w_1\ldots w_k\right)\right)$ באשר $Q_i=\forall$ לכל $i\in\mathbb{N}_{\text{odd}}$ וכן $Q_i=\exists$ לכל $i\in\mathbb{N}_{\text{even}}$.

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

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

טענה: $\mathcal{P}=\Sigma_0=\Pi_0$.

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

טענה: $\text{MinCircuit}\in\Pi_2$.

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

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

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

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

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

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

טענה: יהי $k\in\mathbb{N}$ אזי $\Sigma_k=\left\{L\mid L\le_{\text{LOG}}\text{TQBF}_k^{\exists}\right\}$.

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

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

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

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

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

טענה: $\text{GISO}\in\mathcal{NP}$.

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

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

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

פרוטוקול אינטרקטיבי: יהיו $k, n, m, \ell \in \mathbb{N}_+$ תהא $P : \bigcup_{i=1}^{k} \left(\{0,1\}^n \times \left(\{0,1\}^m\right)^i\right) \to \{0,1\}^\ell$ תהא $V : \{0,1\}^n \times \left(\{0,1\}^m\right)^k \times \left(\{0,1\}^\ell\right)^k \to \{0,1\}$ ותהא $S : \{0,1\}^* \to \{0,1\}^*$ אזי (P, S, V).

מוכיח בפרוטוקול אינטרקטיבי: יהי (P, S, V) פרוטוקול אינטרקטיבי אזי P.

מסווה בפרוטוקול אינטרקטיבי: יהי (P, S, V) פרוטוקול אינטרקטיבי אזי S.

מוודא בפרוטוקול אינטרקטיבי: יהי (P, S, V) פרוטוקול אינטרקטיבי אזי V.

מספר הסיבובים בפרוטוקול אינטרקטיבי: יהיו $k, n, m, \ell \in \mathbb{N}_+$ ויהי (P, S, V) פרוטוקול אינטרקטיבי אזי k.

הרצת פרוטוקול אינטרקטיבי: יהי (P, S, V) פרוטוקול אינטרקטיבי יהי $x \in \{0,1\}^n$ ויהיו $y_1 \ldots y_k \in \{0,1\}^m$ אזי $a_1 \ldots a_k \in \{0,1\}^\ell$ וכן $\text{ANS} \in \{0,1\}$ המקיימים

- לכל $i \in [t]$ מתקיים $a_i = P\left(x, S\left(y_1 \ldots y_{i-1}\right)\right)$.
- $\text{ANS} = V\left(x, y_1 \ldots y_k, b_1 \ldots b_t\right)$.

סימון: יהי Π פרוטוקול אינטרקטיבי יהי $x \in \{0,1\}^n$ ויהיו $y_1 \ldots y_k \in \{0,1\}^m$ אזי $\Pi_{y_1 \ldots y_k}(x) = \text{ANS}$.

הערה: נאמר כי V בוחרת את $y_1 \ldots y_k$ בפרוטוקול וכן V מחשבת את $S\left(y_1 \ldots y_i\right)$ בכל שלב.

פרוטוקול אינטרקטיבי בעל מטבעות פרטיים: פרוטוקול אינטרקטיבי (P, S, V) באשר $S \neq \text{Id}$.

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

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

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

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

פרוטוקול אינטרקטיבי בעל מטבעות פומביים: פרוטוקול אינטרקטיבי (P, S, V) באשר $S = \text{Id}$.

הערה: מכאן פרוטוקול אינטרקטיבי יתייחס לפרוטוקול אינטרקטיבי בעל מטבעות פומביים.

הערה: נסמן פרוטוקול אינטרקטיבי (P, Id, V) כך (P, V).

הגדרה: יהי $n \in \mathbb{N}_+$ יהי $\ell \in \mathbb{N}$ באשר $4n! \leq 2^\ell < 8n!$ ונגדיר $\mathcal{H} = \left\{h : \{0,1\}^{n^2} \to \{0,1\}^\ell \mid \exists a, b \in \mathbb{F}_{2^{n^2}}.h = ax + b\right\}$ אזי נגדיר פרוטוקול אינטרקטיבי $\Pi_{\text{GNISO}}^{\text{pub}}[n]$ כך

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

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

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

ערך של פרוטוקול אינטרקטיבי בו ארתור מתחיל: יהי Π פרוטוקול אינטרקטיבי ויהי $x \in \{0,1\}^n$ אזי $\text{Val}_A(\Pi, x) = \mathbb{P}_{y_1 \ldots y_k}\left(\Pi_{y_1 \ldots y_k}(x) = 1\right)$.

ערך של פרוטוקול אינטרקטיבי בו מרלין מתחיל: יהי Π פרוטוקול אינטרקטיבי ויהי $x \in \{0,1\}^n$ אזי $\text{Val}_M(\Pi, x) = \mathbb{P}_{y_2 \ldots y_k}\left(\Pi_{\varepsilon, y_2 \ldots y_k}(x) = 1\right)$.

ערך של מוודא: יהי V מוודא בפרוטוקול אינטרקטיבי ויהי $X \in \{A, M\}$ אזי $\text{Val}_X(V, x) = \max_P \text{Val}_X((P, V), x)$.

הגדרה Arthur Merlin: יהי $k \in \mathbb{N}$ תהיינה $s, c : \mathbb{N} \to [0,1]$ ותהא L שפה עבורה קיים מוודא פולינומי V של פרוטוקול אינטרקטיבי בעל k סיבובים המקיים

- לכל $x \in \{0,1\}^*$ מתקיים $m, \ell = \text{poly}(|x|)$.
- לכל $x \in \{0,1\}^*$ אם $x \in L$ אז $\text{Val}_A(V, x) \geq c(|x|)$.
- לכל $x \in \{0,1\}^*$ אם $x \notin L$ אז $\text{Val}_A(V, x) \leq s(|x|)$.

אזי $L \in \text{AM}_{[s,c]}(k)$.

הגדרה Merlin Arthur: יהי $k\in\mathbb{N}$ תהיינה $s,c:\mathbb{N}\to[0,1]$ ותהא L שפה עבורה קיים מוודא פולינומי V של פרוטוקול אינטרקטיבי בעל k סיבובים המקיים

- לכל $x\in\{0,1\}^*$ מתקיים $m,\ell=\text{poly}(|x|)$.
- לכל $x\in\{0,1\}^*$ אם $x\in L$ אזי $\text{Val}_M(V,x)\geq c(|x|)$.
- לכל $x\in\{0,1\}^*$ אם $x\notin L$ אזי $\text{Val}_M(V,x)\leq s(|x|)$.

אזי $L\in\text{MA}_{[s,c]}(k)$.

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

הגדרה: $\text{AM}=\text{AM}(2)$.

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

הגדרה: $\text{MA}=\text{MA}_{\left[\frac{1}{3},\frac{2}{3}\right]}(2)$.

טענה: $\text{MA}\subseteq\text{AM}$.

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

מסקנה: $\text{GNISO}\in\text{AM}$.

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

הגדרה Interactive Proof: תהיינה $s,c:\mathbb{N}\to[0,1]$ אזי $\text{IP}_{[s,c]}=\text{AM}_{[s,c]}(\text{poly}(n))$.

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

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

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

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

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

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

טענה: $\forall\mathcal{P}=\text{co}\mathcal{NP}$.

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

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

טענה: $\exists\$\mathcal{P}=\text{MA}$.

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

טענה: $\$\exists\mathcal{P}=\text{AM}$.

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

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

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

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

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

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

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

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

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

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

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

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

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

טענה: יהי $n\in\mathbb{N}$ ויהי $\varphi\in3\text{CNF}$ באשר $\text{FV}(\varphi)=\{x_1\ldots x_n\}$ אזי $P_\varphi(a)=\varphi(a)$ לכל $a\in\{0,1\}^n$.

טענה: יהי $n\in\mathbb{N}$ ויהי $\varphi\in3\text{CNF}$ באשר $\text{FV}\left(\varphi\right)=\left\{ x_{1}\ldots x_{n}\right\}$ אזי (φ אינה ספיקה)$\Longleftrightarrow$($\sum_{a\in\left\{ 0,1\right\} ^{n}}P_{\varphi}\left(a\right)=0$).

הגדרה: יהיו $n,m,k,q\in\mathbb{N}_{+}$ באשר $q>2^{n}$ וכן $k\in\left\{ 0\ldots2^{n}\right\}$ נגדיר פרוטוקול אינטרקטיבי $\Pi_{3\text{SAT}}$ כך

- בהינתן קלט $\varphi\in3\text{CNF}$ באשר $\text{FV}\left(\varphi\right)=\left\{ x_{1}\ldots x_{n}\right\}$ וכן $\varphi=\bigwedge_{i=1}^{m}C_{i}$.
- לכל $i\in\left[n\right]$,
  - P שולח פולינום $A_{i}\in\mathbb{F}_{q}\left[x\right]$ באשר $\deg\left(A_{i}\right)\le3m$.
  - V מגריל $y_{i}\in\mathbb{F}_{q}$ ושולח אותו.
- P שולח $A_{n+1}\in\mathbb{F}_{q}$
- V עונה $\mathbb{1}\left[\left(A_{1}\left(0\right)+A_{1}\left(1\right)=k\right)\wedge\left(\forall i\in\left[n-1\right].A_{i+1}\left(0\right)+A_{i+1}\left(1\right)=A_{i}\left(y_{i}\right)\right)\wedge\left(A_{n+1}=P_{\varphi}\left(y_{1}\ldots y_{n}\right)\right)\right]$.

משפט שמיר: