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

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: יהי $k\in\mathbb{N}$ אזי $\text{Size}\left(\mathcal{O}\left(n^{k}\right)\right)=\bigcup_{c\in\mathbb{N}}\text{Size}\left(c\cdot n^{k}\right)$.

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

הגדרה: תהא $S:\mathbb{N}\to\mathbb{N}$ ותהא L שפה עבורה קיימת קבוצת מעגלים $\left\{ C_{n}\mid n\in\mathbb{N}\right\}$ המקיימת

- לכל $n\in\mathbb{N}$ מתקיים $\text{Size}\left(C_{n}\right)=S\left(n\right)$.
- לכל $x\in\left\{ 0,1\right\} ^{*}$ אם $x\in L$ אזי $\exists w.C_{\left|x\right|}\left(x,w\right)=1$.
- לכל $x\in\left\{ 0,1\right\} ^{*}$ אם $x\notin L$ אזי $\forall w.C_{\left|x\right|}\left(x,w\right)=0$.

אזי $L\in\text{NSize}\left(S\left(n\right)\right)$.

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

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

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

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 $p\in\mathbb{R}\left[x_{1}\ldots x_{n}\right]$ עבורו קיים $\alpha\in\mathbb{R}^{2^{n}}$ וקיימת $\eta\in M_{2^{n}\times n}\left(\mathbb{Z}_{2}\right)$ המקיימים $p=\sum_{i=1}^{2^{n}}\left(\alpha_{i}\cdot\prod_{j=1}^{n}x_{j}^{\eta_{i,j}}\right)$.

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 $f:\{0,1\}^n\to\{0,1\}$ אזי $p\in\mathbb{R}\left[x_1\dots x_n\right]$ מ"ל עבורו $\mathbb{P}_{x\leftarrow\{0,1\}^n}\left(p\left(x\right)=f\left(x\right)\right)\geq 1-\varepsilon$.

טענה: הפולינום 1 מחשב את $\vee_n$ בממוצע עם שגיאה $\frac{1}{3}$.

התפלגות משפחת פולינומים מחשבת פונקציה בוליאנית עם שגיאה ε: יהי $\varepsilon>0$ ותהא $f:\{0,1\}^n\to\{0,1\}$ אזי קבוצת פולינומים מ"ל $P\subseteq\mathbb{R}\left[x_1\dots x_n\right]$ עבורה לכל $x\in\{0,1\}^n$ מתקיים $\mathbb{P}_{p\leftarrow P}\left(p\left(x\right)=f\left(x\right)\right)\geq 1-\varepsilon$.

טענה: יהי $\varepsilon>0$ תהא $f:\{0,1\}^n\to\{0,1\}$ ותהא $P\subseteq\mathbb{R}\left[x_1\dots x_n\right]$ מ"ל המחשבת את f עם שגיאה ε אזי קיים $p\in P$ המחשב בממוצע את f עם שגיאה ε.

סימון: יהי $\left(\Omega,\mathbb{P}\right)$ מרחב הסתברות אזי $\left(x\leftarrow\Omega\right):\Omega\to\Omega$ הינו מ"מ באשר $\mathbb{P}\left(\left(x\leftarrow\Omega\right)=\omega\right)=\mathbb{P}\left(\omega\right)$.

הערה: תהא A קבוצה סופית אזי $x\leftarrow A$ הינו המ"מ כאשר A עם ההתפלגות האחידה.

סימון: יהי $\varepsilon>0$ ותהא $S_{j,k}\leftarrow\mathcal{P}\left([n]\right)$ לכל $k\in\{0\dots\log\left(n\right)\}$ ולכל $j\in\left[c\log\left(\frac{1}{\varepsilon}\right)\right]$ אזי $R_\vee\left(x\right)=1-\prod_{k,j}\left(1-\sum_{i\in S_{j,k}}x_i\right)$.

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

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

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

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

טענה: תהא $f:\{0,1\}^n\to\{0,1\}$ חשיבה על ידי מעגל בוליאני מגודל $s\left(n\right)$ ועומק $d\left(n\right)$ אזי לכל $\varepsilon>0$ קיימת קבוצת פולינומים מ"ל $P\subseteq\mathbb{R}\left[x_1\dots x_n\right]$ מדרגה $\mathcal{O}\left(\left(\log\left(n\right)\cdot\log\left(\frac{s(n)}{\varepsilon}\right)\right)^{d(n)}\right)$ המחשבת את f עם שגיאה ε.

מסקנה: תהא $f:\{0,1\}^n\to\{0,1\}$ חשיבה על ידי מעגל בוליאני מגודל $s\left(n\right)$ ועומק $d\left(n\right)$ אזי לכל $\varepsilon>0$ קיים פולינום מ"ל $p\in\mathbb{R}\left[x_1\dots x_n\right]$ מדרגה $\mathcal{O}\left(\left(\log\left(n\right)\cdot\log\left(\frac{s(n)}{\varepsilon}\right)\right)^{d(n)}\right)$ המחשב את f בממוצע עם שגיאה ε.

למה: יהי $\delta>0$ ויהי $p\in\mathbb{R}\left[x_1\dots x_n\right]$ מ"ל המחשב את parity_n בממוצע עם שגיאה $\frac{1}{2}+\delta$ אזי $\deg\left(p\right)=\Omega\left(\delta\sqrt{n}\right)$.

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

מסקנה: יהי C מעגל המחשב את parity_n בעל fan-in לא מוגבל ועומק $d\left(n\right)$ אזי $\text{Size}\left(C\right)\geq 2^{\Omega\left(n^{\frac{1}{4\cdot d(n)}}\right)}$.

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

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

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

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

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

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 $\text{BinMult}_n\left(x,y\right)=x\cdot y$.

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

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

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

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

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

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

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 ... 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 $\{v_1, \ldots, v_n\}$ קבוצה אזי BruteForceBigCut בעלת סיבוכיות זמן ריצה $\Omega\left(2^n\right)$.

טענה: קיימת מ"ט אקראית M_{supp} עבורה לכל $n \in \mathbb{N}$ ולכל $r \leftarrow \{0,1\}^{\log(n)+1}$ מתקיים כי $M_{\text{supp}}\left(1^n; r\right)$ מחזירה מ"מ $X_1 \ldots X_n : [\log(n)+1] \to \{0,1\}$ עבורם

- $X_1 \ldots X_n$ ב"ת בזוגות.
- $\mathbb{P}\left(X_i = 1\right) = \frac{1}{2}$ לכל $i \in [n]$.
- M_{supp} רצה בזמן $\text{poly}\left(n\right)$.

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 $\{v_1 \ldots v_n\}$ 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 $V = \{v_1 \ldots v_n\}$ 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 $\{v_1, \ldots, v_n\}$ קבוצה אזי

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

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

סימון: תהא E קבוצה יהי $n \in \mathbb{N}$ תהא $\{v_1, \ldots, v_n\}$ קבוצה ויהי $r \in \{0,1\}^n$ אזי $S_r = \{v_i \mid r_i = 1\}$.

אלגוריתם למציאת חתך גדול עם תוחלת מותנית: תהא E קבוצה יהי $n \in \mathbb{N}$ ותהא $\{v_1, \ldots, v_n\}$ קבוצה אזי

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

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

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

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

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

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.

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

יחס הפסוקיות המסופקות: תהא $\varphi \in \text{CNF}$ באשר $\varphi = \bigwedge_{i=1}^{m} C_i$ אזי $\text{RCL}\left(\varphi, \alpha\right) = \frac{1}{m} \cdot \text{Cl}\left(\varphi, \alpha\right)$.

הגדרה: יהי $k \in \mathbb{N}_+$ נגדיר $\max k\text{SAT} : k\text{CNF} \to \mathbb{N}$ כך $\max k\text{SAT}\left(\varphi\right) = \max\left\{\text{RCL}\left(\varphi, \alpha\right) \mid \alpha \in \{0,1\}^{|\text{FV}(\varphi)|}\right\}$.

טענה: תהא $\varphi \in 3\text{CNF}$ בעלת m פסוקיות אזי $\max 3\text{SAT}\left(\varphi\right) \ge \frac{7}{8}$.

הגדרה Exactly kCNF: יהי $k \in \mathbb{N}_+$ אזי $\text{E}k\text{SAT} = \left\{\langle\varphi\rangle \mid \left(\langle\varphi\rangle \in k\text{SAT}\right) \wedge \left(\text{לכל פסוקית } C \text{ מתקיים } |\text{FV}(C)| = k\right)\right\}$.

הגדרה: יהי $k \in \mathbb{N}_+$ נגדיר $\max \text{E}k\text{SAT} : \text{E}k\text{SAT} \to \mathbb{N}$ כך $\max \text{E}k\text{SAT}\left(\varphi\right) = \max\left\{\text{RCL}\left(\varphi, \alpha\right) \mid \alpha \in \{0,1\}^{|\text{FV}(\varphi)|}\right\}$.

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

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 $c_0\ldots c_n$ 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 $\text{DSpace}(S(n))=\{L(M)\mid \mathcal{O}(S(n))\ \text{מ"ט שרצה במקום}\ M\}$.

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

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

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

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

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

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

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

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

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

פונקציה חשיבה במקום: פונקציה $S:\mathbb{N}\to\mathbb{N}$ עבורה קיימת מ"ט M המקיימת לכל $n\in\mathbb{N}$ כי M על הקלט 1^n מחשבת את $(S(n))_2$ במקום $\mathcal{O}(S(n))$.

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

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

מסקנה: לפחות אחד מהבאים נכון

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

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

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

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

רדוקציית מיפוי במקום לוגריתמי: יהיו Σ,Δ אלפבייתים באשר $\Sigma\subseteq\Delta$ תהא $A\subseteq\Sigma^*$ שפה ותהא $B\subseteq\Delta^*$ שפה אזי רדוקציית מיפוי f מ־A ל־B חשיבה במקום לוגריתמי.

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

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

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

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

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

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

סימון: תהיינה A,B שפות ותהא φ רדוקציית מיפוי מ־A ל־B אזי $A\le_\varphi B$.

מחלקה: יהי Σ אלפבית אזי $\mathcal{C}\subseteq\mathcal{P}(\Sigma^*)$.

סימון: תהיינה A,B שפות תהא $\mathcal{C}$ מחלקה ותהא φ רדוקציית מיפוי מ־A ל־B באשר $\varphi\in\mathcal{C}$ אזי $A\le_{\mathcal{C}}B$.

שפה קשה למחלקה: תהא $\mathcal{C}$ מחלקה אזי שפה $\mathcal{L}$ עבורה לכל שפה $L\in\mathcal{C}$ מתקיים $L\le_{\text{Log}}\mathcal{L}$.

שפה שלמה למחלקה: תהא $\mathcal{C}$ מחלקה אזי שפה $\mathcal{L} \in \mathcal{C}$ באשר $\mathcal{L}$ הינה $\mathcal{C}$־קשה.

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

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

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

טענה: CVAL הינה $\mathcal{P}$־שלמה.

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

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

טענה: $\mathsf{TQBF} \in \mathsf{PSPACE}$.

טענה: TQBF הינה PSPACE־שלמה.

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

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

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

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

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

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

טענה: Succ-BoolMatPower הינה PSPACE־שלמה.

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

טענה: CSAT הינה $\mathcal{NP}$־שלמה.

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

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

סדרת מעגלים Log־יוניפורמית: משפחת מעגלים $\mathcal{C}$ עבורה קיימת מ"ט M באשר M רצה במקום $\mathcal{O}(\log(n))$ 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 $\mathsf{u\text{-}AC}(s,d) = \left\{L \subseteq \{0,1\}^* \;\middle|\; \text{קיימת משפחת מעגלים יוניפורמית } C \text{ בעלת fan-in לא מוגבל עבורה } {\scriptstyle \begin{matrix} L(C)=L \\ \mathrm{Size}(C_n)\le s(n) \\ \mathrm{depth}(C_n)\le d(n)\end{matrix}}\right\}$.

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

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

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

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

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

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

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

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

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

מסקנה: $\mathsf{AC} = \mathsf{NC}$.

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

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

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

הערה: 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)$\Longleftrightarrow$(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 $\left(M\left(x,\alpha_{|x|}\right)=1\right)\Longleftrightarrow(x\in L)$ 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: $\mathcal{P}/_{\text{poly}}=\mathsf{Size}(\text{poly})$.

מכונת טיורינג לא דטרמיניסטית 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 לא דטרמיניסטית M עם זמן ריצה T המקיימת $\left(M\left(x,\alpha_{|x|}\right)=1\right)\iff(x\in L)$ אזי $L\in{}^{\text{NTime}(T(n))}/_{a(n)}$.

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

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

טענה: תהא $F:3\text{CNF}\to\{0,1\}^*\cup\{\perp\}$ 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 $R'_{i_\ell}=\pi_{i_\ell}\left(R_{i_\ell}\right)$.
- 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 $A_{\text{stop}}=\min\left\{n\in\mathbb{N}\mid\forall i\in\mathbb{N}_{\ge n}:A^{(i)}(\text{Start}_x)=A^{(n)}(\text{Start}_x)\right\}$.

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

הגדרה: תהיינה $\mathcal{A},\mathcal{B}$ מחלקות 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 $L_{\text{pad}}^f\in\text{DTime}\left(\text{poly}(n)+T\left(f^{-1}(n)\right)\right)$.

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

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

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

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

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 $\mathcal{P}^{\mathcal{C}}=\mathcal{P}^L$.

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

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

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

אזי $L\in\mathcal{ZNP}$.

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

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 מסוים $n\in\mathbb{N}$ מתקיים

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

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

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

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

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

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

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

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

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

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

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

טענה: $\text{PM} \in \mathcal{P}$.

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

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

טענה: $\det \in \mathsf{NC}^2$.

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

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

טענה: יהי G גרף דו־צדדי אזי

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

מודל RAM מקבילי הסתברותי (PPRAM/Probabilistic Parallel RAM): יהי (p,k,Π) מודל PRAM אזי (p,k,Π).

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

אקראיות בקונפיגורציה: יהי (p,k,Π) מודל PPRAM ותהא (T,R,PC,X) קונפיגורציה אזי X.

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

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

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

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

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 $Y_1 \dots Y_n \sim \text{Ber}(p)$ ב"ת אזי $\mathbb{P}\left(\left|\sum_{i=1}^{n} Y_i - pn\right| \ge \alpha \cdot pn\right) \le 2^{-\Omega(\alpha^2 \cdot pn)}$.

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

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 $\mathbb{E}_r(\text{Time}(M(x;r))) = \mathcal{O}\left(|x|^k\right)$.

- 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 $\mathbb{P}_r(M(x;r) = \text{Quit}) \le \frac{1}{2}$.
- נכונות: לכל $x \in \{0,1\}^*$ ולכל r באשר $M(x;r) \ne \text{Quit}$ 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 $(\pi(u), \pi(v)) \in E(K) \Longleftrightarrow (u,v) \in E(G)$ לכל $u, v \in V(G)$.

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

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

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

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

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

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

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

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

```
function IsTreeIsomorphic(T, S, A):
    if (depth(T) ≠ depth(S)) ∨ (|V(T)| ≠ |V(S)|) then
        return False
    return 𝟙[p_T(A_0, ..., A_depth(T)) = p_S(A_0, ..., A_depth(T))]
```

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

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 $d(\alpha, \beta) = |\{i \in [m] \mid \alpha_i \ne \beta_i\}|$.

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 $\mathbb{P}_\alpha(\text{Schöning'sAlgorithm}(\varphi, \alpha) = \text{True}) \ge \frac{1}{2} \cdot \left(\frac{1}{3}\right)^{\frac{m}{2}}$.

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

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: $\mathcal{BPP} \not\subseteq \mathcal{NP}$. 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 (t, A, B, Ret) 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 $\Pi(x, y) = f(x, y)$ לכל $x, y \in \{0,1\}^n$.

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

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

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

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

המטריצה המייצגת של פונקציה בוליאנית: תהא $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ אזי $M_f \in M_n(\mathbb{Z}_2)$ המוגדרת $(M_f)_{i,j} = f(i, j)$ לכל $i, j \in [n]$.

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

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

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-$2^{\mathcal{D}(f)}$ מלבנים מונוכרומטיים.

מסקנה: תהא $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ אזי $\text{rank}(M_f) \leq 2^{\mathcal{D}(f)}$.

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

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 $\varepsilon \in [0,1]$ אזי פרוטוקול תקשורת Π עבורו מתקיים $\mathbb{P}_{r_1, r_2}(\Pi((x; r_1), (y; r_2)) = f(x, y)) \geq 1 - \varepsilon$ לכל $x, y \in \{0,1\}^n$.

הגדרה: יהי $n \in \mathbb{N}_+$ ויהיו $x, y \in \{0,1\}^n$ אזי נגדיר פרוטוקול תקשורת בעל מטבעות פרטיים $\Pi_{r\text{EQ}}[n]$ כך

Communication Protocol $\Pi_{r\text{EQ}}[n](x, y)$**:**

A draws $p \leftarrow \{1, \ldots, n^4\}$
A sends $(p, x \mod p)$
B outputs $\mathbb{1}[x \mod p = y \mod p]$

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

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

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

- ליניאריות: 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 $a\neq b$ מתקיים $\Delta\left(C\left(x\right),C\left(y\right)\right)\geq d$.

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

מרחק של קידוד ליניארי: יהי $\mathbb{F}$ שדה יהיו $n,k,d\in\mathbb{N}_+$ ויהי $C:\mathbb{F}^k\to\mathbb{F}^n$ קוד ליניארי 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 ליניארי)$\Longleftrightarrow$(($\operatorname{Im}\left(C\right)$ תמ"ו של $\mathbb{F}^n$)$\wedge$(לכל $x,y\in\operatorname{Im}\left(C\right)$ שונים מתקיים $\Delta\left(x,y\right)\geq d$)).

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

הגדרה: יהי $\mathbb{F}$ שדה יהי $k\in\mathbb{N}_+$ יהי $n\leq|\mathbb{F}|$ 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 $n\leq|\mathbb{F}|$ 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 $n\leq|\mathbb{F}|$ ויהיו $f_1\ldots f_n\in\mathbb{F}$ אזי קידוד ריד־סולומון הינו $[n,k,n-k]_{|\mathbb{F}|}$.

הגדרה: יהיו $n,m\in\mathbb{N}_+$ יהי $\mathbb{F}$ שדה באשר $|\mathbb{F}|=m$ 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

Communication Protocol $\Pi_{r\texttt{EQ}}[n,m](x,y)$**:**

A draws $i\leftarrow\{1,\ldots,m\}$
A sends $\left(i,\left(C\left(x\right)\right)_i\right)$
B outputs $\mathbb{1}\left[\left(C\left(x\right)\right)_i=\left(C\left(y\right)\right)_i\right]$

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 $C:V\times[D]\to W$ ותהא $A\subseteq V$ אזי $\Gamma\left(A\right)=\left\{C\left(a,i\right)\mid\left(a\in A\right)\wedge\left(i\in[D]\right)\right\}$.

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

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

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 בזמן הרצה $\text{Time}\left(V\right)\cdot\mathcal{O}\left(\log\left(\frac{1}{\delta}\right)\right)$ אשר עדה להיות $L\in\mathcal{RP}_{[\delta]}$.

מקור: יהי $n\in\mathbb{N}$ אזי מ"מ Y מעל $\{0,1\}^n$.

k־מקור: יהיו $n,k\in\mathbb{N}$ באשר $k\leq n$ אזי מקור Y מעל $\{0,1\}^n$ המקיים $\mathbb{P}\left(Y=y\right)\leq 2^{-k}$ לכל $y\in\{0,1\}^n$.

מקור שטוח: יהי $n\in\mathbb{N}$ ותהא $S\subseteq\{0,1\}^n$ אזי מקור Y המקיים $\mathbb{P}\left(Y=s\right)=\mathbb{P}\left(Y=x\right)$ לכל $x,s\in S$.

מרחק סטטיסטי: תהא Ω קבוצה סופית ויהיו X,Y מ"מ מעל Ω אזי $\|X-Y\|=\frac{1}{2}\sum_{s\in\Omega}|\mathbb{P}\left(X=s\right)-\mathbb{P}\left(Y=s\right)|$.

טענה: תהא Ω קבוצה סופית ויהיו X,Y מ"מ מעל Ω אזי $\|X-Y\|=\max_{S\subseteq\Omega}|\mathbb{P}\left(X\in S\right)-\mathbb{P}\left(Y\in S\right)|$.

הגדרה Extractor: יהיו $n,k,d,m\in\mathbb{N}$ באשר $k\leq n$ ויהי $\varepsilon>0$ אזי $f:\{0,1\}^n\times\{0,1\}^d\to\{0,1\}^m$ עבורה לכל k־מקור Y מעל $\{0,1\}^n$ מתקיים $\left\|f\left(Y,\text{Uni}\left(\{0,1\}^d\right)\right)-\text{Uni}\left(\{0,1\}^m\right)\right\|<\varepsilon$.

משפט: יהיו $n,k\in\mathbb{N}$ באשר $k\leq n$ ויהי $\varepsilon>0$ אזי קיים $f:\{0,1\}^n\times\{0,1\}^d\to\{0,1\}^m$ אשר הינו $\left(k,\varepsilon\right)-\text{extractor}$ באשר $d=\log\left(n-k\right)+2\log\left(\frac{1}{\varepsilon}\right)+\mathcal{O}\left(1\right)$ וכן $m=k+d-2\log\left(\frac{1}{\varepsilon}\right)-\mathcal{O}\left(1\right)$.

טענה: יהיו $n,k\in\mathbb{N}$ באשר $k\leq n-1$ יהי $\varepsilon\in\left(0,\frac{1}{2}\right)$ ויהי $f:\{0,1\}^n\to\{0,1\}$ אזי f אינו $\left(k,\varepsilon\right)-\text{extractor}$.

טענה: תהא $L\in\mathcal{BPP}$ אזי קיימת מ"ט הסתברותית M המשתמשת ב־t ביטי אקראיות אשר עדה להיות $L\in\mathcal{BPP}_{\left[2^{-\frac{2}{3}t},1-2^{-\frac{2}{3}t}\right]}$.

טענה: יהיו $n,k,d,m\in\mathbb{N}$ באשר $k\leq n$ יהי $\varepsilon>0$ ותהא $f:\{0,1\}^n\times\{0,1\}^d\to\{0,1\}^m$ באשר f הינה $\left(k,\varepsilon\right)-\text{extractor}$ אזי f הינה $\left(k,\varepsilon\right)-\text{disperser}$.

טענה: תהא $L\in\mathcal{RP}$ אזי קיימת מ"ט הסתברותית M המשתמשת ב־t ביטי אקראיות אשר עדה להיות $L\in\mathcal{RP}_{\left[2^{-\frac{2}{3}t}\right]}$.

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

אלגוריתם פותר בעיית הבטחה: תהא $\left(Y,N\right)$ 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 $L \mapsto (L, \overline{L})$ הינו שיכון לבעיית הבטחה.

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

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

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

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

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

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

function Approx-minVC(G):
- $w \leftarrow \text{solve}\left(\begin{aligned} \min \quad & \sum_{v \in V} w_v \\ \text{s.t.} \quad & w_v + w_u \geq 1 \quad , \forall (v,u) \in E \\ & w_v \in [0,1] \quad , \forall v \in V \end{aligned}\right)$
- **return** $\{v \in V \mid w_v \geq \frac{1}{2}\}$

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 $n\in\mathbb{N}_+$ יהיו $v_1\dots v_n\in\mathbb{S}^{n-1}$ 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 $\text{minCenter}(G)\le|\text{ApproxCenter}(G,d,k)|\le 2\cdot\text{minCenter}(G)$.

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

טענה: DS הינה $\mathcal{NP}$־שלמה.

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

רדוקציית מיפוי פולינומית משמרת מרווח בין בעיות הבטחה: יהיו $(Y,N),(Y',N')$ בעיות הבטחה עבורן קיימת מ"ט פולינומית M המקיימת

- לכל $x\in\{0,1\}^*$ אם $x\in Y$ אז $M(x)\in Y'$.
- לכל $x\in\{0,1\}^*$ אם $x\in N$ אז $M(x)\in N'$.

אזי $(Y,N)\le_p(Y',N')$.

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

טענה: תהא Π בעיית הבטחה אזי (Π הינה Promise-$\mathcal{NP}$־קשה)$\Longleftrightarrow$($\text{3SAT}\le_{\text{LOG}}\Pi$).

בעיית קירוב $\mathcal{NP}$־קשה: יהי $c\ge1$ ותהא $f:X\to\mathbb{R}$ עבורה לכל A אשר c־מקרבת את f מתקיים $\text{SAT}\in\mathcal{P}^A$ אזי בעיית ה־c־קירוב של f.

טענה: תהא X קבוצה תהא $f:X\to\mathbb{R}$ ויהיו $a,b\in\mathbb{R}$ באשר $\text{GAP}_{[a,b]}f$ הינה Promise-$\mathcal{NP}$־קשה אזי בעיית ה־$\frac{b}{a}$ קירוב של f הינה $\mathcal{NP}$־קשה.

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

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

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

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

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

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

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

הגדרה: יהי $b\in\mathbb{N}_+$ אזי $\text{3CNF}(b)=\{\varphi\in\text{3SAT}\mid\text{לכל }x\in\text{FV}(\varphi)\text{ מספר המופעים של }x\text{ ב־}\varphi\text{ הוא לכל היותר }b\}$.

הגדרה: יהי $b\in\mathbb{N}_+$ אזי $\text{3SAT}(b)=\{\langle\varphi\rangle\mid(\varphi\in\text{3CNF}(b))\wedge(\varphi\text{ ספיק})\}$.

טענה: $\text{3SAT}(3)$ הינה $\mathcal{NP}$־קשה.

הגדרה: יהי $b\in\mathbb{N}_+$ אזי נגדיר $\max\text{3SAT}(b):\text{3CNF}(b)\to\mathbb{N}$ כך $\max\text{3SAT}(b)(\varphi)=\max\text{3SAT}(\varphi)$.

טענה: יהי $d\in\mathbb{N}$ באשר $e^2d\cdot\left(\frac{1}{2}\right)^{d-2}\le\frac{1}{2}$ אזי קיימת סדרת גרפים מכוונים $\{G_k\mid k\in\mathbb{N}_+\}$ באשר G_n גרף על n קודקודים וכן $\deg(v)\le d$ לכל $n\in\mathbb{N}$ ולכל $v\in G_n$ עבורה לכל $n\in\mathbb{N}$ ולכל $A\subseteq V(G_n)$ באשר $|A|\le\frac{|V(G_n)|}{2}$ מתקיים $\left|E\left(A,\overline{A}\right)\right|\ge|A|$.

טענה: יהי $d\in\mathbb{N}$ באשר $e^2d\cdot\left(\frac{1}{2}\right)^{d-2}\le\frac{1}{2}$ אזי $\text{GAP}_{[0.9,1]}\max\text{3SAT}\le\text{GAP}_{\left[1-\frac{1}{10(12d+1)},1\right]}\max\text{3SAT}(4d+1)$.

הגדרה Three-variable Linear Equation: $\text{3LIN}=\left\{(A,v)\in M_{m\times n}(\mathbb{Z}_2)\times\mathbb{Z}_2^m\;\middle|\;\forall i\in[m].\sum_{j=1}^{n}\mathbb{1}\left[(A)_{i,j}=1\right]\le3\right\}$.

יחס המשוואות המסופקות: יהיו $m,n\in\mathbb{N}$ תהא $A\in M_{m\times n}(\mathbb{Z}_2)$ ותהא $b\in\mathbb{Z}_2^m$ ויהי $x\in\mathbb{Z}_2^n$ אזי $\text{RTE}(A,v,x)=\frac{1}{m}\left|\{i\in[m]\mid R_i(A)\cdot x=v_i\}\right|$.

הגדרה: נגדיר $\max\text{3LIN}:\text{3LIN}\to\mathbb{N}$ כך $\max\text{3LIN}(A,v)=\max\left\{\text{RTE}(A,v,x)\mid x\in\mathbb{Z}_2^{\text{rows}(A)}\right\}$.

טענה: יהיו $a,b\in[0,1]$ אזי $\text{GAP}_{[a,b]}\max\text{3SAT}\le_{\text{LOG}}\text{GAP}_{\left[\frac{4}{7}a,\frac{4}{7}b\right]}\max\text{3LIN}$.

טענה: יהיו $a,b\in[0,1]$ אזי $\text{GAP}_{[a,b]}\max\text{3SAT}\le_{\text{LOG}}\text{GAP}_{\left[\frac{6+a}{10},\frac{6+b}{10}\right]}\max\text{2SAT}$.

טענה: יהיו $a,b\in[0,1]$ אזי $\text{GAP}_{[a,b]}\max\text{3LIN}\le_{\text{LOG}}\text{GAP}_{\left[\frac{a}{4},\frac{b}{4}\right]}\text{maxIS}$.

מספר הצביעה: יהי G גרף אזי $\chi(G)=\min\{k\in\mathbb{N}_+\mid\text{קיימת צביעה חוקית של }G\text{ ב־}k\text{ צבעים}\}$.

טענה: אם $\mathcal{P}\neq\mathcal{NP}$ אז $\text{GAP}_{\left[2,\sqrt{|V|}\right]}\chi$ אינה Promise-$\mathcal{NP}$־קשה.

טענה: יהי $\varepsilon>0$ אזי $\text{GAP}_{\left[\frac{7}{8}-\varepsilon,\frac{7}{8}+\varepsilon\right]}\max\text{E3SAT}\in$ Promise-$\mathcal{P}$.

הגדרה: יהי $d\in\mathbb{N}$ אזי $\text{GraphDegree}_d=\{G\mid(G\text{ גרף})\wedge(\forall v\in V.\deg(V)\le d)\}$.

הגדרה: יהי $d\in\mathbb{N}$ נגדיר $\text{maxIS}(d):\text{GraphDegree}_d\to\mathbb{N}$ כך $\text{maxIS}(d)(G)=\text{maxIS}(G)$.

טענה: אם $\mathcal{P}\neq\mathcal{NP}$ אז לכל $a,b\in(0,1)$ באשר $a<b$ מתקיים $\text{GAP}_{[a,b]}\text{maxIS}(2)$ אינה Promise-$\mathcal{NP}$־קשה.

טענה: קיימים $a,b\in(0,1]$ באשר $a<b$ וקיים $D\in\mathbb{N}$ עבורם $\text{GAP}_{[a,b]}\text{maxIS}(D)$ הינה Promise-$\mathcal{NP}$־קשה.

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

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

סימון: יהי $k\in\mathbb{N}$ יהי A אלגוריתם ויהי x אזי $\text{Alt}_k^\exists(M,x)=Q_1w_1\ldots Q_kw_k(A(x,w_1\ldots w_k))$ 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 המקיימת כי ($x\in L$)$\Longleftrightarrow$($\text{Alt}_k^\exists(M,x)$ ספיקה) אזי $L\in\Sigma_k$.

סימון: יהי $k \in \mathbb{N}$ יהי A אלגוריתם ויהי x אזי $\text{Alt}_k^{\forall}(M,x) = Q_1 w_1 \ldots Q_k w_k (A(x, w_1 \ldots w_k))$ 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 $(x \in L) \Longleftrightarrow (\text{Alt}_k^{\forall}(M,x)$ ספיקה$)$ 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 $\text{TQBF}_k^{\exists} = \left\{ \langle \varphi \rangle \mid (\varphi \text{ ספיקה}) \wedge \left(\text{קיימת נוסחה } \psi \text{ עבורה } \varphi = \text{Alt}_k^{\exists}(\psi, \varepsilon)\right) \right\}$.

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

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

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

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

למה: יהי $k \in \mathbb{N}$ אזי $\Sigma_4 \not\subseteq \text{Size}\left(\mathcal{O}\left(n^k\right)\right)$.

משפט קאנאן: יהי $k \in \mathbb{N}$ אזי $\Sigma_2 \not\subseteq \text{Size}\left(\mathcal{O}\left(n^k\right)\right)$.

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

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

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: תהיינה $P, V : \{0,1\}^* \to \{0,1\}^*$ ויהי $k \in \mathbb{N}_+$ אזי (P, V).

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

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

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

הרצת פרוטוקול אינטרקטיבי: יהי (P, 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 $a_i = P(x, V(y_1 \ldots y_{i-1}))$.
- $\text{ANS} = V(x, y_1 \ldots y_k, a_1 \ldots a_t)$.

הערה: אלא אם נאמר אחרת $y_1 \ldots y_k \in \{0,1\}^{\text{poly}(|x|)}$ וכן $P : \{0,1\}^* \to \{0,1\}^{\text{poly}(|x|)}$.

הגדרה Deterministic Proof System: יהי $k \in \mathbb{N}$ ותהא L שפה עבורה קיימת מ"ט V פולינומית המקיימת לכל $x \in \{0,1\}^*$ קיימים $y_1 \ldots y_k \in \{0,1\}^{\text{poly}(|x|)}$ המקיימים

- אם $x \in L$ אז קיימת P עבורה $(P, V)(x) = 1$.
- אם $x \notin L$ אז לכל P מתקיים $(P, V)(x) = 0$.

אזי $L \in \text{dIP}(k)$.

הגדרה: $\text{dIP} = \text{dIP}(\text{poly}(n))$.

משפט: $\text{dIP} = \mathcal{NP}$.

פרוטוקול אינטרקטיבי הסתברותי: תהא $P : \{0,1\}^* \to \{0,1\}^*$ תהא V מ"ט הסתברותית ויהי $k \in \mathbb{N}_+$ אזי הפרוטוקול האינטרקטיבי (P, V).

פרוטוקול אינטרקטיבי בעל מטבעות פרטיים: פרוטוקול אינטרקטיבי הסתברותי (P, V) באשר $(y_1 \ldots y_{i-1}) \neq V(y_1 \ldots y_{i-1})$ לכל $i \in [k]$.

פרוטוקול אינטרקטיבי בעל מטבעות פומביים: פרוטוקול אינטרקטיבי הסתברותי (P,V) באשר $V(y_1\dots y_{i-1})=(y_1\dots y_{i-1})$ לכל $i\in[k]$.

הערה: מכאן פרוטוקול אינטרקטיבי יתייחס להסתברותי ואם לא נאמר אחרת אז בעל מטבעות פומביים.

ערך של פרוטוקול אינטרקטיבי: יהי Π פרוטוקול אינטרקטיבי ויהי $x\in\{0,1\}^n$ אזי $\text{Val}(\Pi,x)=\mathbb{P}_{y_1\dots y_k}(\Pi(x)=1)$.

ערך של מוודא: יהי V מוודא בפרוטוקול אינטרקטיבי אזי $\text{Val}(V,x)=\max_P\text{Val}((P,V),x)$.

הגדרה Interactive Proof: יהי $k\in\mathbb{N}$ תהיינה $s,c:\mathbb{N}\to[0,1]$ ותהא L שפה עבורה קיים מוודא V בפרוטוקול אינטרקטיבי בעל מפתחות פרטיים ו־k סיבובים המקיים

- לכל $x\in\{0,1\}^*$ אם $x\in L$ אז $\text{Val}(V,x)\ge c(|x|)$.
- לכל $x\in\{0,1\}^*$ אם $x\notin L$ אז $\text{Val}(V,x)\le s(|x|)$.

אזי $L\in\text{IP}_{[s,c]}(k)$.

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

הגדרה: יהי $n\in\mathbb{N}_+$ ויהיו G_1,G_2 גרפים על n קודקודים אזי נגדיר פרוטוקול אינטרקטיבי בעל מטבעות פרטיים $\Pi^{\text{priv}}_{\text{GNISO}}[n]$ כך

Interactive Proof $\Pi^{\texttt{priv}}_{\texttt{GNISO}}[n](G_1,G_2)$**:**

V draws $\sigma\leftarrow S_n$ and $b\leftarrow\{1,2\}$
V sends $\sigma(G_b)$
P sends $c\in\{1,2\}$
V outputs $\mathbb{1}[b=c]$

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

טענה: יהי $n\in\mathbb{N}_+$ ויהיו G_1,G_2 גרפים לא איזומורפיים על n קודקודים אזי $\mathbb{P}\left(\Pi^{\text{priv}}_{\text{GNISO}}[n](G_1,G_2)=1\right)=0$.

מסקנה: $\text{GNISO}\in\text{IP}_{[0,\frac{1}{2}]}$.

הגדרה: יהי $n\in\mathbb{N}_+$ יהי $\ell\in\mathbb{N}$ באשר $4n!\le 2^\ell<8n!$ נגדיר $\mathcal{H}=\left\{h:\{0,1\}^{n^2}\to\{0,1\}^\ell\mid\exists a,b\in\mathbb{F}_{2^{n^2}}.h=ax+b\right\}$ ויהיו G_1,G_2 גרפים על n קודקודים אזי נגדיר פרוטוקול אינטרקטיבי $\Pi^{\text{pub}}_{\text{GNISO}}[n]$ כך

Interactive Proof $\Pi^{\texttt{pub}}_{\texttt{GNISO}}[n](G_1,G_2)$**:**

V draws $h\leftarrow\mathcal{H}$ and $z\leftarrow\{0,1\}^\ell$
V sends (h,z)
P sends $G\in\{\text{Graph on } n \text{ vertices}\}$ and $\sigma\in S_n$ and $b\in\{1,2\}$
V outputs $\mathbb{1}[(h(G)=z)\wedge(\sigma(G_b)=G)]$

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

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

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

- לכל $x\in\{0,1\}^*$ אם $x\in L$ אז $\text{Val}(V,x)\ge c(|x|)$.
- לכל $x\in\{0,1\}^*$ אם $x\notin L$ אז $\text{Val}(V,x)\le s(|x|)$.

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 V בפרוטוקול אינטרקטיבי בעל k סיבובים המקיים

- לכל $x\in\{0,1\}^*$ אם $x\in L$ אז $\text{Val}(V,x\mid y_1=\varepsilon)\ge c(|x|)$.
- לכל $x\in\{0,1\}^*$ אם $x\notin L$ אז $\text{Val}(V,x\mid y_1=\varepsilon)\le s(|x|)$.

אזי $L\in\text{MA}_{[s,c]}(k)$.

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

הגדרה: תהיינה $s,c:\mathbb{N}\to[0,1]$ אזי $\text{AM}_{[s,c]}=\text{AM}_{[s,c]}(2)$.

הגדרה: $\text{AM}=\text{AM}(2)$.

מסקנה: $\text{GNISO}\in\text{AM}$.

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

הגדרה: תהיינה $s,c:\mathbb{N}\to\left[0,1\right]$ אזי $\mathsf{MA}_{\left[s,c\right]}=\mathsf{MA}_{\left[s,c\right]}\left(2\right)$.

הגדרה: $\mathsf{MA}=\mathsf{MA}\left(2\right)$.

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

משפט: תהיינה $s,c:\mathbb{N}\to\left[0,1\right]$ אזי $\mathsf{IP}_{\left[s,c\right]}=\mathsf{AM}_{\left[s,c\right]}\left(\mathrm{poly}\left(n\right)\right)$.

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

טענה: יהי $\mathbb{F}$ שדה ותהא $A\in M_{n}\left(\mathbb{F}\right)$ אזי $\mathrm{perm}\left(A\right)=\sum_{i=1}^{n}\left(A\right)_{i,1}\cdot\mathrm{perm}\left(A_{i,1}\right)$.

מטריצה פולינומית: יהי $\mathbb{F}$ שדה ויהיו $n,m\in\mathbb{N}_{+}$ אזי $M_{n\times m}\left(\mathbb{F}\left[x\right]\right)$.

דרגה של מטריצה פולינומית: תהא $D\in M_{n\times m}\left(\mathbb{F}\left[x\right]\right)$ אזי $\deg\left(D\right)=\max\left\{ \deg\left(\left(D\right)_{i,j}\right)\mid\left(i\in\left[n\right]\right)\wedge\left(j\in\left[m\right]\right)\right\}$.

טענה: יהי $n\in\mathbb{N}$ יהי $p>2^{n^{2}}$ ותהא $A\in M_{n}\left(\mathbb{F}_{p}\right)$ אזי קיימת $D\in M_{n-1}\left(\mathbb{F}_{p}\left[x\right]\right)$ באשר $\deg\left(D\right)\le n-1$ המקיימת $D\left(i\right)=A_{i,1}$ לכל $i\in\left[n\right]$.

סימון: יהי $n\in\mathbb{N}$ יהי $p>2^{n^{2}}$ תהא $A\in M_{n}\left(\mathbb{F}_{p}\right)$ ותהא $D\in M_{n-1}\left(\mathbb{F}_{p}\left[x\right]\right)$ באשר $\deg\left(D\right)\le n-1$ וכן $D\left(i\right)=A_{i,1}$ לכל $i\in\left[n\right]$ אזי $D_{A}=D$.

הגדרה: יהי $n\in\mathbb{N}$ יהי $q\in\mathbb{P}$ באשר $2^{n^{2}}<q<2^{n^{2}+1}$ יהי $B_{0}\in M_{n}\left(\mathbb{F}_{q}\right)$ ויהי $k\in\mathbb{F}_{q}$ אזי נגדיר פרוטוקול אינטרקטיבי $\Pi_{\mathrm{perm}}\left[n\right]$ כך

Interactive Proof $\Pi_{\mathtt{perm}}[n](B_0,p,k)$**:**

- P sends $g_1\in\mathbb{F}_q[x]$ such that $\deg(g_1)\le(n-1)^2$
- V computes $t_1=\mathbb{1}\left[k=\sum_{i=1}^{n}\left(B_0\right)_{i,1}\cdot g_1\left(i\right)\right]$
- V draws $y_1\leftarrow\mathbb{F}_q$
- V sends y_1
- **for** $m\in\{2,\ldots,n-3\}$ **do**
  - P sends $g_m\in\mathbb{F}_q[x]$ such that $\deg(g_m)\le(n-m)^2$
  - V computes $B_{m-1}=D_{B_{m-2}}(y_{m-1})$ and $t_m=\mathbb{1}\left[g_{m-1}\left(y_{m-1}\right)=\sum_{i=1}^{n-m+1}\left(\left(B_{m-1}\right)_{i,1}\cdot g_m\left(i\right)\right)\right]$
  - V draws $y_m\leftarrow\mathbb{F}_q$
  - V sends y_m
- **end**
- P sends $g_{n-2}\in\mathbb{F}_q[x]$ such that $\deg(g_{n-2})\le 4$
- V computes $B_{n-3}=D_{B_{n-4}}(y_{n-3})$ and $t_{n-2}=\mathbb{1}\left[g_{n-2}=\mathrm{perm}\left(D_{B_{n-3}}\right)\right]$
- V outputs $\mathbb{1}\left[\bigwedge_{i=1}^{n-2}t_i\right]$

טענה: יהי $k\in\mathbb{F}_{p}$ ותהא $A\in M_{n}\left(\mathbb{F}_{p}\right)$ באשר $\mathrm{perm}\left(A\right)=k$ אזי $\mathbb{P}\left(\mathrm{Val}_{M}\left(\Pi_{\mathrm{perm}}\left[n\right],\left(A,k\right)\right)=1\right)=1$.

טענה: יהי $k\in\mathbb{F}_{p}$ ותהא $A\in M_{n}\left(\mathbb{F}_{p}\right)$ באשר $\mathrm{perm}\left(A\right)\ne k$ אזי $\mathbb{P}\left(\mathrm{Val}_{M}\left(\Pi_{\mathrm{perm}}\left[n\right],\left(A,k\right)\right)=1\right)\le\frac{1}{3}$.

מסקנה: תהא $p:\mathbb{N}\to\mathbb{N}$ באשר $2^{n^{2}}<p\left(n\right)<2^{n^{2}+1}$ וכן $p\left(n\right)\in\mathbb{P}$ לכל $n\in\mathbb{N}$ אזי $\mathrm{perm}_{\mathbb{F}_{p\left(n\right)}}\in\mathsf{IP}$.

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

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

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

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

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

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

טענה: $\exists\$_{\left[s,c\right]}\mathcal{P}=\mathsf{MA}_{\left[s,c\right]}$.

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

טענה: $\$_{\left[s,c\right]}\exists\mathcal{P}=\mathsf{AM}_{\left[s,c\right]}$.

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

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

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

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

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

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

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

פרוטוקול אינטרקטיבי מרובה משתתפים: יהיו $m,k \in \mathbb{N}_+$ ותהיינה $P_1 \ldots P_m, V : \{0,1\}^* \to \{0,1\}^*$ אזי $(P_1,\ldots,P_m,V)$.

הרצת פרוטוקול אינטרקטיבי מרובה משתתפים: יהי $(P_1,\ldots,P_m,V)$ פרוטוקול אינטרקטיבי מרובה משתתפים יהי $x \in \{0,1\}^n$ יהי $y \in M_{m\times k}\left(\{0,1\}^{\mu}\right)$ אזי $a \in M_{m\times k}\left(\{0,1\}^{\ell}\right)$ וכן $\mathrm{ANS} \in \{0,1\}$ המקיימים

- לכל $\eta \in [m]$ ולכל $i \in [t]$ מתקיים $(a)_{\eta,i} = P_{\eta}\left(x, V\left((y)_{\eta,1},\ldots,(y)_{\eta,i-1}\right)\right)$.
- $\mathrm{ANS} = V\left(x,(y)_{1,1},\ldots,(y)_{m,k},(a)_{1,1},\ldots,(a)_{m,k}\right)$.

ערך של מוודא: יהי V מוודא בפרוטוקול אינטרקטיבי מרובה משתתפים אזי $\mathrm{Val}(V,x) = \max_{P_1\ldots P_m}\mathrm{Val}\left(\left(P_1\ldots P_m,V\right),x\right)$.

הגדרה Multi-prover Interactive Proofs: יהיו $k,m \in \mathbb{N}_+$ תהיינה $s,c : \mathbb{N} \to [0,1]$ ותהא L שפה עבורה קיים מוודא V בפרוטוקול אינטרקטיבי בעל מפתחות פרטיים ו־m משתתפים ו־k סיבובים המקיים

- לכל $x \in \{0,1\}^*$ אם $x \in L$ אז $\mathrm{Val}(V,x) \geq c(|x|)$.
- לכל $x \in \{0,1\}^*$ אם $x \notin L$ אז $\mathrm{Val}(V,x) \leq s(|x|)$.

אזי $L \in \mathrm{MIP}_{[s,c]}(m,k)$.

טענה: יהי $k \in \mathbb{N}_+$ ותהיינה $s,c : \mathbb{N} \to [0,1]$ אזי $\mathrm{MIP}_{[s,c]}(1,k) = \mathrm{IP}_{[s,c]}(k)$.

הגדרה: יהיו $m,k \in \mathbb{N}_+$ אזי $\mathrm{MIP}(m,k) = \mathrm{MIP}_{\left[\frac{1}{3},\frac{2}{3}\right]}(m,k)$.

משפט: $\mathrm{MIP}(2,2) = \mathrm{NEXP}$.

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 $\varphi \in 3\mathrm{CNF}$ באשר $\mathrm{FV}(\varphi) = \{x_1\ldots x_n\}$ אזי $P_{\varphi}(a) = \varphi(a)$ לכל $a \in \{0,1\}^n$.

טענה: יהי $n \in \mathbb{N}$ ויהי $\varphi \in 3\mathrm{CNF}$ באשר $\mathrm{FV}(\varphi) = \{x_1\ldots x_n\}$ אזי (φ אינה ספיקה)$\iff\left(\sum_{a\in\{0,1\}^n}P_{\varphi}(a) = 0\right)$.

הגדרה: יהיו $n,m,k,q \in \mathbb{N}_+$ באשר $q > 2^n$ וכן $k \in \{0\ldots 2^n\}$ ויהי $\varphi \in 3\mathrm{CNF}$ באשר $\mathrm{FV}(\varphi) = \{x_1\ldots x_n\}$ וכן $\varphi = \bigwedge_{i=1}^{m} C_i$ נגדיר פרוטוקול אינטרקטיבי $\Pi_{3\mathrm{SAT}}[n,m]$ כך

Interactive Proof $\Pi_{\mathtt{perm}}[n,m](q,\varphi,k)$**:**

for $i \in [n]$ **do**
  P sends $A_i \in \mathbb{F}_q[x]$ such that $\deg(A_i) \leq 3m$
  V draws $y_i \leftarrow \mathbb{F}_q$
  V sends y_i
end
P sends $A_{n+1} \in \mathbb{F}_q[x]$
V outputs $\mathbb{1}\left[\left(A_1(0) + A_1(1) = k\right) \wedge \left(\forall i \in [n-1].A_{i+1}(0) + A_{i+1}(1) = A_i(y_i)\right) \wedge \left(A_{n+1} = P_{\varphi}(y_1\ldots y_n)\right)\right]$

מוכיח הוגן: תהא $L \in \mathrm{IP}$ ויהי (P,V) פרוטוקול אינטרקטיבי אשר עד להיות $\mathrm{Val}(V,x) \geq c(|x|)$ לכל $x \in \{0,1\}^*$ אזי P.

משפט שמיר: קיים פרוטוקול אינטרקטיבי (P,V) בעל מוכיח הוגן ל־TQBF באשר P רצה ב־PSPACE.

משפט: אם $\text{PSPACE} \subseteq \mathcal{P}/_{\text{poly}}$ אזי $\text{PSPACE} = \text{AM}$.

השערה: $\text{PSPACE} \not\subseteq \mathcal{P}/_{\text{poly}}$. השערה פתוחה

השערה: $\text{PSPACE} \neq \text{AM}$. השערה פתוחה

טענה: $\text{IP} \subseteq \text{PSPACE}$.

מסקנה: $\text{IP} = \text{PSPACE}$.

משפט אדלמן: $\mathcal{BPP} \subseteq \mathcal{P}/_{\text{poly}}$.

השערה: $\mathcal{BPP} \neq \text{EXP}$. השערה פתוחה

טענה: $\text{AM} \subseteq \mathcal{NP}/_{\text{poly}}$.

טענה: $\text{AM} \subseteq \text{NSize}(\text{poly})$.

למה: אם $\mathcal{NP} = \text{co}\mathcal{NP}$ אזי $\Sigma_2 = \mathcal{NP}$.

הגדרה Correct SAT Solver: יהיו $n, m \in \mathbb{N}$ אזי $\text{CorrectSATSolver} = \{\langle C \rangle \mid (\text{קלטים } m \text{ על } n \text{ מעגל בגודל } C) \wedge (3\text{SAT} \text{ מכריע את } C)\}$.

טענה: $\text{CorrectSATSolver} \in \Pi_2$.

מסקנה: $\text{CorrectSATSolver} \in \Pi_1$.

משפט קארפ־ליפטון: אם $\mathcal{NP} \subseteq \mathcal{P}/_{\text{poly}}$ אזי $\Sigma_2 = \Pi_2$.

משפט סיפסר: $\mathcal{BPP} \subseteq \Sigma_2$.

מסקנה: $\mathcal{BPP} \subseteq \Sigma_2 \cap \Pi_2$.

טענה: $\mathcal{BPP} \subseteq \mathcal{RP}^{\text{SAT}}$.

טענה: $\mathcal{BPP} \subseteq \mathcal{ZPP}^{\text{SAT}}$.

טענה אמפליפיקציה: יהי $c \in \mathbb{N}$ אזי $\text{MA} = \text{MA}_{[2^{-n^c}, 1-2^{-n^c}]}$.

טענה אמפליפיקציה: יהי $c \in \mathbb{N}$ אזי $\text{AM} = \text{AM}_{[2^{-n^c}, 1-2^{-n^c}]}$.

משפט: $\text{MA} = \text{MA}_{[\frac{1}{2}, 1]}$.

טענה: $\text{MA} \subseteq \text{AM}$.

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

טענה: $\text{AM} \subseteq \Pi_2$.

טענה: $\text{MA} \subseteq \Sigma_2$.

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

מסקנה: יהי $k \in \mathbb{N}_+$ אזי $\text{AM}(k) \subseteq \text{AM}$.

טענה: אם GISO הינה $\mathcal{NP}$־קשה אז $\mathcal{PH} = \Sigma_2$.

טענה: תהיינה $s, c : \mathbb{N} \to [0,1]$ אזי $\text{IP}_{[s,c]} \subseteq \text{IP}_{[s,1]}$.

למה: $\text{MAM}_{[\frac{1}{2}, 1]} = \text{AM}_{[\frac{1}{2}, 1]}$.

משפט: $\text{AM} = \text{AM}_{[\frac{1}{2}, 1]}$.

טענה: $\text{AM}_{[0, \frac{1}{2}]} = \mathcal{NP}$.

טענה: $\text{AM}_{[0, \frac{1}{2}]} = \text{MA}_{[0, \frac{1}{2}]}$.

הגדרה: יהי Σ אלפבית תהיינה $r, q : \mathbb{N} \to \mathbb{N}$ תהיינה $s, c : \mathbb{N} \to [0,1]$ ויהי $n \in \mathbb{N}$ אזי נגדיר פרוטוקול אינטרקטיבי $\Pi_{\text{PCP}}(\Sigma, s, c, r, q)[n]$ כך

- בהינתן קלט $x \in \{0,1\}^n$.
- P שולח מחרוזת $w \in \Sigma^m$ באשר $m \leq 2^{r(n)} \cdot q(n)$.
- V מגריל $y \in \{0,1\}^{r(n)}$ ומחשב $i \in [m]^{q(n)}$.
- V עונה $V(x, y, w_{i_1} \dots w_{i_{q(n)}})$.

הגדרה Probabilistically Checkable Proof: יהי Σ אלפבית תהיינה $r, q : \mathbb{N} \to \mathbb{N}$ תהיינה $s, c : \mathbb{N} \to [0,1]$ ותהא L שפה עבורה קיים מוודא V בפרוטוקול האינטרקטיבי $\Pi_{\text{PCP}}(\Sigma, s, c, r, q)$ המקיים

- לכל $x \in \{0,1\}^*$ אם $x \in L$ אז $\text{Val}(V, x \mid y_1 = \varepsilon) \geq c(|x|)$.
- לכל $x \in \{0,1\}^*$ אם $x \notin L$ אז $\text{Val}(V, x \mid y_1 = \varepsilon) \leq s(|x|)$.

אזי $L \in \text{PCP}_{[s,c]}(r(n), q(n))_\Sigma$.

הערה: במחלקה PCP המוכיח לא חייב להיות פולינומי וכן ההודעות לא חייבות להיות פולינומיות.

הגדרה: תהיינה $r,q:\mathbb{N}\to\mathbb{N}$ ותהיינה $s,c:\mathbb{N}\to[0,1]$ אזי $\mathrm{PCP}_{[s,c]}(r(n),q(n))=\mathrm{PCP}_{[s,c]}(r(n),q(n))_{\{0,1\}}$.

טענה: $3\mathrm{SAT}\in\mathrm{PCP}_{\left[1-\frac{1}{n},1\right]}(\log(n),3)$.

משוואה ריבועית: יהי $n\in\mathbb{N}$ ויהי $A\in M_{n\times n}(\mathbb{Z}_2)$ אזי $\mathrm{Quad}_\alpha:\mathbb{Z}_2^n\to\mathbb{Z}$ המוגדרת $\mathrm{Quad}_\alpha(x)=\sum_{i=1}^n\sum_{j=1}^n(A)_{i,j}\cdot x_ix_j$.

מכפלת וקטורים טנזורית: יהיו $n,m\in\mathbb{N}$ יהי $u\in\mathbb{Z}_2^n$ ויהי $v\in\mathbb{Z}_2^m$ אזי $u\otimes v\in\mathbb{Z}_2^{n\cdot m}$ המוגדר $(u\otimes v)_{i,j}=u_i\cdot v_j$.

מערכת משוואות ריבועיות: $\mathrm{QuadEQ}=\{\langle A,b\rangle\mid(A\in M_{m\times n\times n}(\mathbb{Z}_2))\wedge(b\in\mathbb{Z}_2^m)\wedge(\exists x\in\mathbb{Z}_2^n.\forall k\in[m].\mathrm{Quad}_{A_k}(x)=b_k)\}$.

טענה: QuadEQ הינה $\mathcal{NP}$־שלמה.

טענה: $\mathrm{QuadEQ}=\{\langle B,b\rangle\mid(B\in M_{m\times n^2}(\mathbb{Z}_2))\wedge(b\in\mathbb{Z}_2^m)\wedge(\exists u\in\{0,1\}^n.B\cdot(u\otimes u)=b)\}$.

קוד הדמרד: יהי $n\in\mathbb{N}$ אזי $\mathrm{HAD}:\{0,1\}^n\to\{0,1\}^{2^n}$ המוגדר $(\mathrm{HAD}(x))_i=\langle x,(i)_2\rangle$.

טענה: יהי $n\in\mathbb{N}$ אזי קוד הדמרד הינו קידוד ליניארי $\left[2^n,n,2^{n-1}\right]_2$.

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

משפט: אם קיימת $z:\{0,1\}^n\to\{0,1\}$ וקיים $\rho\in\left[\frac{1}{2},1\right)$ עבורם $\mathbb{P}_{x,y}(z(x)+z(y)=z(x+y))\geq\rho$ אז קיימת $u\in\{0,1\}^n$ עבורה $\mathrm{Ag}(z,\mathrm{HAD}(u))\geq\rho\cdot 2^n$.

משפט: $\mathcal{NP}\subseteq\mathrm{PCP}_{[0.9,1]}\left(\mathcal{O}\left(n^2\right),\mathcal{O}(1)\right)$.

משפט ה־PCP: קיים $\gamma<1$ עבורו $\mathcal{NP}=\mathrm{PCP}_{[\gamma,1]}(\mathcal{O}(\log(n)),3)$.

טענה: יהי $\varepsilon>0$ אזי $\mathrm{GAP}_{\left[\frac{7}{8}+\varepsilon,1\right]}\max\mathrm{E3SAT}$ הינה $\mathcal{NP}$־Promise־קשה.

טענה: יהי Σ אלפבית ותהיינה $s,c:\mathbb{N}\to[0,1]$ אזי $\mathrm{PCP}_{[s,c]}(0,0)_\Sigma=\mathcal{P}$.

טענה: יהי Σ אלפבית אזי $\mathrm{PCP}_{\left[\frac{1}{3},\frac{2}{3}\right]}(\mathrm{poly}(n),0)_\Sigma=\mathcal{BPP}$.

טענה: יהי Σ אלפבית ותהיינה $s,c:\mathbb{N}\to[0,1]$ אזי $\mathrm{PCP}_{[s,c]}(\log(n),0)_\Sigma=\mathcal{P}$.

טענה: יהי Σ אלפבית ותהיינה $s,c:\mathbb{N}\to[0,1]$ אזי $\mathrm{PCP}_{[s,c]}(0,\mathrm{poly}(n))_\Sigma=\mathcal{NP}$.

טענה: תהיינה $s,c:\mathbb{N}\to[0,1]$ אזי $\mathrm{PCP}_{[s,c]}(0,\mathrm{poly}(n))=\mathcal{NP}$.

טענה: תהיינה $s,c:\mathbb{N}\to[0,1]$ אזי $\mathrm{PCP}_{[s,c]}(\log\log(n),\mathcal{O}(1))=\mathcal{P}$.

טענה: תהיינה $s,c:\mathbb{N}\to[0,1]$ אזי $\mathrm{PCP}_{[s,c]}(\mathcal{O}(\log(n)),1)=\mathcal{P}$.

טענה: תהיינה $s,c:\mathbb{N}\to[0,1]$ אזי $\mathrm{PCP}_{[s,c]}(\mathcal{O}(\log(n)),1)_{\{1,\ldots,n^c\}}=\mathcal{P}$.

טענה: תהיינה $s,c:\mathbb{N}\to[0,1]$ אזי $\mathrm{PCP}_{[s,c]}(\mathcal{O}(\log(n)),1)_{\{1,\ldots,2^{n^c}\}}=\mathcal{NP}$.

טענה: תהיינה $r,q:\mathbb{N}\to\mathbb{N}$ ותהיינה $s,c:\mathbb{N}\to[0,1]$ אזי $\mathrm{PCP}_{[s,c]}(r(n),q(n))\subseteq\mathrm{NTime}\left(\mathrm{poly}\left(n,2^{r(n)}\cdot q(n)\right)\right)$.

מסקנה: תהיינה $s,c:\mathbb{N}\to[0,1]$ אזי $\mathrm{PCP}_{[s,c]}(\mathcal{O}(\log(n)),\mathcal{O}(1))=\mathcal{NP}$.

מסקנה: תהיינה $s,c:\mathbb{N}\to[0,1]$ אזי $\mathrm{PCP}_{[s,c]}(\mathrm{poly}(n),\mathrm{poly}(n))=\mathrm{NEXP}$.

טענה: יהי Σ אלפבית ותהיינה $s,t:\mathbb{N}\to[0,1]$ אזי $\mathrm{PCP}_{[s,1]}(r(n),q(n))_\Sigma\subseteq\mathrm{PCP}_{[s^t,1]}(r(n)\cdot t(n),q(n)\cdot t(n))_\Sigma$.

טענה: יהי Σ אלפבית אזי $\mathrm{PSPACE}\subseteq\mathrm{PCP}_{\left[\frac{1}{3},\frac{2}{3}\right]}(\mathrm{poly}(n),\mathrm{poly}(n))_\Sigma$.

הייפר גרף: יהי $q\in\mathbb{N}$ תהא V קבוצה ותהא $E\subseteq\mathcal{P}_{\leq q}(V)$ אזי (q,V,E).

הגדרה: יהי Σ אלפבית ויהי $q\in\mathbb{N}_+$ אזי $q\text{-GraphConstraint}_\Sigma=\left\{(G,f)\mid(\text{הייפר גרף } G)\wedge\left(\forall e\in E.f(e):\Sigma^{|e|}\to\{0,1\}\right)\right\}$.

הגדרה: יהי Σ אלפבית ויהי $q\in\mathbb{N}_+$ אזי $\max q\text{-CSP}_\Sigma:q\text{-GraphConstraint}_\Sigma\to\mathbb{N}$ המוגדרת $\max q\text{-CSP}_\Sigma(G,f)=\max_{\sigma:V\to\Sigma}\mathbb{P}_{e\in E}(f_e(\sigma_{\restriction_e})=1)$.

הגדרה q-Constraint Statisfiability Problem: יהי Σ אלפבית יהי $q\in\mathbb{N}_+$ ותהיינה $s,c:\mathbb{N}\to[0,1]$ אזי $q\text{-CSP}_{s,c,\Sigma}=\mathrm{GAP}_{[s,c]}\max q\text{-CSP}_\Sigma$.

טענה: יהי Σ אלפבית תהיינה $r,q:\mathbb{N}\to\mathbb{N}$ תהיינה $s,c:\mathbb{N}\to[0,1]$ ותהא $L\in\mathrm{PCP}_{[s,c]}(\mathcal{O}(\log(n)),q(n))_\Sigma$ אזי $L\leq_p q\text{-CSP}_{[s,c],\Sigma}$.

משפט: קיים $\gamma<1$ עבורו $3\text{-CSP}_{[\gamma,1],\{0,1\}}$ הינה $\mathcal{NP}$־Promise־קשה.

סימון: יהי $\gamma<1$ באשר $3\text{-CSP}_{[\gamma,1],\{0,1\}}$ הינה $\mathcal{NP}$־Promise־קשה אזי $\gamma=\gamma_{\mathrm{hard}}$.

מסקנה: $\mathrm{GAP}_{[\gamma_{\mathrm{hard}},1]}\max 3\mathrm{SAT}$ הינה $\mathcal{NP}$־Promise־קשה.

מסקנה: $\mathrm{GAP}_{\left[\frac{\gamma_{\mathrm{hard}}}{3},\frac{1}{3}\right]}\mathrm{maxClique}$ הינה $\mathcal{NP}$־Promise־קשה.

מסקנה: בעיית ה־$\left(\frac{1}{\gamma_{\mathrm{hard}}}\right)$־קירוב של maxClique הינה $\mathcal{NP}$־קשה.

מסקנה: $\mathrm{GAP}_{\left[\frac{\gamma_{\mathrm{hard}}}{3},\frac{1}{3}\right]}\mathrm{maxIS}$ הינה $\mathcal{NP}$־Promise־קשה.

מסקנה: $\mathrm{GAP}_{\left[\frac{2}{3},1-\frac{\gamma_{\mathrm{hard}}}{3}\right]}\mathrm{minVC}$ הינה $\mathcal{NP}$־Promise־קשה.

מסקנה: בעיית ה־$\left(\frac{3-\gamma_{\mathrm{hard}}}{2}\right)$־קירוב של minVC הינה $\mathcal{NP}$־קשה.

טענה: $\mathcal{NP} = \text{PCP}_{\left[\frac{1}{2},1\right]}\left(\mathcal{O}\left(\log\left(n\right)\right),\mathcal{O}\left(1\right)\right)$.

טענה: $\mathcal{NP} \subseteq \text{PCP}_{\left[2^{-n},1\right]}\left(\mathcal{O}\left(n\log\left(n\right)\right),\mathcal{O}\left(n\right)\right)$.

טענה: $\text{PCP}_{\left[\frac{1}{n},1\right]}\left(\mathcal{O}\left(\log\left(n\right)\right),\mathcal{O}\left(\log\left(n\right)\right)\right) \leq_p \text{GAP}_{\left[\frac{1}{n},1\right]}\text{maxClique}$.

טענה: $\mathcal{NP} = \text{PCP}_{\left[\frac{1}{n},1\right]}\left(\mathcal{O}\left(\log\left(n\right)\right),\mathcal{O}\left(\log\left(n\right)\right)\right)$.

מסקנה: קיים $\alpha > 0$ עבורו בעיית ה־n^{α}־קירוב של maxClique הינה $\mathcal{NP}$־קשה.

מסקנה: יהי $\varepsilon > 0$ אזי $\text{GAP}_{\left[n^{\varepsilon},n^{1-\varepsilon}\right]}\text{maxClique}$ הינה Promise-$\mathcal{NP}$־קשה.