

גודל מעגל בוליאני: יהיו $n, m \in \mathbb{N}$ ויהי C מעגל בוליאני בעל n חוטים וכן m קלטים אזי $\text{Size}(C) = n + m$.

עומק מעגל בוליאני: יהי C מעגל בוליאני אזי $\text{depth}(C)$ הינו אורך המסלול המקסימלי מקלט לפלט.

הגדרה: יהי $n \in \mathbb{N}_{\geq 3}$ אזי $\vee_n : \{0, 1\}^n \rightarrow \{0, 1\}$ המוגדרת $\vee_n(x) = \bigvee_{i=1}^n x_i$.

הגדרה: יהי $n \in \mathbb{N}_{\geq 3}$ אזי $\wedge_n : \{0, 1\}^n \rightarrow \{0, 1\}$ המוגדרת $\wedge_n(x) = \bigwedge_{i=1}^n x_i$.

מעגל בוליאני בעל fan-in לא מוגבל: מעגל בוליאני מעל בסיס הפונקציות הבוליאניות $\{\wedge, \vee, \neg\}$.
הערה: אלא אם נאמר אחרת מעגל בוליאני הוא בעל fan-in מוגבל.

טענה: תהא $f : \{0, 1\}^n \rightarrow \{0, 1\}$ אזי קיים מעגל בוליאני C בעל fan-in לא מוגבל המחשב את f בגודל $\mathcal{O}(n \cdot 2^n)$ ובעומק 2.

טענה: תהא $f : \{0, 1\}^n \rightarrow \{0, 1\}$ אזי קיים מעגל בוליאני C המחשב את f בגודל $\mathcal{O}(n \cdot 2^n)$ ובעומק $n + \log_2(n)$.

מסקנה: תהא L שפה אזי קיימת משפחת מעגלים \mathcal{C} מגודל $\mathcal{O}(n \cdot 2^n)$ ומעומק $n + \log(n)$ המחשבת את L .

מסקנה: יהי $n \in \mathbb{N}$ אזי קיימת $f : \{0, 1\}^n \rightarrow \{0, 1\}$ עבורה לכל מעגל בוליאני C המחשב אותה מתקיים $\text{Size}(C) \geq \frac{2^n}{2n}$.

הגודל של פונקציה בוליאנית: יהי $n \in \mathbb{N}$ ותהא $f : \{0, 1\}^n \rightarrow \{0, 1\}$ אזי $\text{Size}(f) = \min \{\text{Size}(C) \mid (C \text{ מחשבת את } f) \wedge (C \text{ מעגל})\}$.

טענה: יהי $n \in \mathbb{N}$ ותהא $f : \{0, 1\}^n \rightarrow \{0, 1\}$ אזי $\text{Size}(f) \leq 15 \cdot (2^n - 1)$.

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

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

משפט: קיים $C \in \mathbb{R}_+$ עבורו לכל $n \in \mathbb{N}$ ולכל $S : \mathbb{N} \rightarrow \mathbb{N}$ המקיימת $n \leq S < C \cdot \frac{2^n}{n}$ קיימת $f : \{0, 1\}^n \rightarrow \{0, 1\}$ באשר f

חשיבה על ידי מעגל מגודל $S(n) + 10n$ וכן f לא חשיבה על ידי מעגל מגודל $S(n)$.

הגדרה: תהא $S : \mathbb{N} \rightarrow \mathbb{N}$ אזי L חשיבה על ידי משפחת מעגלים מגודל לכל היותר $S(n)$ $\{L \subseteq \{0, 1\}^* \mid S(n) \text{ חשיבה על ידי } L\}$.

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

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

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

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

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

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

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

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

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

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

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

$\{0, 1\} \rightarrow [\log(n) + 1]$ 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 $\text{poly}(n)$.

סימון: יהי $n \in \mathbb{N}$ יהי $r \in \{0, 1\}^{\log(n)+1}$ ותהא $\{v_1 \dots v_n\}$ קבוצה אזי $S_{\text{supp}} = \{v_i \mid M_{\text{supp}}(1^n; r)_i = 1\}$.

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

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

```

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

```

טענה: תהא E קבוצה יהי $n \in \mathbb{N}$ ותהא $\{v_1, \dots, v_n\}$ קבוצה אזי FastBigCut בעלת סיבוכיות זמן ריצה $\text{poly}(n)$.
סימון: תהא E קבוצה יהי $n \in \mathbb{N}$ ותהא $\{v_1, \dots, v_n\}$ 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( $E, \{v_1 \dots v_n\}$ ):
     $S \leftarrow \mathcal{P}(\{v_1 \dots v_n\})$ 
     $a \leftarrow \bigcup_{i=0}^n \{0, 1\}^i$ 
     $a \leftarrow \epsilon$ 
    for  $i \in [1 \dots, n]$  do
         $c_0 \leftarrow \mathbb{E}_{r \leftarrow \{0, 1\}^n} [|E(S_r, \overline{S_r})| \mid (r_1 = a_1), \dots, (r_{i-1} = a_{i-1}), (r_i = 0)]$ 
         $c_1 \leftarrow \mathbb{E}_{r \leftarrow \{0, 1\}^n} [|E(S_r, \overline{S_r})| \mid (r_1 = a_1), \dots, (r_{i-1} = a_{i-1}), (r_i = 1)]$ 
         $a_i \leftarrow \arg \max_{\ell \in \{0, 1\}} (c_\ell)$ 
    end
    return  $S_a$ 

```

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

הגדרה: תהיינה $s, d : \mathbb{N} \rightarrow \mathbb{N}$ אזי קיימת משפחת מעגלים C בעלת fan-in לא מוגבל עבורה $\left| \left\{ L \subseteq \{0, 1\}^* \mid \begin{array}{l} L(C)=L \\ \text{Size}(C_n) \leq s(n) \\ \text{depth}(C_n) \leq d(n) \end{array} \right\} \right|$
הגדרה: יהי $k \in \mathbb{N}$ אזי $\text{nu-AC}^k = \bigcup_{c \in \mathbb{N}} \text{nu-AC}(n^c, \log^k(n))$

הגדרה: תהיינה $s, d : \mathbb{N} \rightarrow \mathbb{N}$ אזי קיימת משפחת מעגלים C עבורה $\left| \left\{ L \subseteq \{0, 1\}^* \mid \begin{array}{l} L(C)=L \\ \text{Size}(C_n) \leq s(n) \\ \text{depth}(C_n) \leq d(n) \end{array} \right\} \right|$

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

מסקנה: תהיינה $s, d : \mathbb{N} \rightarrow \mathbb{N}$ אזי $\text{nu-NC}(s, d) \subseteq \text{nu-AC}(s, d)$

טענה: יהי $k \in \mathbb{N}$ אזי $\text{nu-AC}^k \subseteq \text{nu-NC}^{k+1}$

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

פונקציית זוגיות: יהי $n \in \mathbb{N}_+$ אזי $\text{parity} : \{0, 1\}^n \rightarrow \{0, 1\}$ המוגדרת $\text{parity}(x) = \bigoplus_{i=1}^n x_i$

טענה: קיים מעגל C המחשב את parity_n מגודל $\mathcal{O}(n)$ ועומק $\mathcal{O}(\log(n))$

מסקנה: $\text{parity} \in \text{nu-NC}^1$

פולינום מולטי-לינארי (מ"ל): יהי $n \in \mathbb{N}_+$ אזי $p \in \mathbb{R}[x_1 \dots x_n]$ בעל דרגה 1.

פולינום מחשב פונקציה בוליאנית: תהא $f : \{0, 1\}^n \rightarrow \{0, 1\}$ אזי $p \in \mathbb{R}[x_1 \dots x_n]$ מ"ל עבורו $f(x) = p(x)$ לכל $x \in \{0, 1\}^n$

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

סימון: תהא $f : \{0, 1\}^n \rightarrow \{0, 1\}$ ויהי $p \in \mathbb{R}[x_1 \dots x_n]$ מ"ל המחשב את f אזי $\deg(f) = \deg(p)$

מסקנה: יהי $n \in \mathbb{N}$ אזי $\deg(\vee_n) = n$

טענה: יהי $n \in \mathbb{N}$ אזי $\deg(\text{parity}_n) = n$

פולינום מחשב פונקציה בוליאנית בממוצע עם שגיאה ε : יהי $\varepsilon > 0$ ותהא $f : \{0, 1\}^n \rightarrow \{0, 1\}$ אזי $p \in \mathbb{R}[x_1 \dots x_n]$ מ"ל עבורו $\mathbb{P}_{x \leftarrow \{0, 1\}^n} (p(x) = f(x)) \geq 1 - \varepsilon$.

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

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

טענה: יהי $\varepsilon > 0$ ותהא $f : \{0, 1\}^n \rightarrow \{0, 1\}$ אזי קיים $p \in P$ המחשב בממוצע את f עם שגיאה ε .

סימון: יהי (Ω, \mathbb{P}) מרחב הסתברות אזי $\Omega \rightarrow \Omega : (x \leftarrow \Omega) = \omega = \mathbb{P}(\omega)$ 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 $j \in [\log(\frac{1}{\varepsilon})]$ אזי $R_V(x) = 1 - \prod_{k,j} (1 - \sum_{i \in S_{j,k}} x_i)$ **למה:** יהי $x \in \{0, 1\}^n$ עבורו $\vee_n(x) = 0$ אזי $R_V(x) = 0$ לכל $S_{j,k} \leftarrow \mathcal{P}([n])$.

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

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

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

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

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

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

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

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

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

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

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

מכונת טיורינג בעלת סיבוכיות מקום: תהא $S : \mathbb{N} \rightarrow \mathbb{N}$ אזי מ"ט תלת-סרטית M עבורה לכל קונפיגורציות $c_0 \dots c_n$ באשר $c_0 = q_0 x$ וכן c_{i-1} עוברת ל- c_i לכל $i \in [n]$ מתקיים

• סרט לקריאה בלבד: לכל $i \in [n]$ מתקיים $c_i^1 = x \setminus Q$.

• סרט חסום במקום: לכל $i \in [n]$ מתקיים $|c_{i-1}^2| \leq S(n) + 1$.

• סרט לכתובה חד-פעמית: לכל $i \in [n]$ ולכל $j \in [|c_{i-1}^3|]$ מתקיים $(c_{i-1}^3 \setminus Q)_j = (c_i^3 \setminus Q)_j$.

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

הערה: נקרא למכונת טיורינג בעלת סיבוכיות מקום מכונת טיורינג.

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

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

שפה LOGSPACE : $\text{LOG} = \text{DSpace}(\log(n))$.

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

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

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

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

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

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

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

פונקציה חשיבה במקום: פונקציה $S : \mathbb{N} \rightarrow \mathbb{N}$ 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 $S : \mathbb{N} \rightarrow \mathbb{N}$ חשיבה במקום ותהא $t(n) = o(S(n))$ אזי $\text{DSpace}(t(n)) \subsetneq \text{DSpace}(S(n))$.
מסקנה: $\text{LOG} \subsetneq \text{PSPACE}$.

מסקנה: לפחות אחד מהבאים נכון

$$\bullet \text{LOG} \subsetneq \mathcal{P}$$

$$\bullet \mathcal{P} \subsetneq \text{PSPACE}$$

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

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

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

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

שפה שלמה ביחס למחלקה: תהא \mathcal{C} קבוצה של שפות אזי שפה $\mathcal{L} \in \mathcal{C}$ באשר \mathcal{L} הינה \mathcal{C} -קשה.

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

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

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

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

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

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

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

טענה: CVAL הינה \mathcal{P} -שלמה.

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

הגדרה: $\text{TQBF} = \{\langle \varphi \rangle \mid (\varphi \text{ נוסחה מכומתת לחלוטין}) \wedge (\varphi \text{ ספיקה})\}$.

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

טענה: TQBF הינה PSPACE -שלמה.

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

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

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

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

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

טענה: succ-CVAL הינה $\mathcal{EXPTIME}$ -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: תהיינה $s, d : \mathbb{N} \rightarrow \mathbb{N}$ אזי $\text{u-AC}(s, d) = \left\{ L \subseteq \{0, 1\}^* \mid \begin{array}{l} L(C) = L \\ \text{Size}(C_n) \leq s(n) \\ \text{depth}(C_n) \leq d(n) \end{array} \text{ בעלת fan-in לא מוגבל עבורה} \right\}$.

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

הגדרה: תהינה $s, d : \mathbb{N} \rightarrow \mathbb{N}$ אזי קיימת משפחת מעגלים יוניפורמית C עבורה $\text{u-NC}(s, d) = \left\{ L \subseteq \{0, 1\}^* \mid \begin{array}{l} L(C) = L \\ \text{Size}(C_n) \leq s(n) \\ \text{depth}(C_n) \leq d(n) \end{array} \right\}$

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

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

טענה: תהא $S : \mathbb{N} \rightarrow \mathbb{N}$ יהי M מ"ט רץ בזמן S יהי $x \in \Sigma^*$ ותהא G מטריצה המייצגת את עץ הקונפיגורציות אזי $M(x)$ מקבלת $\iff (I + G)^{S(|x|)}_{x,y} \geq 1$ באשר y קונפיגורציה במצב מקבל.

השערה: קיימת מ"ט M הרצה בזמן פולינומי ובזיכרון $\mathcal{O}(n)$ עבורה לכל מטריצה A המייצגת גרף מכוון בעל n קודקודים ולכל קודקודים s, t מתקיים $\langle \langle A, s, t \rangle \rangle \iff M$ מקבלת \iff (קיים מסלול מ- s ל- t). השערה פתוחה

מודל PRAM: 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 (k, Π) מודל RAM ותהא (T, R, PC) קונפיגורציה במודל RAM 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 $i_1 \dots i_p \in [k]$ עבורם לכל $j \in [k] \setminus \{i_1 \dots i_p\}$ מתקיים $R'_j = R_j$ וכן קיימים $\pi_1 \dots \pi_p \in \Pi \cup \{\text{Id}\}$ עבורם לכל

$R'_{i_\ell} = \pi_{i_\ell}(R_{i_\ell})$ $\ell \in [p]$

• קיימים $i_1 \dots i_p \in \mathbb{N}$ עבורם לכל $j \in \mathbb{N} \setminus \{i_1 \dots i_p\}$ מתקיים $T'(j) = T(j)$ וכן קיימים $\pi_1 \dots \pi_p \in \Pi \cup \{\text{Id}\}$ עבורם לכל

$T'(\ell) = \pi(T(\ell))$ $\ell \in [p]$

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 $T : \mathbb{N} \rightarrow \mathbb{N}$ כך $T(n) = \begin{cases} x & n=0 \\ \text{else} \end{cases}$ אזי $\text{Start}_x = (T, \{0\}, 0)$

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

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

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

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

מקום ריצה במודל PRAM: יהי (p, k, Π) מודל PRAM יהי A אלגוריתם ויהי $x \in \mathbb{N}$ אזי $\max \left\{ \min \left\{ (A^{(i)}(\text{Start}_x))_1^{-1}[\{0\}] \mid i \in [A_{\text{stop}}] \right\} \right\}$

השערה: קיים מודל PRAM (p, k, Π) וקיים אלגוריתם A הפותר את CVAL בזמן $\text{polylog}(n)$ ובמקום $\text{poly}(n)$. השערה פתוחה

השערה: $\mathcal{P} = \text{NC}$

טענה: $\text{APSP} \in \text{NC}$

מכונת טיורינג בעלת אורקל: תהא $\mathcal{O} \subseteq \{0, 1\}^*$ תהא $Q \neq \emptyset$ קבוצה סופית ויהיו $q_{\text{query}}, q_{\text{yes}}, q_{\text{no}} \in Q$ אזי מ"ט דו-סרטיית $M^{\mathcal{O}}$

באשר $(M^{\mathcal{O}})_1 = Q$ 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 $c_0 \cap Q = \{q_{\text{yes}}\}$ אזי $c_0^2 \setminus Q \in \mathcal{O}$

- אם $c_0 \cap Q = \{q_{\text{no}}\}$ אזי $c_0^2 \setminus Q \notin \mathcal{O}$

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

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

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

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 עבודה קיימת מ"ט $M^{\mathcal{O}}$ שרצה בזמן $\text{poly}(n)$ באשר לכל $x \in \Sigma$ מתקיים $(x \in L) \iff$

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

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

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

טענה: קיימת $\mathcal{O} \subseteq \{0, 1\}^*$ עבורה $\mathcal{NP}^{\mathcal{O}} \neq \mathcal{P}^{\mathcal{O}}$.

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

הגדרה: תהא $T : \mathbb{N} \rightarrow \mathbb{N}$ ותהא $L \in \text{DTime}(T(n))$ ותהא f חח"ע חשיבה בזמן באשר $f(n) \geq n$ לכל $n \in \mathbb{N}$ אזי

$L_{\text{pad}}^f = \{x \mid |1^{f(|x|)-|x|-1}| \mid x \in L\}$.

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

מסקנה: $\mathcal{P}^{\mathcal{EXPTIME}} \neq \mathcal{EXPTIME}^{\mathcal{EXPTIME}}$.

הגדרה: $2\mathcal{EXPTIME} = \bigcup_{c=0}^{\infty} \text{DTime}(2^{2^{n^c}})$.

טענה: $\mathcal{EXPTIME}^{\mathcal{EXPTIME}} = 2\mathcal{EXPTIME}$.

טענה: אם $\mathcal{P} = \mathcal{NP}$ אזי $\mathcal{EXPTIME} = \mathcal{NEXPTIME}$.

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

טענה: $\text{E} \neq \mathcal{EXPTIME}$.

טענה: $\text{E} \neq \text{PSPACE}$.