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 $n\in\mathbb{N}_{\ge3}$ אזי $\vee_n:\{0,1\}^n\to\{0,1\}$ המוגדרת $\vee_n(x)=\bigvee_{i=1}^n x_i$.

הגדרה: יהי $n\in\mathbb{N}_{\ge3}$ אזי $\wedge_n:\{0,1\}^n\to\{0,1\}$ המוגדרת $\wedge_n(x)=\bigwedge_{i=1}^n x_i$.

מעגל בוליאני בעל fan-in לא מוגבל: מעגל בוליאני מעל בסיס הפונקציות הבוליאניות $\{\wedge,\vee,\neg\}\cup\left(\bigcup_{n\in\mathbb{N}}\{\vee_n\}\right)\cup\left(\bigcup_{n\in\mathbb{N}}\{\wedge_n\}\right)$.

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

טענה: תהא $f:\{0,1\}^n\to\{0,1\}$ אזי קיים מעגל בוליאני C בעל fan-in לא מוגבל המחשב את f בגודל $\mathcal{O}(n\cdot2^n)$ ובעומק 2.

טענה: תהא $f:\{0,1\}^n\to\{0,1\}$ אזי קיים מעגל בוליאני C המחשב את f בגודל $\mathcal{O}(n\cdot2^n)$ ובעומק $n+\log_2(n)$.

מסקנה: תהא L שפה אזי קיימת משפחת מעגלים $\mathcal{C}$ מגודל $\mathcal{O}(n\cdot2^n)$ ומעומק $n+\log(n)$ המחשבת את L.

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

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

טענה: יהי $n\in\mathbb{N}$ ותהא $f:\{0,1\}^n\to\{0,1\}$ אזי $\text{Size}(f)\le15\cdot(2^n-1)$.

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

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

משפט: קיים $C\in\mathbb{R}_+$ עבורו לכל $n\in\mathbb{N}$ ולכל $S:\mathbb{N}\to\mathbb{N}$ המקיימת $n\le S<C\cdot\frac{2^n}{n}$ קיימת $f:\{0,1\}^n\to\{0,1\}$ באשר f חשיבה על ידי מעגל מגודל $S(n)+10n$ וכן f לא חשיבה על ידי מעגל מגודל $S(n)$.

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

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

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

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

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

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

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

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

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

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

מסקנה: תהיינה $s,d:\mathbb{N}\to\mathbb{N}$ אזי $\text{NC}(s,d)\subseteq\text{AC}(s,d)$.

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

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

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

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

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

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

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

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

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

פולינום מחשב פונקציה בוליאנית בממוצע עם שגיאה ε: יהי $\varepsilon>0$ ותהא $f:\{0,1\}^n\to\{0,1\}$ אזי $p\in\mathbb{R}[x_1\ldots x_n]$ מ"ל עבורו $\mathbb{P}_{x\leftarrow\{0,1\}^n}(p(x)=f(x))\ge1-\varepsilon$.

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

התפלגות משפחת פולינומים מחשבת פונקציה בוליאנית עם שגיאה ε: יהי $\varepsilon>0$ ותהא $f:\{0,1\}^n\to\{0,1\}$ אזי קבוצת פולינומים מ"ל $P\subseteq\mathbb{R}[x_1\ldots x_n]$ עבורה לכל $x\in\{0,1\}^n$ מתקיים $\mathbb{P}_{p\leftarrow P}(p(x)=f(x))\ge1-\varepsilon$.

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

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

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

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

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

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

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

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

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

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

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

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

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

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