

אלפבית: קבוצה Σ המקיימת $0 < |\Sigma| < \aleph_0$.

מילים: יהי Σ אלפבית אזי $\Sigma^* = \bigcup_{n=0}^{\infty} \Sigma^n$.

אורך של מילה: יהי Σ אלפבית ותהא $w \in \Sigma^n$ מילה אזי $|w| = n$.

המילה הריקה: יהי Σ אלפבית אזי $\varepsilon \in \Sigma^*$ עבורה $|\varepsilon| = 0$.

היפוך מילה: תהא $\langle w_1 \dots w_n \rangle \in \Sigma^*$ אזי $\langle w_n \dots w_1 \rangle^R = \langle w_1 \dots w_n \rangle$.

שרשור מילים: תהיינה $\langle w_1 \dots w_n \rangle, \langle \omega_1 \dots \omega_m \rangle \in \Sigma^*$ אזי $\langle w_1 \dots w_n, \omega_1 \dots \omega_m \rangle = \langle w_1 \dots w_n \rangle \langle \omega_1 \dots \omega_m \rangle$.

חזקה של מילה: תהא $\langle w_1 \dots w_n \rangle \in \Sigma^*$ ויהי $m \in \mathbb{N}$ אזי $\langle w_1 \dots w_n \rangle^m = \prod_{i=1}^m \langle w_1 \dots w_n \rangle$.

מספר המופעים של אות במילה: תהא $w \in \Sigma^n$ ותהא $\sigma \in \Sigma$ אות אזי $\#_{\sigma}(w) = |\{i \in [n] \mid w_i = \sigma\}|$.

שפה: יהי Σ אלפבית אזי $L \subseteq \Sigma^*$.

היפוך שפה: תהא $L \subseteq \Sigma^*$ שפה אזי $L^R = \{w^R \mid w \in L\}$.

שרשור שפות: תהיינה $L_1, L_2 \subseteq \Sigma^*$ שפות אזי $L_1 \parallel L_2 = L_1 L_2 = \{w\omega \mid (w \in L_1) \wedge (\omega \in L_2)\}$.

חזקה של שפה: תהא $L \subseteq \Sigma^*$ שפה ויהי $m \in \mathbb{N}$ אזי $L^m = \left\{ \prod_{i=1}^m w_i \mid \forall i \in [m]. w_i \in L \right\}$.

סגור קליני של שפה: תהא $L \subseteq \Sigma^*$ שפה אזי $L^* = \bigcup_{k=0}^{\infty} L^k$.

שפת הרישא: תהא $L \subseteq \Sigma^*$ שפה אזי $\text{prefix}(L) = \{y \in \Sigma^* \mid \exists x \in \Sigma^*. yx \in L\}$.

שפת הסיפא: תהא $L \subseteq \Sigma^*$ שפה אזי $\text{suffix}(L) = \{y \in \Sigma^* \mid \exists x \in \Sigma^*. xy \in L\}$.

אלגוריתם מכריע שפה: תהא $L \subseteq \Sigma^*$ שפה אזי אלגוריתם $A : \Sigma^* \rightarrow \{\text{true}, \text{false}\}$ המקיים

• מקבל: לכל $x \in L$ מתקיים $A(x) = \text{true}$.

• דוחה: לכל $x \notin L$ מתקיים $A(x) = \text{false}$.

פונקציה בולאנית: תהא X קבוצה אזי $f : X \rightarrow \{0, 1\}$.

בסיס דה־מורגן: $B = \{\wedge, \vee, \neg\}$.

מעגל בוליאני: תהיינה $f_1 \dots f_n$ פונקציות בוליאניות ותהיינה $x_1 \dots x_m, y_1 \dots y_k \in \{0, 1\}$ אזי גרף מכוון G מעל

$\{f_1 \dots f_n, x_1 \dots x_m, y_1 \dots y_k\}$ המקיים

• G חסר מעגלים מכוונים.

• לכל $i \in [k]$ מתקיים $\deg^-(y_i) = 1$ וכן $\deg^+(y_i) = 0$.

• לכל $i \in [m]$ מתקיים $\deg^-(x_i) = 0$.

שער: יהי מעגל בוליאני אזי $f_1 \dots f_n$.

הערה: במעגל שער יכול להופיע במספר קודקודים שונים.

חוטים: יהי C מעגל בוליאני אזי $E(C)$.

fan-out: יהי C מעגל בולינארי אזי $\deg^+(v) = \max_{u \in V(C)} \deg^+(u)$.

נוחסאות: יהי C מעגל בולינארי אזי $\{G \leq C \mid 1 \text{ הוא } G \text{ של fan-out}\}$.

שערוד מעגל בולינארי על קלט: יהי C מעגל בולינאני ויהי $v \in \{0, 1\}^m$ אזי $(x_1 \dots x_m) = v$ וכן y_i הינו הפלט הנוצר מהפעלת

הפונקציות הבוליאניות על הקודקודים הנכנסים.

סימון: יהי C מעגל בולינאני ויהי $v \in \{0, 1\}^m$ אזי השערוד של C על v הוא $C(v) = (y_1 \dots y_k)$.

משפט אוניברסליות דה־מורגן: תהא $f : \{0, 1\}^m \rightarrow \{0, 1\}^k$ אזי קיים מעגל בולינאני C עבורו לכל $v \in \{0, 1\}^m$ מתקיים

$C(v) = f(v)$.

משפחה של מעגלים: מעגלים בולינאניים $\{C_n\}_{n \in \mathbb{N}}$ עבורם C_i מקבל קלט באורך i .

משפחה מכריעה שפה: תהא $L \subseteq \Sigma^*$ שפה אזי משפחה של מעגלים $\{C_n\}_{n \in \mathbb{N}}$ עבורה C_n מכריעה את Σ^n .

מודל לא יוניפורמי: משפחה של מעגלים $\{C_n\}_{n \in \mathbb{N}}$ עבורה לכל $n \in \mathbb{N}$ יש אלגוריתם שונה.

מודל יוניפורמי: משפחה של מעגלים $\{C_n\}_{n \in \mathbb{N}}$ עבורה לכל $n \in \mathbb{N}$ יש אלגוריתם זהה.

גודל מעגל: יהי מעגל בולינאני C אזי $|C|$ מספר השערים ב־ C .

חסם עליון לגודל משפחת מעגלים: תהא $\{C_n\}_{n \in \mathbb{N}}$ משפחה של מעגלים אזי $S : \mathbb{N} \rightarrow \mathbb{N}$ עבורה $|C_n| \leq S(n)$.

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

טענה: תהא $f : \{0, 1\}^n \rightarrow \{0, 1\}$ אזי קיים מעגל C שמחשב את f בגודל $\mathcal{O}(2^n)$.

משפט לופיאנוב: תהא $f : \{0, 1\}^n \rightarrow \{0, 1\}$ אזי קיים מעגל C שמחשב את f בגודל $\mathcal{O}\left(\frac{2^n}{n}\right)$. לא הוכח בקורס

טענה שאנון: קיים $n \in \mathbb{N}$ עבורו קיימת $f : \{0, 1\}^n \rightarrow \{0, 1\}$ שאינה ניתנת לחישוב בעזרת מעגל C בגודל קטן מאשר $\frac{2^n}{10n}$.