

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

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

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

**המילה הריקה:** יהי  $\Sigma$  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  $\Sigma$  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  $L^m = \left\{ \prod_{i=1}^m w_i \mid \forall i \in [k]. w_i \in L \right\}$ .

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

**שפת הרישוא:** 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 בוליאנית:** תהיינה  $n, m \in \mathbb{N}$  אזי  $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$ .

**בסיס פונקציות בוליאניות:** תהיינה  $f_1 \dots f_n$  פונקציות בוליאניות אזי  $\{f_1 \dots f_n\}$ .

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

**הערה:** תמיד נוסיף לבסיס את הפונקציות הקבועות.

**מעגל בוליאני:** יהי  $\mathcal{B}$  בסיס פונקציות בוליאניות תהיינה  $k_1 \dots k_n \in \mathbb{N}_+$  תהיינה  $f_1 \dots f_n \in \mathcal{B}$  באשר  $f_i : \{0, 1\}^{k_i} \rightarrow \{0, 1\}$  לכל

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

• לכל  $i \in [n]$  מתקיים  $\deg^-(f_i) = k_i$ .

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

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

**חוטים:** יהי  $C$  מעגל בוליאני אזי  $E(C)$ .

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

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

**שערוך 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 השערוך של  $C$  על  $v$  הוא  $C(v) = (y_1 \dots y_k)$ .

**מעגל מקבל מילה:** יהי  $C$  מעגל בעל פלט יחיד אזי  $w \in \{0, 1\}^n$  עבורו  $C(w) = 1$ .

**שפה של מעגל:** יהי  $C$  מעגל בעל פלט יחיד אזי  $C$  מקבל את  $x \in \{0, 1\}^n$  אזי  $L(C) = \{x \in \{0, 1\}^n \mid C(x) = 1\}$ .

**מעגל מחשב פונקציה:** תהא  $f : \{0, 1\}^n \rightarrow \{0, 1\}$  אזי מעגל בולינאני  $C$  עבורו לכל  $v \in \{0, 1\}^n$  מתקיים  $C(v) = f(v)$ .

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

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

**הערה:** מכאן והלאה כל המעגלים הם בולינאניים ומעל בסיס דה־מורגן.

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

**שפה של משפחת מעגלים:** תהא  $\mathcal{C}$  משפחה של מעגלים אזי  $L(\mathcal{C}) = \{x \in \{0, 1\}^* \mid x \in L(C_{|x|})\}$ .

**משפחה מכריעה שפה:** תהא  $\mathcal{L} \subseteq \{0, 1\}^*$  שפה אזי משפחה של מעגלים  $\mathcal{C}$  עבורה  $L(\mathcal{C}) = \mathcal{L}$ .

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

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

**גודל מעגל:** יהי מעגל בוליאני  $C$  אזי  $|C|$  מספר השערים ב- $C$ .

**חסם עליון לגודל משפחת מעגלים:** תהא  $\mathcal{C}$  משפחה של מעגלים אזי  $S : \mathbb{N} \rightarrow \mathbb{N}$  עבורה  $|\mathcal{C}_n| \leq S(n)$ .

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

**מסקנה:** תהא  $\mathcal{L} \subseteq \{0, 1\}^n$  אזי קיים מעגל  $C$  עבורו  $L(C) = \mathcal{L}$  וכן  $|C| = \mathcal{O}(n \cdot 2^n)$ .

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

**מסקנה:** תהא  $\mathcal{L} \subseteq \{0, 1\}^n$  אזי קיים מעגל  $C$  עבורו  $L(C) = \mathcal{L}$  וכן  $|C| = \mathcal{O}(2^n)$ .

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

**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  $\frac{2^n}{10n}$ .

**אוטומט סופי דטרמיניסטי (אס"ד):** תהא  $Q \neq \emptyset$  קבוצה סופית יהי  $\Sigma$  אלפבית תהא  $\delta : Q \times \Sigma \rightarrow Q$  ויהי  $q \in Q$  ותהא  $F \subseteq Q$  אזי  $(Q, \Sigma, \delta, q, F)$ .

**מצבים באוטומט סופי דטרמיניסטי:** יהי  $(Q, \Sigma, \delta, q, F)$  אס"ד אזי  $Q$ .

**אלפבית באוטומט סופי דטרמיניסטי:** יהי  $(Q, \Sigma, \delta, q, F)$  אס"ד אזי  $\Sigma$ .

**פונקציית מעברים באוטומט סופי דטרמיניסטי:** יהי  $(Q, \Sigma, \delta, q, F)$  אס"ד אזי  $\delta$ .

**מצב התחלתי באוטומט סופי דטרמיניסטי:** יהי  $(Q, \Sigma, \delta, q, F)$  אס"ד אזי  $q$ .

**מצבים מקבלים באוטומט סופי דטרמיניסטי:** יהי  $(Q, \Sigma, \delta, q, F)$  אס"ד אזי  $F$ .

**פונקציית המעברים המורחבת:** יהי  $(Q, \Sigma, \delta, q_0, F)$  אס"ד אזי  $\hat{\delta} : Q \times \Sigma^* \rightarrow Q$  עבורה לכל  $q \in Q$  מתקיים  $\hat{\delta}(q, \varepsilon) = q$  וכן לכל  $x \in \Sigma^n$  מתקיים  $\hat{\delta}(q, x) = \delta(\hat{\delta}(q, x_1 \dots x_{n-1}), x_n)$ .

**אוטומט סופי דטרמיניסטי מקבל מילה:** יהי  $(Q, \Sigma, \delta, q_0, F)$  אס"ד אזי  $x \in \Sigma^*$  המקיים  $\hat{\delta}(q_0, x) \in F$ .

**טענה:** יהי  $A$  אס"ד ויהי  $x \in \Sigma^n$  אזי  $(A$  מקבל את  $x) \iff (x$  קיימים  $q_1 \dots q_n \in Q$  עבורם  $\delta(q_{i-1}, x_i) = q_i$  לכל  $i \in [n]$  וכן  $q_n \in F)$ .

**שפה של אוטומט סופי דטרמיניסטי:** יהי  $A$  אס"ד אזי  $L(A) = \{x \in \Sigma^* \mid x \text{ מקבל את } A\}$ .

**שפה רגולרית:** יהי  $\Sigma$  אלפבית אזי שפה  $\mathcal{L} \subseteq \Sigma^*$  עבורה קיים אס"ד  $A$  המקיים  $L(A) = \mathcal{L}$ .

**טענה:**  $\emptyset$  רגולרית.

**טענה:**  $\{\varepsilon\}$  רגולרית.

**טענה:**  $\{x \mid \#_1(x) = 1 \pmod{2}\}$  רגולרית.

**טענה:**  $\{y 1 0^{2k} \mid (y \in \{0, 1\}^*) \wedge (k \in \mathbb{N})\}$  רגולרית.

**טענה:** יהיו  $L_1, L_2, L_3 \subseteq \Sigma^*$  שפות אזי  $L_1(L_2L_3) = (L_1L_2)L_3$ .

**טענה:** תהא  $L \subseteq \Sigma^*$  שפה באשר  $L \neq \emptyset$  וכן  $L \neq \{\varepsilon\}$  אזי  $L^*$  אינסופית.

**משפט:** תהינה  $L, \mathcal{L} \subseteq \Sigma^*$  שפות רגולריות אזי

•  $L \cup \mathcal{L}$  רגולרית.

•  $L \cap \mathcal{L}$  רגולרית.

•  $\bar{L}$  רגולרית.

•  $L \parallel \mathcal{L}$  רגולרית.

• לכל  $n \in \mathbb{N}$  מתקיים כי  $L^n$  רגולרית.

•  $L^*$  רגולרית.

**מסקנה:**  $\{x \mid \#_1(x) = 0 \pmod{2}\}$  רגולרית.

**אוטומט סופי לא-דטרמיניסטי מינוס (אסלד"ם):** תהא  $Q \neq \emptyset$  קבוצה סופית יהי  $\Sigma$  אלפבית תהא  $\delta : Q \times \Sigma \rightarrow \mathcal{P}(Q)$  ותהינה  $S, F \subseteq Q$  אזי  $(Q, \Sigma, \delta, S, F)$ .

**מצבים באוטומט סופי לא-דטרמיניסטי מינוס:** יהי  $(Q, \Sigma, \delta, S, F)$  אסלד"ם אזי  $Q$ .

**אלפבית באוטומט סופי לא-דטרמיניסטי מינוס:** יהי  $(Q, \Sigma, \delta, S, F)$  אסלד"ם אזי  $\Sigma$ .

**פונקציית מעברים באוטומט סופי לא-דטרמיניסטי מינוס:** יהי  $(Q, \Sigma, \delta, S, F)$  אסלד"ם אזי  $\delta$ .

**מצבים התחלתיים באוטומט סופי לא-דטרמיניסטי מינוס:** יהי  $(Q, \Sigma, \delta, S, F)$  אסלד"ם אזי  $S$ .

**מצבים מקבלים באוטומט סופי לא-דטרמיניסטי מינוס:** יהי  $(Q, \Sigma, \delta, S, F)$  אסלד"ם אזי  $F$ .

**פונקציית המעברים המורחבת:** יהי  $(Q, \Sigma, \delta, S, F)$  אסלד"ם אזי  $\hat{\delta} : \mathcal{P}(Q) \times \Sigma^* \rightarrow \mathcal{P}(Q)$  עבורה לכל  $T \subseteq Q$  מתקיים  $\hat{\delta}(T, \varepsilon) = T$  וכן לכל  $x \in \Sigma^n$  מתקיים  $\hat{\delta}(q, x) = \bigcup_{q \in \hat{\delta}(T, x_1 \dots x_{n-1})} \delta(q, x_n)$ .

**אוטומט סופי לא-דטרמיניסטי מינוס מקבל מילה:** יהי  $(Q, \Sigma, \delta, S, F)$  אסלד"ם אזי  $x \in \Sigma^*$  המקיים  $\hat{\delta}(S, x) \cap F \neq \emptyset$ .  
**טענה:** יהי  $M$  אסלד"ם ויהי  $x \in \Sigma^n$  אזי  $(M \text{ מקבל את } x) \iff (x \text{ קיימים } q_0 \dots q_n \in Q \text{ עבורם } q_0 \in S \text{ וכן } q_i \in \delta(q_{i-1}, x_i) \text{ לכל } i \in [n] \text{ וכן } q_n \in F)$ .

**שפה של אוטומט סופי לא-דטרמיניסטי מינוס:** יהי  $M$  אסלד"ם אזי  $L(M) = \{x \in \Sigma^* \mid x \text{ מקבל את } M\}$ .  
**אוטומט סופי דטרמיניסטי מינוס החזקה:** יהי  $M = (Q, \Sigma, \delta, S, F)$  אסלד"ם אזי אסלד"ד  $(Q', \Sigma, \delta', q_0, F')$  באשר

$$Q' = \mathcal{P}(Q) \bullet$$

$$\delta'(T, x) = \bigcup_{q \in T} \delta(q, x) \bullet$$

$$q_0 = S \bullet$$

$$F' = \{T \subseteq Q \mid T \cap F \neq \emptyset\} \bullet$$

**למה:** יהי  $M$  אסלד"ם יהי  $A$  אסלד"ד החזקה של  $M$  תהא  $T \subseteq Q_N$  ויהי  $x \in \Sigma^*$  אזי  $\hat{\delta}_A(T, x) = \hat{\delta}_M(T, x)$

**משפט:** יהי  $M$  אסלד"ם אזי קיים אסלד"ד  $A$  עבורו  $L(M) = L(A)$

**סימון:** יהי  $\Sigma$  אלפבית אזי  $\Sigma_\varepsilon = \Sigma \cup \{\varepsilon\}$

**אוטומט סופי לא-דטרמיניסטי (אסלד"ד):** תהא  $Q \neq \emptyset$  קבוצה סופית יהי  $\Sigma$  אלפבית תהא  $\delta : Q \times \Sigma_\varepsilon \rightarrow \mathcal{P}(Q)$  ותהיינה  $S, F \subseteq Q$  אזי  $(Q, \Sigma, \delta, S, F)$

**מצבים באוטומט סופי לא-דטרמיניסטי:** יהי  $(Q, \Sigma, \delta, S, F)$  אסלד"ד אזי  $Q$

**אלפבית באוטומט סופי לא-דטרמיניסטי:** יהי  $(Q, \Sigma, \delta, S, F)$  אסלד"ד אזי  $\Sigma$

**פונקציית מעברים באוטומט סופי לא-דטרמיניסטי:** יהי  $(Q, \Sigma, \delta, S, F)$  אסלד"ד אזי  $\delta$

**מצבים התחלתיים באוטומט סופי לא-דטרמיניסטי:** יהי  $(Q, \Sigma, \delta, S, F)$  אסלד"ד אזי  $S$

**מצבים מקבלים באוטומט סופי לא-דטרמיניסטי:** יהי  $(Q, \Sigma, \delta, S, F)$  אסלד"ד אזי  $F$

**סביבת  $\varepsilon$ :** יהי  $N$  אסלד"ד ויהי  $q \in Q$  אזי  $E(q) = \{q' \in Q \mid \exists a \in Q^{k+1}. (a_0 = q) \wedge (\forall i \in [k]. a_i \in \delta(a_{i-1}, \varepsilon)) \wedge (a_k = q')\}$

**סביבת  $\varepsilon$ :** יהי  $N$  אסלד"ד ויהי  $T \subseteq Q$  אזי  $E(T) = \bigcup_{q \in T} E(q)$

**פונקציית המעברים המורחבת:** יהי  $(Q, \Sigma, \delta, S, F)$  אסלד"ד אזי  $\hat{\delta} : \mathcal{P}(Q) \times \Sigma^* \rightarrow \mathcal{P}(Q)$  עבורה לכל  $T \subseteq Q$  מתקיים

$$\hat{\delta}(T, \varepsilon) = E(T) \text{ וכן לכל } x \in \Sigma^n \text{ מתקיים } \hat{\delta}(T, x) = E\left(\bigcup_{q \in \hat{\delta}(T, x_1 \dots x_{n-1})} \delta(q, x_n)\right)$$

**אוטומט סופי לא-דטרמיניסטי מקבל מילה:** יהי  $(Q, \Sigma, \delta, S, F)$  אסלד"ד אזי  $x \in \Sigma^*$  המקיים  $\hat{\delta}(S, x) \cap F \neq \emptyset$

**סימון:** יהי  $x \in \Sigma^*$  יהיו  $\sigma_1 \dots \sigma_n \in \Sigma \setminus \{\varepsilon\}$  ויהיו  $k_0 \dots k_n \in \mathbb{N}$  עבורם  $x = \varepsilon^{k_0} \sigma_0 \varepsilon^{k_1} \sigma_1 \varepsilon^{k_2} \dots \sigma_n \varepsilon^{k_n}$  אזי  $x^\# = \sigma_1 \dots \sigma_n$

**טענה:** יהי  $A$  אסלד"ד ויהי  $x \in \Sigma^n$  אזי  $(A \text{ מקבל את } x) \iff (x \text{ קיימים } q_0 \dots q_n \in Q \text{ עבורם } q_0 \in S \text{ וכן } q_i \in \delta(q_{i-1}, x_i^\#) \text{ לכל } i \in [n] \text{ וכן } q_n \in F)$

**שפה של אוטומט סופי לא-דטרמיניסטי:** יהי  $A$  אסלד"ד אזי  $L(A) = \{x \in \Sigma^* \mid x \text{ מקבל את } A\}$

**משפט:** יהי  $N$  אסלד"ד אזי קיים אסלד"ם  $M$  עבורו  $L(N) = L(M)$

**מסקנה:** יהי  $N$  אסלד"ד אזי קיים אסלד"ד  $A$  עבורו  $L(A) = L(N)$

**מסקנה:** יהי  $\Sigma$  אלפבית ותהא  $\Sigma^*$  שפה  $\mathcal{L} \subseteq \Sigma^*$  אזי  $(\mathcal{L} \text{ רגולרית}) \iff (x \text{ קיים אסלד"ד } N \text{ המקיים } L(N) = \mathcal{L})$

**ביטוי רגולרי (ב"ר):** יהי  $\Sigma$  אלפבית אזי

$$\emptyset \bullet$$

$$a \text{ יהי } a \in \Sigma_\varepsilon \bullet$$

$$R_1, R_2 \text{ ביטויים רגולריים אזי } R_1 \cup R_2 \bullet$$

$$R_1, R_2 \text{ ביטויים רגולריים אזי } R_1 R_2 \bullet$$

$$R \text{ ביטוי רגולרי אזי } R^* \bullet$$

**שפה נוצרת מביטוי רגולרי:** יהי  $\Sigma$  אלפבית אזי

$$L(\emptyset) = \emptyset \bullet$$

$$a \in \Sigma_\varepsilon \text{ אזי } L(a) = \{a\} \bullet$$

$$R_1, R_2 \text{ ביטויים רגולריים אזי } L(R_1 \cup R_2) = L(R_1) \cup L(R_2) \bullet$$

$$R_1, R_2 \text{ ביטויים רגולריים אזי } L(R_1 R_2) = L(R_1) L(R_2) \bullet$$

$$R \text{ ביטוי רגולרי אזי } L(R^*) = L(R)^* \bullet$$

**סימון:** יהי  $\Sigma$  אלפבית אזי  $\{r \in \Sigma^* \mid r \text{ ביטוי רגולרי}\} = R(\Sigma)$

**הערה:** קיים סדר פעולות לביטויים רגולריים

- סגור קליני.
- שרשור.
- איחוד.

**משפט:** יהי  $\Sigma$  אלפבית ותהא  $\mathcal{L} \subseteq \Sigma^*$  שפה אזי  $(\mathcal{L} \text{ רגולרית}) \iff$  (קיים  $r \in R(\Sigma)$  עבורו  $(L(r) = \mathcal{L})$ ).

**שפה ניתנת לניפוח:** שפה  $\mathcal{L}$  וקבוע  $\ell > 0$  עבורם לכל  $w \in \mathcal{L}$  באשר  $|w| \leq \ell$  קיימים  $x, y, z \in \Sigma^*$  באשר  $|y| > 0$  וכן  $|xy| \leq \ell$  וכן  $w = xyz$  וכן  $xy^kz \in \mathcal{L}$  מתקיים  $k \in \mathbb{N}$  לכל  $k$ .

**טענה למת הניפוח:** תהא  $\mathcal{L}$  שפה רגולרית אזי קיים  $\ell > 0$  עבורו  $\mathcal{L}$  ניתנת לניפוח  $\ell$ .

**קבוע הניפוח:** תהא  $\mathcal{L}$  שפה רגולרית אזי  $\min \{ \ell \in \mathbb{N}_+ \mid \mathcal{L} \text{ ניתנת לניפוח } \ell \}$ .

**טענה:**  $\{x \in \{0, 1\}^* \mid \#_0(x) = \#_1(x)\}$  אינה רגולרית.

**טענה:**  $\{0^i 1^j \mid i > j\}$  אינה רגולרית.

**טענה:**  $\{a^p \mid a \in \Sigma, p \text{ ראשוני}\}$  אינה רגולרית.

**טענה:** השפה  $\{a^i b^n c^n \mid n \in \mathbb{N}, i \in \mathbb{N}_+\} \cup \{b^n c^n \mid n, m \in \mathbb{N}\}$  ניתנת לניפוח 1 וכן אינה רגולרית.

**הגדרה:** תהא  $L \subseteq \Sigma^*$  שפה אזי  $\sim_L = \{(x, y) \in (\Sigma^*)^2 \mid \forall z \in \Sigma^*. (yz \in L) \iff (xz \in L)\}$ .

**טענה:** תהא  $L \subseteq \Sigma^*$  שפה אזי  $\sim_L$  הינו יחס שקילות.

**הגדרה:** יהי  $A$  אס"ד אזי  $\sim_A = \{(x, y) \in (\Sigma^*)^2 \mid \hat{\delta}(q_0, x) = \hat{\delta}(q_0, y)\}$ .

**טענה:** יהי  $A$  אס"ד ויהיו  $x, y \in \Sigma^*$  עבורם  $x \sim_A y$  אזי  $x \sim_{L(A)} y$ .

**מסקנה:** יהי  $A$  אס"ד אזי  $|\Sigma^*/\sim_A| \geq |\Sigma^*/\sim_{L(A)}|$ .

**מסקנה:** תהא  $L \subseteq \Sigma^*$  שפה רגולרית אזי  $\Sigma^*/\sim_L$  סופית.

**משפט מייהל-נרוד:** תהא  $L \subseteq \Sigma^*$  שפה אזי  $(L \text{ רגולרית}) \iff (\Sigma^*/\sim_L \text{ סופית})$ .

**סימון:** תהא  $L \subseteq \Sigma^*$  שפה באשר  $\Sigma^*/\sim_L$  סופית תהא  $\{x_1 \dots x_n\}$  קבוצת נציגים של  $\Sigma^*/\sim_L$  ויהי  $y \in \Sigma^*$  עבורו  $y \sim_L x_i$  אזי  $\text{Class}(y) = i$ .

**אוטומט סופי דטרמיניסטי המחלקות:** תהא  $L \subseteq \Sigma^*$  שפה באשר  $\Sigma^*/\sim_L$  סופית ותהא  $\{x_1 \dots x_n\}$  קבוצת נציגים של  $\Sigma^*/\sim_L$  אזי אס"ד

$(Q, \Sigma, \delta, q_0, F)$  באשר

•  $Q = |\Sigma^*/\sim_L|$ .

•  $\delta(i, \sigma) = \text{Class}(x_i \sigma)$ .

•  $q_0 = \text{Class}(\varepsilon)$ .

•  $F = \{i \in Q \mid x_i \in L\}$ .

**טענה:** תהא  $L \subseteq \Sigma^*$  שפה באשר  $\Sigma^*/\sim_L$  סופית תהא  $\{x_1 \dots x_n\}$  קבוצת נציגים של  $\Sigma^*/\sim_L$  יהי  $A$  אס"ד המחלקות של  $L$  ויהי  $\hat{\delta}_A(q_0, y) = \text{Class}(y)$  אזי  $y \in \Sigma^*$ .

**טענה:** יהי  $n \in \mathbb{N}_+$  אזי קיים אס"ד  $N$  מעל  $[n]$  באשר  $|Q| = n$  עבורו  $L(N) = \{x \in [n]^* \mid \exists \sigma \in \Sigma. \#_\sigma(x) = 0\}$ .

**טענה:** יהי  $n \in \mathbb{N}_+$  ויהי  $A$  אס"ד מעל  $[n]$  עבורו  $L(A) = \{x \in [n]^* \mid \exists \sigma \in \Sigma. \#_\sigma(x) = 0\}$  אזי  $|Q| \geq 2^n$ .

**מכונת טיורינג (מ"ט):** תהא  $Q \neq \emptyset$  קבוצה סופית יהי  $\Sigma$  אלפבית יהי  $\Gamma$  אלפבית עבורו  $\Sigma \subseteq \Gamma$  וכן  $\sqcup \in \Gamma \setminus \Sigma$  יהיו  $q_0, q_a, q_r \in Q$  באשר  $q_a \neq q_r$  ותהא  $\delta : (Q \setminus \{q_a, q_r\}) \times \Gamma \rightarrow Q \times \Gamma \times \{L, R\}$  אזי  $(Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r)$ .

**מצבים במכונת טיורינג:** תהא  $(Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r)$  מ"ט אזי  $Q$ .

**אלפבית במכונת טיורינג:** תהא  $(Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r)$  מ"ט אזי  $\Sigma$ .

**אלפבית סרט במכונת טיורינג:** תהא  $(Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r)$  מ"ט אזי  $\Gamma$ .

**פונקציית מעברים במכונת טיורינג:** תהא  $(Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r)$  מ"ט אזי  $\delta$ .

**מצב התחלתי במכונת טיורינג:** תהא  $(Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r)$  מ"ט אזי  $q_0$ .

**מצב מקבל במכונת טיורינג:** תהא  $(Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r)$  מ"ט אזי  $q_a$ .

**מצב דוחה במכונת טיורינג:** תהא  $(Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r)$  מ"ט אזי  $q_r$ .

**קונפיגורציה:** תהא  $M$  מ"ט אזי  $c \in \Gamma^* Q \Gamma^*$ .

**קונפיגורציה התחלתית:** תהא  $M$  מ"ט אזי קונפיגורציה  $c \in \Gamma^* Q \Gamma^*$  עבורה קיים  $v \in \Sigma^*$  המקיימת  $c = q_0 v$ .

**קונפיגורציה מקבלת:** תהא  $M$  מ"ט אזי קונפיגורציה  $c \in \Gamma^* Q \Gamma^*$  עבורה קיימים  $u, v \in \Sigma^*$  המקיימים  $c = u q_a v$ .

**קונפיגורציה דוחה:** תהא  $M$  מ"ט אזי קונפיגורציה  $c \in \Gamma^* Q \Gamma^*$  עבורה קיימים  $u, v \in \Sigma^*$  המקיימים  $c = u q_r v$ .

**הערה:** תהא  $M$  מ"ט ותהא  $c$  קונפיגורציה אזי נזהה את  $\sqcup$  עם  $c$ .

**קונפיגורציה עוברת/צעד:** תהא  $M$  מ"ט תהא  $c$  קונפיגורציה אזי קונפיגורציה  $c'$  המקיימת אחד הבאים

- קיימים  $a, b, b' \in \Gamma$  וקיימים  $u, v \in \Gamma^*$  וקיימים  $q, q' \in Q$  עבורם  $c = uaqbv$  וכן  $\delta(q, b) = (q', b', L)$  וכן  $c' = uq'ab'v$ .
- קיימים  $b, b' \in \Gamma$  וקיימים  $u, v \in \Gamma^*$  וקיימים  $q, q' \in Q$  עבורם  $c = qbv$  וכן  $\delta(q, b) = (q', b', L)$  וכן  $c' = q'b'v$ .
- קיימים  $b, b' \in \Gamma$  וקיימים  $u, v \in \Gamma^*$  וקיימים  $q, q' \in Q$  עבורם  $c = uqbv$  וכן  $\delta(q, b) = (q', b', R)$  וכן  $c' = ub'q'v$ .

**מכונת טיורינג מקבלת מילה:** תהא  $M$  מ"ט אזי  $x \in \Sigma^*$  עבורו קיימים  $c_0 \dots c_n$  קונפיגורציות באשר  $c_0 = q_0x$  וכן  $c_{i-1}$  עוברת ל- $c_i$  לכל  $i \in [n]$  וכן  $c_n$  קונפיגורציה מקבלת.

**מכונת טיורינג דוחה מילה:** תהא  $M$  מ"ט אזי  $x \in \Sigma^*$  עבורו קיימים  $c_0 \dots c_n$  קונפיגורציות באשר  $c_0 = q_0x$  וכן  $c_{i-1}$  עוברת ל- $c_i$  לכל  $i \in [n]$  וכן  $c_n$  קונפיגורציה דוחה.

**שפה של מכונת טיורינג:** תהא  $M$  מ"ט אזי  $\{x \in \Sigma^* \mid x \text{ מקבל את } M\}$   $L(M)$ .

**מכונת טיורינג לא עוצרת על קלט:** תהא  $M$  מ"ט אזי  $x \in \Sigma^*$  עבורו  $M$  לא מקבלת ולא דוחה את  $x$ .

**מודלים שקולים:** מודלים  $M, M'$  עבורם לכל  $A$  מסוג  $M$  וכן לכל  $B$  מסוג  $M'$  מתקיים

- קיימת  $A'$  מסוג  $M'$  המקיימת  $L(A) = L(A')$ .
- קיימת  $B'$  מסוג  $M$  המקיימת  $L(B) = L(B')$ .

**מסקנה:** אס"ד, אסל"ד ואסלד"ס הינם מודלים שקולים.

**מכונת טיורינג נחה:** תהא  $Q \neq \emptyset$  קבוצה סופית יהי  $\Sigma$  אלפבית יהי  $\Gamma$  אלפבית עבורו  $\Sigma \subseteq \Gamma$  וכן  $\sqcup \in \Gamma \setminus \Sigma$  יהיו  $q_0, q_a, q_r \in Q$  באשר  $q_a \neq q_r$  ותהא  $\delta : (Q \setminus \{q_a, q_r\}) \times \Gamma \rightarrow Q \times \Gamma \times \{L, R, S\}$  אזי  $\delta : (Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r)$ .  
**הערה:** את כל הפעולות ממכונת טיורינג נכליל בצורה הטבעית עבור מכונת טיורינג נחה.

**מסקנה:** מכונת טיורינג ומכונת טיורינג נחה הינן מודלים שקולים.

**מכונת טיורינג רב-סרטית:** יהי  $k \in \mathbb{N}_+$  תהא  $Q \neq \emptyset$  קבוצה סופית יהי  $\Sigma$  אלפבית יהי  $\Gamma$  אלפבית עבורו  $\Sigma \subseteq \Gamma$  וכן  $\sqcup \in \Gamma \setminus \Sigma$  יהיו  $q_0, q_a, q_r \in Q$  באשר  $q_a \neq q_r$  ותהא  $\delta : (Q \setminus \{q_a, q_r\}) \times \Gamma^k \rightarrow Q \times \Gamma^k \times \{L, R\}^k$  אזי  $\delta : (k, Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r)$ .  
**הערה:** את כל הפעולות ממכונת טיורינג נכליל בצורה הטבעית עבור מכונת טיורינג רב-סרטית.

**קונפיגורציה במכונת טיורינג רב-סרטית:** תהא  $M$  מ"ט רב-סרטית ותהינה  $c_1 \dots c_k \in \Gamma^* Q \Gamma^*$  אזי  $c_1 \$ c_2 \$ \dots \$ c_k$ .

**קונפיגורציה התחלתית במכונת טיורינג רב-סרטית:** תהא  $M$  מ"ט רב-סרטית אזי קונפיגורציה  $c$  עבורה קיים  $v \in \Sigma^*$  המקיימת  $c = q_0 v \sqcup \$ q_0 \sqcup \$ \dots \$ q_0 \sqcup$ .

**מסקנה:** יהי  $k \in \mathbb{N}_+$  אזי מכונת טיורינג ומכונת טיורינג רב-סרטית הינן מודלים שקולים.

**מודל RAM:** יהי  $k \in \mathbb{N}$  ותהינה  $\pi_1 \dots \pi_p$  אזי  $(k, (\pi_1 \dots \pi_p))$ .

**מספר הרגיסטרים במודל RAM:** יהי  $(k, \Pi)$  מודל RAM אזי  $k$ .

**פקודות במודל RAM:** יהי  $(k, \Pi)$  מודל RAM אזי  $\Pi$ .

**קונפיגורציה במודל RAM:** יהי  $(k, \Pi)$  מודל RAM אזי  $PC \in \mathbb{N}$  וכן  $R_0 \dots R_k \in \mathbb{N}$  וכן  $T : \mathbb{N} \rightarrow \mathbb{N}$ .

**מונה התוכנית בקונפיגורציה:** יהי  $(k, \Pi)$  מודל RAM ותהא  $(T, R, PC)$  קונפיגורציה אזי  $PC$ .

**רגיסטרים בקונפיגורציה:** יהי  $(k, \Pi)$  מודל RAM ותהא  $(T, R, PC)$  קונפיגורציה אזי  $R$ .

**זיכרון בקונפיגורציה:** יהי  $(k, \Pi)$  מודל RAM ותהא  $(T, R, PC)$  קונפיגורציה אזי  $T$ .

**הערה:** ריצת מודל RAM זהה לריצת מעבד MIPS.

**טענה:** מכונת טיורינג ומודל RAM הם מודלים שקולים.

**מכונת טיורינג לא-דטרמיניסטית (מטל"ד):** תהא  $Q \neq \emptyset$  קבוצה סופית יהי  $\Sigma$  אלפבית יהי  $\Gamma$  אלפבית עבורו  $\Sigma \subseteq \Gamma$  וכן  $\sqcup \in \Gamma \setminus \Sigma$  יהיו  $q_0, q_a, q_r \in Q$  באשר  $q_a \neq q_r$  ותהא  $\delta : (Q \setminus \{q_a, q_r\}) \times \Gamma \rightarrow \mathcal{P}(Q \times \Gamma \times \{L, R\})$  אזי  $\delta : (Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r)$ .  
**קונפיגורציה עוברת:** תהא  $N$  מטל"ד תהא  $q \in Q$  ותהא  $b \in \Gamma$  ותהינה  $u, v \in \Gamma^*$  באשר  $uqbv$  קונפיגורציה אזי קונפיגורציה  $c'$  עבורה קיימת  $\delta' : (Q \setminus \{q_a, q_r\}) \times \Gamma \rightarrow Q \times \Gamma \times \{L, R\}$   $\delta' : (q, b) \in \delta(q, b)$  וכן  $uqbv$  הינה  $\delta'$ -עוברת ל- $c'$ .  
**עץ חישוב:** תהא  $N$  מטל"ד ויהי  $x \in \Sigma^*$  אזי עץ קונפיגורציות  $T_{N,x}$  עם שורש  $q_0 \sqcup$  עבורו לכל  $c, c'$  קונפיגורציות מתקיים  $c$  צאצא של  $c' \iff (c' \text{ עוברת ל-} c)$ .

**מכונת טיורינג לא-דטרמיניסטית מקבלת מילה:** תהא  $N$  מטל"ד אזי  $x \in \Sigma^*$  עבורו קיים עלה מקבל ב- $T_{N,x}$ .

**מכונת טיורינג לא-דטרמיניסטית דוחה מילה:** תהא  $N$  מטל"ד אזי  $x \in \Sigma^*$  עבורו  $T_{N,x}$  סופי וכן  $x$  אינו מתקבל על ידי  $N$ .

**שפה של מכונת טיורינג לא-דטרמיניסטית:** תהא  $N$  מטל"ד אזי  $\{x \in \Sigma^* \mid x \text{ מקבל את } N\}$   $L(N)$ .

**מכונת טיורינג לא-דטרמיניסטית לא עוצרת על קלט:** תהא  $N$  מטל"ד אזי  $x \in \Sigma^*$  עבורו  $N$  לא מקבלת ולא דוחה את  $x$ .

**טענה:** מכונת טיורינג ומכונת טיורינג לא-דטרמיניסטית הינן מודלים שקולים.

**שפות כריעות למחצה/שפות ניתנות למניה רקורסיבית/שפות ניתנות לקבלה:** יהי  $\Sigma$  אלפבית אזי

קיימת מ"ט  $M$  עבורה  $\mathcal{RE} = \{\mathcal{L} \subseteq \Sigma^* \mid \mathcal{L} = L(M)\}$ .

**מכונת טיורינג מכריע שפה:** תהא  $\mathcal{L} \subseteq \Sigma^*$  שפה אזי מ"ט  $M$  עבורה  $\mathcal{L} = L(M)$  וכן לכל  $x \in \Sigma^*$  מתקיים כי  $M$  עוצרת על  $x$ .

**שפות כריעות/שפות רקורסיביות:** יהי  $\Sigma$  אלפבית אזי קיימת מ"ט  $M$  המכריעה את  $\mathcal{L}$   $\mathcal{R} = \{\mathcal{L} \subseteq \Sigma^* \mid \mathcal{L} \text{ המכריעה את } \mathcal{L}\}$ .

**מסקנה:**  $\mathcal{R} \subseteq \mathcal{RE}$ .

**מונה עבור שפה:** תהא  $\mathcal{L} \subseteq \Sigma^*$  שפה אזי מ"ט  $E$  מעל האלפבית  $\Sigma \cup \{\$\}$  עבורו

• לכל  $q \in Q$  ולכל  $\sigma \in \Gamma$  מתקיים  $\delta(q, \sigma) = (q', \sigma', R)$ .

• הרצת  $E$  על הקונפיגורציה  $\varepsilon$  מקיימת

- לכל  $x \in L$  מתקיים כי  $\$x\$$  על הסרט לאחר מספר סופי של צעדים.

- לכל  $x \notin L$  מתקיים כי  $\$x\$$  לא על הסרט לעולם.

**טענה:** תהא  $\mathcal{L} \subseteq \Sigma^*$  שפה אזי  $(\mathcal{L} \in \mathcal{RE}) \iff (\text{קיים } \mathcal{L}\text{-מונה})$ .

**מונה לקסיקוגרפי:** תהא  $\mathcal{L} \subseteq \Sigma^*$  שפה אזי מונה  $E$  עבור  $\mathcal{L}$  עבורו לכל  $x, y \in \mathcal{L}$  באשר  $x \leq_{\text{lex}} y$  מתקיים כי  $\$x\$$  רשום על הסרט לפני  $\$y\$$ .

**טענה:** תהא  $\mathcal{L} \subseteq \Sigma^*$  שפה אזי  $(\mathcal{L} \in \mathcal{R}) \iff (\text{קיים } \mathcal{L}\text{-מונה לקסיקוגרפי})$ .

**הגדרה:** יהי  $\Sigma$  אלפבית אזי  $\text{co}\mathcal{RE} = \{\mathcal{L} \subseteq \Sigma^* \mid \bar{\mathcal{L}} \in \mathcal{RE}\}$ .

**טענה:**  $\mathcal{R} = \mathcal{RE} \cap \text{co}\mathcal{RE}$ .

**קידוד בינארי של מכונת טיורינג:** פונקציה  $f : \{M \mid M \text{ מ"ט}\} \rightarrow \{0, 1\}^*$  חח"ע עד כדי שינוי שמות.

**סימון:** תהא  $M$  מ"ט אזי  $\langle M \rangle$  הינו הקידוד הבינארי של  $M$ .

**הערה:** נשתמש בסימון  $\langle \cdot \rangle$  על מנת לקודד כל אובייקט לקידוד בינארי.

**הערה:** נניח כי קידוד ופענוח הן פעולות פשוטות ובדיקת נכונות קידוד היא  $\mathcal{R}$ .

**סימון:** תהא  $M$  מ"ט ותהא  $x$  מילה אזי  $\langle M, x \rangle$  הינו הקידוד הבינארי של  $M$  מאותחל עם  $x$ .

**משפט מכונת טיורינג אוניברסלית:** קיימת מ"ט  $U$  מעל  $\{0, 1\}$  עבורה

• לכל מ"ט  $M$  ולכל קלט  $x$  של  $M$  מתקיים  $(U \text{ מקבלת את } \langle M, x \rangle) \iff (M \text{ מקבלת את } x)$ .

• לכל מ"ט  $M$  ולכל קלט  $x$  של  $M$  מתקיים  $(U \text{ דוחה את } \langle M, x \rangle) \iff (M \text{ דוחה את } x)$ .

• לכל מ"ט  $M$  ולכל קלט  $x$  של  $M$  מתקיים  $(U \text{ לא עוצרת עבור } \langle M, x \rangle) \iff (M \text{ לא עוצרת עבור } x)$ .

• לכל  $x \in \{0, 1\}^*$  באשר  $x \notin \text{Im}(f)$  מתקיים כי  $U$  דוחה את  $x$ .

**טענה:** קיימת  $\mathcal{L} \subseteq \{0, 1\}^*$  שפה עבורה  $L \notin \mathcal{RE} \cup \text{co}\mathcal{RE}$ .

**הגדרה:**  $\text{ACC} = \{\langle M, x \rangle \mid (M \text{ מ"ט}) \wedge (x \text{ מילה}) \wedge (x \text{ מקבלת את } M)\}$ .

**טענה:**  $\text{ACC} \in \mathcal{RE}$ .

**למה:** לא קיימת מ"ט  $M$  מעל  $\{0, 1\}$  עבורה  $L(M) = \{\langle N \rangle \mid \langle N \rangle \notin L(N)\}$ .

**למה:** תהא  $M$  מ"ט המכריעה את  $\text{ACC}$  אזי קיימת מ"ט  $N$  המכריעה את  $\{\langle N \rangle \mid \langle N \rangle \notin L(N)\}$ .

**טענה:**  $\text{ACC} \notin \mathcal{R}$ .

**הגדרה:**  $\text{HALT} = \{\langle M, x \rangle \mid \langle M, x \rangle \mid (M \text{ מ"ט}) \wedge (x \text{ מילה}) \wedge (x \text{ עוצרת על } M)\}$ .

**טענה:**  $\text{HALT} \in \mathcal{RE} \setminus \mathcal{R}$ .

**הגדרה:**  $\text{EMPTY} = \{\langle M \rangle \mid (M \text{ מ"ט}) \wedge (L(M) = \emptyset)\}$ .

**טענה:**  $\text{EMPTY} \notin \mathcal{R}$ .

**מכונת טיורינג מחשבת פונקציה:** תהא  $M$  מ"ט ותהא  $D \subseteq \Sigma$  אזי  $f : D \rightarrow (\Gamma \setminus \{\sqcup\})^*$  עבורה לכל  $x \in D$  מתקיים כי  $M$  עוצרת על  $x$  וכן הסרט בסוף הריצה הינו  $f(x)\sqcup^*$ .

**פונקציה חשיבה:** תהא  $D \subseteq \Sigma$  אזי  $f : D \rightarrow (\Gamma \setminus \{\sqcup\})^*$  עבורה קיימת מ"ט  $M$  המחשבת את  $f$ .

**רדוקציית מיפוי:** יהיו  $\Sigma, \Delta$  אלפביתים באשר  $\Sigma \subseteq \Delta$  תהא  $A \subseteq \Sigma^*$  שפה ותהא  $B \subseteq \Delta^*$  שפה אזי  $f : \Sigma^* \rightarrow \Delta^*$  חשיבה עבורה

לכל  $x \in \Sigma^*$  מתקיים  $(f(x) \in B) \iff (x \in A)$ .

**סימון:** יהיו  $\Sigma, \Delta$  אלפביתים באשר  $\Sigma \subseteq \Delta$  תהא  $A \subseteq \Sigma^*$  שפה ותהא  $B \subseteq \Delta^*$  שפה אזי  $f : \Sigma^* \rightarrow \Delta^*$  רדוקציית מיפוי אזי

$A \leq_m B$

**טענה:**  $\text{EMPTY} \in \text{co}\mathcal{RE}$ .

**טענה:** תהיינה  $A, B$  שפות באשר  $B \in \mathcal{R}$  וכן  $A \leq_m B$  אזי  $A \in \mathcal{R}$ .

**מסקנה:** תהיינה  $A, B$  שפות באשר  $A \notin \mathcal{R}$  וכן  $A \leq_m B$  אזי  $B \notin \mathcal{R}$ .

**הערה:** יש דבר כזה רדוקציה כללית שמכלילה את רדוקציית המיפוי, לא עברנו על זה פורמלית, מסומן  $\leq$ .

**מסקנה:**  $\{ \langle M \rangle \mid \langle M \rangle \notin L(M) \} \leq \text{ACC}$ .

**מסקנה:**  $\text{ACC} \leq_m \text{HALT}$ .

**מסקנה:**  $\text{ACC} \leq \text{EMPTY}$ .

**הגדרה:**  $\text{REG} = \{ \langle M \rangle \mid L(M) \text{ רגולרית} \}$ .

**טענה:**  $\text{REG} \notin \mathcal{R}$ .

**הגדרה:**  $\text{EQ} = \{ \langle M_1, M_2 \rangle \mid L(M_1) = L(M_2) \}$ .

**טענה:**  $\text{EQ} \notin \mathcal{R}$ .

**הגדרה:**  $\text{HALT}_\varepsilon = \{ \langle M \rangle \mid M \text{ עוצר על } \varepsilon \}$ .

**טענה:**  $\text{HALT} \leq_m \text{HALT}_\varepsilon$ .

**טענה:** תהא  $A \in \mathcal{R}$  ותהא  $B \in \mathcal{P}(\Sigma^*) \setminus \{\Sigma^*, \emptyset\}$  אזי  $A \leq_m B$ .

**למה:** תהיינה  $A, B$  שפות ותהא  $f$  רדוקציית מיפוי מ- $A$  ל- $B$  אזי  $f$  רדוקציית מיפוי מ- $\bar{A}$  ל- $\bar{B}$ .

**טענה:** תהיינה  $A, B$  שפות באשר  $A \leq_m B$  אזי

• אם  $B \in \mathcal{RE}$  אזי  $A \in \mathcal{RE}$ .

• אם  $B \in \text{co}\mathcal{RE}$  אזי  $A \in \text{co}\mathcal{RE}$ .

**טענה:**  $\text{ACC} \leq_m \text{EQ}$  וכן  $\text{ACC} \leq_m \text{EQ}$ .

**מסקנה:**  $\text{EQ} \notin \mathcal{RE} \cup \text{co}\mathcal{RE}$ .

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

**הגדרה:** תהא  $\mathcal{C}$  תכונה סמנטית אזי  $L_{\mathcal{C}} = \{ \langle M \rangle \mid L(M) \in \mathcal{C} \}$ .

**משפט רייס:** תהא  $\mathcal{C} \in \mathcal{P}(\mathcal{RE}) \setminus \{\mathcal{RE}, \emptyset\}$  תכונה סמנטית אזי  $L_{\mathcal{C}} \notin \mathcal{R}$ .

**טענה:** תהא  $\mathcal{C} \in \{\mathcal{RE}, \emptyset\}$  אזי  $L_{\mathcal{C}} \in \mathcal{R}$ .

**הגדרה:**  $\text{PRIME} = \{ (p)_2 \mid p \in \mathbb{P} \}$ .

**הערה:** קידוד מספרים תמיד יעשה בבסיס 2.

**הגדרה:**  $\text{EQPRIME} = \{ \langle M \rangle \mid L(M) = \text{PRIME} \}$ .

**טענה:**  $\text{EQPRIME} \notin \mathcal{R}$ .

**טענה משפט רייס הרחבה ראשונה:** תהא  $\mathcal{C} \in \mathcal{P}(\mathcal{RE} \setminus \{\emptyset\}) \setminus \{\emptyset\}$  אזי  $L_{\mathcal{C}} \notin \text{co}\mathcal{RE}$ .

**טענה משפט רייס הרחבה שנייה:** תהא  $\mathcal{C} \in \mathcal{P}(\mathcal{RE}) \setminus \{\mathcal{RE}\}$  באשר  $\emptyset \in \mathcal{C}$  אזי  $L_{\mathcal{C}} \notin \mathcal{RE}$ .

**מסקנה:**  $\text{REG} \notin \mathcal{RE}$ .

**הגדרה:**  $\text{ALL} = \{ \langle M \rangle \mid L(M) = \Sigma^* \}$ .

**למה:**  $\overline{\text{HALT}} \leq_m \text{ALL}$ .

**טענה:**  $\text{ALL} \notin \mathcal{RE} \cup \text{co}\mathcal{RE}$ .

**חסם עליון לזמן ריצה של מכונת טיורינג:** תהא  $M$  מ"ט אזי  $T : \mathbb{N} \rightarrow \mathbb{N}$  עבורה לכל  $n \in \mathbb{N}$  ולכל  $x \in \Sigma^n$  מתקיים כי  $M$  על הקלט

$x$  מבצעת לכל היותר  $T(n)$  צעדים.

**הגדרה:** תהא  $T : \mathbb{N} \rightarrow \mathbb{N}$  אזי  $M$  מ"ט שרצה בזמן  $\mathcal{O}(T(n))$   $\text{DTime}(T(n)) = \{ L(M) \mid \mathcal{O}(T(n)) \}$ .

**טענה:**  $\{ 0^k 1^k \mid k \geq 0 \} \in \text{DTime}(n^2)$ .

**מסקנה:**  $\{ 0^k 1^k \mid k \geq 0 \} \in \text{DTime}(n \log(n))$ .

**משפט:** תהא  $t(n) = o(n \log(n))$  ותהא  $L \in \text{DTime}(t(n))$  אזי  $L$  רגולרית.

**מסקנה:** תהא  $t(n) = o(n \log(n))$  אזי  $\{ 0^k 1^k \mid k \geq 0 \} \notin \text{DTime}(t(n))$ .

**פונקציה חשיבה בזמן:** פונקציה  $T : \mathbb{N} \rightarrow \mathbb{N}$  עבורה קיימת מ"ט  $M$  המקיימת לכל  $n \in \mathbb{N}$  כי  $M$  על הקלט  $1^n$  מחשבת את  $(T(n))_2$

בזמן  $\mathcal{O}(T(n))$ .

**טענה:** תהא  $T : \mathbb{N} \rightarrow \mathbb{N}$  חשיבה בזמן שאינה קבועה אזי  $T(n) = \Omega(n)$ .

**משפט מכונת טיורינג אוניברסלית עם טיימר:** קיימת מ"ט אוניברסלית  $U$  וקיים  $C \in \mathbb{R}$  עבורם לכל מ"ט  $M$  ולכל קלט  $x$  באשר  $M$

עוצרת על הקלט  $x$  לאחר  $t$  צעדים מתקיים כי  $U$  עוצרת על הקלט  $\langle M, x \rangle$  תוך  $C \cdot t$  צעדים.

**משפט:** קיימת מ"ט אוניברסלית  $U$  וקיים  $C \in \mathbb{R}$  עבורם לכל מ"ט  $M$  ולכל קלט  $x$  ולכל  $t \in \mathbb{N}$  מתקיים



- אם  $M$  עוצרת על הקלט  $x$  לאחר לכל היותר  $t$  צעדים אזי  $U$  מקבלת את  $\langle M, x, t \rangle$ .
- אם  $M$  דוחה את  $x$  או לא עוצרת לאחר  $t$  צעדים אזי  $U$  דוחה את  $\langle M, x, t \rangle$ .
- $U$  עוצרת לאחר  $C \cdot t \log(t)$  צעדים.

**משפט היררכיית הזמן:** תהא  $T: \mathbb{N} \rightarrow \mathbb{N}$  חשיבה בזמן ותהא  $t(n) = o\left(\frac{T(n)}{\log(T(n))}\right)$  אזי  $\text{DTime}(t(n)) \subsetneq \text{DTime}(T(n))$ .

**מסקנה:** יהיו  $1 \leq c < d$  אזי  $\text{DTime}(n^c) \subsetneq \text{DTime}(n^d)$ .

**טענה:** תהא  $T: \mathbb{N} \rightarrow \mathbb{N}$  באשר  $T(n) \geq n$  ותהא  $M$  מ"ט רב-סרטיית שרצה בזמן  $T(n)$  אזי קיימת מ"ט  $M'$  שרצה בזמן  $\mathcal{O}(T^2(n))$  עבורה  $L(M) = L(M')$ .

**טענה:** תהא  $T: \mathbb{N} \rightarrow \mathbb{N}$  באשר  $T(n) \geq n$  ותהא  $M$  מודל RAM שרצה בזמן  $T(n)$  אזי קיימת מ"ט  $M'$  שרצה בזמן  $\mathcal{O}(T^3(n))$  עבורה  $L(M) = L(M')$ .

**חסם עליון לזמן ריצה של מכונת טיורינג לא-דטרמיניסטית:** תהא  $N$  מטל"ד אזי  $T: \mathbb{N} \rightarrow \mathbb{N}$  עבורה לכל  $n \in \mathbb{N}$  ולכל  $x \in \Sigma^n$  מתקיים כי  $T_{N,x}(n)$  בעומק לכל היותר  $T(n)$ .

**הגדרה:** תהא  $T: \mathbb{N} \rightarrow \mathbb{N}$  אזי  $N$  מטל"ד שרצה בזמן  $\mathcal{O}(T(n))$   $\text{NTime}(T(n)) = \{L(N) \mid \mathcal{O}(T(n))\}$ .

**טענה:** תהא  $T: \mathbb{N} \rightarrow \mathbb{N}$  באשר  $T(n) \geq n$  ותהא  $N$  מטל"ד שרצה בזמן  $T(n)$  אזי קיימת מ"ט  $M$  שרצה בזמן  $2^{\mathcal{O}(T(n))}$  עבורה  $L(N) = L(M)$ .

**שפה  $\mathcal{P}$ :**  $\mathcal{P} = \bigcup_{c \in \mathbb{N}} \text{DTime}(n^c)$ .

**הגדרה:**  $G$  גרף מכוון עם מסלול מ- $s$  ל- $t$   $\text{PATH} = \{\langle G, s, t \rangle \mid t \text{ מ-} s \text{ מסלול}\}$ .

**טענה:**  $\text{PATH} \in \mathcal{P}$ .

**משפט:**  $\text{PRIME} \in \mathcal{P}$ .

**שפה  $\mathcal{NP}$ :**  $\mathcal{NP} = \bigcup_{c \in \mathbb{N}} \text{NTime}(n^c)$ .

**מסקנה:**  $\mathcal{P} \subseteq \mathcal{NP}$ .

**הגדרה:**  $G$  גרף מכוון עם מסלול המילטוני מ- $s$  ל- $t$   $\text{HAMPATH} = \{\langle G, s, t \rangle \mid t \text{ מ-} s \text{ מסלול המילטוני}\}$ .

**טענה:**  $\text{HAMPATH} \in \mathcal{NP}$ .

**השערה:**  $\text{HAMPATH} \notin \mathcal{P}$ . השערה פתוחה

**שפה  $\mathcal{EXP}$ :**  $\mathcal{EXP} = \bigcup_{k \in \mathbb{N}} \text{DTime}(2^{n^k})$ .

**שפה  $\mathcal{NEXP}$ :**  $\mathcal{NEXP} = \bigcup_{k \in \mathbb{N}} \text{NTime}(2^{n^k})$ .

**טענה:**  $\mathcal{EXP} \subseteq \mathcal{NEXP}$ .

**מסקנה:**  $\mathcal{P} \subseteq \mathcal{NP} \subseteq \mathcal{EXP} \subseteq \mathcal{NEXP}$ .

**טענה:**  $\mathcal{P} \subsetneq \mathcal{EXP}$ .

**טענה:**  $\mathcal{NP} \subsetneq \mathcal{NEXP}$ .

**סימון:** תהא  $M$  מ"ט ויהי  $x \in \Sigma^*$  אזי  $M(x)$  הינו ריצת  $M$  על  $x$ .

**מוודא לשפה:** תהא  $\mathcal{L} \subseteq \Sigma^*$  שפה אזי מ"ט  $V$  מעל אלפבית  $\{", "\} \cup \Sigma$  המקיים

• שלמות: יהי  $x \in \mathcal{L}$  אזי קיים  $w \in \Sigma^*$  עבורו  $V(x, w)$  מקבלת.

• נאותות: יהי  $x \notin \mathcal{L}$  אזי לכל  $w \in \Sigma^*$  מתקיים כי  $V(x, w)$  דוחה.

**טענה:** תהא  $\mathcal{L} \subseteq \Sigma^*$  שפה אזי  $(\mathcal{L} \in \mathcal{RE}) \iff (\text{קיים מוודא ל-}\mathcal{L})$ .

**מדווא פולינומי לשפה:** תהא  $\mathcal{L} \subseteq \Sigma^*$  שפה אזי מוודא  $V$  ל- $\mathcal{L}$  עבורו קיים  $p \in \mathbb{N}[x]$  המקיים כי לכל  $x, w \in \Sigma^*$  מתקיים כי  $V(x, w)$

עוצרת לכל היותר אחרי  $p(|x|)$  צעדים.

**הגדרה:**  $\text{CLIQUE} = \{\langle G, k \rangle \mid k \text{ בעל קליקה מגודל } k \text{ ב-} G\}$ .

**טענה:** קיים מוודא פולינומי ל- $\text{CLIQUE}$ .

**הגדרה:**  $\text{IS} = \{\langle G, k \rangle \mid k \text{ בעל קבוצה בת"ל מגודל } k \text{ ב-} G\}$ .

**טענה:** קיים מוודא פולינומי ל- $\text{IS}$ .

**הגדרה:**  $\text{FACTOR} = \{\langle N, k \rangle \mid \exists d \in [k]. (d|N)\}$ .

**טענה:** קיים מוודא פולינומי ל- $\text{FACTOR}$ .

**הגדרה:**  $\text{SUBSETSUM} = \{\langle S, t \rangle \mid (S \subseteq \mathbb{N}) \wedge (\exists T \subseteq S. \sum_{i \in T} i = t)\}$ .

**טענה:** קיים מוודא פולינומי ל- $\text{SUBSETSUM}$ .

**משפט:** תהא  $\mathcal{L} \subseteq \Sigma^*$  שפה אזי  $(\mathcal{L} \in \mathcal{NP}) \iff (\text{קיים מוודא פולינומי ל-}\mathcal{L})$ .



**מסקנה:** CLIQUE, IS, FACTOR, SUBSETSUM  $\in \mathcal{NP}$ .

**השערה:**  $\mathcal{P} \neq \mathcal{NP}$  השערה פתוחה

**פונקציה חשיבה פולינומית:** תהא  $D \subseteq \Sigma$  אזי  $f : D \rightarrow (\Gamma \setminus \{\perp\})^*$  עבורה קיימת מ"ט  $M$  המחשבת את  $f$  וכן קיים  $p \in \mathbb{N}[x]$  המקיים כי לכל  $x \in \Sigma^*$  מתקיים כי  $M(x)$  עוצרת לכל היותר אחרי  $p(|x|)$  צעדים.

**רדוקציית מיפוי פולינומית:** יהיו  $\Delta, \Sigma$  אלפבייטים באשר  $\Sigma \subseteq \Delta$  תהא  $A \subseteq \Sigma^*$  שפה ותהא  $B \subseteq \Delta^*$  שפה אזי רדוקציית מיפוי  $f : \Sigma^* \rightarrow \Delta^*$   $A$ -ל- $B$  חשיבה פולינומית.

**סימון:** יהיו  $\Delta, \Sigma$  אלפבייטים באשר  $\Sigma \subseteq \Delta$  תהא  $A \subseteq \Sigma^*$  שפה ותהא  $B \subseteq \Delta^*$  שפה ותהא  $f : \Sigma^* \rightarrow \Delta^*$  רדוקציית מיפוי פולינומית אזי  $A \leq_p B$ .

**טענה:** CLIQUE  $\leq_p$  IS.

**טענה:** תהיינה  $A, B$  שפות באשר  $B \in \mathcal{P}$  וכן  $A \leq_p B$  אזי  $A \in \mathcal{P}$ .

**שפה  $\mathcal{NP}$ -קשה:**  $\mathcal{NP}\mathcal{H} = \{\mathcal{L} \mid \forall L \in \mathcal{NP} (L \leq_p \mathcal{L})\}$

**שפה  $\mathcal{NP}$ -שלמה:**  $\mathcal{NP}\mathcal{C} = \mathcal{NP} \cap \mathcal{NP}\mathcal{H}$

**טענה:** תהא  $\mathcal{L} \in \mathcal{NP}\mathcal{C}$  אזי  $(\mathcal{L} \in \mathcal{P}) \iff (\mathcal{P} = \mathcal{NP})$ .

**הגדרה:** קיים  $w$  עבורו  $M(x, w)$  מקבלת לכל היותר אחרי  $t$  צעדים  $\{ \langle M, x, 1^t \rangle \mid \text{ACC}_{\mathcal{NP}} = \{ \langle M, x, 1^t \rangle \mid \text{ACC}_{\mathcal{NP}} \in \mathcal{NP}\mathcal{C} \}$

**טענה:**  $\text{ACC}_{\mathcal{NP}} \in \mathcal{NP}\mathcal{C}$

**טענה:** תהיינה  $A, B \in \mathcal{NP}$  שפות באשר  $A \in \mathcal{NP}\mathcal{C}$  וכן  $A \leq_p B$  אזי  $B \in \mathcal{NP}\mathcal{C}$ .

**מעגל ספיק:** מעגל  $C$  עבורו קיים  $x \in \{0, 1\}^n$  המקיים  $C(x) = 1$ .

**פסוק  $k$ -CNF:** פסוק  $\varphi \in \text{CNF}$  עבורה קיים  $m \in \mathbb{N}$  וקיימת  $A \in M_{m \times k}(\{p_i\} \cup \{\neg p_i\})$  המקיימת  $\varphi = \bigwedge_{i=1}^m \bigvee_{j=1}^k (A)_{i,j}$ .

**הגדרה:** יהי  $k \in \mathbb{N}_+$  אזי  $k\text{SAT} = \{ \langle \varphi \rangle \mid (\varphi \in k\text{CNF}) \wedge (\varphi \text{ ספיקה}) \}$

**טענה:** יהי  $k \in \mathbb{N}_+$  אזי  $k\text{SAT} \in \mathcal{NP}$

**טענה:**  $2\text{SAT} \in \mathcal{P}$

**משפט קוק-ליוין:**  $3\text{SAT} \in \mathcal{NP}\mathcal{C}$

**טענה:** יהיו  $k, \ell \in \mathbb{N}_+$  באשר  $k \leq \ell$  אזי  $k\text{SAT} \leq_p \ell\text{SAT}$

**מסקנה:** יהי  $k \in \mathbb{N} \setminus \{0, 1, 2\}$  אזי  $k\text{SAT} \in \mathcal{NP}\mathcal{C}$

**משפט:**  $3\text{SAT} \leq_p \text{CLIQUE}$

**מסקנה:** CLIQUE, IS  $\in \mathcal{NP}\mathcal{C}$

**סימון:** תהא  $A \in M_{m \times k}(\{p_i\} \cup \{\neg p_i\})$  ותהא  $v$  השמה אזי

$N\left(\bigwedge_{i=1}^m \bigvee_{j=1}^k (A)_{i,j}, v\right) = \left| \left\{ i \in [m] \mid \overline{v}\left(\bigvee_{j=1}^k (A)_{i,j}\right) = \text{True} \right\} \right|$

**הגדרה:**  $CCNF = \{ \langle \varphi, k \rangle \mid (\varphi \in \text{CNF}) \wedge (\exists v (N(\varphi, v) = k)) \}$

**טענה:**  $CCNF \in \mathcal{NP}\mathcal{C}$

**הגדרה:**  $\text{DNFCNF} = \{ \langle \varphi \rangle \mid (\varphi \in \text{DNF}) \wedge (\varphi \text{ ספיקה}) \}$

**טענה:**  $\text{DNFCNF} \in \mathcal{P}$

**כיסוי קודקודים:** יהי  $G$  גרף לא מכוון אזי  $C \subseteq V$  עבורה לכל  $\{u, v\} \in E$  מתקיים  $(u \in C) \vee (v \in C)$ .

**הגדרה:**  $VC = \{ \langle G, k \rangle \mid k \text{ כיסוי קודקודים מגודל } k \}$

**טענה:**  $VC \in \mathcal{NP}\mathcal{C}$

**בסיס פונקציות:** יהי  $\Sigma$  אלפבית אזי  $B \subseteq \bigcup_{n=1}^{\infty} (\Sigma^n \rightarrow \Sigma)$

**מעגל:** יהי  $\Sigma$  אלפבית יהי  $B$  בסיס פונקציות מעל  $\Sigma$  תהיינה  $k_1 \dots k_n \in \mathbb{N}_+$  תהיינה  $f_1 \dots f_n \in B$  באשר  $f_i : \Sigma^{k_i} \rightarrow \Sigma$  לכל

$i \in [n]$  ותהיינה  $x_1 \dots x_m, y_1 \dots y_k \in \Sigma$  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  $i \in [m]$  מתקיים  $\deg^-(x_i) = 0$

• לכל  $i \in [n]$  מתקיים  $\deg^-(f_i) = k_i$

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

**הערה:** נשמור על הטרמינולוגיה ממעגל בוליאני כהכללה טבעית.

**מטריצת הקונפיגורציות/טאבלו:** תהא  $T : \mathbb{N} \rightarrow \mathbb{N}$  חשיבה בזמן באשר  $n \leq T(n)$  תהא  $M$  מ"ט שרצה בזמן  $T(n)$  יהי  $z \in \{0, 1\}^n$

ותהיינה  $c_1 \dots c_i$  קונפיגורציות הריצה של  $M(z)$  אזי  $M(z)$   $(\Sigma \uplus \Gamma)$   $\tau_{M,z} \in M_{T(n)+1}$  המקיימת  $R_i(\tau_{M,z}) = c_i$ .

**הערה:** במטריצת הקונפיגורציות נניח כי  $\delta(q_r, \sigma) = (q_r, \sigma, R)$  וכן  $\delta(q_a, \sigma) = (q_a, \sigma, R)$

**הגדרה:**  $\text{CIRSAT} = \{ \langle C, x \rangle \mid (C \text{ מעגל בוליאני}) \wedge (\exists w \in \{0, 1\}^* (C(x, w) = 1)) \}$

**הגדרה:** תהא  $T : \mathbb{N} \rightarrow \mathbb{N}$  חשיבה בזמן באשר  $n \leq T(n)$  ותהא  $M$  מ"ט רצה בזמן  $T(n)$  נגדיר מעגלים מעל  $\Sigma \uplus \Gamma$  כך

- יהי  $z \in \Sigma \uplus \Gamma$  אזי  $C_{\text{inp}}(z) = R_0(\tau_{M,z})$

- יהי  $z \in \Sigma \uplus \Gamma$  ויהי  $i \in \{0, \dots, T(n) - 1\}$  אזי  $C_{\text{next}}(R_i(\tau_{M,z})) = R_{i+1}(\tau_{M,z})$

- יהי  $z \in \Sigma \uplus \Gamma$  אזי  $C_{\text{out}}(R_{T(n)}(\tau_{M,z})) = M(z)$

- יהי  $z \in \Sigma \uplus \Gamma$  אזי  $C_{M,n}^{\Sigma \uplus \Gamma}(z) = (C_{\text{out}} \circ C_{\text{next}} \circ \dots \circ C_{\text{next}} \circ C_{\text{inp}})(z)$

**טענה:** תהא  $T : \mathbb{N} \rightarrow \mathbb{N}$  חשיבה בזמן באשר  $n \leq T(n)$  ותהא  $M$  מ"ט רצה בזמן  $T(n)$  אזי  $|C_{M,n}^{\Sigma \uplus \Gamma}| = \mathcal{O}(T^2(n))$  וכן קיימת

פונקציה  $f$  חשיבה בזמן  $\text{poly}(T(n))$  עבורה  $f(1^n) = \langle C_{M,n}^{\Sigma \uplus \Gamma} \rangle$

**מסקנה:** תהא  $T : \mathbb{N} \rightarrow \mathbb{N}$  חשיבה בזמן באשר  $n \leq T(n)$  ותהא  $M$  מ"ט רצה בזמן  $T(n)$  ויהי  $z \in \Sigma \uplus \Gamma$  אזי  $C_{M,n}^{\Sigma \uplus \Gamma}(z) = M(z)$

**טענה:** יהי  $\Pi$  אלפבית אזי קיימת פונקציה חשיבה פולינומית  $f$  עבורה לכל מעגל בוליאני  $C$  מתקיים כי  $f(C)$  מעגל בוליאני מעל

בסיס דה-מורגן באשר  $f(C)(z) = C(z)$  לכל  $z \in \{0, 1\}^n$  וכן  $|f(C)| = \mathcal{O}(|C|)$

**למה:** תהא  $T : \mathbb{N} \rightarrow \mathbb{N}$  חשיבה בזמן באשר  $n \leq T(n)$  ותהא  $M$  מ"ט רצה בזמן  $T(n)$  אזי קיימת פונקציה חשיבה  $f$  בזמן

$\text{poly}(T(n))$  עבורה  $f(1^n) = \langle C_{M,n} \rangle$  באשר  $C_{M,n}$  מעגל עבורו  $|C_{M,n}| = \mathcal{O}(T^2(n))$  וכן לכל  $z \in \{0, 1\}^n$  מתקיים  $M(z) =$

מקבלת  $(C_{M,n}(z) = 1) \iff (C_{M,n}(z) = 1)$

**טענה:**  $\text{CIRSAT} \in \mathcal{NPC}$

**מסקנה:** תהא  $T : \mathbb{N} \rightarrow \mathbb{N}$  חשיבה בזמן באשר  $n \leq T(n)$  ותהא  $f : \{0, 1\}^* \rightarrow \{0, 1\}$  לא ניתנת לחישוב על ידי משפחת מעגלים

מגודל  $\mathcal{O}(T(n))$  אזי  $f$  לא ניתנת לחישוב על ידי מ"ט בזמן  $\sqrt{T(n)}$

**טענה:**  $\text{CIRSAT} \leq_p 3\text{SAT}$

**טענה:**  $3\text{SAT} \leq_p \text{SUBSETSUM}$

**מסקנה:**  $\text{SUBSETSUM} \in \mathcal{NPC}$

**טענה:**  $3\text{SAT} \leq_p \text{HAMPATH}$

**מסקנה:**  $\text{HAMPATH} \in \mathcal{NPC}$

**שפה**  $\text{coNP} = \{L \mid \bar{L} \in \mathcal{NP}\}$

**השערה:**  $\text{coNP} \neq \mathcal{NP}$  השערה פתוחה

**טענה:** תהיינה  $A, B$  שפות באשר  $A \leq_p B$  אזי

- אם  $B \in \mathcal{NP}$  אזי  $A \in \mathcal{NP}$

- אם  $B \in \text{coNP}$  אזי  $A \in \text{coNP}$

**מסקנה:** תהא  $\mathcal{L} \in \mathcal{NPC}$  אזי  $(\mathcal{L} \in \text{coNP}) \iff (\text{coNP} = \mathcal{NP})$

**טענה:**  $\mathcal{P} \subseteq \mathcal{NP} \cap \text{coNP}$

**השערה:**  $\mathcal{P} \neq \mathcal{NP} \cap \text{coNP}$  השערה פתוחה

**טענה:**  $\text{FACTOR} \in \mathcal{NP} \cap \text{coNP}$

**השערה:**  $\mathcal{P} \neq \mathcal{NP} \cap \text{coNP}$  השערה פתוחה

**הגדרה:**  $\text{MATMULT} = \{ \langle A, B, C \rangle \mid (A, B, C \in M_n(\mathbb{Z})) \wedge (A \cdot B = C) \}$

**טענה:** תהא  $D \in M_n(\mathbb{Z})$  באשר  $D \neq 0$  אזי  $\mathbb{P}_{r \leftarrow \{0, 1\}^n} (D \cdot r = 0) \leq 0.5$

**מסקנה:** קיימת מ"ט  $M$  אשר רצה בזמן  $\mathcal{O}(n^2)$  עבורה

- לכל  $x \in \{0, 1\}^*$  אשר אינו קידוד של שלשת מטריצות  $M(x)$  דוחה.

- לכל  $x \in \{0, 1\}^*$  עבורו קיימות  $A, B, C \in M_n(\mathbb{Z})$  המקיימות  $A \cdot B = C$  וכן  $x = \langle A, B, C \rangle$  מתקיים  $M(x)$  מקבלת.

- לכל  $x \in \{0, 1\}^*$  עבורו קיימות  $A, B, C \in M_n(\mathbb{Z})$  המקיימות  $A \cdot B \neq C$  וכן  $x = \langle A, B, C \rangle$  מתקיים

$\mathbb{P}(M(x)) \leq 2^{-100}$

**נוסחה אריתמטית:** יהי  $\mathbb{F}$  שדה ויהי  $C$  מעגל מעל  $\mathbb{F}$  עם הבסיס  $\{+, \times\}$  אזי נוסחה ב- $C$

**סימון:** תהא  $\varphi$  נוסחה אריתמטית מעל  $\mathbb{F}$  עבורה לכל  $x_1 \dots x_n \in \mathbb{F}$  מתקיים  $\varphi(x_1 \dots x_n) = 0$  אזי  $\varphi \equiv 0$

**הגדרה:**  $\text{ZE}_{\mathbb{F}} = \{ \langle \varphi \rangle \mid \varphi \equiv 0 \}$  עבורה  $\mathbb{F}$  מעל  $\mathbb{F}$

**טענה:**  $\overline{\text{ZE}_{\mathbb{Z}_2}} \in \mathcal{NPC}$

**טענה:** תהא  $\varphi$  נוסחה אריתמטית בעומק  $h$  מעל  $\mathbb{F}$  אזי  $\varphi$  מחשבת פולינום מדרגה לכל היותר  $2^h$

**טענה:** תהא  $\varphi$  נוסחה אריתמטית מעל  $\mathbb{F}$  המחשבת  $f \in \mathbb{F}[x_1, \dots, x_n]$  באשר  $\deg(f) < |\mathbb{F}|$  אזי  $(\varphi \equiv 0) \iff (f = 0)$ .

**מסקנה:** יהי  $\mathbb{F}$  שדה אינסופי אזי  $\mathbb{Z}\mathbb{E}_{\mathbb{F}} \in \mathcal{R}$ .

**למה שוורץ-זיפל:** יהי  $f \in \mathbb{F}[x_1, \dots, x_n]$  באשר  $f \neq 0$  ותהא  $S \subseteq \mathbb{F}$  סופית אזי  $\frac{\deg(f)}{|S|} \mathbb{P}_{a_1, \dots, a_n \leftarrow S} (f(a_1 \dots a_n) = 0) \leq$

**מסקנה:** קיימת מ"ט  $M$  עבורה לכל  $x \in \{0, 1\}^*$  מתקיים

• אם  $x$  אינו קידוד של נוסחה אריתמטית מעל  $\mathbb{R}$  מתקיים  $M(x)$  דוחה.

• אם קיימת  $\varphi$  נוסחה אריתמטית מעל  $\mathbb{R}$  המקיימת  $\varphi \equiv 0$  וכן  $x = \langle \varphi \rangle$  מתקיים  $M(x)$  מקבלת בזמן  $\text{poly}(|\varphi|)$ .

• אם קיימת  $\varphi$  נוסחה אריתמטית מעל  $\mathbb{R}$  המקיימת  $\varphi \not\equiv 0$  וכן  $x = \langle \varphi \rangle$  מתקיים  $M(x) \leq 0.01$  (מקבלת)  $\mathbb{P}$  בזמן  $\text{poly}(|\varphi|)$ .

**מכונת טיורינג אקראית:** תהא  $T(n)$  חשיבה בזמן אזי מ"ט דו-סרטית  $M$  עם קונפיגורציה התחלתית  $x\$r$  באשר  $r \in \{0, 1\}^{T(|x|)}$ .

**זמן ריצה של מכונת טיורינג אקראית:** תהא  $T(n)$  חשיבה בזמן ותהא  $M$  מכונת טיורינג אקראית אזי  $T$ .

**סימון:** תהא  $M$  מ"ט אקראית עם זמן ריצה  $T(n)$  יהי  $x \in \{0, 1\}^*$  ויהי  $r \in \{0, 1\}^{T(|x|)}$  אזי  $M(x; r) = M(x\$r)$ .

**קלט של מכונת טיורינג אקראית:** תהא  $M$  מ"ט אקראית עם זמן ריצה  $T(n)$  יהי  $x \in \{0, 1\}^*$  ויהי  $r \in \{0, 1\}^{T(|x|)}$  אזי  $x$ .

**אקראיות של מכונת טיורינג אקראית:** תהא  $M$  מ"ט אקראית עם זמן ריצה  $T(n)$  יהי  $x \in \{0, 1\}^*$  ויהי  $r \in \{0, 1\}^{T(|x|)}$  אזי  $r$ .

**סימון:** תהא  $M$  מ"ט אקראית עם זמן ריצה  $T(n)$  יהי  $x$  קלט אזי  $M(x)$  משתנה מקרי לקבלת  $M(x; r)$  עבור  $r \in \{0, 1\}^{T(|x|)}$  אקראית.

**הגדרה:** תהא  $\alpha : \mathbb{N} \rightarrow [0, 1]$  ותהא שפה  $\mathcal{L}$  עבורה קיימת מ"ט אקראית  $M$  עם זמן ריצה פולינומי  $T(n)$  המקיימת כי החל ממקום מסויים  $n \in \mathbb{N}$  מתקיים

• לכל  $x \in \mathcal{L} \cap \Sigma^n$  מתקיים  $\mathbb{P}_{r \leftarrow \{0, 1\}^{T(n)}} (M(x; r)) \geq \alpha(n)$  (מקבלת)  $M(x; r)$ .

• לכל  $x \notin \mathcal{L} \cap \Sigma^n$  מתקיים  $\mathbb{P}_{r \leftarrow \{0, 1\}^{T(n)}} (M(x; r)) = 0$ .

אזי  $\mathcal{L} \in \mathcal{RP}(\alpha)$ .

**טענה:** תהייה  $\alpha, \beta : \mathbb{N} \rightarrow [0, 1]$  באשר  $\alpha \leq \beta$  החל ממקום מסויים אזי  $\mathcal{RP}(\beta) \subseteq \mathcal{RP}(\alpha)$ .

**טענה:**  $\mathcal{RP}(1) = \mathcal{P}$ .

**טענה:** תהא  $\alpha : \mathbb{N} \rightarrow [0, 1]$  באשר  $0 < \alpha$  החל ממקום מסויים אזי  $\mathcal{RP}(\alpha) \subseteq \mathcal{NP}$ .

**הגדרה:** תהא  $\alpha : \mathbb{N} \rightarrow [0, 1]$  אזי  $\text{coRP}(\alpha) = \{\bar{L} \mid L \in \mathcal{RP}(\alpha)\}$ .

**טענה:** תהא  $\alpha : \mathbb{N} \rightarrow [0, 1]$  ותהא שפה  $\mathcal{L}$  אזי  $\mathcal{L} \in \text{coRP}(\alpha)$  אם"ס קיימת מ"ט אקראית  $M$  עם זמן ריצה פולינומי  $T(n)$  המקיימת כי החל ממקום מסויים  $n \in \mathbb{N}$  מתקיים

• לכל  $x \in \mathcal{L} \cap \Sigma^n$  מתקיים  $\mathbb{P}_{r \leftarrow \{0, 1\}^{T(n)}} (M(x; r)) = 1$ .

• לכל  $x \notin \mathcal{L} \cap \Sigma^n$  מתקיים  $\mathbb{P}_{r \leftarrow \{0, 1\}^{T(n)}} (M(x; r)) \leq 1 - \alpha(n)$ .

**טענה:**  $\mathbb{Z}\mathbb{E}_{\mathbb{R}} \in \text{coRP}(0.99)$ .

**טענה:** יהיו  $c, d \in \mathbb{N}$  אזי  $\mathcal{RP}(n^{-c}) = \mathcal{RP}(1 - 2^{-n^d})$ .

**סימון:**  $\mathcal{RP} = \mathcal{RP}(0.5)$ .

**סימון:**  $\text{coRP} = \text{coRP}(0.5)$ .

**הגדרה:** תהייה  $\alpha, \beta : \mathbb{N} \rightarrow [0, 1]$  ותהא שפה  $\mathcal{L}$  עבורה קיימת מ"ט אקראית  $M$  עם זמן ריצה פולינומי  $T(n)$  המקיימת כי החל ממקום מסויים  $n \in \mathbb{N}$  מתקיים

• לכל  $x \in \mathcal{L} \cap \Sigma^n$  מתקיים  $\mathbb{P}_{r \leftarrow \{0, 1\}^{T(n)}} (M(x; r)) \geq \beta(n)$ .

• לכל  $x \notin \mathcal{L} \cap \Sigma^n$  מתקיים  $\mathbb{P}_{r \leftarrow \{0, 1\}^{T(n)}} (M(x; r)) \leq \alpha(n)$ .

אזי  $\mathcal{L} \in \mathcal{BPP}(\alpha, \beta)$ .

**סימון:**  $\mathcal{BPP} = \mathcal{BPP}(\frac{1}{3}, \frac{2}{3})$ .

**טענה:** תהא  $\alpha : \mathbb{N} \rightarrow [0, 1]$  אזי  $\mathcal{RP}(\alpha) = \mathcal{BPP}(0, \alpha)$ .

**טענה:** תהא  $\alpha : \mathbb{N} \rightarrow [0, 1]$  אזי  $\text{coRP}(\alpha) = \mathcal{BPP}(1 - \alpha, 1)$ .

**טענה:** תהייה  $\alpha, \beta, \gamma, \delta : \mathbb{N} \rightarrow [0, 1]$  עבורן  $\alpha \leq \beta \leq \gamma \leq \delta$  החל ממקום מסויים אזי  $\mathcal{BPP}(\alpha, \delta) \subseteq \mathcal{BPP}(\beta, \gamma)$ .

**משפט צ'רנוף-הופדינג:** יהי  $\delta > 0$  יהי  $n \in \mathbb{N}$  ויהיו  $A_1, \dots, A_n \sim \text{Ber}(p)$  אזי  $\mathbb{P}(|p - \frac{1}{n} \sum_{i=1}^n A_i| \geq \delta) \leq 2^{-\Theta(\delta^2 n)}$ .

**טענה:** יהיו  $c, d \in \mathbb{N}$  ותהא  $\alpha : \mathbb{N} \rightarrow [0, 1]$  חשיבה בזמן פולינומי באשר  $n^{-c} \leq \alpha(n) \leq 1 - n^{-c}$  החל ממקום מסויים אזי  $\mathcal{BPP}(\alpha(n) - n^{-c}, \alpha(n) + n^{-c}) \subseteq \mathcal{BPP}(2^{-n^d}, 1 - 2^{-n^d})$ .