# דפנוס גרסה של שלושה עמודים

**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 $|\varepsilon| = 0$ עבורה $\varepsilon \in \Sigma^*$.

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

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

**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 $L^R = \left\{w^R \mid w \in L\right\}$.

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

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

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

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

**אלגוריתם מכריע שפה:** תהא $L \subseteq \Sigma^*$ שפה אזי אלגוריתם $A : \Sigma^* \to \{\text{true}, \text{false}\}$ 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 $f : \{0,1\}^n \to \{0,1\}^m$.

**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 ותהיינה $k_1 \dots k_n \in \mathbb{N}_+$ ותהיינה $f_1 \dots f_n \in \mathcal{B}$ באשר $f_i : \{0,1\}^{k_i} \to \{0,1\}$ 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 $f_1 \dots f_n$.

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

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

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

**שערוך מעגל בוליאנרי על קלט:** יהי $C$ מעגל בוליאנרי ויהי $v \in \{0,1\}^m$ אזי $v = (x_1 \dots x_m)$ וכן $y_i$ הינו הפלט הנוצר מהפעלת הפונקציות הבוליאניות על הקודקודים הנכנסים.

**סימון:** יהי $C$ מעגל בוליאני 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 $L(C) = \{x \in \{0,1\}^n \mid \text{מקבל את } x\ C\}$.

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

**משפחה אוניברסלית דה־מורגן:** תהא $f : \{0,1\}^m \to \{0,1\}^k$ אזי קיים מעגל בוליאני $C$ מעל בסיס דה־מורגן עבורו לכל $v \in \{0,1\}^m$ מתקיים $C(v) = f(v)$.

**הערה:** מכאן והלאה כל המעגלים הם בוליאניים 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 $L(\mathcal{C}) = \left\{x \in \{0,1\}^* \mid x \in L\left(\mathcal{C}_{|x|}\right)\right\}$.

**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 $S : \mathbb{N} \to \mathbb{N}$ עבורה $|\mathcal{C}_n| \leq S(n)$.

**טענה:** תהא $f : \{0,1\}^n \to \{0,1\}$ 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 $f : \{0,1\}^n \to \{0,1\}$ 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 $f : \{0,1\}^n \to \{0,1\}$ 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 $f : \{0,1\}^n \to \{0,1\}$ שאינה ניתנת לחישוב בעזרת מעגל $C$ בגודל קטן מאשר $\frac{2^n}{10n}$.

**אוטומט סופי דטרמיניסטי (אס"ד):** תהא $Q \neq \varnothing$ קבוצה סופית יהי $\Sigma$ אלפבית תהא $\delta : Q \times \Sigma \to Q$ יהי $q \in Q$ 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 $\hat{\delta} : Q \times \Sigma^* \to Q$ עבורה לכל $q \in Q$ מתקיים $\hat{\delta}(q, \varepsilon) = q$ וכן לכל $x \in \Sigma^n$ מתקיים $\hat{\delta}(q, x) = \hat{\delta}\left(\hat{\delta}\left(q, x_1 \dots x_{n-1}\right), x_n\right)$.

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

**טענה:** יהי $(Q, \Sigma, \delta, q, F)$ אס"ד אזי $L(A) = \{x \in \Sigma^* \mid \text{מקבל את } A\ x\}$.

**שפה של אוטומט סופי דטרמיניסטי:** יהי $A$ אס"ד אזי $L(N) = L(M)$ עבורו $N$ אס"ד אזי קיים אס"ד $M$.

**מקבילות:** יהי $N$ אס"ד אזי קיים אס"ד $A$ עבורו $L(A) = L(M)$.

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

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

- $\varnothing$.
- יהי $a \in \Sigma_\varepsilon$ אזי $a$.
- יהיו $R_1, R_2$ ביטויים רגולרים אזי $R_1 \cup R_2$.
- יהיו $R_1, R_2$ ביטויים רגולרים אזי $R_1 R_2$.
- יהי $R$ ביטוי רגולרי אזי $R^*$.

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

- $L(\varnothing) = \varnothing$.
- יהי $a \in \Sigma_\varepsilon$ אזי $L(a) = \{a\}$.
- יהיו $R_1, R_2$ ביטויים רגולרים אזי $L(R_1 \cup R_2) = L(R_1) \cup L(R_2)$.
- יהיו $R_1, R_2$ ביטויים רגולרים אזי $L(R_1 R_2) = L(R_1) L(R_2)$.
- יהי $R$ ביטוי רגולרי אזי $L(R^*) = L(R)^*$.

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

**הערה:** קיים סדר פעולות לביטויים רגולרים

- סגור קליני.
- שרשור.
- איחוד.

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

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

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

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

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

- $L \cup \mathcal{L}$ רגולרית.
- $L \cap \mathcal{L}$ רגולרית.
- $\overline{L}$ רגולרית.
- $L \| \mathcal{L}$ רגולרית.
- לכל $n \in \mathbb{N}$ מתקיים כי $L^n$ רגולרית.
- $L^*$ רגולרית.

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

**אוטומט סופי לא־דטרמיניסטי מינוס (אסלד"ם):** תהא $Q \neq \varnothing$ קבוצה סופית יהי $\Sigma$ אלפבית תהא $\delta : Q \times \Sigma \to \mathcal{P}(Q)$ ותהיינה $S, F \subseteq Q$ 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 $\hat{\delta} : \mathcal{P}(Q) \times \Sigma^* \to \mathcal{P}(Q)$ עבורה לכל $T \subseteq Q$ מתקיים $\hat{\delta}(T, \varepsilon) = T$ וכן לכל $x \in \Sigma^n$ מתקיים $\hat{\delta}(q, x) = \bigcup_{q \in \hat{\delta}\left(T, x_1 \dots x_{n-1}\right)} \delta(q, x_n)$.

**אוטומט סופי לא־דטרמיניסטי מינוס מקבל מילה:** יהי $(Q, \Sigma, \delta, S, F)$ אסלד"ם אזי $\hat{\delta}(S, x) \cap F \neq \varnothing$ המקיים $x \in \Sigma^*$.

**טענה:** יהי $M$ אסלד"ם ויהי $x \in \Sigma^n$ אזי $M$ מקבל את $x$ $\Longleftrightarrow$ (קיימים $q_0 \dots q_n \in Q$ עבורם $q_0 \in S$ וכן $q_i \in \delta\left(q_{i-1}, x_i\right)$ לכל $i \in [n]$ וכן $q_n \in F$).

**שפה של אוטומט סופי לא־דטרמיניסטי מינוס:** יהי $M$ אסלד"ם אזי $L(M) = \{x \in \Sigma^* \mid \text{מקבל את } x\ M\}$.

**אוטומט סופי דטרמיניסטי מינוס החזקה:** יהי $M = (Q, \Sigma, \delta, S, F)$ אסלד"ם אזי אס"ד $\left(Q', \Sigma, \delta', q_0, F'\right)$ באשר

- $Q' = \mathcal{P}(Q)$.
- $\delta'(T, x) = \bigcup_{q \in T} \delta(q, x)$.
- $q_0 = S$.
- $F' = \{T \subseteq Q \mid T \cap F \neq \varnothing\}$.

**למה:** יהי $M$ אסלד"ם יהי $A$ אס"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 אס"ד $A$ עבורו $L(M) = L(A)$.

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

**אוטומט סופי לא־דטרמיניסטי (אסל"ד):** תהא $Q \neq \varnothing$ קבוצה סופית יהי $\Sigma$ אלפבית תהא $\delta : Q \times \Sigma_\varepsilon \to \mathcal{P}(Q)$ ותהיינה $S, F \subseteq Q$ אזי $(Q, \Sigma, \delta, S, F)$.

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

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

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

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

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

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

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

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

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

**מסקנה:** יהי $N$ אסל"ד אזי קיים אס"ד $A$ עבורו $L(A) = L(M)$.

**מסקנה:** יהי $\mathcal{L} \subseteq \Sigma^*$ שפה אזי $\mathcal{L}$ רגולרית $\Longleftrightarrow$ (קיים אסל"ד $N$ המקיים $L(N) = \mathcal{L}$).

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

- $\varnothing$.
- יהי $a \in \Sigma_\varepsilon$ אזי $a$.
- יהיו $R_1, R_2$ ביטויים רגולרים אזי $R_1 \cup R_2$.
- יהיו $R_1, R_2$ ביטויים רגולרים אזי $R_1 R_2$.
- יהי $R$ ביטוי רגולרי אזי $R^*$.

**הערה:** קיים סדר פעולות לביטויים רגולרים

- סגור קליני.
- שרשור.
- איחוד.

**משפט:** יהי $\Sigma$ אלפבית ותהא $\mathcal{L} \subseteq \Sigma^*$ שפה אזי $\mathcal{L}$ רגולרית $\Longleftrightarrow$ (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 $|w| > \ell$ קיימים $x, y, z \in \Sigma^*$ באשר $|y| > 0$ וכן $|xy| \leq \ell$ וכן $w = xyz$ וכן לכל $k \in \mathbb{N}$ מתקיים $xy^k z \in L$.

**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 $\min\left\{\ell \in \mathbb{N}_+ \mid \mathcal{L} \text{ ניתנת לניפוח } \ell\right\}$.

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

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

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

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

**הגדרה:** תהא $L \subseteq \Sigma^*$ שפה אזי $\sim_L = \left\{(x, y) \in (\Sigma^*)^2 \;\middle|\; \forall z \in \Sigma^* . (yz \in L) \Longleftrightarrow (xz \in L)\right\}$.

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

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

**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 $|Q| \geq |\Sigma^*/\sim_A| \geq \left|\Sigma^*/\sim_{L(A)}\right|$.

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

**משפט מייהיל־נרוד:** תהא $L \subseteq \Sigma^*$ שפה אזי $L$ רגולרית) $\Longleftrightarrow$ ($\Sigma^*/\sim_L$ 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 $\text{Class}(y) = i$ אזי $y \sim_L x_i$.

**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

- $Q = \left[\left|\Sigma^*/\sim_L\right|\right]$.
- $\delta(i, \sigma) = \text{Class}(x_i \sigma)$.
- $q_0 = \text{Class}(\varepsilon)$.
- $F = \{i \in Q \mid x_i \in L\}$.

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

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

**מכונת טיורינג (מ"ט):** תהא $Q \neq \varnothing$ 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 $\delta : (Q \setminus \{q_a, q_r\}) \times \Gamma \to Q \times \Gamma \times \{L, R\}$ 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 $c\sqcup$ עם $c$.

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

- קיימים $q, q' \in Q$ וקיימים $a, b, b' \in \Gamma$ וקיימים $u, v \in \Gamma^*$ עבורם $c = uaqbv$ וכן $c' = uq'ab'v$ וכן $\delta(q, b) = \left(q', b', L\right)$.
- קיימים $q, q' \in Q$ וקיימים $b, b' \in \Gamma$ וקיימים $u, v \in \Gamma^*$ עבורם $c = qbv$ וכן $\delta(q, b) = \left(q', b', L\right)$ וכן $c' = q'b'v$.
- קיימים $q, q' \in Q$ וקיימים $b, b' \in \Gamma$ וקיימים $u, v \in \Gamma^*$ עבורם $c = uqbv$ וכן $\delta(q, b) = \left(q', b', R\right)$ 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 $c_0 = q_0 x$ 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 $c_0 = q_0 x$ 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 $L(M) = \{x \in \Sigma^* \mid \text{מקבל את } x\ M\}$.

**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 $L(A) = L\left(A'\right)$.
- קיימת $B'$ מסוג $M$ המקיימת $L(B) = L\left(B'\right)$.

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

**מכונת טיורינג נחה:** תהא $Q \neq \varnothing$ 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 $\delta : (Q \setminus \{q_a, q_r\}) \times \Gamma \to Q \times \Gamma \times \{L, R, S\}$ אזי $(Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r)$.

**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 $Q \neq \varnothing$ 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 $\delta : (Q \setminus \{q_a, q_r\}) \times \Gamma^k \to Q \times \{L, R\}^k$ אזי $(k, Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r)$.

**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 ותהיינה $c_1 \dots c_k \in \Gamma^* Q \Gamma^*$ 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 $c = q_0 v \$ \sqcup \$ \dots \$ \sqcup \$ q_0$.

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

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

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

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

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

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

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

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

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

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

**מכונת טיורינג לא־דטרמיניסטית (מטל״ד):** תהא $Q \neq \varnothing$ 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 $\delta : (Q \setminus \{q_a, q_r\}) \times \Gamma \to \mathcal{P}(Q \times \Gamma \times \{L, R\})$ אזי $(Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r)$.

**קונפיגורציה עוברת:** תהא $N$ מטל״ד תהא $q \in Q$ ותהא $b \in \Gamma$ ותהיינה $u, v \in \Gamma^*$ באשר $uqbv$ קונפיגורציה איז קונפיגורציה $c'$ עבורה קיימת $\delta' : (Q \setminus \{q_a, q_r\}) \times \Gamma \to Q \times \Gamma \times \{L, R\}$ סופי וכן $x$ אינו מתקבל על ידי $N$. $\delta'(q, b) \in \delta(q, b)$ המקיימת $uqbv$ הינה $\delta'$־עוברת ל־$c'$.

**עץ חישוב:** תהא $N$ מטל״ד ויהי $x \in \Sigma^*$ אזי עץ קונפיגורציות $T_{N,x}$ עם שורש $q_0 x \sqcup$ עבורו לכל $c, c'$ קונפיגורציות מתקיים $c$ עוברת ל־$c'$ $\iff$ ($c'$ צאצא של $c$).

**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 $L(N) = \{x \in \Sigma^* \mid N \text{ מקבל את } x\}$.

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

**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 $\mathcal{R} = \{\mathcal{L} \subseteq \Sigma^* \mid \text{קיימת מ״ט } M \text{ המכריעה את } \mathcal{L}\}$.

**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 $(\mathcal{L} \in \mathcal{RE}) \iff$ ($\mathcal{L}$ 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 $(\mathcal{L} \in \mathcal{R}) \iff$ ($\mathcal{L}$ מונה לקסיקוגרפי).

**הגדרה:** יהי $\Sigma$ אלפבית אזי $\mathrm{co}\mathcal{RE} = \left\{\mathcal{L} \subseteq \Sigma^* \mid \overline{\mathcal{L}} \in \mathcal{RE}\right\}$.

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

**קידוד בינארי של מכונת טיורינג:** פונקציה $f : \{M \mid \text{מ״ט } M\} \to \{0,1\}^*$ 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 כנותו 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 $x \notin \mathrm{Im}(f)$ מתקיים כי $U$ דוחה את $x$.

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

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

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

**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 ACC אזי קיימת מ״ט $N$ המכריעה את $\{\langle N \rangle \mid \langle N \rangle \notin L(N)\}$.

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

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

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

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

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

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

**פונקציה חשיבה:** תהא $\Sigma \subseteq D$ אזי $f : D \to (\Gamma \setminus \{\sqcup\})^*$ המחשבת את $f$.

**רדוקציית מיפוי:** יהיו $\Sigma, \Delta$ אלפבייתים באשר $\Sigma \subseteq \Delta$ ותהא $A \subseteq \Sigma^*$ ותהא $B \subseteq \Delta^*$ שפה אזי $f : \Sigma^* \to \Delta^*$ חשיבה עבורה לכל $x \in \Sigma^*$ מתקיים $(x \in A) \iff (f(x) \in B)$.

**סימון:** יהיו $\Sigma, \Delta$ אלפבייתים באשר $\Sigma \subseteq \Delta$ ותהא $A \subseteq \Sigma^*$ ותהא $B \subseteq \Delta^*$ שפה ותהא $f : \Sigma^* \to \Delta^*$ רדוקציית מיפוי אזי $A \leq_m B$.

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

**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 שמכילה את רדוקציית המיפוי, לא עברנו על זה פורמלית, מסומן $\leq$.

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

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

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

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

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

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

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

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

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

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

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

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

- אם $B \in \mathcal{RE}$ אזי $A \in \mathcal{RE}$.
- אם $B \in \mathrm{co}\mathcal{RE}$ אזי $A \in \mathrm{co}\mathcal{RE}$.

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

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

**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 $\mathcal{C} \in \mathcal{P}(\mathcal{RE}) \setminus \{\mathcal{RE}, \varnothing\}$ תכונה סמנטית אזי $L_{\mathcal{C}} \notin \mathcal{R}$.

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

**הגדרת** $\mathrm{PRIME} = \{(p)_2 \mid p \in \mathbb{P}\}$.

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

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

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

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

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

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

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

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

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

**חסם עליון לזמן ריצה של מכונת טיורינג:** תהא $M$ מ״ט אזי $T : \mathbb{N} \to \mathbb{N}$ 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 $M$ אזי $T : \mathbb{N} \to \mathbb{N}$ מ״ט שרצה בזמן $\mathrm{DTime}(T(n)) = \{L(M) \mid \mathcal{O}(T(n))\}$.

**טענה:** $\mathrm{DTime}(n^2) \ni \left\{0^k 1^k \mid k \geq 0\right\}$.

**מסקנה:** $\mathrm{DTime}(n \log(n)) \ni \left\{0^k 1^k \mid k \geq 0\right\}$.

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

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

**פונקציה חשיבה בזמן:** פונקציה $T : \mathbb{N} \to \mathbb{N}$ 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 $T : \mathbb{N} \to \mathbb{N}$ 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 $M$ לכל 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 $\langle M, x, t \rangle$.

$C \cdot t \log(t)$ צעדים.

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

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

**טענה:** תהא $T : \mathbb{N} \to \mathbb{N}$ באשר $T(n) \geq n$ ותהא $M$ מ״ט רב־סרטית שרצה בזמן $T(n)$ אזי קיימת מ״ט $M'$ שרצה בזמן $\mathcal{O}\left(T^2(n)\right)$ עבורה $L(M) = L(M')$.

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

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

**הגדרה:** תהא $T : \mathbb{N} \to \mathbb{N}$ אזי $\mathrm{NTime}(T(n)) = \{L(N) \mid \mathcal{O}(T(n))\}$.

**טענה:** תהא $T : \mathbb{N} \to \mathbb{N}$ 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** $\mathcal{P}$: $\mathcal{P} = \bigcup_{c \in \mathbb{N}} \mathrm{DTime}(n^c)$.

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

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

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

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

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

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

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

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

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

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

**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 $\Sigma \cup \{\text{,}\}$ עבורה קיים $V(x, w)$ מקבלת.

- 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 $(\mathcal{L} \in \mathcal{RE}) \iff$ ($\mathcal{L}$ 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:** $\mathrm{CLIQUE} = \{\langle G, k \rangle \mid G \text{ גרף לא מכוון בעל קליקה מגודל } k\}$.

**טענה:** קיים מוודא פולינומי ל־CLIQUE.

**הגדרה:** $\mathrm{IS} = \{\langle G, k \rangle \mid G \text{ גרף לא מכוון בעל קבוצה בת״ל מגודל } k\}$.

**טענה:** קיים מוודא פולינומי ל־IS.

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

**טענה:** קיים מוודא פולינומי ל־FACTOR.

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

**טענה:** קיים מוודא פולינומי ל־SUBSETSUM.

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

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

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

**פונקציה חשיבה פולינומית:** תהא $\Sigma \subseteq D$ אזי $f : D \to (\Gamma \setminus \{\sqcup\})^*$ 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 $\Sigma, \Delta$ אלפבייתים באשר $\Sigma \subseteq \Delta$ ותהא $A \subseteq \Sigma^*$ ותהא $B \subseteq \Delta^*$ שפה אזי רדוקציית מיפוי $f$ מ־$A$ ל־$B$ חשיבה פולינומית.

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

**טענה:** $\mathrm{CLIQUE} \leq_p \mathrm{IS}$.

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

**שפה** $\mathcal{NPH}$־**קשה:** $\mathcal{NPH} = \{\mathcal{L} \mid \forall L \in \mathcal{NP}\ (L \leq_p \mathcal{L})\}$.

**שפה** $\mathcal{NPC}$־**שלמה:** $\mathcal{NPC} = \mathcal{NP} \cap \mathcal{NPH}$.

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

**הגדרה:** $\mathrm{ACC}_{\mathcal{NP}} = \left\{\left\langle M, x, 1^t \right\rangle \mid \text{קיים } w \text{ עבורו } M(x, w) \text{ מקבלת אחרי מקסימום } t \text{ צעדים}\right\}$.

**טענה:** $\mathrm{ACC}_{\mathcal{NP}} \in \mathcal{NPC}$.

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

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

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

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

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

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

**משפט קוק־לוין:** $3\mathrm{SAT} \in \mathcal{NPC}$.

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

**מסקנה:** יהי $k \in \mathbb{N} \setminus \{0, 1, 2\}$ אזי $k\mathrm{SAT} \in \mathcal{NPC}$.

**משפט:** $3\mathrm{SAT} \leq_p \mathrm{CLIQUE}$.

**מסקנה:** $\mathrm{CLIQUE}, \mathrm{IS} \in \mathcal{NPC}$.

**סימון:** תהא $A \in M_{m \times k}(\{p_i\} \cup \{\neg p_i\})$ ותהא $v$ השמה אזי $N\left(\bigwedge_{i=1}^m \bigvee_{j=1}^k (A)_{i,k}, v\right) = \left|\left\{i \in [m] \;\middle|\; \overline{v}\left(\bigvee_{j=1}^k (A)_{i,k}\right) = \mathrm{True}\right\}\right|$.

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

**טענה:** $C\mathrm{CNF} \in \mathcal{NPC}$.

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

**טענה:** $\mathrm{DNFCNF} \in \mathcal{P}$.

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

**הגדרה:** $\mathrm{VC} = \{\langle G, k \rangle \mid G \text{ גרף לא מכוון בעל כיסוי קודקודים מגודל } k\}$.

**טענה:** $\mathrm{VC} \in \mathcal{NPC}$.

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

**מעגל:** יהי $\Sigma$ אלפבית יהי $\mathcal{B}$ בסיס פונקציות מעל $\Sigma$ תהיינה $k_1 \dots k_n \in \mathbb{N}_+$ $f_1 \dots f_n \in \mathcal{B}$ באשר $f_i : \Sigma^{k_i} \to \Sigma$ 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 $T : \mathbb{N} \to \mathbb{N}$ 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 $\tau_{M,z} \in M_{T(n)+1}(\Sigma \uplus \Gamma)$ המקיימת $R_i(\tau_{M,z}) = c_i$.

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

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

**הגדרה:** תהא $T : \mathbb{N} \to \mathbb{N}$ 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 $T:\mathbb{N}\to\mathbb{N}$ חשיבה בזמן באשר $n\le T(n)$ ותהא $M$ מ״ט רצה בזמן $T(n)$ אזי $\left|C_{M,n}^{\Sigma\uplus\Gamma}\right|=\mathcal{O}\left(T^2(n)\right)$ וכן קיימת פונקציה $f$ חשיבה בזמן $\text{poly}(T(n))$ עבורה $f(1^n)=\left\langle C_{M,n}^{\Sigma\uplus\Gamma}\right\rangle$.

**מסקנה:** תהא $T:\mathbb{N}\to\mathbb{N}$ חשיבה בזמן באשר $n\le T(n)$ תהא $M$ 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 $C(z)=f(C)(z)$ לכל $z\in\{0,1\}^n$ וכן $|f(C)|=\mathcal{O}(|C|)$.

**למה:** תהא $T:\mathbb{N}\to\mathbb{N}$ חשיבה בזמן באשר $n\le T(n)$ ותהא $M$ מ״ט רצה בזמן $T(n)$ אזי קיימת פונקציה $f$ חשיבה בזמן $\text{poly}(T(n))$ עבורה $f(1^n)=\left\langle C_{M,n}\right\rangle$ באשר $C_{M,n}$ מעגל עבורו $\left|C_{M,n}\right|=\mathcal{O}\left(T^2(n)\right)$ וכן לכל $z\in\{0,1\}^n$ מתקיים $(C_{M,n}(z)=1\iff$ מקבלת $M(z))$.

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

**מסקנה:** תהא $T:\mathbb{N}\to\mathbb{N}$ חשיבה בזמן באשר $n\le T(n)$ ותהא $f:\{0,1\}^*\to\{0,1\}$ 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:** $\text{3SAT}\le_p\text{CIRSAT}$.

**טענה:** $\text{SUBSETSUM}\le_p\text{3SAT}$.

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

**טענה:** $\text{HAMPATH}\le_p\text{3SAT}$.

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

**שפה** co$\mathcal{NP}$: $\text{co}\mathcal{NP}=\left\{L\mid\overline{L}\in\mathcal{NP}\right\}$.

**השערה:** $\text{co}\mathcal{NP}\ne\mathcal{NP}$. השערה פתוחה

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

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

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

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

**השערה:** $\mathcal{P}\ne\mathcal{NP}\cap\text{co}\mathcal{NP}$. השערה פתוחה

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

**השערה:** $\mathcal{P}\ne\mathcal{NP}\cap\text{co}\mathcal{NP}$. 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 $D\ne0$ אזי $\mathbb{P}_{r\leftarrow\{0,1\}^n}(D\cdot r=0)\le0.5$.

**מסקנה:** קיימת מ״ט $M$ אשר רצה בזמן $\mathcal{O}\left(n^2\right)$ 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 $A\cdot B\ne C$ וכן $x=\langle A,B,C\rangle$ מתקיים $\mathbb{P}(M(x)\text{ מקבלת})\le2^{-100}$.

**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 $\varphi\equiv0$.

**הגדרה:** $\text{ZE}_{\mathbb{F}}=\{\langle\varphi\rangle\mid\varphi\equiv0\text{ עבורה}\}$.

**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 $(f=0)\iff(\varphi\equiv0)$.

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

**למה שוורץ־זיפל:** יהי $f\in\mathbb{F}[x_1,\dots,x_n]$ באשר $f\ne0$ ותהא $S\subseteq\mathbb{F}$ סופית אזי $\mathbb{P}_{a_1,\dots,a_n\leftarrow S}(f(a_1\dots a_n)=0)\le\frac{\deg(f)}{|S|}$.

**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 $\varphi\equiv0$ וכן $x=\langle\varphi\rangle$ מתקיים $M(x)$ מקבלת בזמן $\text{poly}(|\varphi|)$.
- אם קיימת $\varphi$ נוסחה אריתמטית מעל $\mathbb{R}$ המקיימת $\varphi\not\equiv0$ וכן $x=\langle\varphi\rangle$ מתקיים $\mathbb{P}(M(x)\text{ מקבלת})\le0.01$ 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 $\alpha:\mathbb{N}\to[0,1]$ ותהא שפה $\mathcal{L}$ עבורה קיימת מ״ט אקראית $M$ עם זמן ריצה פולינומי $T(n)$ המקיימת כי החל ממקום $n\in\mathbb{N}$ מתקיים

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

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

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

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

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

**הגדרה:** תהא $\alpha:\mathbb{N}\to[0,1]$ אזי $\text{co}\mathcal{RP}(\alpha)=\left\{\overline{L}\mid L\in\mathcal{RP}(\alpha)\right\}$.

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

- לכל $x\in\Sigma^n\cap\mathcal{L}$ מתקיים $\mathbb{P}_{r\leftarrow\{0,1\}^{T(n)}}(M(x;r))=1$ מקבלת.
- לכל $x\notin\mathcal{L}\cap\Sigma^n$ מתקיים $\mathbb{P}_{r\leftarrow\{0,1\}^{T(n)}}(M(x;r))\le1-\alpha(n)$ מקבלת.

**טענה:** $\text{ZE}_{\mathbb{R}}\in\text{co}\mathcal{RP}(0.99)$.

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

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

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

**הגדרה:** תהיינה $\alpha,\beta:\mathbb{N}\to[0,1]$ 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 $x\in\Sigma^n\cap\mathcal{L}$ מתקיים $\mathbb{P}_{r\leftarrow\{0,1\}^{T(n)}}(M(x;r))\ge\beta(n)$ מקבלת.
- לכל $x\notin\mathcal{L}\cap\Sigma^n$ מתקיים $\mathbb{P}_{r\leftarrow\{0,1\}^{T(n)}}(M(x;r))\le\alpha(n)$ מקבלת.

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

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

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

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

**טענה:** תהיינה $\alpha,\beta,\gamma,\delta:\mathbb{N}\to[0,1]$ עבורן $\alpha\le\beta\le\gamma\le\delta$ 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

$$\mathbb{P}\left(\left|p-\frac{1}{n}\sum_{i=1}^n A_i\right|\ge\delta\right)\le2^{-\Theta\left(\delta^2n\right)}.$$

**טענה:** יהיו $c,d\in\mathbb{N}$ ותהא $\alpha:\mathbb{N}\to[0,1]$ חשיבה בזמן פולינומי באשר $n^{-c}\le\alpha(n)\le1-n^{-c}$ החל ממקום מסויים אזי $\mathcal{BPP}\left(\alpha(n)-n^{-c},\alpha(n)+n^{-c}\right)\subseteq\mathcal{BPP}\left(2^{-n^d},1-2^{-n^d}\right)$.

# דפנוס גרסה של ארבעה עמודים

**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 $\langle w_1 \dots w_n \rangle^R = \langle w_n \dots w_1 \rangle$.
**שרשור מילים:** תהיינה $\langle w_1 \dots w_n \rangle, \langle \omega_1 \dots \omega_m \rangle \in \Sigma^*$ אזי
$\langle w_1 \dots w_n \rangle \langle \omega_1 \dots \omega_m \rangle = \langle w_1 \dots w_n, \omega_1 \dots \omega_m \rangle$.
**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 $L^R = \left\{ w^R \mid w \in L \right\}$.
**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
$L^m = \left\{ \prod_{i=1}^{k} w_i \mid \forall i \in [k] . w_i \in L \right\}$.
**סגור קליני של שפה:** תהא $L \subseteq \Sigma^*$ שפה אזי $L^* = \bigcup_{k=0}^{\infty} L^k$.
**שפת 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 $A : \Sigma^* \to \{\text{true}, \text{false}\}$ המקיים
- מקבל: לכל $x \in L$ מתקיים $A(x) = \text{true}$.
- דוחה: לכל $x \notin L$ מתקיים $A(x) = \text{false}$.

**פונקציה בולאנית:** תהיינה $n, m \in \mathbb{N}$ אזי $f : \{0,1\}^n \to \{0,1\}^m$.
**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 ותהיינה $k_1 \dots k_n \in \mathbb{N}_+$ תהיינה $f_1 \dots f_n \in \mathcal{B}$ באשר $f_i : \{0,1\}^{k_i} \to \{0,1\}$ 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 בוליאנרי אזי $\max_{v \in V(C)} \deg^+(v)$.
**נוחסאות:** יהי $C$ מעגל בוליאנרי אזי $\{G \leq C \mid \text{ה־fan-out של } G \text{ הוא } 1\}$.
**שערוך מעגל בוליאנרי על קלט:** יהי $C$ מעגל בוליאני 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 בוליאני 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 $L(C) = \{ x \in \{0,1\}^n \mid C \text{ מקבל את } x \}$.
**מעגל מחשב פונקציה:** תהא $f : \{0,1\}^n \to \{0,1\}$ אזי מעגל בוליאני $C$ עבורו לכל $v \in \{0,1\}^n$ מתקיים $C(v) = f(v)$.
**משפט אוניברסליות דה־מורגן:** תהא $f : \{0,1\}^m \to \{0,1\}^k$ אזי קיים מעגל בוליאני $C$ מעל בסיס דה־מורגן עבורו לכל $v \in \{0,1\}^m$ מתקיים $C(v) = f(v)$.
**הערה:** מכאן והלאה כל המעגלים הם בוליאניים 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
$L(\mathcal{C}) = \{ x \in \{0,1\}^* \mid x \in L(\mathcal{C}_{|x|}) \}$.
**משפחה מכריעה שפה:** תהא $L(\mathcal{C}) = \mathcal{L} \subseteq \{0,1\}^*$ 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 $S : \mathbb{N} \to \mathbb{N}$ עבורה $|\mathcal{C}_n| \leq S(n)$.
**טענה:** תהא $f : \{0,1\}^n \to \{0,1\}$ אזי קיים מעגל $C$ שמחשב את $f$ בגודל $\mathcal{O}(n \cdot 2^n)$.
**מסקנה:** תהא $L(C) = \mathcal{L} \subseteq \{0,1\}^n$ אזי קיים מעגל $C$ עבורו $L(C) = \mathcal{L}$ וכן $|C| = \mathcal{O}(n \cdot 2^n)$.
**טענה:** תהא $f : \{0,1\}^n \to \{0,1\}$ אזי קיים מעגל $C$ שמחשב את $f$ בגודל $\mathcal{O}(2^n)$.
**מסקנה:** תהא $L(C) = \mathcal{L} \subseteq \{0,1\}^n$ אזי קיים מעגל $C$ עבורו $L(C) = \mathcal{L}$ וכן $|C| = \mathcal{O}(2^n)$.
**משפט לופיאנוב:** תהא $f : \{0,1\}^n \to \{0,1\}$ 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 $f : \{0,1\}^n \to \{0,1\}$ שאינה ניתנת לחישוב בעזרת מעגל $C$ בגודל קטן מאשר $\frac{2^n}{10n}$.
**אוטומט סופי דטרמיניסטי (אס"ד):** תהא $Q \neq \varnothing$ קבוצה סופית יהי $\Sigma$ אלפבית תהא $\delta : Q \times \Sigma \to Q$ יהי $q \in Q$ 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 $\hat{\delta} : Q \times \Sigma^* \to Q$ עבורה לכל $q \in Q$ מתקיים $\hat{\delta}(q, \varepsilon) = q$ וכן לכל $x \in \Sigma^*$ מתקיים
$\hat{\delta}(q, x) = \delta\left(\hat{\delta}(q, x_1 \dots x_{n-1}), x_n\right)$.
**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 $x$)$\Longleftrightarrow$(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 $L(A) = \{ x \in \Sigma^* \mid A \text{ מקבל את } x \}$.
**שפה רגולרית:** יהי $\Sigma$ אלפבית אזי שפה $\mathcal{L} \subseteq \Sigma^*$ עבורה קיים אס"ד $A$ המקיים $L(A) = \mathcal{L}$.
**טענה:** $\varnothing$ רגולרית.
**טענה:** $\{\varepsilon\}$ רגולרית.
**טענה:** $\{x \mid \#_1(x) = 1 \mod 2\}$ רגולרית.
**טענה:** $\left\{ y\, 1\, 0^{2k} \mid (y \in \{0,1\}^*) \wedge (k \in \mathbb{N}) \right\}$ רגולרית.
**טענה:** יהיו $L_1, L_2, L_3 \subseteq \Sigma^*$ שפות אזי $L_1(L_2 L_3) = (L_1 L_2) L_3$.
**טענה:** תהא $L \subseteq \Sigma^*$ שפה באשר $L \neq \varnothing$ וכן $L \neq \{\varepsilon\}$ אזי $L^*$ אינסופית.
**משפט:** תהיינה $L, \mathcal{L} \subseteq \Sigma^*$ שפות רגולריות אזי
- $L \cup \mathcal{L}$ רגולרית.
- $L \cap \mathcal{L}$ רגולרית.
- $\overline{L}$ רגולרית.
- $L \| \mathcal{L}$ רגולרית.
- לכל $n \in \mathbb{N}$ מתקיים כי $L^n$ רגולרית.
- $L^*$ רגולרית.

**מסקנה:** $\{x \mid \#_1(x) = 0 \mod 2\}$ רגולרית.
**אוטומט סופי לא־דטרמיניסטי מינוס (אסלד"ם):** תהא $Q \neq \varnothing$ קבוצה סופית יהי $\Sigma$ אלפבית תהא $\delta : Q \times \Sigma \to \mathcal{P}(Q)$ ותהיינה $S, F \subseteq Q$ 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 $\hat{\delta} : \mathcal{P}(Q) \times \Sigma^* \to \mathcal{P}(Q)$ עבורה לכל $T \subseteq Q$ מתקיים $\hat{\delta}(T, \varepsilon) = T$ וכן לכל $x \in \Sigma^*$ 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 $\hat{\delta}(S, x) \cap F \neq \varnothing$.
**טענה:** יהי $M$ אסלד"ם ויהי $x \in \Sigma^n$ אזי ($M$ מקבל את $x$)$\Longleftrightarrow$(קיימים $q_0 \dots q_n \in Q$ עבורם $q_0 \in S$ וכן $q_i \in \delta(q_{i-1}, x_i)$ לכל $i \in [n]$ וכן $q_n \in F$).
**שפה של אוטומט סופי לא־דטרמיניסטי מינוס:** יהי $M$ אסלד"ם אזי $L(M) = \{ x \in \Sigma^* \mid M \text{ מקבל את } x \}$.

**אוטומט סופי דטרמיניסטי מינוס החזקה:** יהי $M = (Q, \Sigma, \delta, S, F)$ אסלד"ם אזי אס"ד $(Q', \Sigma, \delta', q_0, F')$ באשר
- $Q' = \mathcal{P}(Q)$.
- $\delta'(T, x) = \bigcup_{q \in T} \delta(q, x)$.
- $q_0 = S$.
- $F' = \{ T \subseteq Q \mid T \cap F \neq \varnothing \}$.

**למה:** יהי $M$ אסלד"ם יהי $A$ אס"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 אס"ד $A$ עבורו $L(M) = L(A)$.
**סימון:** יהי $\Sigma$ אלפבית אזי $\Sigma_\varepsilon = \Sigma \cup \{\varepsilon\}$.
**אוטומט סופי לא־דטרמיניסטי (אסל"ד):** תהא $Q \neq \varnothing$ קבוצה סופית יהי $\Sigma$ אלפבית תהא $\delta : Q \times \Sigma_\varepsilon \to \mathcal{P}(Q)$ ותהיינה $S, F \subseteq Q$ אזי $(Q, \Sigma, \delta, S, F)$.
**מצבים באוטומט סופי לא־דטרמיניסטי:** יהי $(Q, \Sigma, \delta, S, F)$ אסל"ד אזי $Q$.
**אלפבית באוטומט סופי לא־דטרמיניסטי:** יהי $(Q, \Sigma, \delta, S, F)$ אסל"ד אזי $\Sigma$.
**פונקציית מעברים באוטומט סופי לא־דטרמיניסטי:** יהי $(Q, \Sigma, \delta, S, F)$ אסל"ד אזי $\delta$.
**מצבים התחלתיים באוטומט סופי לא־דטרמיניסטי:** יהי $(Q, \Sigma, \delta, S, F)$ אסל"ד אזי $S$.
**מצבים מקבלים באוטומט סופי לא־דטרמיניסטי:** יהי $(Q, \Sigma, \delta, S, F)$ אסל"ד אזי $F$.
**סביבת $\varepsilon$:** יהי $N$ אסל"ד ויהי $q \in Q$ אזי
$E(q) = \left\{ q' \in Q \mid \exists a \in Q^{k+1} . (a_0 = q) \wedge \left( \forall i \in [k] . a_i \in \delta\left(a_{i-1}, \varepsilon\right) \right) \wedge \left( a_k = q' \right) \right\}$.
**סביבת $\varepsilon$:** יהי $N$ אסל"ד ויהי $T \subseteq Q$ אזי $E(T) = \bigcup_{q \in T} E(q)$.
**פונקציית המעברים המורחבת:** יהי $(Q, \Sigma, \delta, S, F)$ אסל"ד אזי $\hat{\delta} : \mathcal{P}(Q) \times \Sigma^* \to \mathcal{P}(Q)$ עבורה לכל $T \subseteq Q$ מתקיים $\hat{\delta}(T, \varepsilon) = E(T)$ וכן לכל $x \in \Sigma^n$ מתקיים
$\hat{\delta}(q, x) = R\left( \bigcup_{q \in \hat{\delta}(T, x_1 \dots x_{n-1})} \delta(q, x_n) \right)$.
**אוטומט סופי לא־דטרמיניסטי מקבל מילה:** יהי $(Q, \Sigma, \delta, S, F)$ אסל"ד אזי $x \in \Sigma^*$ המקיים $\hat{\delta}(S, x) \cap F \neq \varnothing$.
**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 $x^\varepsilon = \sigma_1 \dots \sigma_n$.
**טענה:** יהי $A$ אסל"ד ויהי $x \in \Sigma^n$ אזי ($A$ מקבל את $x$)$\Longleftrightarrow$(קיימים $q_0 \dots q_n \in Q$ עבורם $q_0 \in S$ וכן $q_i \in \delta(q_{i-1}, x_i^\varepsilon)$ לכל $i \in [n]$ וכן $q_n \in F$).
**שפה של אוטומט סופי לא־דטרמיניסטי:** יהי $A$ אסל"ד אזי $L(A) = \{ x \in \Sigma^* \mid A \text{ מקבל את } x \}$.
**משפט:** יהי $N$ אסל"ד אזי קיים אסלד"ם $M$ עבורו $L(N) = L(M)$.
**מסקנה:** יהי $N$ אסל"ד אזי קיים אס"ד $A$ עבורו $L(A) = L(M)$.
**מסקנה:** יהי $\Sigma$ אלפבית ותהא $\mathcal{L} \subseteq \Sigma^*$ שפה אזי ($\mathcal{L}$ רגולרית)$\Longleftrightarrow$(קיים אסל"ד $N$ המקיים $L(N) = \mathcal{L}$).
**ביטוי רגולרי (ב"ר):** יהי $\Sigma$ אלפבית אזי
- $\varnothing$.
- יהי $a \in \Sigma_\varepsilon$ אזי $a$.
- יהיו $R_1, R_2$ ביטויים רגולרים אזי $R_1 \cup R_2$.
- יהיו $R_1, R_2$ ביטויים רגולרים אזי $R_1 R_2$.
- יהי $R$ ביטוי רגולרי אזי $R^*$.

**שפה נוצרת מביטוי רגולרי:** יהי $\Sigma$ אלפבית אזי
- $L(\varnothing) = \varnothing$.
- יהי $a \in \Sigma_\varepsilon$ אזי $L(a) = \{a\}$.
- יהיו $R_1, R_2$ ביטויים רגולרים אזי $L(R_1 \cup R_2) = L(R_1) \cup L(R_2)$.
- יהיו $R_1, R_2$ ביטויים רגולרים אזי $L(R_1 R_2) = L(R_1) L(R_2)$.
- יהי $R$ ביטוי רגולרי אזי $L(R^*) = L(R)^*$.

**סימון:** יהי $\Sigma$ אלפבית אזי $R(\Sigma) = \{ r \in \Sigma^* \mid r \text{ ביטוי רגולרי} \}$.
**הערה:** קיים סדר פעולות לביטויים רגולריים
- סגור קליני.
- שרשור.
- איחוד.

**משפט:** יהי $\Sigma$ אלפבית ותהא $\mathcal{L} \subseteq \Sigma^*$ שפה אזי ($\mathcal{L}$ רגולרית)$\Longleftrightarrow$(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 לכל $k \in \mathbb{N}$ מתקיים $xy^k z \in L$.
**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 $\min\{\ell \in \mathbb{N}_+ \mid \ell \text{ ניתנת לניפוח}\}$.

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

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

**טענה:** $\{a^p \mid a \in \Sigma, p$ 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 $\sim_A = \left\{(x,y) \in (\Sigma^*)^2 \;\middle|\; \hat{\delta}(q_0, x) = \hat{\delta}(q_0, y)\right\}$.

**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 $|Q| \geq \left|\Sigma^*/\sim_A\right| \geq \left|\Sigma^*/\sim_{L(A)}\right|$.

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

**משפט מייהיל-נרוד:** תהא $L \subseteq \Sigma^*$ שפה אזי ($L$ רגולרית)$\iff$($\Sigma^*/\sim_L$ 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

- $Q = \left[\left|\Sigma^*/\sim_L\right|\right]$.
- $\delta(i, \sigma) = \text{Class}(x_i \sigma)$.
- $q_0 = \text{Class}(\varepsilon)$.
- $F = \{i \in Q \mid x_i \in L\}$.

**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 $y \in \Sigma^*$ אזי $\hat{\delta}_A(q_0, y) = \text{Class}(y)$.

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

**מכונת טיורינג (מ"ט):** תהא $Q \neq \varnothing$ קבוצה סופית יהי $\Sigma$ אלפבית יהי $\Gamma$ אלפבית עבורו $\Sigma \subseteq \Gamma$ וכן $\sqcup \in \Gamma \backslash \Sigma$ יהיו $q_0, q_a, q_r \in Q$ באשר $q_a \neq q_r$ ותהא
$\delta : (Q \backslash \{q_a, q_r\}) \times \Gamma \to Q \times \Gamma \times \{L, R\}$ 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 $\sqcup c$ 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 $c_0 = q_0 x$ 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 $c_0 = q_0 x$ 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 $L(M) = \{x \in \Sigma^* \mid x$ מקבל את $M\}$.

**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"ם הינם מודלים שקולים.

**מכונת טיורינג נחה:** תהא $Q \neq \varnothing$ קבוצה סופית יהי $\Sigma$ אלפבית יהי $\Gamma$ אלפבית עבורו $\Sigma \subseteq \Gamma$ וכן $\sqcup \in \Gamma \backslash \Sigma$ יהיו $q_0, q_a, q_r \in Q$ באשר $q_a \neq q_r$ ותהא $\delta : (Q \backslash \{q_a, q_r\}) \times \Gamma \to Q \times \Gamma \times \{L, R, S\}$ אזי $(Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r)$.

**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 $Q \neq \varnothing$ קבוצה סופית יהי $\Sigma$ אלפבית יהי $\Gamma$ אלפבית עבורו $\Sigma \subseteq \Gamma$ וכן $\sqcup \in \Gamma \backslash \Sigma$ יהיו $q_0, q_a, q_r \in Q$ באשר $q_a \neq q_r$ ותהא $\delta : (Q \backslash \{q_a, q_r\}) \times \Gamma^k \to Q \times \Gamma^k \times \{L, R\}^k$ אזי $(k, Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r)$.

**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 ותהיינה $c_1 \dots c_k \in \Gamma^* Q \Gamma^*$ 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 $k \in \mathbb{N}$ ותהיינה $\pi_1 \dots \pi_p$ 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 $\text{PC} \in \mathbb{N}$ וכן $R_0 \dots R_k \in \mathbb{N}$ וכן $T : \mathbb{N} \to \mathbb{N}$.

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

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

**זיכרון בקונפיגורציה:** יהי $(k, \Pi)$ מודל RAM ותהא $(T, R, \text{PC})$ 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 $Q \neq \varnothing$ קבוצה סופית יהי $\Sigma$ אלפבית יהי $\Gamma$ אלפבית עבורו $\Sigma \subseteq \Gamma$ וכן $\sqcup \in \Gamma \backslash \Sigma$ יהיו $q_0, q_a, q_r \in Q$ באשר $q_a \neq q_r$ ותהא $\delta : (Q \backslash \{q_a, q_r\}) \times \Gamma \to \mathcal{P}(Q \times \Gamma \times \{L, R\})$ אזי $(Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r)$.

**קונפיגורציה עוברת:** תהא $N$ מטל"ד תהא $q \in Q$ ותהא $b \in \Gamma$ ותהיינה $u, v \in \Gamma^*$ באשר $uqbv$ קונפיגורציה אזי קונפיגורציה $c'$ עבורה קיימת $\delta' : (Q \backslash \{q_a, q_r\}) \times \Gamma \to Q \times \Gamma \times \{L, R\}$ המקיימת $\delta'(q, b) \in \delta(q, b)$ 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 $q_0 x \sqcup$ עבורו לכל $c, c'$ קונפיגורציות מתקיים ($c$ צאצא של $c'$)$\iff$($c'$ 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
$L(N) = \{x \in \Sigma^* \mid x$ מקבל את $N\}$.

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

**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
$\mathcal{R} = \{\mathcal{L} \subseteq \Sigma^* \mid \mathcal{L}$ המכריעה את $M$ קיימת מ"ט$\}$.

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

**מונה עבור שפה:** תהא $\Sigma^* \subseteq \mathcal{L}$ 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 $\Sigma^* \subseteq \mathcal{L}$ שפה אזי ($\mathcal{L} \in \mathcal{RE}$)$\iff$(קיים ל־$\mathcal{L}$ מונה).

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

**הגדרה:** יהי $\Sigma$ אלפבית אזי $\text{co}\mathcal{RE} = \left\{\mathcal{L} \subseteq \Sigma^* \;\middle|\; \overline{\mathcal{L}} \in \mathcal{RE}\right\}$.

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

**קידוד בינארי של מכונת טיורינג:** פונקציה $f : \{M \mid M$ מ"ט$\} \to \{0,1\}^*$ 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 ($U$ מקבלת את $\langle M, x \rangle$)$\iff$($M$ מקבלת את $x$).
- לכל מ"ט $M$ ולכל קלט $x$ של $M$ מתקיים ($U$ דוחה את $\langle M, x \rangle$)$\iff$($M$ דוחה את $x$).
- לכל מ"ט $M$ ולכל קלט $x$ של $M$ מתקיים ($U$ לא עוצרת עבור $\langle M, x \rangle$)$\iff$($M$ לא עוצרת עבור $x$).
- לכל $x \in \{0,1\}^*$ באשר $x \notin \text{Im}(f)$ מתקיים כי $U$ דוחה את $x$.

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

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

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

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

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

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

**מכונת טיורינג מחשבת פונקציה:** תהא $M$ מ"ט ותהא $D \subseteq \Sigma$ אזי $f : D \to (\Gamma \backslash \{\sqcup\})^*$ 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 $f : D \to (\Gamma \backslash \{\sqcup\})^*$ עבורה קיימת מ"ט $M$ המחשבת את $f$.

**רדוקציית מיפוי:** יהיו $\Sigma, \Delta$ אלפבייתים באשר $\Sigma \subseteq \Delta$ תהא $A \subseteq \Sigma^*$ שפה ותהא $B \subseteq \Delta^*$ שפה אזי $f : \Sigma^* \to \Delta^*$ חשיבה עבורה לכל $x \in \Sigma^*$ מתקיים $(x \in A) \iff (f(x) \in B)$.

**סימון:** יהיו $\Sigma, \Delta$ אלפבייתים באשר $\Sigma \subseteq \Delta$ תהא $A \subseteq \Sigma^*$ שפה תהא $B \subseteq \Delta^*$ שפה ותהא $f : \Sigma^* \to \Delta^*$ רדוקציית מיפוי אזי $A \leq_m B$.

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

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

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

**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:** $\text{REG} = \{\langle M \rangle \mid L(M)$ 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:** $\text{HALT}_\varepsilon = \{\langle M \rangle \mid M$ עוצר על $\varepsilon\}$.

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

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

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

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

- אם $B \in \mathcal{RE}$ אזי $A \in \mathcal{RE}$.
- אם $B \in \mathrm{co}\mathcal{RE}$ אזי $A \in \mathrm{co}\mathcal{RE}$.

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

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

**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 $\mathcal{C} \in \mathcal{P}(\mathcal{RE}) \setminus \{\mathcal{RE}, \varnothing\}$ תכונה סמנטית אזי $L_{\mathcal{C}} \notin \mathcal{R}$.

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

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

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

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

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

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

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

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

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

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

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

**חסם עליון לזמן ריצה של מכונת טיורינג:** תהא $M$ מ"ט אזי $T : \mathbb{N} \to \mathbb{N}$ 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 $T : \mathbb{N} \to \mathbb{N}$ אזי $M$ מ"ט שרצה בזמן $\mathrm{DTime}(T(n)) = \{L(M) \mid \mathcal{O}(T(n))$.

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

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

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

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

**פונקציה חשיבה בזמן:** פונקציה $T : \mathbb{N} \to \mathbb{N}$ 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 $T : \mathbb{N} \to \mathbb{N}$ 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 $M$ לכל 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 $T : \mathbb{N} \to \mathbb{N}$ חשיבה בזמן ותהא $t(n) = o\left(\frac{T(n)}{\log(T(n))}\right)$ אזי $\mathrm{DTime}(t(n)) \subsetneq \mathrm{DTime}(T(n))$.

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

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

**טענה:** תהא $T : \mathbb{N} \to \mathbb{N}$ 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 $T : \mathbb{N} \to \mathbb{N}$ עבורה לכל $n \in \mathbb{N}$ ולכל $x \in \Sigma^n$ מתקיים כי $T_{N,x}$ בעומק לכל היותר $T(n)$.

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

**טענה:** תהא $T : \mathbb{N} \to \mathbb{N}$ 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 $\mathcal{P}$:** $\mathcal{P} = \bigcup_{c \in \mathbb{N}} \mathrm{DTime}(n^c)$.

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

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

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

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

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

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

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

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

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

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

**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 $\Sigma \cup \{\text{"}\,\text{"}\}$ 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 ($\mathcal{L} \in \mathcal{RE}$)$\Longleftrightarrow$(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:** $\mathrm{CLIQUE} = \{\langle G, k \rangle \mid$ $G$ גרף לא מכוון בעל קליקה מגודל $k\}$.

**טענה:** קיים מוודא פולינומי ל־CLIQUE.

**הגדרה:** $\mathrm{IS} = \{\langle G, k \rangle \mid$ $G$ גרף לא מכוון בעל קבוצה בת"ל מגודל $k\}$.

**טענה:** קיים מוודא פולינומי ל־IS.

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

**טענה:** קיים מוודא פולינומי ל־FACTOR.

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

**טענה:** קיים מוודא פולינומי ל־SUBSETSUM.

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

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

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

**פונקציה חשיבה פולינומית:** תהא $D \subseteq \Sigma$ אזי $f : D \to (\Gamma \setminus \{\sqcup\})^*$ 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 $\Sigma, \Delta$ אלפבייתים באשר $\Sigma \subseteq \Delta$ תהא $A \subseteq \Sigma^*$ שפה ותהא $B \subseteq \Delta^*$ שפה אזי רדוקציית מיפוי $f$ מ־$A$ ל־$B$ חשיבה פולינומית.

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

**טענה:** $\mathrm{CLIQUE} \leq_p \mathrm{IS}$.

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

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

**שפה $\mathcal{NP}$-שלמה:** $\mathcal{NPC} = \mathcal{NP} \cap \mathcal{NPH}$.

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

**הגדרה:** $\mathrm{ACC}_{\mathcal{NP}} = \left\{\langle M, x, 1^t \rangle \mid$ קיים $w$ עבורו $M(x, w)$ מקבלת אחרי מקסימום $t$ צעדים$\right\}$.

**טענה:** $\mathrm{ACC}_{\mathcal{NP}} \in \mathcal{NPC}$.

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

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

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

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

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

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

**משפט קוק־לוין:** $3\mathrm{SAT} \in \mathcal{NPC}$.

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

**מסקנה:** יהי $k \in \mathbb{N} \setminus \{0, 1, 2\}$ אזי $k\mathrm{SAT} \in \mathcal{NPC}$.

**משפט:** $3\mathrm{SAT} \leq_p \mathrm{CLIQUE}$.

**מסקנה:** $\mathrm{CLIQUE, IS} \in \mathcal{NPC}$.

**סימון:** תהא $A \in M_{m \times k}(\{p_i\} \cup \{\neg p_i\})$ ותהא $v$ השמה אזי $N\left(\bigwedge_{i=1}^m \bigvee_{j=1}^k (A)_{i,k}, v\right) = \left|\left\{i \in [m] \;\middle|\; \overline{v}\left(\bigvee_{j=1}^k (A)_{i,k}\right) = \mathrm{True}\right\}\right|$.

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

**טענה:** $C\mathrm{CNF} \in \mathcal{NPC}$.

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

**טענה:** $\mathrm{DNFCNF} \in \mathcal{P}$.

**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:** $\mathrm{VC} = \{\langle G, k \rangle \mid$ $G$ גרף לא מכוון בעל כיסוי קודקודים מגודל $k\}$.

**טענה:** $\mathrm{VC} \in \mathcal{NPC}$.

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

**מעגל:** יהי $\Sigma$ אלפבית יהי $\mathcal{B}$ בסיס פונקציות מעל $\Sigma$ תהיינה $k_1 \ldots k_n \in \mathbb{N}_+$ תהיינה $f_1 \ldots f_n \in \mathcal{B}$ באשר $f_i : \Sigma^{k_i} \to \Sigma$ לכל $i \in [n]$ ותהיינה $x_1 \ldots x_m, y_1 \ldots y_k \in \Sigma$ אזי גרף מכוון $G$ מעל $\{f_1 \ldots f_n, x_1 \ldots x_m, y_1 \ldots y_k\}$ 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 $T : \mathbb{N} \to \mathbb{N}$ חשיבה בזמן באשר $n \leq T(n)$ תהא $M$ מ"ט שרצה בזמן $T(n)$ יהי $z \in \{0,1\}^n$ ותהיינה $c_1 \ldots c_i$ קונפיגורציות הריצה של $M(z)$ אזי $R_i(\tau_{M,z}) = c_i$ המקיימת $\tau_{M,z} \in M_{T(n)+1}(\Sigma \uplus \Gamma)$.

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

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

**הגדרה:** תהא $T : \mathbb{N} \to \mathbb{N}$ 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 $C_{\mathrm{inp}}(z) = R_0(\tau_{M,z})$.
- יהי $z \in \Sigma \uplus \Gamma$ ויהי $i \in \{0, \ldots, T(n) - 1\}$ אזי $C_{\mathrm{next}}(R_i(\tau_{M,z})) = R_{i+1}(\tau_{M,z})$.
- יהי $z \in \Sigma \uplus \Gamma$ אזי $C_{\mathrm{out}}\left(R_{T(n)}(\tau_{M,z})\right) = M(z)$.
- יהי $z \in \Sigma \uplus \Gamma$ אזי $C_{M,n}^{\Sigma \uplus \Gamma}(z) = (C_{\mathrm{out}} \circ C_{\mathrm{next}} \circ \ldots \circ C_{\mathrm{next}} \circ C_{\mathrm{inp}})(z)$.

**טענה:** תהא $T : \mathbb{N} \to \mathbb{N}$ חשיבה בזמן באשר $n \leq T(n)$ ותהא $M$ מ"ט רצה בזמן $T(n)$ אזי $\left|C_{M,n}^{\Sigma \uplus \Gamma}\right| = \mathcal{O}(T^2(n))$ וכן קיימת פונקציה $f$ חשיבה בזמן $\mathrm{poly}(T(n))$ עבורה $f(1^n) = \left\langle C_{M,n}^{\Sigma \uplus \Gamma} \right\rangle$.

**מסקנה:** תהא $T : \mathbb{N} \to \mathbb{N}$ חשיבה בזמן באשר $n \leq T(n)$ תהא $M$ 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 $C(z) = f(C)(z)$ לכל $z \in \{0,1\}^n$ וכן $|f(C)| = \mathcal{O}(|C|)$.

**למה:** תהא $T : \mathbb{N} \to \mathbb{N}$ חשיבה בזמן באשר $n \leq T(n)$ ותהא $M$ מ"ט רצה בזמן $T(n)$ אזי קיימת פונקציה $f$ חשיבה בזמן $\mathrm{poly}(T(n))$ 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$\Longleftrightarrow(C_{M,n}(z) = 1)$.

**טענה:** $\mathrm{CIRSAT} \in \mathcal{NPC}$.

**מסקנה:** תהא $T : \mathbb{N} \to \mathbb{N}$ חשיבה בזמן באשר $n \leq T(n)$ ותהא $f : \{0,1\}^* \to \{0,1\}$ 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:** $\mathrm{CIRSAT} \leq_p 3\mathrm{SAT}$.

**טענה:** $3\mathrm{SAT} \leq_p \mathrm{SUBSETSUM}$.

**מסקנה:** $\mathrm{SUBSETSUM} \in \mathcal{NPC}$.

**טענה:** $3\mathrm{SAT} \leq_p \mathrm{HAMPATH}$.

**מסקנה:** $\mathrm{HAMPATH} \in \mathcal{NPC}$.

**שפה $\mathrm{co}\mathcal{NP}$:** $\mathrm{co}\mathcal{NP} = \left\{L \mid \overline{L} \in \mathcal{NP}\right\}$.

**השערה:** $\mathrm{co}\mathcal{NP} \neq \mathcal{NP}$. השערה פתוחה

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

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

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

**מסקנה:** תהא $\mathcal{L} \in \mathcal{NPC}$ אזי $(\mathcal{L} \in \mathrm{co}\mathcal{NP}) \iff (\mathrm{co}\mathcal{NP} = \mathcal{NP})$.

**טענה:** $\mathcal{P} \subseteq \mathcal{NP} \cap \mathrm{co}\mathcal{NP}$.

**השערה:** $\mathcal{P} \neq \mathcal{NP} \cap \mathrm{co}\mathcal{NP}$. השערה פתוחה

**טענה:** $\mathrm{FACTOR} \in \mathcal{NP} \cap \mathrm{co}\mathcal{NP}$.

**השערה:** $\mathcal{P} \neq \mathcal{NP} \cap \mathrm{co}\mathcal{NP}$. השערה פתוחה

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

**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 $\mathbb{P}(M(x) \text{ מקבלת}) \leq 2^{-100}$.

**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 $x_1 \ldots x_n \in \mathbb{F}$ מתקיים $\varphi(x_1 \ldots x_n) = 0$ אזי $\varphi \equiv 0$.

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

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

**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 $f \in \mathbb{F}[x_1, \ldots, x_n]$ באשר $\deg(f) < |\mathbb{F}|$ אזי $(\varphi \equiv 0) \iff (f = 0)$.

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

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

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

**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 $\alpha : \mathbb{N} \to [0,1]$ 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 $\mathbb{P}_{r \leftarrow \{0,1\}^{T(n)}}(M(x; r) \text{ מקבלת}) \geq \alpha(n)$.
- לכל $x \notin \mathcal{L} \cap \Sigma^n$ מתקיים $\mathbb{P}_{r \leftarrow \{0,1\}^{T(n)}}(M(x; r) \text{ מקבלת}) = 0$.

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

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

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

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

**הגדרה:** תהא $\alpha : \mathbb{N} \to [0,1]$ אזי $\mathrm{co}\mathcal{RP}(\alpha) = \left\{\overline{L} \mid L \in \mathcal{RP}(\alpha)\right\}$.

**טענה:** תהא $\alpha : \mathbb{N} \to [0,1]$ ותהא שפה $\mathcal{L}$ אזי $\mathcal{L} \in \mathrm{co}\mathcal{RP}(\alpha)$ אם"ם 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 $\mathbb{P}_{r \leftarrow \{0,1\}^{T(n)}}(M(x; r) \text{ מקבלת}) = 1$.
- לכל $x \notin \mathcal{L} \cap \Sigma^n$ מתקיים $\mathbb{P}_{r \leftarrow \{0,1\}^{T(n)}}(M(x; r) \text{ מקבלת}) \leq 1 - \alpha(n)$.

**טענה:** $\mathrm{ZE}_{\mathbb{R}} \in \mathrm{co}\mathcal{RP}(0.99)$.

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

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

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

**הגדרה:** תהיינה $\alpha, \beta : \mathbb{N} \to [0,1]$ 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 $\mathbb{P}_{r \leftarrow \{0,1\}^{T(n)}}(M(x; r) \text{ מקבלת}) \geq \beta(n)$.
- לכל $x \notin \mathcal{L} \cap \Sigma^n$ מתקיים $\mathbb{P}_{r \leftarrow \{0,1\}^{T(n)}}(M(x; r) \text{ מקבלת}) \leq \alpha(n)$.

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

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

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

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

**טענה:** תהיינה $\alpha, \beta, \gamma, \delta : \mathbb{N} \to [0,1]$ 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 $A_1, \ldots, A_n \sim \mathrm{Ber}(p)$ אזי $\mathbb{P}\left(\left|p - \frac{1}{n}\sum_{i=1}^n A_i\right| \geq \delta\right) \leq 2^{-\Theta\left(\delta^2 n\right)}$.

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