דפנוס גרסה של שלושה עמודים

```
\#_\sigma\left(w
ight)=\left|\left\{i\in[n]\mid w_i=\sigma
ight\}
ight| אות אזי \sigma\in\Sigma אות אות במילה: תהא מספר המופעים של אות במילה: עה w\in\Sigma^n ותהא
                                                                                                                                                                                                                                                                                                                                   בוולרים I.II.C
                     טענה: השפה \left\{a^ib^nc^n\mid n\in\mathbb{N},i\in\mathbb{N}_+
ight\}\cup\left\{b^nc^n\mid n,m\in\mathbb{N}
ight\} ניתנת לניפוח 1 וכן אינה רגולרית.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                L\subseteq \Sigma^* שפה: יהי \Sigma אלפבית אזי
                                                                                                                                                                                                                                                                                                     תנלרית. בי לכל n \in \mathbb{N} מתקיים כי n \in \mathbb{N} רגולרית.
                                                                                                                                    אזי אפה אזי L\subset \Sigma^* מפה אזי
                                                                                                                                                                                                                                                                                                                                                                                                                                                                  L^R = \left\{ w^R \mid w \in L 
ight\} שפה אזי L \subseteq \Sigma^* תהא היפוך שפה: תהא
                                                                                                                                                                                                                                                                                                                                      . רגולרית L^*
                                                           \sim_L = \{(x, y) \in (\Sigma^*)^2 \mid \forall z \in \Sigma^* . (yz \in L) \iff (xz \in L)\}
                                                                                                                                                                                                                                                                                                 מסקנה: \{x \mid \#_1(x) = 0 \mod 2\} רגולרית.
                                                                                                                                                                                                                                                                                                                                                                                         L_1 \parallel L_2 = L_1 L_2 = \{w\omega \mid (w \in L_1) \wedge (\omega \in L_2)\} שפות אזי ער שפות: תהיינה L_1, L_2 \subseteq \Sigma^* שרשור שפות: תהיינה
                                                                                                       .
טענה: תהא \Sigma^* \subseteq L שפה אזי L \subseteq \Sigma הינו יחס שקילות.
                                                                                                                                                                                                                                                                                                                                                                                                           L^m=\left\{\prod_{i=1}^k w_i \mid \forall i \in [k] \,.w_i \in L 
ight\} אוי m \in \mathbb{N} אוי עפה ויהי עפה ויהי תהא בפה: תהא
                                                                                                                                                                                        אוטומט סופי לא־דטרמיניסטי מינוס (אסלד"ם): תהא Q 
eq \mathcal{D} קבוצה סופית יהי \mathcal{D} אלפבית הא \delta: Q \times \Sigma \to \mathcal{P} (ער האינה אלפבית הא
                                                     \sim_A = \left\{ (x,y) \in (\Sigma^*)^2 \;\middle|\; \hat{\delta}\left(q_0,x
ight) = \hat{\delta}\left(q_0,y
ight) 
ight\} הגדרה: יהי A אט"ד איי איי
                                                                                                                                                                                                                                                                                                                                                                                                                                                                   L^* = igcup_{k=0}^\infty L^k סגור קליני של שפה: תהא L \subseteq \Sigma^* תהא שפה:
                                                                                                                                                                                                                                                                                                                   (Q, \Sigma, \delta, S, F) אא S, F \subset Q
                                                                    x\sim_{L(A)}y אזיx\sim_{A}y עבורם x,y\in\Sigma^{*} ויהיו אס"ד ויהיו אס"ד אזי x\sim_{L(A)}y
                                                                                                                                                                                                                                                        Q אזי אוילד"ם אוי (Q, \Sigma, \delta, S, F) אוי מינוס: יהי ארדטרמיניסטי סופי ארדטרמיניסטי מינוס: יהי
                                                                                                                                                                                                                                                                                                                                                                                                                              .prefix (L)=\{y\in \Sigma^*\mid \exists x\in \Sigma^*.yx\in L\} שפה אזי עפה אזי עפה ברישא: תהא L\subseteq \Sigma^* אחת.
                                                                                 |Q| \geq \left|\Sigma^*/{\sim_A}\right| \geq \left|\Sigma^*/{\sim_{L(A)}}\right| מסקנה: יהי A אס"ד איז איז מסקנה: יהי א
                                                                                                                                                                                                                                                       \Sigma אזי אסלד"ם אזי (Q,\Sigma,\delta,S,F) אסלד"ם אזי אסלד"ם אזי אסלד"ם אזי
                                                                                                                                                                                                                                                                                                                                                                                                                               .suffix (L)=\{y\in\Sigma^*\mid\exists x\in\Sigma^*.xy\in L\} שפה איז L\subset\Sigma^* תהא שמת הסיפא: תהא
                                                                                                                                                                                                                                           .
\delta אזי סאלד"ם אסלד"ם ( Q,\, \Sigma,\, \delta,\, S,\, F)יהי מינוס: לא־דטרמיניסטי סופי אסלד"ם אזי מעברים אסלד
                                                                                               מסקנה: תהא \Sigma^*/\sim_L שפה רגולרית אזי בL\subseteq \Sigma^* סופית.
                                                                                                                                                                                                                                                                                                                                                                                                                                אלגוריתם מכריע שפה: תהא A:\Sigma^*	o \{	ext{true}, 	ext{false}\} שפה אזי אלגוריתם L\subset\Sigma^* המקיים
                                                                                                                                                                                                                                         S אזי אסלד"ם אסלד"ם אסלד"ם אזי אסלד"ם אזי אסלד"ם אזי אסלד"ם אזי אסלד"ם אזי אסלד"ם אזי
                                                                 . (סופית) שפט מייהיל־נרוד: תהא \Sigma^*/\sim L שפה אזי שפט בה רגולרית) שפט מייהיל־נרוד: תהא בה על בברוד שפה אזי ווער הא
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   A\left(x
ight)= true מקבל: לכל x\in L מתקיים \bullet
                                                                                                                                                                                                                                            F אזי אויים אויר אסלד"ם אויר אסלד"ם אויים מקבלים באוטומט אופי איז מינוס: איז מינוס: אויי אויים אויים מקבלים אויי
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  A\left(x
ight)= false מתקיים x
otin L לכל •
 עבורו y\in \Sigma^* ויהי \Sigma^*/\sim_L ויהי פוצת עניגים של \Sigma^*/\sim_L ויהי שפה באשר \Sigma^*/\sim_L שפה באשר בער \Sigma^*/\sim_L שפה באשר בער בער איני שייט שייטון: תהא
                                                                                                                                                                                         T\subset Q מתקיים \hat{\delta}:\mathcal{P}\left(Q
ight)	imes \mathcal{D}^*	o \mathcal{P}\left(Q
ight) איי (Q,\Sigma,\delta,S,F) מרכל עבורה לכל (Q,\Sigma,\delta,S,F) מתקיים
                                                                                                                                                                                                                                                                                                                                                                                                                                                         f:\{0,1\}^n 	o \{0,1\}^m איי n,m\in\mathbb{N} פונקציה בולאנית: תהיינה
                                                                                                                                    .Class (y) = i אזי y \sim_L x_i
                                                                                                                                                                                                                       .\mathring{\delta}\left(q,x
ight)=igcup_{q\in\mathring{\delta}\left(T,x_{1}\dots x_{n-1}
ight)}\delta\left(q,x_{n}
ight) מרקיים x\in\Sigma^{n} וכן לכל \mathring{\delta}\left(T,arepsilon
ight)
.\{f_1 \dots f_n\} אזי פונקציות בוליאניות: תהיינה f_1 \dots f_n פונקציות בוליאניות
                                                                                                             באשר (Q,\Sigma,\delta,q_0,F) אזי אס״ד \Sigma^*/{\sim}_L
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              \mathcal{B} = \{\wedge, \vee, \neg\} בסיס דה־מורגן:
                                                                                                                                                                                           .\hat{\delta}\left(S,x
ight)\cap F
eqarnothingה המקיים x\in\Sigma^* אוטומט סופי לא־דטרמיניסטי מינוס מקבל מילה: יהי (Q,\Sigma,\delta,S,F) איזי
                                                                                                                                  Q = [|\Sigma^*/\sim L|]
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                הערה: תמיד נוסיף לבסיס את הפונקציות הקבועות.
                                                                                                                                                                                        טענה: יהי M אסלד"ם ויהי x \in \Sigma^n אזי (x \in \Sigma^n אזי ויהי x \in \Sigma^n טענה: יהי א אסלד"ם ויהי אזי אזי (x \in \Sigma^n אזי ויהי
                                                                                                                                                                                                                                                                                                                                                                                                           באשר f_1 \dots f_n \in \mathcal{B} תהיינה k_1 \dots k_n \in \mathbb{N}_+ באשר בוליאני: יהי \mathcal{B} בסיס פונקציות בוליאניות תהיינה
                                                                                                                          .\delta(i, \sigma) = Class(x_i \sigma) \bullet
                                                                                                                                                                                                                                                                                           (q_n \in F \mid i \in [n] לכל q_i \in \delta (q_{i-1}, x_i)
                                                                                                                                        .q_0 = \mathrm{Class}\,(arepsilon) •
                                                                                                                                                                                                                                                                                                                                                                                מעל G וותהיינה x_1 \dots x_m, y_1 \dots y_k \in \{0,1\} וותהיינה ווה לכל הכינון i \in [n] איי גרף מכוון איי מעל i \in [n]
                                                                                                                                                                                                                   L\left(M
ight)=\left\{x\in\Sigma^{st}\mid x מקבל את מקבל את אסלד"ם אזי M אסלד"ם יהי M אסלד"ם אוי מעניסטי מינוס: אוי אוי מעניסטי מינוס: אחלד"ם אוי
                                                                                                                    .F = \{i \in Q \mid x_i \in L\} \quad \bullet
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   המקיים \{f_1 \ldots f_n, x_1 \ldots x_m, y_1 \ldots y_k\}
טענה: תהא \Sigma^*/\sim_L שפה באשר \Sigma^*/\sim_L סופית תהא קבוצת נציגים של \Sigma^*/\sim_L שפה באשר באשר באשר אס"ד סופית תהא באשר באשר אס"ד המחלקות של
                                                                                                                                                                                                  אוטומט סופי דטרמיניסטי מינוס החזקה: יהי (Q',\Sigma,\delta',q_0,F') אוטומט סופי אוטומט אוא אס"ד M=(Q,\Sigma,\delta,S,F) יהי
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 חסר מעגלים מכוונים. G
                                                                                                          .\delta_A(q_0,y) = Class(y) אזי y \in \Sigma^* ויהי L
                                                                                                                                                                                                                                                                                                                                .Q' = \mathcal{P}(Q) \bullet
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  .deg – \left(x_i\right)=0 מתקיים i\in[m] לכל •
                                                                          עבורו |Q|=n באשר איז [n] מעל N מעל איז קיים איז איז איז קיים אסל"ד אווו איז מענה: יהי חn\in\mathbb{N}_{+}
                                                                                                                                                                                                                                                                                                      .\delta'(T,x) = \bigcup_{q \in T} \delta(q,x) \bullet
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 \deg^-\left(f_i
ight)=k_i מתקיים i\in[n] לכל •
                                                                                              L(N) = \{x \in [n]^* \mid \exists \sigma \in \Sigma . \#_{\sigma}(x) = 0\}
                                                                                                                                                                                                                                                                                                                                         .q_0 = S \bullet
                                                                                                                                                                                                                                                                                                                                                                                                                                                 \deg^+\left(y_i
ight)=0 וכן \deg^-\left(y_i
ight)=1 מתקיים i\in[k] לכל •
 |Q|>2^n אזי L\left(A
ight)=\{x\in[n]^*\mid\exists\,\sigma\in\Sigma.\#_{\sigma}\left(x
ight)=0\} עונה: אם אס"ד מעל n\in\mathbb{N}_{\perp} אזי n\in\mathbb{N}_{\perp} אזי הירי
                                                                                                                                                                                                                                                                                               .F' = \{T \subseteq Q \mid T \cap F \neq \emptyset\} \bullet
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           f_1 \dots f_n שער: יהי מעגל בוליאני אזי
\sqcup\in\Gamma\setminus\Sigma כו כו \Sigma\subset\Gamma מכונת טיורינג (מ"ט): תהא Q
eq\emptyset קבוצה סופית יהי \Omega אלפבית עבורו \Omega
                                                                                                                                                                                                    .\hat{\delta}_A\left(T,x
ight)=\hat{\delta}_M\left(T,x
ight) אויי x\in\Sigma^* ויהי T\subseteq Q_N תהא M של אס"ד החזקה של אס"ד היהי M אסלד"ם יהי א
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          .E\left(C
ight) אזי מעגל בוליאני אזי מעגל מעגל רהי יהי
איי \delta:(Q\setminus\{q_a,q_r\})	imes\Gamma	o Q	imes\Gamma	imes\{L,R\} תחוו q_a
eq q_r באשר q_0,q_a,q_r\in Q היהי
                                                                                                                                                                                                                                                                         L\left(M
ight)=L\left(A
ight) עבורו A עבורו אסלד"ם אזי קיים אס"ד א עבורו M אסלד"ם אזי קיים אס"ד
                                                                                                                                                                                                                                                                                                                                                                                                                                                                      \max_{v \in V(C)} \deg^+(v) מעגל בולינארי אזי fan-out:
                                                                                                                                    (Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r)
                                                                                                                                                                                                                                                                                                                                                                                                                                                          \{G \leq C \mid 1 הוא של fan-out מעגל בולינארי אזי מעגל הולינארי אזי מעגל הייהי מעגל מעגל בולינארי אזי מעגל היידי היי
                                                                                                                                                                                                                                                                                                          \Sigma_{\varepsilon} = \Sigma \cup \{\varepsilon\}אזי אלפבית אלפבית יהי \Sigmaיהי שימון: יהי
                                                                              .Qאוי מ"ט (Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r) מייט מייט אוי מצבים במכונת מיורינג: תהא
                                                                                                                                                                                                                                                                                                                                                                                 שערוך מעגל בולינארי על קלט: יהי y_i וכן (x_1 \dots x_m) = v אזי v \in \{0,1\}^m הינו הפלט הנוצר מעגל בולינארי על קלט: יהי
                                                                                                                                                                                        ותהיינה \delta:Q	imes\Sigma_{arepsilon}	o\mathcal{P}(Q) אוטומט סופי לא־דטרמיניסטי (אסל"ד): תהא א קבוצה סופית יהי בוצה סופית הא א קבוצה סופית הא
                                                                             .\Sigma אזי ט מ"ט (Q,\,\Sigma,\,\Gamma,\,\delta,\,q_0\,,\,q_a\,,\,q_r) מהט מיורינג: תהא מפבית במכונת מיורינג:
                                                                                                                                                                                                                                                                                                                   (Q, \Sigma, \delta, S, F) אוז S, F \subset Q
                                                                        .\Gamma איט איז (Q,\Sigma,\Gamma,\delta,q_0,q_a,q_r) מ"ט איז מכונת סיורינג: תהא
                                                                                                                                                                                                                                                                                                                                                                                                             C\left(v
ight)=\left(y_{1}\ldots y_{k}
ight) הוא v על על על אזי השערוך אי אזי v\in\left\{ 0,1
ight\} ^{m} מעגל בולינאני ויהי מעגל מעגל מעגל בולינאני ויהי
                                                                                                                                                                                                                                                                  Q אסל"ד אזי (Q, \Sigma, \delta, S, F) אסל"ד אזי אסל"ד אזי אסל"ד אזי
                                                                  .\delta אזי מעברים מעברים מעברים מיט מיורינג: תהא (Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r) מ"ט מייט אזי
                                                                                                                                                                                                                                                                                                                                                                                                                                         C\left(w
ight)=1 עבורו w\in\{0,1\}^n אזיי אזיי מעגל מקבל מילה: יהי C מעגל מקבל מילה: אזיי עבורו
                                                                                                                                                                                                                                                                 .\Sigma אזי אזי (Q,\Sigma,\delta,S,F) אסל"ד אזי אסל"ד אזי אסל"ד אזי אזי
                                                                     q_0 מ"ט אזי (Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r) מ"ט אזי מצב התחלתי במכונת טיורינג: תהא
                                                                                                                                                                                                                                                                                                                                                                                                                            L\left(C
ight)=\left\{x\in\left\{0,1
ight\}^{n}\mid x אז מקבל את אזי פלט יחיד אזי בעל פלט יחיד אזי C מקבל את C
                                                                                                                                                                                                                                                      .\delta אזי אזי (Q,\Sigma,\delta,S,F) אסל"ד אזי אסל"ד אזי אסל"ד אזי אסל"ד אזי
                                                                        .q_a איי איי (Q,\,\Sigma,\,\Gamma,\,\delta,\,q_0,\,q_a\,,\,q_r) תהא שייט איי מקבל מקבל מקבל מקבל מיורינג:
                                                                                                                                                                                                                                                                                                                                                                                v \in \{0,1\}^n אוז מעגל מחשב פונקציה: תהא t:\{0,1\}^n 	o \{0,1\} אוז מעגל מחשב פונקציה: תהא
                                                                                                                                                                                                                                                    S אזי אזי (Q, \Sigma, \delta, S, F) אזי אזי לא־דטרמיניסטי: אזי באוטומט אסל"ד אזי
                                                                        q_{T} איי איי (Q, \Sigma, \Gamma, \delta, q_{0}, q_{a}, q_{T}) מצב דוחה במכונת טיורינג: תהא
                                                                                                                                                                                                                                                      F אזי אזי (Q,\Sigma,\delta,S,F) אסל"ד אזי אזי אסל"ד אזי אסל"ד אזי אזי
                                                                                                                .c \in \Gamma^*Q\Gamma^* קונפיגורציה: תהא M מ"ט אזי
                                                                                                                                                                                                                                                                                                                                                                                משפט אוניברסליות דה־מורגן: תהא f:\{0,1\}^m 	o \{0,1\}^k משפט אוניברסליות משפט אוניברסליות אויים מעגל בוליאני
                                                                                                                                                                                                                                                                                                                 a \in Q אסל"ד ויהי N אסל"ד אזי פריבת a \in Q אזי
                      .C\left(v\right)=f\left(v\right)מתקיים v\in\left\{ 0,1\right\} ^{m}
                                                                                                                                                                                               .E\left(q\right) = \left\{q' \in Q \mid \exists a \in Q^{k+1}. \left(a_0 = q\right) \land \left(\forall i \in [k]. a_i \in \delta\left(a_{i-1}, \varepsilon\right)\right) \land \left(a_k = q'\right)\right\}
              .c=uq_{a}\,v המקיימים u,v\in \Sigma^{*} עבורה קיימים בבורה מ"ט אזי קונפיגורציה מונפיגורציה מבלת: עבורה מ"ט אזי קונפיגורציה מי"ט מ"ט אזי קונפיגורציה בר
                                                                                                                                                                                                                                                                                                                                                                                                                                                                        .
הערה: מכאן והלאה כל המעגלים הם בוליאניים ומעל בסיס דה־מורגן.
                                                                                                                                                                                                                                                                    E\left(T
ight)=igcup_{q\in T}E\left(q
ight) אוי אי T\subseteq Q איז אסל"ד ויהי N אסל"ד ויהי פביבת S: יהי א
               .i באורך מקבל מקבל עבורם \left\{C_{n}\right\}_{n\in\mathbb{N}} מעגלים: מעגלים שפחה של עבורם אל מעגלים
                                                                                                                                                                                        מתקיים מתקיים \hat{\delta}:\mathcal{P}\left(Q
ight)	imes\Sigma^*	o\mathcal{P}\left(Q
ight) אזי אסל"ד אי שסל"ד אי עבורה לכל Q,\Sigma,\delta,S,F פונקציית המוברים המורחבת: יהי
                                                                                         c עם cע מ"ט נתהא מינפיגורציה אזי נזהה את מ"ט ותהא d
                                                                                                                                                                                                                                                                                                                                                                                                          L\left(\mathcal{C}
ight)=\left\{x\in\{0,1\}^*\mid x\in L\left(\mathcal{C}_{|x|}
ight)
ight\} איי מעפחה של משפחת מעגלים: תהא משפחה של מענלים איי
                                            קונפיגורציה c^\prime המקיימת אחד מ"ט תהא קונפיגורציה אזי קונפיגורציה מ"ט תהא מ"ט תהא מ"ט תהא אזי קונפיגורציה אזי קונפיגורציה אחד הבאים
                                                                                                                                                                                                     .\mathring{\delta}\left(q,x\right)=R\left(\bigcup_{q\in\mathring{\delta}\left(T,x_{1}\dots x_{n-1}\right)}\delta\left(q,x_{n}\right)\right) מוכן לכל \delta\left(T,\varepsilon\right)=E\left(T\right)
                                                                                                                                                                                                                                                                                                                                                                                                                             L\left(\mathcal{C}
ight)=\mathcal{L} עבורה ענגלים \mathcal{C} עבורה אזי משפחה של מעגלים \mathcal{L}\subset\left\{0,1
ight\}^* משפחה מכריעה שפה: תהא
                               וכן c=uaqbv עבורם q,q'\in Qוקיימים u,v\in\Gamma^*וקיימים a,b,b'\in\Gamma קיימים \bullet
                                                                                                                                                                                                                                                                                                                                                                                                                                                       אודל לא יוניפורמי: משפחה של מעגלים \mathcal C עבורה לכל n\in\mathbb N יש אלגוריתם שונה.
                                                                                       c' = uq'ab'v וכן \delta(q, b) = (q', b', L)
                                                                                                                                                                                                     .\hat{\delta}\left(S,x
ight)\cap F
eq arnothing המקיים x\in\Sigma^* אזי אזי (Q,\Sigma,\delta,S,F) יהי יהי מקבל מילה: אוטומט סופי לא־דטרמיניסטי מקבל מילה: יהי
                                                                                                                                                                                                                                                                                                                                                                                                                                                            . אהה. שלגוריתם אלגוריתם n\in\mathbb{N} עבורה לכל עבורה של מעגלים אלגוריתם ההה.
                                                                                                                                                                                                                                                  עבורם k_0\ldots k_n\in\mathbb{N} ויהיו \sigma_1\ldots\sigma_n\in\Sigmaackslash\{arepsilon\} יהיו x\in\Sigma^* יהי
\delta\left(q,b\right)=\left(q',b',L\right) א נפורם q,q'\in Q וקיימים u,v\in\Gamma^* וקיימים u,b,b'\in\Gamma פיימים u,v\in\Gamma^*
                                                                                                                                                                                                                                                                                                                                                                                                                                                                              Cב מעגל: יהי מעגל בוליאני C אזי |C| מספר השערים ב־
                                                                                                                                                                                                                                                                  x^{\varepsilon} = \sigma_1 \dots \sigma_nאיז x = \varepsilon^{k_0} \sigma_0 \varepsilon^{k_1} \sigma_1 \varepsilon^{k_2} \dots \sigma_n \varepsilon^{k_n}
                                                                                                                                       .c' = q'b'v וכן
                                                                                                                                                                                                                                                                                                                                                                                                                   |\mathcal{C}_n| < S(n) עבורה S: \mathbb{N} 	o \mathbb{N} אזי אלים מעגלים: תהא מעגלים: תהא מעגלים: משפחה של מעגלים אזי
                                                                                                                                                                                       וכן q_0 \in S עבורם q_0 \ldots q_n \in Q וכן \iff (x) אזי (x \in \Sigma^n אזי ויהי אסל"ד ויהי אסל"ד x \in \Sigma^n אזי (x \in \Sigma^n אזי ויהי אסל"ד ויהי
\delta\left(q,b
ight)=\left(q',b',R
ight)וכן c=uqbv עבורם q,q'\in Q וקיימים u,v\in\Gamma^* וקיימים b,b'\in\Gamma פיימים b,b'\in\Gamma
                                                                                                                                                                                                                                                                                                                                                                                                                             \mathcal{O}\left(n\cdot 2^n\right) טענה: תהא f אזי בגודל f:\left\{0,1\right\}^n 
ightarrow \left\{0,1\right\} אזי קיים מעגל f:\left\{0,1\right\}^n
                                                                                                                                                                                                                                                                                           (q_n \in F \mid i \in [n] לכל q_i \in \delta \left(q_{i-1}, x_i^{\varepsilon}\right)
                                                                                                                                                                                                                                                                                                                                                                                                                        |C|=\mathcal{O}\left(n\cdot 2^n
ight) וכן L\left(C
ight)=\mathcal{L} אזי קיים מעגל C אזי קיים מעגל בורו L\left(C
ight)=\mathcal{L} וכן L\left(C
ight)=\mathcal{L}
                                                                                                                                    .c' = ub'q'v וכן
                                                                                                                                                                                                                                L\left(A
ight)=\left\{x\in\Sigma^{st}\mid x אסל"ד אזי A מקבל את A א אסל"ד אזי איז אוטומט סופי לא־דטרמיניסטי: יהי A אסל"ד אזי אוי
                                                                                                                                                                                                                                                                                                                                                                                                                                   \mathcal{O}\left(2^{n}\right) טענה: תהא f:\{0,1\}^{n} 
ightarrow \{0,1\} אזי קיים מעגל f:\{0,1\}^{n}
 L\left(N
ight)=L\left(M
ight) עבורו M עבורו אזי קיים אסלד"ם איז איז עבורו N
                                                                                                                                                                                                                                                                                                                                                                                                                                |C|=\mathcal{O}\left(2^{n}
ight) וכן L\left(C
ight)=\mathcal{L} אזי קיים מעגל C עבורו L\left(C
ight)=\mathcal{L} וכן \mathcal{L}\subseteq\{0,1\}^{n} מסקנה: תהא
                                                                                                      עוברת ל־c_nוכן וכן i \in [n]לכל לכל כיברת עוברת וברת וכן 
                                                                                                                                                                                                                                                                           L\left(A
ight)=L\left(M
ight) עבורו A עבור אזי קיים אסל"ד איי אסל"ד איי אסל"ד איי אסל"ד איי אסל"ד איי
                                                                                                                                                                                                                                                                                                                                                                                                                    \mathcal{O}\left(rac{2^n}{a}
ight) אזי קיים מעגל f:\{0,1\}^n	o\{0,1\} בגודל f:\{0,1\}^n
 c_{i-1} וכן c_0=q_0x באשר אוורציות קיימים באור קיימים עבורו איימים x\in\Sigma^* מיט איי מ"ט איי מ"ט איי מיט איי אוור איימים מיטריגג אוורציות מילה: מיטריגג איי
                                                                                                                                                                                                                     (L(N)=\mathcal{L} המקיים N המקיים M המקיים M שפה אזי \mathcal{L} רגולרית) אינה: יהי M אלפבית ותהא M
                                                                                                        . עוברת ל־c_nוכן i \in [n]לכל לכל לים עוברת אוברת וכן i \in [n]
                                                                                                                                                                                                                                                                                                                                                                                 .rac{2^n}{10n} אשעה מעגל C בגודת בעזרת ניתנת לחישוב בעזרת f:\{0,1\}^n 	o \{0,1\} מענה קיים און: קיים און פיימת אינה היים און אינה ניתנת לחישוב בעזרת מעגל אינה ניתנת לחישוב בעזרת מעגל אינה ניתנת לחישוב בעזרת מעגל אינה היים אינה ניתנת לחישוב בעזרת מעגל אינה היים אינה מעגל אינה מעגל אינה מעגל אינה מעגל אינה מעגל אינה ניתנת לחישוב בעזרת מעגל אינה מעגל א
                                                                                                                                                                                                                                                                                                                       ביטוי רגולרי (ב"ר): יהי Σ אלפבית אזי
                                                          L\left(M
ight)=\left\{x\in\Sigma^{*}\mid x מקבל את מ"ט אזי M מ"ט אזי M מהא מכונת טיוריגנ: תהא
                                                                                                                                                                                                                                                                                                                                                                                אוטומט שופי דטרמיניסטי (אס"ד): תהא Q 
eq Q קבוצה סופית יהי \Sigma אלפבית תהא \delta: Q 	imes \Sigma 	o \sigma יהי ותהא q \in Q ותהא
                                           x את אחוה אל לא מקבלת לא עבורו עבורו מ"ט אזי א מ"ט אזי מ"ט אזי א עבורו אל עוצרת אל קלט: תהא או מ"ט אזי מכונת אורינג א
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 (Q, \Sigma, \delta, q, F) אזי F \subseteq Q
                                                                                                                                                                                                                                                                                                                           .a יהי a\in \Sigma_{arepsilon} אזי a\in \Sigma_{arepsilon}
                                                         מתקיים M' מסוג M מסוג M וכן לכל M מסוג M מחקיים מודלים שקולים: מודלים מודלים עבורם לכל מ
                                                                                                                                                                                                                                                                                                                                                                                                                                                                Q אזי אזי (Q, \Sigma, \delta, q, F) אס"ד אזי אס"ד אזי אזי אזי אזי
                                                                                                                                                                                                                                                                                      R_1 \cup R_2 יהיו אזי R_1, איי פיטויים רגולרים אזי יהיו •
                                                                                     L(A) = L(A') המקיימת M' מסוג A' מסוג •
                                                                                                                                                                                                                                                                                                                                                                                                                                                              .\Sigma אזי אזי (Q,\,\Sigma,\,\delta,\,q,\,F) אזי אזי דטרמיניסטי: אזי אזי (Q,\,\Sigma,\,\delta,\,q,\,F) אזי
                                                                                                                                                                                                                                                                                           R_1R_2 יהיו רגולרים אזי R_1,R_2 יהיו •
                                                                                                                                                                                                                                                                                                                                                                                                                                                    .
אס"ד אזי (Q,\, \Sigma,\, \delta,\, q,\, F)יהי דטרמיניסטי: אס"ד אס"ד אס"ד אס
                                                                                       L\left(B\right)=L\left(B'\right) המקיימת M מסוג B' קיימת \bullet
                                                                                                                                                                                                                                                                                                                  R^*יהי יהי ביטוי רגולרי אזי יהי
                                                                                                           מסקנה: אס"ד. אסל"ד ואסלד"ם הינם מודלים שקולים.
                                                                                                                                                                                                                                                                                                                                                                                                                                                         q אס"ד אזי (Q, \Sigma, \delta, q, F) אס"ד אזי דטרמיניסטי: יהי
                                                                                                                                                                                                                                                                                                              שפה נוצרת מביטוי רגולרי: יהי Σ אלפבית אזי
 מכונת טיוריגג נחה: תהא Q 
eq 0 קבוצה סופית יהי Z אלפבית עבורו C אלפבית עבורה קבוצה סופית יהי C אלפבית עבורו אלפבית עבורו אייריגג נחה אייריגג מחה אייריגג נחה אייריגג וווי אוריגג וווי אוריגגג וווי אוריגג ווווי אוריגג וווי אוריגג וווי אוריגג וווי אוריגג וווי אוריגג וווי אורי
                                                                                                                                                                                                                                                                                                                                                                                                                                                     .F אזי אזי (Q,\,\Sigma,\,\delta,\,q,\,F) אזי אזי דטרמיניסטי: אזי אזי אזי אזי
                                                                                                                                                                                                                                                                                                                                   L(\varnothing) = \varnothing •
                                                                                                                                                                                                                                                                                                                                                                                \hat{\delta}\left(q,arepsilon
ight)=q מתקיים q\in Q עבורה לכל \hat{\delta}:Q	imes\Sigma^*	o Q אס"ד אזי עם ל(Q,\Sigma,\delta,q_0,F) מתקיים ממורחבת: יהי
איי \delta : (Q \setminus \{q_a,q_r\}) \times \Gamma \to Q \times \Gamma \times \{L,R,S\} ותהא q_a \neq q_r באשר q_0,q_a,q_r \in Q
                                                                                                                                                                                                                                                                                                      .L\left(a
ight)=\left\{ a
ight\} אזי a\in\Sigma_{arepsilon} יהי
                                                                                                                                                                                                                                                                                                                                                                                                                                               \hat{\delta}\left(q,x
ight)=\delta\left(\hat{\delta}\left(q,x_{1}\ldots x_{n-1}
ight),x_{n}
ight) מתקיים x\in\Sigma^{n} וכן לכל
                                                                                                                                    (Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r)
                                                                                                                                                                                                                                      L\left(R_1\cup R_2
ight)=L\left(R_1
ight)\cup L\left(R_2
ight) איי היו ביטויים רגולרים איי רגולרים איי היו R_1,R_2יהיי יהיו
                                                                  הערה: את כל הפעולות ממכונת טיורינג נכליל בצורה הטבעית עבור מכונת טיורינג נחה.
                                                                                                                                                                                                                                                 L\left(R_{1}R_{2}
ight)=L\left(R_{1}
ight)L\left(R_{2}
ight) איי היו R_{1}, R_{2} ביטויים רגולרים איי היו
                                                                                                                                                                                                                                                                                                                                                                                                         .\delta\left(q_{0},x
ight)\in F המקיים x\in\Sigma^{*} אזיי אזיי אזיי (Q,\Sigma,\delta,q_{0},F) היהי מקבל מילה: יהי
                                                                                              מסקנה: מכונת טיורינג ומכונת טיורינג נחה הינו מודלים שקולים.
                                                                                                                                                                                                                                                                                      L\left(R^{*}\right)=L\left(R\right)^{*} יהי R ביטוי רגולרי אזי
                                                                                                                                                                                                                                                                                                                                                                                \sqcup\in\Gammaackslash\Sigma בכן \Sigma\subset\Gamma אלפבית עבורו \Sigma\subset\Gamma אלפבית עבורו ביסרטית: יהי הא k\in\mathbb{N}_{+} יהי הא k\in\mathbb{N}_{+} וכן כ
                                                                                                                                                                                                                                                                          R\left(\Sigma
ight)=\left\{r\in\Sigma^{*}\mid ביטוי רגולרי r
ight\} אלפבית אזי אלפבית רגולרי אזי רגולרי רגולרי אלפבית אזי
אזיי \delta:(Q\setminus\{q_a,q_r\})	imes\Gamma^k	o Q	imes\Gamma^k	imes\{L,R\}^k אוזיי q_a
eq q_r באשר q_0,q_a,q_r\in Q אזיי
                                                                                                                                                                                                                                                                                                                 הערה: קיים סדר פעולות לביטויים רגולריים
                                                                                                                                                                                                                                                                                                                                                                                                                              L\left(A
ight)=\left\{x\in\Sigma^{st}\mid x מקבל את A מקבל אר אס"ד איזי A אס"ד איזי אוטומט סופי דטרמיניסטי: יהי A אס"ד איזי
                                                                                                                                (k, Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r)
                                                                                                                                                                                                                                                                                                                                          סוור הליוי
                                                                                                                                                                                                                                                                                                                                                                                                                                L\left(A
ight)=\mathcal{L} המקיים A דיים אס"ד \mathcal{L}\subset\Sigma^* עבורה אזי שפה אלפבית היים אלפבית אזי שפה אלפבית אזי שפה בולרית: יהי
                                                         יערנעור •
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        טענה: Ø רגולרית.
       .c_1גc_2ג. . . גc_L אזיי, אוי .c_1 אזי. . . .  אוי אוי הרא א מ"ט רב־סרטית ותהינה . 
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      . רגולרית \{\varepsilon\} רגולרית
```

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

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

. רגולרית  $L \cup \mathcal{L}$ 

רגולרית.  $L \cap \mathcal{L}$ 

. רגולרית $\overline{L}$ 

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

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

. אינסופית  $L^*$  אזי אזי  $L 
eq \{arepsilon\}$  וכן  $L 
eq \{arepsilon\}$  אינסופית.  $L \subseteq \Sigma^*$  אזי  $L \subseteq \Sigma^*$ 

 $0<|\Sigma|<leph_0$  אלפבית: קבוצה ב המקיימת אלפבית:

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

 $\|w\|=n$  מילה אזי  $w\in \Sigma^n$  ותהא אלפבית מילה אזי מילה אזי  $w\in \Sigma^n$ 

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

 $.\langle w_1 \ldots w_n \rangle \, \langle \omega_1 \ldots \omega_m \rangle = \langle w_1 \ldots w_n, \omega_1 \ldots \omega_m \rangle$ 

 $(w_1\dots w_n)^R=\langle w_n\dots w_1
angle$  אזי  $\langle w_1\dots w_n
angle\in \Sigma^*$  היפוך מילה: תהא

 $(w_1\dots w_n)^m=\prod_{i=1}^m \langle w_1\dots w_n \rangle$  אזי איי  $m\in\mathbb{N}$  ויהי ווהי  $\langle w_1\dots w_n \rangle\in\Sigma^*$  תהא

|arepsilon|=0 עבורה  $arepsilon\in\Sigma^*$  אלפבית אזי אוי יהי עבורה אוי יהי

 $(L(r)=\mathcal{L}$  עבורו  $r\in R(\Sigma)$  קיים (קיים בורו  $\mathcal{L}\subset \Sigma^*$  עבורו  $\mathcal{L}\subset \Sigma^*$  אלפבית ותהא

 $\|xy^kz\| \in L$  מתקיים  $\|xy\| \leq \ell$  וכן  $\|xy\| \leq \ell$ 

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

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

. אינה רגולרית.  $\{a^p \mid a \in \Sigma,$  ראשוני ענה:  $\{a^p \mid a \in \Sigma,$ 

 $\ell$  ניתנת לניפוח: תהא עבורו ניתנת אזי קיים  $\ell>0$  שפה רגולרית שפה לניפוח מענה למת הניפוח: תהא

 $\min\left\{\ell\in\mathbb{N}_{+}\mid\ell$  ניתנת לניפוח שפה רגולרית אזי שפה רגולרית אזי ביוע הניפוח: תהא  $\mathcal{L}$  שפה רגולרית אזי

שפה ניתנת לניפוח: שפה  $x,y,z\in \Sigma^*$  שפה ניתנת לניפוח: שפה  $x,y,z\in \Sigma^*$  שפה ניתנת לניפוח: שפה לכל עבורם לכל  $w\in \mathcal{L}$  באשר עבורם לכל

```
.EQ \notin \mathcal{R} :טענה
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       (k,(\pi_1\ldots\pi)) אזי \pi_1\ldots\pi_p ותהיינה k\in\mathbb{N} יהי RAM: יהי
                                                                                                                                                             ענדים. עוצרת אחרי אחרי לכל ענדים עוצרת עוצרת לכל עוצרת עוצרת לכל V\left(x,\,w\right)
                                                                                                                                                                                                                                                                                                                                                                                                                                                         .
HALT _{arepsilon}=\{\,\langle\,M\,
angle\,\,|\,\,arepsilon\,\, עוצר על א עוצר M\,\}
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                .k אזי RAM מספר הרגיסטרים במודל RAM: יהי (k, \Pi) מודל
                                                                                                                      .
CLIQUE = \{\langle G,k\rangle \mid k גרף מגודל בעל מכוון גרף אז מכוו<br/> G\} הגדרה:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 .HALT \leq_m HALT_{arepsilon} :
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 \Pi אזי RAM מודל (k, \Pi) אזי (RAM אזי RAM פקודות במודל
                                                                                                                                                                                              .CLIQUE טענה: קיים מוודא פולינומי
                                                                                                                                                                                                                                                                                                                                                                                       A <_m B אזי B \in \mathcal{P}\left(\Sigma^*\right) \setminus \left\{\Sigma^*,\varnothing\right\} ותהא A \in \mathcal{R} אזי A \in \mathcal{R}
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   T:\mathbb{N}	o\mathbb{N} וכן R_0\ldots R_k\in\mathbb{N} וכן PC וכן אזי RAM מודל (k,\Pi) יהי (RAM יהי יהי
                                                                                                                     \mathsf{LS} = \{ \langle G, k \rangle \mid k מגודל בת"ל בוצה בעל מכוון און מכוון בעל מגודל מגודל מגודל מגודל מכוון בעל מכוון בעל מבוצה בת"ל
                                                                                                                                                                                                                                                                                                                                                        \overline{B}ל \overline{A}ה מיפוי מיפוי f רדוקציית מיפוי מ־A ל־B ל־\overline{A} רדוקציית מיפוי מ־A שפות ותהא
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   .PC אזי קונפיגורציה (T,R, PC) ותהא (RAM מודל (k,\Pi) יהי קונפיגורציה קונפיגורציה אזי
                                                                                                                                                                                                                                                                                                                                                                                                                                                טענה: תהיינה A \leq_m B שפות באשר A, B אזי
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           R אוי אוי (T,R, PC) אודל מודל (R, \Pi) מודל אוי קונפיגורציה (R, \Pi) קונפיגורציה אוי
                                                                                                                                               .FACTOR = \{\langle N, k \rangle \mid \exists d \in [k] . (d|N)\} הגדרה:
                                                                                                                                                                                                                                                                                                                                                                                                                                                            A \in \mathcal{RE} אוא B \in \mathcal{RE} אם •
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 T איי קונפיגורציה (T,R, PC) אודל RAM מודל (t,\Pi) יהי יהי קונפיגורציה איי (t,\Pi) אונפיגורציה איי
                                                                                                                                                                                            .FACTOR טענה: קיים מוודא פולינומי ל
                                                                                                                                                                                                                                                                                                                                                                                                                                                   A\in \mathrm{co}\mathcal{RE} אזי B\in \mathrm{co}\mathcal{RE} אם ullet
                                                                                    .SUBSETSUM = \left\{ \langle S,k \rangle \mid (S \subseteq \mathbb{N}) \land \left(\exists T \subseteq S. \sum_{i \in T} i = t\right) \right\} הגדרה:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                     \overline{	ext{ACC}} \leq_m בענה: ACC \leq_m בענה: ACC \leq_m בענה:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  טענה: מכונת טיורינג ומודל RAM הם מודלים שקולים.
                                                                                                                                                                                      .SUBSETSUM: סענה: קיים מוודא פולינומי
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       .EQ \notin \mathcal{RE} \cup co\mathcal{RE} מסקנה:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 \sqcup \in \Gamma \setminus \Sigma כו \Sigma \subset \Gamma אלפבית יהי אלפבית אלפבית (מטל"ד): תהא עQ 
eq \emptyset הוצה סופית היהי אלפבית יהי אלפבית עבורו
                                                                                                                                                                                                                                                                                                                                                                                                                                                \mathcal{C}\subseteq\mathcal{P}\left(\Sigma^{*}
ight) אלפבית אזי הי ממנטית: יהי מלפבית אזי
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                איי \delta : (Q\setminus\{q_a,q_r\}) 	imes \Gamma 	o \mathcal{P} (Q	imes\Gamma	imes\{L,R\}) ותהא q_a 
eq q_r באשר q_0,q_a,q_r \in Q ייהיי
                                                                                                      (\mathcal{L} - \mathcal{L}) שפה אזי (\mathcal{L} \in \mathcal{NP}) שפה אזי (פיים מוודא פולינומי ל\mathcal{L} \subseteq \Sigma^*).
                                                                                                                                                             .CLIQUE, IS, FACTOR, SUBSETSUM \in \mathcal{NP} :מסקנה
                                                                                                                                                                                                                                                                                                                                                                                                     L_{\mathcal{C}} = \{\langle M 
angle \mid L\left(M
ight) \in \mathcal{C}\} הגדרה: תהא תכונה סמנטית אזי
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     (Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r)
                                                                                                                                                                                                                                                                                                                                                                                L_{\mathcal{C}} \notin \mathcal{R} אזי חכונה סמנטית אזי \mathcal{C} \in \mathcal{P}\left(\mathcal{RE}\right) \setminus \{\mathcal{RE},\varnothing\} משפט רייס: תהא
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  קונפיגורציה איי קונפיגורציה עף עף באשר באי ותהא איי ותהא איי ותהא עף איי ותהא איי קונפיגורציה איי קוניי קוניניי אורציה איי קוניי אוניי קוניי אורי איי קוניי אוניי אוניי איי קוניי אוניי 
                                                                                                                                                                                              השערה: \mathcal{P} 
eq \mathcal{NP}. השערה פתוחה
                                                                                                                                                                                                                                                                                                                                                                                                                                                      L_{\mathcal{C}} \in \mathcal{R} אוי \mathcal{C} \in \{\mathcal{RE}, \varnothing\} טענה: תהא
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 פיים או המחשבת את M היימת מ"ט f:D	o (\Gamma \setminus \{\sqcup\})^* אא אי D\subseteq \Sigma המחשבת את M המחשבת את M וכן קיים
                                                                                                                                                                                                                                                                                                                                                                                                                                                                        .PRIME = \{(p)_2 \mid p \in \mathbb{P}\} :הגדרה
                                                              עדים. p\left(\left|x\right|\right) אחרי לכל היותר עוצרת עוצרת מתקיים כי x\in\Sigma^*לכל כי המקיים המקיים p\in\mathbb{N}\left[x\right]
                                                                                                                                                                                                                                                                                                                                                                                                                                                                    .2 הערה: קידוד מספרים תמיד יעשה בבסיס
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 c, עם שורש q_0xעם שורש קונפיגורציות איז עץ קונפיגורציות איז עץ קונפיגורציות איז עץ קונפיגורציות איז עץ איז עץ קונפיגורציות איז ער איז עך איז איז עץ קונפיגורציות איז ער איי
 שפה אוי דדוקציית מיפוי B\subseteq \Delta^* שפה ותהא באיי באשר באר באר באשר באייתים באשר אוי פור אוי פור מיפוי באשר באר באר באר באר באר באר באיי מיפוי באשר באיי מיפוי אוי דדוקציית מיפוי מיפוי אוי הדוקציית מיפוי באשר באייתים באייתים באשר באייתים באייתים באשר באייתים באשר באייתים באשר באייתים באשר באייתים באשר באייתים באיית באייתים באייתים באייתי
                                                                                                                                                                                                                                                                                                                                                                                                                                          .EQPRIME = \{\langle M \rangle \mid L\left(M\right) = \text{PRIME}\} .
                                                                                                                                                                                                          . מ־A ל־B חשיבה פולינומית f
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              T_{N,\,x}מכונת טיוריגנ לא־דטרמיניסטית מקבלת מילה: תהא מטל"ד אזי בx\in \Sigma^* אזי מטל"ד מהבלת מילה: מקבלת מילה: מטוריגנ מיוריגנ א
f:\Sigma^*	o\Delta^* שפה ותהא שפה הוא שפה תהא ביאר A\subseteq\Sigma^* תהא ביית באשר בייתים באשר בייתים באשר בייתים מון: אויית באשר בייתים בייתים באשר בייתים באשר בייתים באשר בייתים באשר בייתים באשר בייתים באשר בייתים 
                                                                                                                                                                                                                                                                                                                                                        L_{\mathcal{C}} \notin \mathrm{co}\mathcal{RE} אזי \mathcal{C} \in \mathcal{P}\left(\mathcal{RE} \setminus \{\varnothing\}\right) \setminus \{\varnothing\} אזי תהא הרחבה ראשונה: תהא
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  N אינו מתקבל על ידי x סופי וכן אינו סיוריגנ אב־דטרמיניסטית דוחה מילה: תהא מטל"ד אזיx \in \Sigma^* עבורו מטל"ד אזי אינו מתקבל על ידי מידטרמיניסטית אינו מתקבל על ידי
                                                                                                                                                                                                       A \leq_{p} B מיפוי פולינומית אזי
                                                                                                                                                                                                                                                                                                                                             L_{\mathcal{C}} \notin \mathcal{RE} אזיי \varnothing \in \mathcal{C} באשר \mathcal{C} \in \mathcal{P} (\mathcal{RE}) \setminus \{\mathcal{RE}\} מענה משפט רייס הרחבה שנייה: תהא
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   L\left(N
ight)=\left\{x\in\Sigma^{*}\mid x מקבל את מה מטל"ד אוי N מטל"ד הוי תהא N מטל"ד אוי לא־דטרמיניסטית: תהא אוי מיוריגנ
                                                                                                                                                                                                                         .CLIQUE \leq_p IS טענה:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            x מטל"ד איז x\in \Sigma^* עבורו x\in \Sigma^* איז א מטל"ד אות א עוצרת על קלט: תהא א מסל"ד איז א עבורו א א מסל"ד אות א מכונת טיורינג לא־דטרמיניסטית לא עוצרת על קלט:
                                                                                                               A\in\mathcal{P} אזי A\leq_{p}B וכן B\in\mathcal{P} אפות באשר A,B שפות מענה: תהיינה
                                                                                                                                                                                                                                                                                                                                                                                                                                                         ALL = \{\langle M \rangle \mid L(M) = \Sigma^* \} הגדרה:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      טענה: מכונת טיורינג ומכונת טיורינג לא־דטרמיניסטית הינן מודלים שקולים.
                                                                                                                          \mathcal{NPH}=\left\{\mathcal{L}\mid\forall L\in\mathcal{NP}\left(L\leq_{p}\mathcal{L}
ight)
ight\} שפה \mathcal{NP}-קשה:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         \overline{\text{HALT}} \leq_m ALL למה:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      שפות בריעות למחצה/שפות ניתנות למניה רקורסיבית/שפות ניתנות לקבלה: יהי אלפבית אזי שפות בריעות למחצה/שפות היהי ב
                                                                                                                                                                  \mathcal{NPC}=\mathcal{NP}\cap\mathcal{NPH} שפה \mathcal{NP}-שלמה:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         .ALL \notin \mathcal{RE} \cup co\mathcal{RE} :
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   \mathcal{RE} = \{\mathcal{L} \subseteq \Sigma^* \mid \mathcal{L} = L(M) \text{ עבורה } \}
                                                                                                                               (\mathcal{P}=\mathcal{NP})\Longleftrightarrow (\mathcal{L}\in\mathcal{P}) אזי \mathcal{L}\in\mathcal{NPC} טענה: תהא
                                                                                                                                                                                                                                                                                 אסט עליון לזמן ריצה של מכונת טיורינג: תהא M מ"ט אזי T:\mathbb{N} 	o \mathbb{N} עבורה לכל n\in \mathbb{N} ולכל א מתקיים כי M מת מייט מי
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  x עוצרת על M ממקיים כי x\in \Sigma^* וכן לכל בורה על L=L (M) שפה אזי מ"ט שפה אזי שפה בהא בהא על בורה על בורה אזי מיט שבה: תהא בהא בהא מכונת טיורינג מכריע שבה: תהא
                                                  	ext{ACC}_{\mathcal{NP}} = \left\{\left\langle M, x, 1^t 
ight
angle אחרי מקסימום t צעדים t מקבלת M\left(x, w
ight) מקבלת t מקבלת אחרי מקסימום אינויים t
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                \mathcal{R}=\{\mathcal{L}\subseteq \Sigma^*\mid \mathcal{L} את המכריעה מ"ט M קיימת אזי \{קיימת אזי היי \Sigma אלפבית: יהי אלפבית אזי המכריעה המכריעה אזי אוני
                                                                                                                                                                                                            .\mathrm{Acc}_{\mathcal{NP}}\in\mathcal{NPC} טענה:
                                                                                                                                                                                                                                                                                                                                     .DTime (T\left(n
ight))=\{L\left(M
ight)\mid\mathcal{O}\left(T\left(n
ight)
ight) שרצה בזמן שרצה בזמן M\} אזי T:\mathbb{N}	o\mathbb{N} הגדרה: תהא
                                                                                                                                                                                                                                                                                                                                                                                                                                                        \left\{0^{k}1^{k}\mid k\geq0
ight\}\in DTime \left(n^{2}
ight) טענה:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 עבורו \Sigma \cup \{\$\} מעל האלפבית שפה: תהא \mathcal{L} \subseteq \Sigma^* שפה אזי מ"ט מונה עבור שפה: תהא
                                                                       B\in\mathcal{NPC} אזי A\leq_{p}B וכן A\in\mathcal{NPC} שפות באשר A,B\in\mathcal{NP} איי איי טענה: תהיינה
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     \delta\left(q,\sigma
ight)=\left(q',\sigma',R
ight) מתקיים \sigma\in\Gamma ולכל q\in Q לכל
                                                                                                                                                                                                                                                                                                                                                                                                                                     \left\{0^{k}1^{k}\mid k\geq0
ight\}\in DTime \left(n\log\left(n
ight)
ight) .
                                                                                                                      .C\left(x
ight)=1 המקיים x\in\left\{ 0,1
ight\} ^{n} מעגל ספיק: מעגל עבורו קיים C
                                                                                                                                                                                                                                                                                                                                                                           L אזי L\in DTime (t(n)) ותהא t(n)=o(n\log(n)) אזי L רגולרית. L\in DTime
                                           A\in M_{m	imes k} (\{p_i\}\cup\{\lnot p_i\}) וקיימת m\in\mathbb{N} בסוק עבורה עבורה אבורה \varphi\in CNF בסוק ווקיימת אבורה פסוק אבורה קיים ווקיימת אבורה אבו
                                                                                                                                                                                                                                                                                                                                                                   \left\{0^{k}1^{k}\mid k\geq0
ight\}
otinegin{align}  DTime (t\left(n
ight)) אזיי t\left(n
ight)=o\left(n\log\left(n
ight)
ight) מסקנה: תהא
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  . מתקיים סופי אל אחר מספר ארסרט אל געדים כי מתקיים מתקיים אל x \ מתקיים אוכל -
                                                                                                                                                                                                  \varphi = \bigwedge_{i=1}^{m} \bigvee_{j=1}^{k} (A)_{i,k}
                                                                                                                                                                                                                                                                                 את מ"ט M על הקלט M כו פונקציה M על הקלט M בורה קיימת מ"ט M עבורה קיימת מ"ט עבורה עבורה M כו פונקציה M על הקלט M מישבת את
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     . לעולם אינ x לא על מתקיים מx \notin L לכל -
                                                                                                     .kSAT =\{\langle \varphi \rangle \mid (\varphi \in kCNF) \wedge (ספיקה) אוי k \in \mathbb{N}_+ יהי הגדרה: יהי k \in \mathbb{N}_+
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             . מונה) שענה: תהא \mathcal{L}\subseteq \Sigma^* שפה אזי (\mathcal{L}\in\mathcal{RE}) שפה אזי ב\mathcal{L}\subseteq \Sigma^*
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     \mathcal{O}\left(T\left(n
ight)
ight) בזמן בזמן \left(T\left(n
ight)
ight)_{2}
                                                                                                                                                                                 .kSAT \in \mathcal{NP} אזי k \in \mathbb{N}_+ טענה: יהי
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 T\left(n
ight)=\Omega\left(n
ight) אזי קבועה אזי חשיבה חשיבה T:\mathbb{N}
ightarrow\mathbb{N} תהא
                                                                                                                                                                                                                                .2SAT \in \mathcal{P} :טענה
                                                                                                                                                                                                                                                                                  M באשר x ולכל קלט M ולכל מיור לכל מיור תיים מכונת מיורינג אוניברסלית עם טיימר: קיימת מ"ט אוניברסלית עם אוניברסלית עם טיימר: קיימת מ"ט אוניברסלית עם היימר אוניברסלית עם היימר אוניברסלית עם היימר מכונת מיור אוניברסלית עם היימר מיימר מכונת מ
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       הסרט לפני $y$.
                                                                                                                                                                                                  .3SAT \in \mathcal{NPC} :משפט קוק־לוין
                                                                                                                                                                                                                                                                                                                                                           עוצרת על הקלט (M,x) תוך עוצרת כי מתקיים מתקיים עוצרת אודים מחקלט (M,x) עוצרת על הקלט אוצרת על מתקיים אודים.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          . עענה: תהא \Sigma^* \subseteq \Sigma^* מונה לקסיקוגרפי). שפה אזי \mathcal{L} \subseteq \Sigma^* מונה לקסיקוגרפי).
                                                                                                                                        kSAT \leq_{\mathcal{D}} \ellSAT אזי איזי k \leq \ell באשר k, \ell \in \mathbb{N}_+ יהיי
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             .co\mathcal{RE}=\left\{\mathcal{L}\subseteq\Sigma^*\mid\overline{\mathcal{L}}\in\mathcal{RE}
ight\} אלפבית אזי אלפבית אזי הגדרה: יהי
                                                                                                                                                                                                                                                                                                                                           מתקיים t\in\mathbb{N} ולכל x ולכל מ"ט M לכל מ"ט עבורם לכל חיים C\in\mathbb{R} וקיים וקיים אוניברסלית משפט:
                                                                                                                                                   .kSAT \in \mathcal{NPC} אזיי k \in \mathbb{N} \setminus \{0,1,2\} מסקנה: יהי
                                                                                                                                                                                                                                                                                                                                                   .\langle M,\, x,\, t\rangle אם U אזי צעדים לכל היותר לכל לאחר לאחר על הקלט x עוצרת עוצרת אח\bullet
                                                                                                                                                                                                                 .3SAT \leq_p CLIQUE משפט:
                                                                                                                                                                                                                                                                                                                                                                A(M,x,t) אם A(M,x,t) או לא עוצרת לאחר א צעדים אזי A(M,x,t) או או א דוחה את א שו
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        . חח"ע עד כדי שינוי שמות. f:\{M\mid u"ט M\}	o \{0,1\}^* מינוי שמות. פונקציה
                                                                                                                                                                                                       .CLIQUE, IS \in \mathcal{NPC} מסקנה:
                                                                                                                                                                                                                                                                                                                                                                                                                                                צעדים. C \cdot t \log (t) צעדים U \bullet
                                                                                                                                                                                                                                                                                                                                                 משפט היררכיית הזמן: תהא t\left(n
ight)=o\left(rac{T(n)}{\log(T(n))}
ight) משפט היררכיית הזמן: תהא T:\mathbb{N}	o\mathbb{N} אזי
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 . מערה: נשתמש בסימון \langle \, \cdot \, \rangle על מנת לקודד כל אובייקט לקידוד בינארי.
                                                                                                                       v השמה אזי A \in M_{m 	imes k}\left(\left\{p_i
ight\} \cup \left\{\lnot p_i
ight\}
ight) ותהא
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  \mathcal R היא קידוד נניח כי קידוד ופענוח הן פעולות פשוטות ובדיקת נכונות קידוד היא
                                                                   N\left(\bigwedge_{i=1}^{m}\bigvee_{j=1}^{k}(A)_{i,k},v\right)=\left|\left\{i\in[m]\mid\overline{v}\left(\bigvee_{j=1}^{k}(A)_{i,k}\right)=\text{True}\right\}\right|
                                                                                                                                                                                                                                                                                                                                                                                                                                                                          .DTime (t(n)) \subseteq DTime(T(n))
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              .xעם אותחל Mשל הבינארי הקידוד הינו \langle M, x \rangle מילה מילה x מאותחל מ"ט תהא M הינו הקידוד מימון: מילה מילה מילה אוי
                                                                                                      .CCNF = \{\langle arphi, k \rangle \mid (arphi \in \text{CNF}) \land (\exists v \ (N \ (arphi, v) = k))\} הגדרה:
                                                                                                                                                                                                                                                                                                                                                                                                                      .DTime (n^c)\subseteq DTime(n^d) אוי 1\leq c < d מסקנה: יהיו
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 עבורה \{0,\,1\} מעל שפט מכונת מייט אוניברסלית: אוניברסלית: עבורה משפט מכונת טיורינג אוניברסלית:
                                                                                                                                                                                                                   .CCNF \in \mathcal{NPC} :טענה
                                                                                                                                                                                                                                                                                 M' טענה: איז קיימת מ"ט איז איז איז איז פיימת T\left(n
ight) \geq n אוי איז איז איז איז שרצה איז שרצה איז תהא T\left(n
ight) \geq T באשר
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   (x את מקבלת M) \Longleftrightarrow (\langle M,x\rangle את מקבלת של מתקיים M של איט ולכל אל לכל מ"ט M ולכל איט לכל או M
                                                                                                                                                                                                                                                                                                                                                                                                                                                    L\left(M\right)=L\left(M'\right) עבורה \mathcal{O}\left(T^{2}\left(n\right)\right)
                                                                                                                                           .DNFCNF = \{\langle \varphi \rangle \mid (\varphi \in {\sf DNF}) \land ({\sf pergn})\} הגדרה:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         (x) או דוחה את (x) אולכל קלט (x) של (x) אולכל מ"ט (x) אולכל קלט (x) אולכל קלט (x) אולכל מ"ט (x)
                                                                                                                                                                                                                           .DNFCNF \in \mathcal{P} :טענה
                                                                                                                                                                                                                                                                                 M' שרצה אזי קיימת מ"ט T (n) איזי קיימת מ"ט ותהא M מודל תהא T (n) איזי T באשר T : \mathbb{N} איזי T באשר אזי סענה: תהא T
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  (x) מתקיים M מתקיים (M לא עוצרת עבור (M,x) אוצרת עבור M לא עוצרת עבור M
                                                                                                                                                                                                                                                                                                                                                                                                                                                   L\left(M\right)=L\left(M'\right) עבורה \mathcal{O}\left(T^{3}\left(n\right)\right)
                               (u \in C) \lor (v \in C) מתקיים \{u,v\} \in E עבורה לכל עבורה אזי אזי C \subseteq V אזי גרף אז מכוון אזי מיסיי קודקודים: יהי
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  x \notin \operatorname{Im}(f) את דוחה את x \notin \operatorname{Im}(f) באשר x \in \{0,1\}^* לכל
                                                                                                                                                                                                                                                                                 x\in \Sigma^n ולכל n\in \mathbb{N} בבורה לכל T:\mathbb{N} 	o \mathbb{N} מטל"ד אזי אוי T:\mathbb{N} 	o \mathbb{N} וולכל איז וולכל מיורינג לא־דטרמיניסטית: תהא
                                                                                                            .VC = \{\langle G,k\rangle \mid k גרף גרף א מכוון בעל כיסוי קודקודים מגודל מגרף גרף א גרף א מכוון הגדרה:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 L 
otin \mathcal{RE} \cup \infty \mathcal{RE} שפה עבורה L \subseteq \{0,1\}^* סענה: קיימת
                                                                                                                                                                                                                                                                                                                                                                                                                                                          T\left( n
ight) בעומק לכל היותר T_{N,\,x} מתקיים כי
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 .ACC = \{\langle M,x \rangle \mid (מ"ט) \wedge (מ"ט) \wedge (x מילה M) \wedge (מ"ט) \wedge (
                                                                                                                                                                                                                                                                                                                                  .NTime (T\left(n
ight))=\{L\left(N
ight)\mid\mathcal{O}\left(T\left(n
ight)
ight) מטל"ד שרצה בזמן מטל"ד שרצה בזמן N\} אזי T:\mathbb{N}
ightarrow\mathbb{N} הגדרה: תהא
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              ACC \in \mathcal{RE} :טענה
                                                                                                                                 \mathcal{B}\subseteq igcup_{n=1}^\infty \left(\Sigma^n
ightarrow \Sigma
ight) אלפבית אזי איזי פונקציות: יהי \Sigma אלפבית אזי
                                                                                                                                                                                                                                                                                  2^{\mathcal{O}(T(n))} שרצה בזמן M שרצה בזמן T אוי קיימת מ"ט T שרצה בזמן T ותהא T ותהא T ותהא T מטל"ד שרצה בזמן T אוי קיימת מ"ט T
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                L\left(M
ight)=\{\langle N
angle \mid \langle N
angle 
otin L\left(N
ight)\} עבורה עבורה \{0,1\} מעל M מעל מיימת מ"ט M מעל
f_1 \dots f_n \ \in \ \mathcal{B} תהיינה k_1 \dots k_n \ \in \ \mathbb{N}_+ מעגל: יהי \mathcal{L} אלפבית יהי בסיס פונקציות מעל
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            L(N) = L(M) עבורה
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           \{\langle N \rangle \mid \langle N \rangle \notin L\left(N
ight)\} אזי קיימת מ"ט N המכריעה את ACC אזי המכריעה מ"ט מ"ט המכריעה את M
G באשר x_1 \ldots x_m, y_1 \ldots y_k \in \Sigma ותהיינה ווה i \in [n] אזי גרף מכוון i \in [n] מעל
                                                                                                                                                                                                                                                                                                                                                                                                                                                                        \mathcal{P} = igcup_{c \in \mathbb{N}} DTime (n^c): \mathcal{P} שפה
                                                                                                                                                     המקיים \{f_1\ldots f_n, x_1\ldots x_m, y_1\ldots y_k\}
                                                                                                                                                                                                                                                                                                                                                                                                            .PATH =\{\langle G,s,t
angle \mid tל מ־s לים מסלול מכG\} גרף מכוון עם מסלול מ־s
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         .HALT =\{\langle M,x\rangle\mid \langle M,x\rangle\mid (מ"ט) \wedge (מ"ט) \wedge (עוצרת על M) \wedge (עוצרת על M) אודרה:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 .PATH \in \mathcal{P} :טענה
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   .HALT \in \mathcal{RE} \setminus \mathcal{R} :טענה
                                                                                                                                                  \deg^-(x_i) = 0 מתקיים i \in [m] לכל •
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              .PRIME \in \mathcal{P} משפט:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  .EMPTY = \{\langle M \rangle \mid (a"b) \land (L(M) = \varnothing)\} הגדרה:
                                                                                                                                                 .deg – (f_i) = k_i מתקיים i \in [n] לכל •
                                                                                                                                                                                                                                                                                                                                                                                                                                                           \mathcal{NP} = igcup_{c \in \mathbb{N}} NTime (n^c): \mathcal{NP} שפה
                                                                                                  \deg^+(y_i)=0 וכן \deg^-(y_i)=1 מתקיים i\in[k] •
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           \mathcal{P} \subseteq \mathcal{NP} :מסקנה
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  M מתקיים כי x\in D מתקיים לכל עבורה לכל f:D	o (\Gamma\backslash \{\sqcup\})^* אזי שותהא מ"ט ותהא מ"ט ותהא מיט ותהא
                                                                                                                                               הערה: נשמור על הטרמינולוגיה ממעגל בוליאני כהכללה טבעית.
                                                                                                                                                                                                                                                                                                                                                                                .
HAMPATH = \{\langle G,s,t\rangle\mid tל המילטוני מ־sל המילטוני מסלול עם מכוון אוף מכוון עם מסלול המילטוני מ־
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               f(x) בסוף הריצה הינו x וכן הסרט בסוף הריצה הינו
מטריצת הקונפיגורציות/טאבלו: תהא M מ"ט שרצה בזמן באשר T : \mathbb{N} א חשיבה בזמן מטריצת הקונפיגורציות/טאבלו: תהא א חשיבה בזמן השיבה בזמן הא מטריצת הקונפיגורציות/טאבלו
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  .HAMPATH \in \mathcal{NP} :טענה
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        f:D	o (\Gamma\backslash \{\sqcup\})^* אזי חשיבה: תהא D\subseteq \Sigma אחי f:D	o (\Gamma\backslash \{\sqcup\})^* אזי מיט
 המקיימת 	au_{M,z}\in M_{T(n)+1} (\Sigma\uplus\Gamma) איז איז M(z) קונפיגורציות קונפיגורציות בc_1\ldots c_i ותהיינה z\in\{0,1\}^n
                                                                                                                                                                                                                                                                                                                                                                                                                                                                      השערה: אורה פתוחה השערה פתוחה השערה וארה השערה פתוחה
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 \mathcal{EXP} = igcup_{k \in \mathbb{N}} DTime \left(2^{n^k}
ight) :\mathcal{EXP} שפה
                                                                                                                                                                                                                      R_i \left( \tau_{M,z} \right) = c_i
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 (x\in A)\Longleftrightarrow (f(x)\in B) מתקיים x\in \Sigma^* לכל חשיבה עבורה לכל
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  ר רדוקציית f:\Sigma^*	o\Delta^* שפה ותהא שפה תהא באשר A\subseteq\Sigma^* תהא ב\Sigma\subseteq\Delta שפה תהא באשר A\subseteq\Sigma
                                                   . \delta\left(q_{T},\sigma
ight)=\left(q_{T},\sigma,R
ight) וכן וכן \delta\left(q_{a},\sigma
ight)=\left(q_{a},\sigma,R
ight) כי נניח נניח הקונפיגורציות נניח כי
                                                                                                                                                                                                                                                                                                                                                                                                                               \mathcal{NEXP} = \bigcup_{k \in \mathbb{N}} \text{ NTime } \left(2^{n^k}\right) : \mathcal{NEXP} שפה
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         A \leq_m B מיפוי אזי
                                                         .CIRSAT = \{\langle C,x\rangle\mid ( מעגל בוליאני C)\wedge (\exists w\in\{0,1\}^*(C(x,w)=1))\} הגדרה:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            \mathcal{E}\dot{\mathcal{X}}\mathcal{P} \subset \mathcal{N}\mathcal{E}\mathcal{X}\mathcal{P} :טענה
          כך \Sigma \uplus \Gamma חשיבה מעלים מעל T (n) הגדיר מיט רצה מיט ותהא א וותהא M האדר מעלים מעל חשיבה בזמן חשיבה בזמן א וותהא וותהא T: \mathbb{N} \to \mathbb{N}
                                                                                                                                                                                                                                                                                                                                                                                                                                                   \mathcal{P} \subset \mathcal{NP} \subset \mathcal{EXP} \subset \mathcal{NEXP} מסקנה:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             A\in\mathcal{R} אזי A\leq_{m}B וכן B\in\mathcal{R} שפות באשר A,B אזי איי
                                                                                                                                C_{\mathrm{inp}}\left(z\right)=R_{0}\left(	au_{M,z}\right) איי z\in\Sigma שירי •
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          \mathcal{P} \subsetneq \mathcal{EXP} :טענה
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          B 
otin \mathcal{R} אזי A \leq_m B וכן A 
otin \mathcal{R} שפות באשר A, B אזי A \leq_m B וכן
                                                                                                                    אזי i\in\{0,\ldots,T\left(n
ight)-1\} ווהי z\in\Sigma\sqcup\Gamma יהי יהי z\in\Sigma
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              \mathcal{NP} \subsetneq \mathcal{NEXP} טענה:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               . בו עברנו על זה פורמלית, מסומן ... את רדוקציית המיפוי, לא עברנו על זה פורמלית, מסומן ...
                                                                                                                                    C_{\text{next}}\left(R_i\left(\tau_{M,z}\right)\right) = R_{i+1}\left(\tau_{M,z}\right)
                                                                                                                                                                                                                                                                                                                                                                                                          x על M מ"ט ויהי X\in \Sigma^* אזי אזי M הינו ריצת M על X
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  \{\langle M \rangle \mid \langle M \rangle \not\in L\left(M
ight)\} \leq 	ext{ACC} מסקנה:
                                                                                                   .C_{\mathrm{out}}\left(R_{T(n)}\left(	au_{M,z}
ight)
ight)=M\left(z
ight) איזי z\in\Sigma ש הי הי z\in\Sigma
                                                                                                                                                                                                                                                                                                                                                                              מוודא לשפה: תהא \Sigma \cup \{","\} מעל אלפבית עים אזי מ"ט שפה אזי המקיים ב\mathcal{L} \subseteq \Sigma^* מוודא לשפה: מוודא 
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   .ACC \leq_m HALT מסקנה:
                                                 .C_{M,n}^{\Sigma orall \Gamma}(z) = \left( C_{	ext{out}} \circ C_{	ext{next}} \circ \ldots \circ C_{	ext{next}} \circ C_{	ext{inp}} 
ight)(z) אוי z \in \Sigma \uplus \Gamma יהי
                                                                                                                                                                                                                                                                                                                                                                                   . מקבלת V\left(x,w\right) עבורו w\in\Sigma^{*} אזי קיים x\in\mathcal{L} מקבלת.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       .ACC < EMPTY מסקנה:
```

.REG  $= \{\langle M \rangle \mid$  רגולרית  $L\left(M
ight)\}$ 

 $ext{EQ} = \{ \langle M_1, M_2 \rangle \mid L\left(M_1
ight) = L\left(M_2
ight) \}$  הגדרה:

.REG  $\notin \mathcal{R}$  :טענה

המסיימת  $v \in \Sigma^*$  עבורה פיים c עבורה מיים m מ"ט רב־סרטית אזי הונפיגורציה c עבורה היים  $v \in \Sigma^*$  המסיימת

. מסקנה: יהי אזי מכונת טיורינג ומכונת טיורינג מכונת אזי מכונת אזי אזי מכונת אזי מכונת אזי מכונת מיורינג ומכונת מסקנה: יהי אוי מכונת מכונ

 $.c = q_0 v \sqcup q_0 \sqcup \dots q_0 \sqcup$ 

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

מתקיים כי  $x,w\in \Sigma^*$  המקיים כי לכל א פוודא v ל־U שפה איי מוודא בור שפה איי מוודא ל־v שפה איי מוודא בור בור פולינומי לשפה: תהא בור עבור לי

 $(\mathcal{L}^+)$  שפה אזי ( $\mathcal{L}\in\mathcal{RE}$ ) שפה אזי (ב $\mathcal{L}\subset\Sigma^*$  עענה: תהא

```
\left|C_{M,n}^{\Sigma oxplus T}
ight|=\mathcal{O}\left(T^{2}\left(n
ight)
ight) אוי T\left(n
ight) אוי מ"ט רצה מותה אוות א מ"ט באשר חשיבה בזמן באשר T:\mathbb{N}	o\mathbb{N} אוי מענה: תהא
                                                                                                             f\left(1^{n}
ight)=\left\langle C_{M,n}^{\Sigmaoxtimes\Gamma}
ight
angle עבורה poly \left(T\left(n
ight)
ight) חשיבה אחשיבה בזמן אפון אינון אינות פונקציה אחשיבה בזמן אינות האונות אינות אות אינות אות אות אונות אינות אונות אונות אינות אינות אונות אינות אינות אינות אינות אינות אינות אינות אונות אינות אינות אינות אינות אינות אונות אונות אינות אינות אינות אינות אינות אונות אונות אינות אינות אונות אינות אונות או
z\in \Sigma \uplus \Gamma ויהי T ויהי T ויהי T אזי z\in \Sigma \uplus \Gamma ויהי T ויהי T ויהי T אזי T אזי T מסקנה: תהא
                                                                                                                                                                                                                                             C_{M,n}^{\Sigma \uplus \Gamma}(z) = M(z)
חשיבה f מייט רצה בזמן T (n) אזי קיימת פונקציה M חשיבה בזמן באשר T : \mathbb{N} א אזי קיימת פונקציה n חשיבה חשיבה בזמן באשר אזי קיימת פונקציה n
וכן לכל \left|C_{M,n}
ight|=\mathcal{O}\left(T^{2}\left(n
ight)
ight) מעגל עבורו \left(C_{M,n}
ight)=\left\langle C_{M,n}
ight
angle וכן לכל poly \left(T\left(n
ight)
ight)
                                                                                                                                        (C_{M,n}\left(z
ight)=1)מקבלת) מקבלת M\left(z
ight) מתקיים z\in\left\{ 0,1\right\} ^{n}
 משפחת לחישוב על ידי משפחת f:\{0,1\}^* \to \{0,1\} וותהא ווא בימ בימן באשר משפחת משפחת משפחת משפחת משפחת משפחת משפחת משפחת משפחת
                                                                                                                       \sqrt{T\left(n\right)} מעגלים מגודל T\left(n\right) אזי f לא ניתנת לחישוב על ידי מ"ט בזמן \mathcal{O}\left(T\left(n\right)\right)
                                                                                                                                                                                                                                                    .CIRSAT \leq_{\mathcal{P}} 3SAT מענה:
                                                                                                                                                                                                                                        .3SAT \leq_{\mathcal{D}} SUBSETSUM :טענה
                                                                                                                                                                                                                                     .SUBSETSUM \in \mathcal{NPC} מסקנה:
                                                                                                                                                                                                                                            .3SAT \leq_{\mathcal{D}} HAMPATH טענה:
                                                                                                                                                                                                                                          .HAMPATH \in \mathcal{NPC} מסקנה:
                                                                                                                                                                                             .co\mathcal{NP}=\left\{L\mid\overline{L}\in\mathcal{NP}
ight\} :co\mathcal{NP} שפה
                                                                                                                                                                                                                           השערה: א\mathcal{NP} 
eq \mathcal{NP}. השערה פו
                                                                                                                                                                                             אזי A \leq_{\mathcal{D}} B שפות באשר A, B אזי אינה: תהיינה
                                                                                                                                                                                                   A \in \mathcal{NP} אא B \in \mathcal{NP} אס •
                                                                                                                                                                                          A \in co \mathcal{NP} אזי B \in co \mathcal{NP} אם \bullet
```

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

. הוחה  $M\left(x\right)$  אשר אינו קידוד של שלשת מטריצות  $x\in\left\{ 0,1\right\} ^{st}$  לכל

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

 $\mathcal{P} \subseteq \mathcal{NP} \cap \mathrm{co}\mathcal{NP}$  טענה: השערה:  $\mathcal{P} 
eq \mathcal{NP} \cap \mathcal{coNP}$ . השערה פתוחה

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

השערה:  $\mathcal{P} 
eq \mathcal{NP} \cap \mathcal{CoNP}$ . השערה פתוחה .MATMULT =  $\{\langle A, B, C \rangle \mid (A, B, C \in M_n(\mathbb{Z})) \land (A \cdot B = C)\}$  הגדרה:

 $\mathbb{P}_{r\leftarrow\{0,1\}}n\;(D\cdot r=0)\leq 0.5$  איז D
eq 0 באשר באשר  $D\in M_n$ 

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

 $x=\langle A,B,C \rangle$  וכן  $A\cdot B \neq C$  המקיימות  $A,B,C \in M_n$  ( $\mathbb Z$ ) עבורו קיימות  $x\in\{0,1\}^*$  לכל  $\mathbb{P}\left(M\left(x
ight)\right) \leq 2^{-100}$ מתקיים מתקיים

Cב אזי נוסחה ב־  $\{+,\times\}$  עם הבסיס אזי מעגל מעל C אזי ווסחה ביה נוסחה אריתמטית: יהי

 $arphi\equiv 0$  אזי  $arphi\;(x_1\ldots x_n)=0$  מתקיים  $x_1\ldots x_n\in\mathbb{F}$  אזי עבורה עבורה אריתמטית מעל arphi $\mathrm{ZE}_{\mathbb{F}}=\{\langle arphi
angle \mid arphi\equiv 0$  עבורה עבורה אריתמטית אריתמטית מעל arphi $\overline{ ext{ZE}_{\mathbb{Z}_2}}\in\mathcal{NPC}$  :טענה

> $2^h$  מעל פולינום מדרגה פולינום מא מעל אזי פעומק איזי בעומק א מעל פוסחה אריתמטית מעל פוסחה איזי ענה: תהא פולינום מדרגה לכל היותר אזי  $\deg\left(f
> ight)<|\mathbb{F}|$  באשר  $f\in\mathbb{F}\left[x_{1},\ldots,x_{n}
> ight]$  המחשבת שענה: תהא arphi נוסחה אריתמטית מעל

 $(\varphi \equiv 0) \iff (f = 0)$ 

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

 $\mathbb F$  ותהא f
eq 0 באשר  $f\in \mathbb F[x_1,\ldots,x_n]$  ותהא  $f
eq f\in \mathbb F[x_1,\ldots,x_n]$  $\mathbb{P}_{a_1,\ldots,a_n\leftarrow S}\left(f\left(a_1\ldots a_n\right)=0\right)\leq \frac{\deg(f)}{|S|}$ 

.poly (|arphi|) מקבלת בזמן M (x) מתקיים  $x=\langle arphi \rangle$  וכן  $arphi \in \mathbb{R}$  מתקיים מעל  $\omega$  מקבלת מעל  $\omega$ בזמן  $\mathbb{P}\left( m(x) \right) \leq 0.01$  מתקיים  $x=\langle \varphi \rangle$  וכן  $\varphi \not\equiv 0$  המקיימת מעל m(x) מקבלת הריתמטית מעל  $\varphi$ 

 $x\in\{0,1\}^{T(|x|)}$  באשר x\$r באשר xמכונת טיורינג אקראית: תהא במן אזי מ"ט דו־סרטית xט דו־סרטית איז פונפיגורציה התחלתית באשר וויים חשיבה בזמן אזי מ"ט דו־סרטית איז פונפיגורציה התחלתית באשר וויים חשיבה בזמן אזי מ"ט דו־סרטית באונפיגורציה התחלתית באשר וויים וויים באשר וויים באשר וויים וויים באשר וויים באשר

T אזי אקראית טיורינג אקראית מכונת M מכונת חשיבה בזמן תהא אוי T (n) אזי אקראית אקראית מכונת איזי Tאזי  $r \in \{0,1\}^{T(|x|)}$  אזי ווהי  $x \in \{0,1\}^*$  יהי יהי און זמן זמן אקראית עם אקראית עם זמן יהי א זיהי יהי אויהי

M(x;r) = M(x\$r)קלט של מכונת טיורינג אקראית: תהא M מ"ט אקראית עם זמן ריצה T (n) יהי T (n) אזי אקראית: תהא M מ"ט אקראית: תהא א מ"ט אקראית עם זמן ריצה אויהי

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

עבור M (x: r) אפתנה מקרי לקבלת (x: M משתנה מקרי לקבלת (x: x) עבור איזי M מיט אקראית עם זמו ריצה (x: x) יהי x קלט אזי xאקראית.  $r \in \{0,1\}^{T(|x|)}$ 

 המקיימת כי החל ממקום תהא עם ומן ריצה פולינומי מ"ט אברה שפה T (n) המקיימת מ"ט אקראית עם אפרה עבורה פיימת מ"ט אברה תהא מון מול ממקום  $lpha:\mathbb{N} o [0,1]$ מסויים  $n \in \mathbb{N}$  מתקיים

 $\mathbb{P}_{r\leftarrow\{0.1\}T(n)}$  מקבלת) מקבלת  $M\left(x;r
ight)\geqlpha\left(n
ight)$  מתקיים  $x\in\mathcal{L}\cap\Sigma^{n}$  לכל  $\star$ 

 $\mathbb{P}_{r\leftarrow\{0,1\}}T(n)$  מקבלת) אינ מתקיים  $M\left(x;r
ight)=0$  מתקיים  $x
otin\mathcal{L}\cap\Sigma^{n}$  לכל  $x\in\mathcal{L}$  $\mathcal{L} \in \mathcal{RP}(\alpha)$  אזי

 $\mathcal{RP}\left(\beta\right)\subseteq\mathcal{RP}\left(\alpha\right)$  איינה מסויים מסויים  $\alpha\leq\beta$  באשר  $\alpha,\beta:\mathbb{N} o [0,1]$  טענה: תהיינה

 $\mathcal{RP}\left(lpha
ight)\subset\mathcal{NP}$  איי מסויים מסויים באשר 0<lpha באשר  $lpha:\mathbb{N} o[0,1]$  עענה: תהא

 $.co\mathcal{RP}\left(lpha
ight)=\left\{\overline{L}\mid L\in\mathcal{RP}\left(lpha
ight)
ight\}$  איי  $lpha:\mathbb{N}
ightarrow\left[0,1
ight]$  הגדרה: תהא  $T\left(n
ight)$  אם זמן ריצה פולינומי מ"ט אקראית M עם אם קיימת מ"ט אם בה  $\mathcal{L}\in\mathrm{co}\mathcal{RP}\left(lpha
ight)$  אויי ההא שפה lpha אויי מויי איי איי המויע אייט אקראית מ"ט אקראית  $lpha:\mathbb{N} o [0,1]$ מתקיים  $n \in \mathbb{N}$  ממקום מסויים מחקיים

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

 $\mathbb{P}_{r\leftarrow\{0,1\}T(n)}$  (מקבלת  $M\left(x;r
ight)$  בול X
otin T(n) מתקיים א מתקיים X
otin T(n) הכל

. $ZE_{\mathbb{R}}\in co\mathcal{RP}\left(0.99
ight)$  טענה:  $c,d\in\mathbb{N}$  טענה: יהיו א  $c,d\in\mathbb{N}$  טענה: יהיו

המקיימת  $T\left(n\right)$  המקיימת עם זמן עבורה היימת מ"ט אקראית M עם זמן עבורה המקיימת lpha, eta ותהא שפה lpha, eta ותהא שפה lpha, עבורה היימת מ"ט אקראית a, און דיצה פולינומי

 $\Gamma_{r\leftarrow\{0,1\}}T(n)$  מקבלת) מקבלת  $M\left(x;r
ight)\geqeta\left(n
ight)$  מתקיים  $x\in\mathcal{L}\cap\Sigma^{n}$  לכל •

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

 $\mathcal{L} \in \mathcal{BPP}\left(lpha,eta
ight)$ אזי

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

 $\mathcal{RP}\left(\alpha\right)=\mathcal{BPP}\left(0,\alpha\right)$  אוי  $\alpha:\mathbb{N} 
ightarrow \left[0,1\right]$  טענה: תהא

.co $\mathcal{RP}(\alpha) = \mathcal{BPP}(1-\alpha,1)$  איז  $\alpha: \mathbb{N} \to [0,1]$  סענה: תהא טענה: תהיינה ממקום מסויים אזי  $lpha \leq eta \leq \gamma \leq \delta$  עבורן  $lpha, eta, \gamma, \delta: \mathbb{N} o [0,1]$  אזי סענה: תהיינה  $\mathcal{BPP}(\alpha, \delta) \subseteq \mathcal{BPP}(\beta, \gamma)$ 

אזי  $A_1,\ldots,A_n\sim \mathrm{Ber}\,(p)$  ויהיו  $n\in\mathbb{N}$  יהי  $\delta>0$  יהי הופדינג: משפט צ'רנוף־הופדינג:

.  $\mathbb{P}\left(\left|p-\frac{1}{n}\sum_{i=1}^{n}A_{i}\right|\geq\delta\right)\leq2^{-\Theta\left(\delta^{2}n\right)}$  שענה: יהי  $\alpha:\mathbb{N}\to[0,1]$  החל ממקום מסויים  $\alpha:\mathbb{N}\to[0,1]$  החל ממקום מסויים מסויי  $\mathcal{BPP}\left(lpha\left(n
ight)-n^{-c},lpha\left(n
ight)+n^{-c}
ight)\subseteq\mathcal{BPP}\left(2^{-n^d},1-2^{-n^d}
ight)$  אא דפנוס גרסה של ארבעה עמודים

```
0<|\Sigma|<\aleph_0 אלפבית: קבוצה המקיימת \Sigma
                                                           .\Sigma^* = igcup_{n=0}^\infty \Sigma^n מילים: יהי \Sigma אלפבית אזי
                                  |w|=n מילה אזי w\in \Sigma^n אלפבית ותהא אלפבית יהי מילה: אורך של מילה:
                                           |arepsilon|=0 עבורה arepsilon\in\Sigma^* אלפבית אזי arepsilon\in\Sigma^*
                   \langle w_1 \dots w_n 
angle^R = \langle w_n \dots w_1 
angle אזי \langle w_1 \dots w_n 
angle \in \Sigma^* היפוך מילה: תהא
                                      אזי \langle w_1 \dots w_n \rangle , \langle \omega_1 \dots \omega_m \rangle \in \Sigma^* אזי תהיינה
                                         \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
                                          אזי m\in\mathbb{N} ויהי \langle w_1\dots w_n
angle\in\Sigma^* אזי מילה: תהא
                                                               \langle w_1 \dots w_n \rangle^m = \prod_{i=1}^m \langle w_1 \dots w_n \rangle
                               אות אזי \sigma \in \Sigma ותהא w \in \Sigma^n אות אזי מספר המופעים של אות במילה:
                                                                     \#_{\sigma}(w) = |\{i \in [n] \mid w_i = \sigma\}|
                                                                         L\subset \Sigma^* שפה: יהי \Sigma אלפבית אזי
                                     L^R = \left\{ w^R \mid w \in L 
ight\} היפוך שפה: תהא L \subseteq \Sigma^* היפור אזי
                                                           שרשור שפות: תהיינה \Sigma^* \subseteq \Sigma^* שפות אזי
                                         L_1 \parallel L_2 = L_1 L_2 = \{ w\omega \mid (w \in L_1) \land (\omega \in L_2) \}
                                                   אזי m\in\mathbb{N} אזי שפה ויהי L\subset\Sigma^* אזי אזי m\in\mathbb{N}
                                                           L^{m} = \left\{ \prod_{i=1}^{k} w_{i} \mid \forall i \in [k] . w_{i} \in L \right\}
                                     L^* = igcup_{k=0}^\infty L^k שפה אזי L \subseteq \Sigma^* מגור קליני של שפה: תהא
           .prefix (L)=\{y\in \Sigma^*\mid \exists x\in \Sigma^*.yx\in L\} שפה אזי שנת הרישא: תהא L\subseteq \Sigma^* שפה אזי
           .suffix (L)=\{y\in\Sigma^*\mid\exists x\in\Sigma^*.xy\in L\} שפה אזי L\subseteq\Sigma^* תהא שפת הסיפא: תהא
      אלגוריתם מכריע שפה: תהא L \subseteq \Sigma^* שפה אזי אלגוריתם מכריע שפה: תהא אלגוריתם L \subseteq \Sigma^*
                                                    A(x) = \text{true} מקבל: לכל x \in L מתקיים
                                                    A\left(x\right)= false מתקיים x\notin L לכל
                               f:\{0,1\}^n 	o \{0,1\}^m אזי n,m \in \mathbb{N} פונקציה בולאנית: תהיינה
                \{f_1\dots f_n\} אזי בסיס פונקציות בוליאניות: תהיינה \{f_1\dots f_n\} פונקציות בוליאניות היינה
                                                                         \mathcal{B} = \{\wedge, \vee, \neg\} בסיס דה־מורגן:
                                                       הערה: תמיד נוסיף לבסיס את הפונקציות הקבועות.
f_1 \dots f_n \in \mathcal{B} מעגל בוליאני: יהי k_1 \dots k_n \in \mathbb{N}_+ מעגל בוליאני: יהי פונקציות בוליאניות תהיינה
באשר x_1\dots x_m,y_1\dots y_k\in\{0,1\} ותהיינה i\in[n] לכל f_i:\{0,1\}^{k_i}	o\{0,1\} אזי
                                     המקיים \{f_1 \dots f_n, x_1 \dots x_m, y_1 \dots y_k\} המקיים גרף מכוון
                                                                           .חסר מעגלים מכוונים G
                                                       \deg^-(x_i)=0 מתקיים i\in[m] • לכל
                                                       \deg^-(f_i) = k_i מתקיים i \in [n] לכל •
                              \operatorname{deg}^+(y_i) = 0 וכן \operatorname{deg}^-(y_i) = 1 מתקיים i \in [k] •
                                                                    f_1 \dots f_n יהי מעגל בוליאני אזי מעגל יהי
                                                                   E\left(C\right) יהי מעגל בוליאני אזי מעגל מעגל מעגל יהי
                                         \max_{v \in V(C)} \deg^+(v) יהי מעגל בולינארי אזי :fan-out
                           \{G \leq C \mid 1 \text{ הוא } G \text{ של fan-out} \} מוחסאות: יהי C מעגל בולינארי אזי
(x_1 \dots x_m) = v אזי v \in \{0,1\}^m שערוך מעגל בולינארי על קלט: יהי מעגל מעגל בולינארי על אזי
                   וכן y_i הינו הפלט הנוצר מהפעלת הפונקציות הבוליאניות על הקודקודים הנכנסים.
                      v על v אזי השערוך של C איז האערוך על v \in \{0,1\}^m אוי ויהי v \in \{0,1\}^m על על הוא
                                                                                      .C(v) = (y_1 \dots y_k)
              C\left(w
ight)=1 עבורו w\in\left\{ 0,1
ight\} ^{n} עבורו אזי פעגל בעל מעגל מקבל מילה: יהי C מעגל מקבל מילה:
    L(C) = \{x \in \{0,1\}^n \mid x שפה של מעגל: יהי C מעגל בעל פלט יחיד אזי C מקבל את מעגל: יהי C
v \in \{0,1\}^n עבורו לכל עבורו C אזי מעגל בולינאני f:\{0,1\}^n 	o \{0,1\} מעגל מחשב פונקציה: תהא
                                                                                    .C(v) = f(v) מתקיים
משפט אוניברסליות דה־מורגן: תהא f:\{0,1\}^m 	o \{0,1\}^k מעל בוליאני משפט אוניברסליות משפט אוניברסליות משפט אוניברסליות משפט אוניברסליות משפט אוניברסליות מעל בוליאני
                                 C\left(v\right)=f\left(v\right) מתקיים v\in\left\{ 0,1\right\} ^{m} בסיס דה־מורגן עבורו לכל
                                 הערה: מכאן והלאה כל המעגלים הם בוליאניים ומעל בסיס דה־מורגן.
                            i משפחה של מעגלים: מעגלים עבורם \{C_n\}_{n\in\mathbb{N}} משפחה של מעגלים: מעגלים
                                               שפה של משפחת מעגלים: תהא \mathcal C משפחה של מעגלים אזי
                                                           L(C) = \{x \in \{0,1\}^* \mid x \in L(C_{|x|})\}
   L\left(\mathcal{C}
ight)=\mathcal{L} עבורה ענלים שפחה מעגלים אזי משפחה שפה ענהא \mathcal{L}\subset\{0,1\}^* עבורה שפה: תהא
                   מודל לא יוניפורמי: משפחה של מעגלים \mathcal C עבורה לכל n\in\mathbb N יש אלגוריתם שונה.
                         . הה. שלגוריתם אלגוריתם החדל יוניפורמי: משפחה של מעגלים \mathcal C עבורה לכל n\in\mathbb N יש אלגוריתם החדל
                                         Cב מספר השערים ב־|C| מזיי מעגל בוליאני הי מעגל מעגל: יהי מעגל בוליאני
```

```
עבורה S:\mathbb{N} 	o \mathbb{N} אזי אזי משפחה של מעגלים: תהא \mathcal{C} אחסם מעגלים: עבורה
                                                                                 |\mathcal{C}_n| < S(n)
```

 $\mathcal{O}\left(n\cdot 2^n\right)$  אזי קיים מעגל  $f:\{0,1\}^n o\{0,1\}$  אחי שמחשב את  $f:\{0,1\}^n$  $|C|=\mathcal{O}\left(n\cdot 2^n
ight)$ וכן  $L\left(C
ight)=\mathcal{L}$  אזי קיים מעגל אזי פיים מעגל בורו אזי תהא  $\mathcal{L}\subseteq\{0,1\}^n$  מסקנה: תהא  $\mathcal{O}\left(2^{n}
ight)$  אזי איי פיים מעגל  $f:\{0,1\}^{n}
ightarrow\{0,1\}$  שמחשב את איי קיים מעגל ל $f:\{0,1\}^{n}
ightarrow\{0,1\}$  $L(C)=\mathcal{O}\left(2^{n}
ight)$  וכן וכן  $L\left(C
ight)=\mathcal{L}$  אזי קיים מעגל אזי עבורו  $\mathcal{L}\subseteq\left\{ 0,1\right\} ^{n}$  מסקנה: תהא  $\mathcal{O}\left(rac{2^n}{n}
ight)$  אזי קיים מעגל C שמחשב את  $f:\{0,1\}^n o\{0,1\}$  משפט לופיאנוב: תהא טענה שאנון: קיים  $n\in\mathbb{N}$  עבורו קיימת  $f:\{0,1\}^n o\{0,1\}$  שאינה ניתנת לחישוב בעזרת  $n\in\mathbb{N}$ 

 $\frac{2^n}{10n}$  מעגל C בגודל קטן מאשר אוטומט סופית יהי אלפבית תהא  $Q 
eq \varnothing$  תהא אלפבית יהי אלפבית תהא  $(Q,\Sigma,\delta,q,F)$  אזי  $F\subseteq Q$  ותהא  $q\in Q$  יהי  $\delta:Q imes\Sigma o Q$ Q אס"ד אזי ( $Q, \Sigma, \delta, q, F$ ) אס"ד אזי אס"ד אזי אס"ד אזי  $\Sigma$  אס"ד אזי ( $Q,\Sigma,\delta,q,F$ ) אס"ד אזי אזי אס"ד אזי אזי

 $.\delta$  אס"ד אזי  $(Q,\Sigma,\delta,q,F)$  אהי אוי אוי אס סופי דטרמיניסטי: יהי  $Q, \Sigma, \delta, q, F$  אס"ד איי אוי אס"ד איי אס"ד איי אס"ד איי אוי אס"ד איי אוי .F אז אזי  $(Q,\Sigma,\delta,q,F)$  אס אס טופי דטרמיניסטי: יהי

עבורה לכל  $\hat{\delta}:Q imes\Sigma^* o Q$  אס"ד אזי ( $Q,\Sigma,\delta,q_0,F$ ) איזי יהי מתקיים  $x\in \Sigma^n$  וכן לכל  $\hat{\delta}\left(q,arepsilon
ight)=q$  מתקיים  $q\in Q$ 

 $\hat{\delta}(q,x) = \delta\left(\hat{\delta}(q,x_1\dots x_{n-1}),x_n\right)$ אמיים אוט אזי אזי אזי  $x\in \Sigma^*$  אס"ד אזי איזי ( $Q,\Sigma,\delta,q_0,F$ ) אוטומט סופי דטרמיניסטי מקבל מילה: יהי  $\hat{\delta}(q_0,x) \in F$ 

טענה: יהי A אס"ד ויהי  $x \in \Sigma^n$  אזי  $x \in \Sigma^n$  אזי יהי A אס"ד ויהי יהי A אס"ד ויהי  $\delta (q_n \in F \;$ וכן  $i \in [n] \;$ לכל  $\delta (q_{i-1}, x_i) = q_i$ 

 $L\left(A
ight)=\{x\in\Sigma^{st}\mid x$  מקבל את אזי  $A\}$  מקביניסטי: יהי יהי אס"ד אזי מקבל את אוטומט סופי דטרמיניסטי:  $L\left(A
ight)=\mathcal{L}$  המקיים A המקיים אס"ד  $\mathcal{L}\subset\Sigma^*$  עבורה אזי שפה  $\Sigma$  אלפבית אזי שפה רגולרית: יהי טענה: Ø רגולרית.

. רגולרית  $\{\varepsilon\}$ 

טענה:  $\{x \mid \#_1(x) = 1 \mod 2\}$  רגולרית. טענה:  $\{y \ 1 \ 0^{2k} \mid (y \in \{0,1\}^*) \land (k \in \mathbb{N})\}$  רגולרית.  $L_1\left(L_2L_3
ight)=\left(L_1L_2
ight)L_3$  שפות אזי  $L_1,L_2,L_3\subseteq\Sigma^*$  טענה: יהיו טענה: תהא  $L^*$  אזי א $L \neq \{arepsilon\}$  וכן  $L \neq \varnothing$  אינסופית.  $L \subseteq \Sigma^*$  אינסופית. משפט: תהיינה  $L, \mathcal{L} \subseteq \Sigma^*$  שפות רגולריות אזי

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

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

אוטומט סופית יהי  $\Sigma$  אלפבית תהא אוטומט סופית יהי לא־דטרמיניסטי מינוס (אסלד"ם): תהא אוטומט סופית יהי לא־דטרמיניסטי מינוס  $(Q,\Sigma,\delta,S,F)$  אזי  $S,F\subseteq Q$  ותהיינה  $\delta:Q imes\Sigma o\mathcal{P}(Q)$ 

Q אזי אוים אוי אסלד"ם אזי ( $Q, \Sigma, \delta, S, F$ ) אוי מינוס: יהי לא־דטרמיניסטי מינוס:

 $\Sigma$  אזי אסלד"ם אזי ( $Q,\Sigma,\delta,S,F$ ) אדער מינוסי מינוסי אסלד"ם אסלד"ם אזי  $.\delta$  אזט אוי ( $Q,\Sigma,\delta,S,F$ ) יהי מעברים אוי אסלד"ם אוי אסלד"ם אוי אסלד"ם אוי

S אזי אזי  $(Q,\Sigma,\delta,S,F)$  אהי מינוס: יהי אסלד"ם אזי אסלד"ם אזי אזי מצבים התחלתיים באוטומט סופי לא־דטרמיניסטי F אסלד"ם אזי ( $Q, \Sigma, \delta, S, F$ ) יהי מינוס: לא־דטרמיניסטי סופי האיטומט מקבלים מקבלים אזי  $\hat{\delta}:\mathcal{P}\left(Q
ight) imes\Sigma^* o\mathcal{P}\left(Q
ight)$  אסלד"ם אזי  $(Q,\Sigma,\delta,S,F)$  יהי יהי עבורה לכל  $x\in \Sigma^n$  מתקיים  $\hat{\delta}\left(T,arepsilon
ight)=T$  מתקיים מתקיים לכל  $\hat{\delta}(q,x) = \bigcup_{q \in \hat{\delta}(T,x_1...x_{n-1})} \delta(q,x_n)$ 

 $x\in \Sigma^*$  אזי אוטומט סופי איזי מינוס מקבל מילה: יהי מינוס מקבל מילה אזי מינוס מינוס מינוס מינוס מינוס מינוס מילה:  $\hat{\delta}(S,x)\cap F\neq\varnothing$  המקיים

עבורם  $q_0\ldots q_n\in Q$  עבורם (קיימים m) אזי אזי (m מקבל את אסלד"ם ויהי אסלד"ם ויהי אזי אזי (m מקבל את אזי אזי (m $(q_n \in F \mid i \in [n]$ לכל  $q_i \in \delta (q_{i-1}, x_i)$ וכן  $q_0 \in S$ 

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

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

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

אזי  $x \in \Sigma^*$  ויהי  $T \subset Q_N$  אחלה של M אס"ד החזקה של M אס"ד אס"ד אזי  $T \in Q_N$  אזי  $\hat{\delta_A}(T,x) = \hat{\delta_M}(T,x)$ 

 $L\left(M
ight)=L\left(A
ight)$  עבורו A עבורו אזי קיים אזי קיים אזי קיים אס"ד אסלד"ם אזי יהי

 $\Sigma_{arepsilon}=\Sigma\cup\{arepsilon\}$  אלפבית אזי אלפבית יהי לימון: יהי

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

Q אסל"ד אזי ( $Q, \Sigma, \delta, S, F$ ) אסל"ד אזי אסל"ד אזי סופי לא־דטרמיניסטי:

 $\Sigma$  אסל"ד אזי ( $Q,\Sigma,\delta,S,F$ ) אסל"ד אזי אסל"ד אזי אסל"ד אזי

 $\delta$  אזי אזי ( $Q,\Sigma,\delta,S,F$ ) אסל"ד אזי אזי אסל"ד אזי אסל"ד אזי אזי S אזי אזי ( $Q, \Sigma, \delta, S, F$ ) אזי אזי לא־דטרמיניסטי: אסל"ד אזי

Aאסל"ד אזי  $(Q,\Sigma,\delta,S,F)$  יהי אסל"ד אזי אסל"ד אזי אסל"ד אזי

 $q \in Q$  אזי אסל"ד ויהי  $r \in Q$  אזי אזי יהי ויהי

 $.E\left(q\right) = \left\{q' \in Q \mid \exists a \in Q^{k+1}. \left(a_0 = q\right) \land \left(\forall i \in [k]. a_i \in \delta\left(a_{i-1}, \varepsilon\right)\right) \land \left(a_k = q'\right)\right\}$  $E\left(T
ight)=igcup_{q\in T}E\left(q
ight)$  אזי  $T\subseteq Q$  אסל"ד ויהי N אסל"ד ויהי arepsilon

 $\hat{\delta}:\mathcal{P}\left(Q
ight) imes\Sigma^* o\mathcal{P}\left(Q
ight)$  אסל"ד אזי  $(Q,\Sigma,\delta,S,F)$  יהי יהי עבורה לכל  $x\in \Sigma^n$  מתקיים  $\hat{\delta}\left(T,arepsilon
ight)=E\left(T
ight)$  מתקיים מתקיים לכל

 $\hat{\delta}(q,x) = R\left(\bigcup_{q \in \hat{\delta}(T,x_1...x_{n-1})} \delta(q,x_n)\right)$ המקיים  $x\in \Sigma^*$  אזי אזי  $(Q,\Sigma,\delta,S,F)$  המקיים מקבל מילה: אוי אזי אזי אזי אזי

 $.\hat{\delta}(S,x) \cap F \neq \emptyset$ 

עבורם  $k_0\ldots k_n\in\mathbb{N}$  ויהיו  $\sigma_1\ldots\sigma_n\in\Sigma\setminus\{arepsilon\}$  יהיי  $x\in\Sigma^*$  יהי שימון: יהי  $x^{\varepsilon} = \sigma_1 \dots \sigma_n$  אא  $x = \varepsilon^{k_0} \sigma_0 \varepsilon^{k_1} \sigma_1 \varepsilon^{k_2} \dots \sigma_n \varepsilon^{k_n}$ 

 $q_0\dots q_n\in Q$  עבורם (x)אזי ( $x\in \Sigma^n$  אזי אסל"ד ויהי אסל"ד אסל"ד אזי אזי ( $x\in \Sigma^n$  אזי אסל"ד ויהי  $(q_n \in F \mid i \in [n]$ לכל  $q_i \in \delta (q_{i-1}, x_i^{\varepsilon})$  וכן  $q_0 \in S$ 

 $L\left(A
ight)=\left\{x\in\Sigma^{*}\mid x$  מקבל את אסל"ד אזי A אסל"ד אסל"ד אזי אסרמיניסטי: יהי ארדטרמיניסטי: יהי א  $L\left(N
ight)=L\left(M
ight)$  עבורו M עבורו אזי קיים אסל"ד אזי קיים אסלד"ם M

 $L\left(A
ight)=L\left(M
ight)$  עבורו אסל"ד אזי קיים אס"ד א אסל"ד אזי קיים אס אסל"ד אזי קיים אס

N המקיים אסל"ד M המקיים אסל"ד אלפבית ותהא  $\mathcal{L}(L(N) = \mathcal{L})$ 

אלפבית אזי היי צולרי (ב"ר): יהי אלפבית אזי ביטוי רגולרי

- .a יהי $a\in\Sigma_{arepsilon}$  אזי •
- $R_1 \cup R_2$  יהיו אזי  $R_1, R_2$  ביטויים רגולרים אזי
  - $R_1R_2$  יהיו  $R_1$  ביטויים רגולרים אזי  $R_1$ 
    - $.R^*$  יהי R ביטוי רגולרי אזי •

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

- $L(\varnothing) = \varnothing$  •
- $L\left(a\right)=\left\{ a
  ight\}$  אזי  $a\in\Sigma_{arepsilon}$  יהי •
- $L(R_1 \cup R_2) = L(R_1) \cup L(R_2)$  יהיו רגולרים אזי רגולרים אזי רגולרים אזי רגולרים אזי
  - $L(R_1R_2) = L(R_1)L(R_2)$  יהיו רגולרים אזי רגולרים אזי רגולרים אזי פיטויים  $R_1, R_2$ 
    - $L\left(R^{*}\right)=L\left(R\right)^{*}$  יהי R ביטוי רגולרי אזי יהי R

 $R\left(\Sigma\right)=\left\{r\in\Sigma^{*}\mid$  ייטוי רגולרי rלפבית אזי אלפבית אזי רגולרי אלפבית אזי אלפבית אזי רגולרי הערה: קיים סדר פעולות לביטויים רגולריים

- סגור קליני.
  - שרשור.

עבורו  $r\in R\left(\Sigma
ight)$  ייהי  $m\in R\left(\Sigma
ight)$  שפה אזי ( $\mathcal{L}$  רגולרית) שפט: יהי אלפבית ותהא  $\mathcal{L}\subseteq\Sigma^*$  שפה אזי ( $\mathcal{L}$  $\mathcal{L}(L(r) = \mathcal{L})$ 

 $x,y,z\in \Sigma^*$  שפה ניתנת לניפוח: שפה  $\ell>0$  וקבוע  $\ell>0$  עבורם לכל שפה ניתנת לניפוח: שפה  $\ell>0$  $xy^kz\in L$  מתקיים  $k\in\mathbb{N}$  וכן לכל w=xyz וכן וכן  $|xy|\leq \ell$  וכן וכן  $\ell$  ניתנת לניפוח עבורו  $\ell>0$  שפה רגולרית אזי קיים שפה עבורו  $\ell>0$  ניתנת לניפוח  $\min \left\{ \ell \in \mathbb{N}_{+} \mid \ell$  ניתנת לניפוח: תהא  $\mathcal{L}$  שפה רגולרית אזי  $\mathcal{L}$  ניתנת לניפוח: תהא

```
\sim_A = \left\{ (x,y) \in (\Sigma^*)^2 \;\middle|\; \hat{\delta}\left(q_0,x
ight) = \hat{\delta}\left(q_0,y
ight) 
ight\} הגדרה: יהי A אס"ד אזי
                   משפט מייהיל־נרוד: תהא L \subseteq \Sigma^* שפה אזי (L \subset \Sigma^* סופית).
\Sigma^*/_{\sim L} שפה באשר \Sigma^*/_{\sim L} סופית תהא \{x_1\dots x_n\} קבוצת נציגים של באשר באשר באשר סימון: תהא
אוטומט סופי \Sigma^*/_{\sim L} שפה באשר באשר המחלקות: תהא אוטומט המיניסטי המחלקות:
                     באשר (Q,\Sigma,\delta,q_0,F) אזי אס"ד \Sigma^*/_{\sim_L} באשר נציגים של \{x_1\dots x_n\}
\Sigma^*/_{\sim_L} טענה: תהא \{x_1\dots x_n\} קבוצת נציגים של באשר שפה באשר באשר באשר \Sigma^*/_{\sim_L} טענה: תהא
\Sigma \subset \Gamma מכונת טיורינג (מ"ט): תהא Q 
eq \emptyset קבוצה סופית יהי אלפבית יהי אלפבית עבורו מכונת טיורינג (מ"ט): מכונת טיורינג
                (Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r) אז \delta: (Q \setminus \{q_a, q_r\}) \times \Gamma \rightarrow Q \times \Gamma \times \{L, R\}
                     \delta מ"ט איי (Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r) מייט איי מעברים במכונת טיורינג: תהא
u,v\in \Sigma^* עבורה קיימים c\in \Gamma^*Q\Gamma^* קונפיגורציה מקבלת: תהא M מ"ט אזי קונפיגורציה
```

```
מכונת טיוריגנ דוחה מילה: תהא M מ"ט אזי x \in \Sigma^* עבורו קיימים מילה: תהא מילה: תהא מיט אזי
                        וכן c_n קונפיגורציה דוחה. i \in [n] לכל לכן עוברת כc_{i-1} וכן c_0 = q_0 x
            L\left(M
ight)=\{x\in\Sigma^{st}\mid x שפה של מכונת טיוריגנ: תהא M מ"ט אזי M מקבל את של מכונת טיוריגנ:
מתקיים M' מסוג M מסוג M מסוג M מחלים: מודלים שקולים: מודלים M,M' מתקיים
                                      L\left(A\right)=L\left(A'\right) המקיימת M' מסוג A' מסוג \bullet
                                       L\left(B\right)=L\left(B'\right) המקיימת M מסוג B' מסוג \bullet
                                              מסקנה: אס"ד, אסל"ד ואסלד"ם הינם מודלים שקולים.
\Sigma \subset \Gamma מכונת טיוריגנ נחה: תהא Q 
eq \emptyset קבוצה סופית יהי אלפבית יהי אלפבית עבורו מכונת טיוריגנ נחה:
\delta:(Q\backslash\{q_a,q_r\})	imes\Gamma	o ותהא q_a
eq q_r באשר באשר קq_0,q_a,q_r\in Q יהיי וורה היי
                                            (Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r) איז Q \times \Gamma \times \{L, R, S\}
           הערה: את כל הפעולות ממכונת טיורינג נכליל בצורה הטבעית עבור מכונת טיורינג נחה.
                                    מסקנה: מכונת טיורינג ומכונת טיורינג נחה הינו מודלים שקולים.
\Gamma מכונת טיורינג רב־סרטית: יהי \Sigma אלפבית הא k\in\mathbb{N}_+ מכונת טיורינג רב־סרטית: יהי
ותהא q_a \neq q_r באשר באשר קq_0,q_a,q_r \in Q יהיו וכן \Sigma \subset \Gamma באשר אלפבית עבורו אלפבית עבורו
       (k, Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r) אזי \delta: (Q \setminus \{q_a, q_r\}) \times \Gamma^k \to Q \times \Gamma^k \times \{L, R\}^k
     הערה: את כל הפעולות ממכונת טיורינג נכליל בצורה הטבעית עבור מכונת טיורינג רב־סרטית.
c_1 \dots c_k \in \Gamma^*Q\Gamma^* קונפיגורציה במכונת טיורינג רב־סרטית: תהא M מ"ט רב־סרטית
                                                                                .c_1 \$c_2 \$ \dots \$c_k אא
קונפיגורציה c עבורה איי קונפיגורציה איי סיורינג רב־סרטית: תהא ש"ט רב־סרטית איי קונפיגורציה c
                                          c=q_0vהמקיימת בq_0...q_0 המקיימת המקיימת ט
          מסקנה: יהי k \in \mathbb{N}_+ אזי מכונת טיורינג ומכונת טיורינג רב־סרטית הינן מודלים שקולים.
                                 (k,(\pi_1\ldots\pi)) אזי (אור ההיינה k\in\mathbb{N} יהי :RAM מודל
                                      k אזי RAM מספר הרגיסטרים במודל RAM: יהי (k,\Pi) מודל
                                                \Pi אזי RAM מודל ויהי (k,\Pi) מודל אזי RAM פקודות במודל
וכן R_0 \dots R_k \in \mathbb{N} וכן PC \in \mathbb{N} אזי RAM מודל (k,\Pi) יהי והי (RAM קונפיגורציה במודל
       .PC מונה התוכנית בקונפיגורציה: יהי (k,\Pi) מודל RAM ותהא (T,R,PC) קונפיגורציה אזי
            R ותהא (T,R, PC) מודל (R מודל (R אזי הונפיגורציה) קונפיגורציה אזי (R קונפיגורציה אזי אזי רגיסטרים בקונפיגורציה: יהי
                T אזי אונפיגורציה (T,R,PC) מודל RAM ותהא (k,\Pi) קונפיגורציה אזי אינרון בקונפיגורציה: יהי
                                                    .MIPS זהה לריצת מעבד RAM זהה לריצת מעבד
                                               טענה: מכונת טיורינג ומודל RAM הם מודלים שקולים.
\Gamma יהי אלפבית יהי \Sigma אלפבית סיוריגנ לא־דטרמיניסטית (מטל"ד): תהא Q \neq \varnothing הבוצה סופית יהי
ותהא q_a \neq q_r באשר q_0, q_a, q_r \in Q יהיי ווה \Sigma \subset \Gamma באשר בורו אלפבית עבורו בי וכן
         (Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r) אזי \delta: (Q \setminus \{q_a, q_r\}) \times \Gamma \to \mathcal{P} (Q \times \Gamma \times \{L, R\})
uqbv באשר u,v\in\Gamma^* ותהיינה b\in\Gamma ותהא q\in Q מטל"ד תהא מטל"ד מטל"ד תהא אונפיגורציה עוברת: ח
\delta': (Q \setminus \{q_a, q_r\}) \times \Gamma \to Q \times \Gamma \times \{L, R\} קונפיגורציה אזי קונפיגורציה ליימת עבורה קיימת
                                   (c'-טוברת ל־\delta' הינה uqbv וכן \delta' (q,b) \in \delta (q,b) המקיימת
עבורו לכל q_0xעם שורש עס אזי עץ קונפיגורציות אזי עץ אזי ער איז ויהי אויהי א מטל"ד ויהי אזי עץ אזי עץ אזי עץ אזי ער מטל"ד ויהי
                                 (c^{-1}) עוברת (c^{\prime}) עוברת של (c^{\prime}) עוברת ל־(c^{\prime}) עוברת ל־(c^{\prime})
מכונת טיוריגנ לא־דטרמיניסטית מקבלת מילה: תהא א מטל"ד מייב עבורו קיים עלה מקבל מכונת טיוריגנ מיוריגנ ארדטרמיניסטית מקבלת מילה: עבורו מיים עלה מקבל
x סופי וכן סופי עבורו T_{N,x} עבורו אזי אזי x\in \Sigma^* מטל"ד אזי מרונת מילה: תהא מילה: תהא
                                                                                                           u,v\in \Sigma^* עבורה קיימים c\in \Gamma^*Q\Gamma^* קונפיגורציה מ"ט אזי קונפיגורציה מ"ט מ"ט אזי קונפיגורציה אור מ"ט מ
                                                                              N אינו מתקבל על ידי
                                      שפה של מכונת טיוריגנ לא־דטרמיניסטית: תהא N מטל"ד אזי
                                                          L(N) = \{x \in \Sigma^* \mid x מקבל את N\}
                                                                                                           קונפיגורציה אזי קונפיגורציה מ"ט תהא d מ"ט תהא מ"ט מונפיגורציה אזי קונפיגורציה תהא M המקיימת אחד
```

```
\mathcal{R} \subseteq \mathcal{RE} :מסקנה
                 עבורו \Sigma \cup \{\$\} מעל האלפבית מ"ט E שפה אזי מ"ט \mathcal{L} \subset \Sigma^* עבורו
                              \delta(q,\sigma)=(q',\sigma',R) מתקיים \sigma\in\Gamma ולכל •
                                                         על הקונפיגורציה \varepsilon מקיימת •
             . לכל x \in L מתקיים כיx \in \mathbb{R} על הסרט לאחר מספר סופי של צעדים.
                                  \mathcal{L} \subset \Sigma^* מונה). שפה אזי \mathcal{L} \subset \Sigma^* מונה) שפה אזי ענה: תהא
x <_{	ext{lex}} y באשר x,y \in \mathcal{L} עבורו לכל עבור שפה אזי מונה E שפה אזי מונה לקסיקוגרפי: תהא
                                                            \$y$ מתקיים כי
                       . (קטיקוגרפי) שפה אזי (\mathcal{L} \in \mathcal{R}) שפה אזי שפה \mathcal{L} \subset \Sigma^* מונה לקסיקוגרפי).
                                    \mathrm{co}\mathcal{RE}=\left\{\mathcal{L}\subset\Sigma^*\mid\overline{\mathcal{L}}\in\mathcal{RE}
ight\} הגדרה: יהי \Sigma אלפבית אזי
                                                                             \mathcal{R} = \mathcal{RE} \cap \mathrm{co}\mathcal{RE} :טענה
יע עד כדי שינוי f:\{M\mid מ"ט M\}	o\{0,1\}^* חח"ע עד כדי שינוי
                                        M מ"ט אזי \langle M \rangle הינו הקידוד הבינארי של M מ"ט אזי
                               . הערה: נשתמש בסימון \langle \cdot \rangle על מנת לקודד כל אובייקט לקידוד בינארי.
                      \mathcal{R} הערה: נניח כי קידוד ופענוח הן פעולות פשוטות ובדיקת נכונות קידוד היא
     x מאותחל עם M מ"ט ותהא M מילה אזי \langle M, x \rangle הינו הקידוד הבינארי של
                                משפט מכונת טיורינג אוניברסלית: קיימת מ"ט U מעל \{0,1\} עבורה
                                                                                      .ACC \in \mathcal{RE} :טענה
                                                                                         .ACC \notin \mathcal{R} :טענה
```

```
את של M ולכל הלט M של M מתקיים (M מקבלת את את אולכל הלט M ולכל הלט M של M
את את M ולכל קלט M של M מתקיים (M דוחה את M) של M ולכל קלט M של M
```

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

לא M של M מתקיים M לא עוצרת עבור (M,x) אולכל פלט M של M לא של M

 $x \notin \operatorname{Im}(f)$  את דוחה את  $x \notin \operatorname{Im}(f)$  באשר  $x \in \{0,1\}^*$  $L \notin \mathcal{RE} \cup \mathrm{co}\mathcal{RE}$  שפה עבורה  $L \subseteq \{0,1\}^*$  שענה: קיימת  $ACC = \{\langle M, x \rangle \mid ($ מ"ט $) \wedge ($ מ"ט $) \wedge (x$  מקבלת את א $) \wedge ($ מ"ט $) \wedge ($ 

 $L\left(M
ight)=\{\langle N
angle\mid\langle N
angle
otin L\left(N
ight)\}$  עבורה  $\{0,1\}$  עבור מ"ט M מעל  $\{\langle N \rangle \mid \langle N \rangle \notin L(N)\}$  מ"ט המכריעה את ACC אזי קיימת מ"ט א המכריעה את M מ"ט המכריעה את

 $AHALT = \{ \langle M, x \rangle \mid \langle M, x \rangle \mid (M'') \rangle \land (M'') \land (x ) \land (M'') \}$  הגדרה: .HALT  $\in \mathcal{RE} \backslash \mathcal{R}$  :

> .EMPTY =  $\{\langle M \rangle \mid (a"b) \land (L(M) = \varnothing)\}$  הגדרה: .EMPTY  $\notin \mathcal{R}$  :טענה

עבורה  $f:D o (\Gamma\backslash\{\sqcup\})^*$  אזי  $D\subset \Sigma$  מיט ותהא M מ"ט ותהא פונקציה: מחשבת פונקציה:  $f\left(x
ight)$ ים מתקיים כי M עוצרת על x וכן הסרט בסוף הריצה הינו  $x\in D$  לכל

את המחשבת מ"ט M עבורה קיימת  $f:D o (\Gamma \setminus \{ \sqcup \})^*$  אזי  $D \subseteq \Sigma$  אחי השלבה: תהא

שפה  $B\subset \Delta^*$  שפה ותהא  $A\subset \Sigma^*$  תהא  $\Sigma,\Delta$  שפה אלפבייתים באשר  $\Sigma,\Delta$  $(x \in A) \Longleftrightarrow (f(x) \in B)$  מתקיים  $x \in \Sigma^*$  חשיבה עבורה לכל  $f: \Sigma^* \to \Delta^*$  אזי

שפה ותהא  $B\subset \Delta^*$  שפה תהא שפה תהא  $A\subset \Sigma^*$  שפה באשר באשר באשר  $\Sigma,\Delta$  שפה שפה ותהא  $A <_m B$  רדוקציית מיפוי אזי  $f: \Sigma^* \to \Delta^*$ 

.EMPTY  $\in \operatorname{co}\mathcal{RE}$  :

 $A \in \mathcal{R}$  אזי  $A \leq_m B$  וכן  $B \in \mathcal{R}$  שפות באשר A, B אזי אינה: תהיינה  $A \notin \mathcal{R}$  אזי  $A \leq_m B$  וכן  $A \notin \mathcal{R}$  שפות באשר A, B אזי  $A \leq_m B$ 

**הערה:** יש דבר כזה רדוקציה כללית שמכלילה את רדוקציית המיפוי. לא עברנו על זה פורמלית. מסומו

 $\{\langle M \rangle \mid \langle M \rangle \notin L(M)\} < ACC$  מסקנה:

 $ACC \leq_m HALT$  מסקנה: מסקנה: ACC < EMPTY.

 $REG = \{ \langle M \rangle \mid L(M) \}$  הגדרה: L(M)

.REG  $\notin \mathcal{R}$  :טענה

 $EQ = \{ \langle M_1, M_2 \rangle \mid L(M_1) = L(M_2) \}$  הגדרה: .EQ ∉ R :טענה

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

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

. טענה:  $\{x \in \{0,1\}^* \mid \#_0(x) = \#_1(x)\}$  אינה רגולרית. טענה:  $\{0^i 1^j \mid i > i\}$  אינה רגולרית. . אינה רגולרית  $\{a^p \mid a \in \Sigma, \, \text{ראשוני} \, p\}$ טענה: השפה  $\{a^ib^nc^n\mid n\in\mathbb{N},i\in\mathbb{N}_+\}\cup\{b^nc^n\mid n,m\in\mathbb{N}\}$  ניתנת לניפוח 1 וכן אינה

הגדרה: תהא  $L \subseteq \Sigma^*$  שפה אזי

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

 $x\sim_{L(A)}y$  אזי $x\sim_Ay$  עבורם  $x,y\in\Sigma^*$  אזי  $x\sim_Ay$ 

 $\hat{A}_A\left(q_0,y
ight)= ext{Class}\left(y
ight)$  אזי  $y\in\Sigma^*$  ויהי L אס"ד המחלקות של A

עבורו |Q|=n אזי קיים אסל"ד N מעל [n] באשר  $n\in\mathbb{N}_+$  עבורו יהי

 $|Q| \ge 2^n$  אזי  $L(A) = \{x \in [n]^* \mid \exists \sigma \in \Sigma . \#_{\sigma}(x) = 0\}$ 

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

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

 $.\Gamma$  אייט איי ( $Q,\Sigma,\Gamma,\delta,q_0,q_a,q_r$ ) אלפבית סרט במכונת טיורינג: תהא

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

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

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

c עם cע מ"ט ותהא קונפיגורציה אזי נזהה את מ"ט ותהא M

c' = uq'ab'v וכן  $\delta(q, b) = (q', b', L)$ 

c' = q'b'v וכן  $\delta(q, b) = (q', b', L)$ 

c' = ub'q'v וכן  $\delta(q,b) = (q',b',R)$ 

וכן c=uaqbv עבורם  $q,q'\in Q$  וקיימים  $u,v\in\Gamma^*$  וקיימים  $a,b,b'\in\Gamma$  פיימים

וכן c=qbv עבורם  $q,q'\in Q$  וקיימים  $u,v\in \Gamma^*$  וקיימים  $b,b'\in \Gamma$  סיימים •

וכן c=uqbv עבורם  $q,q'\in Q$  וקיימים  $u,v\in \Gamma^*$  וקיימים  $b,b'\in \Gamma$  סיימים •

מכונת טיוריגג מקבלת מילה: תהא M מ"ט אזי  $x \in \Sigma^*$  עבורו קיימים  $c_0 \dots c_n$  קונפיגורציות

. באשר  $c_n$  וכן  $c_n$  וכן  $c_{i-1}$  עוברת ל־ $c_i$  לכל  $i \in [n]$  לכל לכל עוברת באשר מקבלת.

ותהא  $q_a \neq q_r$  באשר  $q_0, q_a, q_r \in Q$  ותהא וכן  $\Gamma \setminus \Sigma$  וכן

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

מסקנה: תהא  $\Sigma^*/_{\sim L}$  שפה רגולרית אזי  $L\subset \Sigma^*$  סופית.

.Class (y)=i אזי  $y\sim_L x_i$  עבורו  $y\in\Sigma^*$  ויהי

 $Q = \left[ \left| \Sigma^* /_{\sim_I} \right| \right] \bullet$ 

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

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

 $F = \{i \in Q \mid x_i \in L\}$  •

 $L(N) = \{x \in [n]^* \mid \exists \sigma \in \Sigma . \#_{\sigma}(x) = 0\}$ 

עבורו [n] עבורו אס"ד מעל  $n\in\mathbb{N}_+$  יהי טענה: יהי

 $c\in\Gamma^*Q\Gamma^*$  מ"ט אזי M מהא M

 $.c = uq_a v$  המקיימים

 $c = u q_r v$  המקיימים

. שפה אזי יחס שקילות שפילות אוי  $\sim_L \subseteq \Sigma^*$  עענה: תהא

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

**טענה**: מכונת טיורינג ומכונת טיורינג לא־דטרמיניסטית הינו מודלים שקולים.

שפות כריעות למחצה/שפות ניתנות למניה רקורסיבית/שפות ניתנות לקבלה: יהי  $\Sigma$  אלפבית אזי  $\mathcal{RE} = \{ \mathcal{L} \subseteq \Sigma^* \mid \mathcal{L} = L(M) \text{ עבורה } M \text{ עבורה} \}$ 

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

שפות כריעות/שפות רקורסיביות: יהי  $\Sigma$  אלפבית אזי

```
.CCNF \in \mathcal{NPC} :טענה
                                                                                                                                                                                 .HAMPATH = \{\langle G,s,t\rangle\mid tל מ־לטוני מ־sל מסלול מסלול מסלון עם מסלול מרץ מ־לטוני מ־לטוני מ־א מכוון עם מסלול מסלול מייני מיינ
                                                                                                                                                                                                                                                                                                                                                                                       טענה: תהיינה A <_m B שפות באשר A, B אזי
                                                           .DNFCNF = \{\langle \varphi \rangle \mid (\varphi \in \text{DNF}) \land (\varphi \in \varphi)\} הגדרה:
                                                                                                                                                                                                                                                                  .HAMPATH \in \mathcal{NP} :טענה
                                                                                                                                                                                                                                                                                                                                                                                                      A \in \mathcal{RE} אזי B \in \mathcal{RE} אם
                                                                                                                  .DNFCNF \in \mathcal{P} :טענה
                                                                                                                                                                                                                                           השערה: HAMPATH ∉ P. השערה פתוחה
                                                                                                                                                                                                                                                                                                                                                                                               A\in \mathrm{co}\mathcal{RE} אזי B\in \mathrm{co}\mathcal{RE} .
מתקיים \{u,v\} \in E מכל עבורה לכל עבורה אז מכוון אזי C \subseteq V מתקיים יהי יהי יהי
                                                                                                                                                                                                                                  \mathcal{E}\mathcal{X}\mathcal{P} = igcup_{k\in\mathbb{N}} DTime \left(2^{n^k}\right):\mathcal{E}\mathcal{X}\mathcal{P} שפה
                                                                                                                                                                                                                                                                                                                                                                                                      \overline{ACC} <_m EQ וכן ACC <_m EQ טענה:
                                                                                                               (u \in C) \lor (v \in C)
                                                                                                                                                                                                                                                                                                                                                                                                                    .EQ \notin \mathcal{RE} \cup co\mathcal{RE} מסקנה:
                                                                                                                                                                                                                         \mathcal{NEXP} = \bigcup_{k \in \mathbb{N}} \mathsf{NTime}\left(2^{n^k}\right) : \mathcal{NEXP} שפה
                                                                                                                                                                                                                                                                                                                                                                                     \mathcal{C} \subseteq \mathcal{P}\left(\Sigma^*\right) אלפבית אזי יהי \Sigma אלפבית יהי
                                  \mathrm{NC} = \{\langle G, k \rangle \mid k גרף גרף לא מכוון בעל כיסוי קודקודים מגודל G\} גרף גרף לא
                                                                                                                                                                                                                                                                 \mathcal{E} \hat{\mathcal{X}} \mathcal{P} \subset \mathcal{N} \mathcal{E} \mathcal{X} \mathcal{P} טענה:
                                                                                                                                                                                                                                                                                                                                                           L_{\mathcal{C}} = \{\langle M \rangle \mid L(M) \in \mathcal{C}\} הגדרה: תהא \mathcal{C} תכונה סמנטית אזי
                                                                                                                   .VC \in \mathcal{NPC} :טענה
                                                                                                                                                                                                                                       \mathcal{P}\subseteq\mathcal{NP}\subseteq\mathcal{EXP}\subseteq\mathcal{NEXP} :מסקנה
                                                    \mathcal{B}\subseteq igcup_{n=1}^\infty \left(\Sigma^n	o\Sigma
ight) אלפבית אזי יהי אלפבית היי פונקציות: יהי
                                                                                                                                                                                                                                                                                                                                             L_{\mathcal{C}} 
otin \mathcal{R} משפט רייס: תהא \mathcal{C} \in \mathcal{P}\left(\mathcal{R}\mathcal{E}\right) \setminus \{\mathcal{R}\mathcal{E},\varnothing\} משפט רייס: תהא
                                                                                                                                                                                                                                                                           \mathcal{P} \subseteq \mathcal{EXP} :טענה
תהיינה k_1 \dots k_n \in \mathbb{N}_+ תהיינה בסיס פונקציות מעל בסיס היינה \Sigma אלפבית היי אלפבית היינה מעגל:
                                                                                                                                                                                                                                                                                                                                                                                               L_{\mathcal{C}} \in \mathcal{R} אזי \mathcal{C} \in \{\mathcal{RE}, \varnothing\} טענה: תהא
                                                                                                                                                                                                                                                                   \mathcal{NP} \subseteq \mathcal{NEXP} טענה:
x_1\dots x_m,y_1\dots y_k\in \Sigma ותהיינה i\in [n] לכל f_i:\Sigma^{k_i}	o \Sigma באשר באשר f_1\dots f_n\in \mathcal{B}
                                                                                                                                                                                                                                                                                                                                                                                                         .PRIME = \{(p)_2 \mid p \in \mathbb{P}\} הגדרה:
                                                                                                                                                                                                    M על M מ"ט ויהי X \in \Sigma^* אזי M הינו ריצת M על M
                                               המקיים \{f_1 \dots f_n, x_1 \dots x_m, y_1 \dots y_k\} המקיים גרף מכוון G
                                                                                                                                                                                                                                                                                                                                                                                               .2 הערה: קידוד מספרים תמיד יעשה בבסיס
                                                                                                                                                                               מוודא לשפה: תהא \Sigma \cup \{","\} שפה אזי מ"ט V מעל אלפבית שפה \mathcal{L} \subseteq \Sigma^* המקיים
                                                                                                .חסר מעגלים מכוונים G
                                                                                                                                                                                                                                                                                                                                                                                     .EQPRIME = \{\langle M \rangle \mid L(M) = PRIME\} :הגדרה:
                                                                                                                                                                                          . מקבלת V\left(x,w\right) עבורו w\in\Sigma^{*} אזי קיים x\in\mathcal{L} מקבלת.
                                                                       \deg^-(x_i) = 0 מתקיים i \in [m] לכל
                                                                                                                                                                                                                                                                                                                                                                                                                               .EOPRIME \notin \mathcal{R} :
                                                                                                                                                                                      . דוחה V\left(x,w
ight) מתקיים כי w\in\Sigma^{*} אזי לכל x
otin\mathcal{L} אזי היי
                                                                       \deg^-(f_i) = k_i מתקיים i \in [n] לכל •
                                                                                                                                                                                                                                                                                                                           L_{\mathcal{C}}\notin\mathrm{co}\mathcal{RE} אוי \mathcal{C}\in\mathcal{P}\left(\mathcal{RE}ackslash\{\varnothing\}
ight)ackslash\left\{\varnothing\right\} אוי אוי הרחבה ראשונה: תהא
                                                                                                                                                                                                    \mathcal{L} \subset \Sigma^* עענה: תהא \mathcal{L} \subset \Sigma^* שפה אזי שפה אזי \mathcal{L} \subset \Sigma^*
                                        \operatorname{deg}^+(y_i) = 0 וכן \operatorname{deg}^-(y_i) = 1 מתקיים i \in [k] •
                                                                                                                                                                                                                                                                                                                   L_{\mathcal{C}}\notin\mathcal{RE} אזי \varnothing\in\mathcal{C} באשר \mathcal{C}\in\mathcal{P}\left(\mathcal{RE}
ight)\setminus\left\{\mathcal{RE}\right\} אוי תהא פענה משפט רייס הרחבה שנייה: תהא
                                                                                                                                                        מדווא פולינומי לשפה: תהא p\in\mathbb{N}\left[x
ight] שפה אזי מוודא V ל־U עבורו קיים ב\Sigma^* המקיים כי
                                                     הערה: נשמור על הטרמינולוגיה ממעגל בוליאני כהכללה טבעית.
                                                                                                                                                                                                                                                                                                                                                                                                                                 .REG \notin \mathcal{RE} מסקנה:
                                                                                                                                                                                 לכל p\left(|x|
ight) אחרי לכל היותר אחרי V\left(x,w
ight) צעדים. לכל x,w\in\Sigma^*
M תהא n \leq T\left(n
ight) באשר בימן חשיבה חשיבה תהא תהא תהא תהא תהא מטריצת הקונפיגורציות/טאבלו:
                                                                                                                                                                                                                                                                                                                                                                                                 ALL = \{\langle M \rangle \mid L(M) = \Sigma^* \} :הגדרה
                                                                                                                                                                                                .CLIQUE = \{\langle G, k \rangle \mid k מכוון בעל קליקה מגודל לא מכוון בעל מכוון הגדרה: G\}
אזי M\left(z\right) אזי הריצה הריצה קונפיגורציות ותהיינה z\in\left\{ 0,1\right\} ^{n} יהי T\left(n\right) אזי שרצה בזמן
                                                                                                                                                                                                                                                                                                                                                                                                                                \overline{HALT} \leq_m ALL למה:
                                                                                                                                                                                                                                                .CLIQUE: סענה: קיים מוודא פולינומי ל
                                                      R_i(\tau_{M,z}) = c_i המקיימת \tau_{M,z} \in M_{T(n)+1}(\Sigma \uplus \Gamma)
                                                                                                                                                                                                                                                                                                                                                                                                                     .ALL \notin \mathcal{RE} \cup co\mathcal{RE}: טענה
                                                                                                                                                                                                .IS = \{\langle G, k \rangle \mid k מגודל מגודל בעל קבוצה בעל מכוון בעל מכוון גרף לא מכוון בעל הדרה:
 \delta\left(q_{r},\sigma\right)=\left(q_{r},\sigma,R\right) וכן \delta\left(q_{a},\sigma\right)=\left(q_{a},\sigma,R\right) כי נניח נניח נניח כי \delta\left(q_{a},\sigma\right)=\left(q_{a},\sigma,R\right)
                                                                                                                                                                                                                                                                                                              ולכל n\in\mathbb{N} עבורה לכל T:\mathbb{N}	o\mathbb{N} מ"ט אזי מ"ט איז מכונת טיורינג: תהא ולכל חסם עליון לזמן ריצה של מכונת טיורינג:
                                                                                                                                                                                                                                                         שענה: קיים מוודא פולינומי ל־IS.
       .CIRSAT = \{\langle C, x \rangle \mid ( מעגל בוליאני C) \wedge (\exists w \in \{0, 1\}^* (C(x, w) = 1))\} הגדרה:
                                                                                                                                                                                                                                                                                                                                                       צעדים. צעדים כי M על הקלט x מבצעת לכל היותר x \in \Sigma^n
                                                                                                                                                                                                                         .FACTOR =\{\langle N,k\rangle\mid\exists d\in[k]\,.\,(d|N)\} הגדרה:
נגדיר T\left(n
ight) מיט רצה בזמן מיט מיט רצה בזמן באשר אנדיר T:\mathbb{N} 	o \mathbb{N} מייט רצה בזמן הגדרה: תהא
                                                                                                                                                                                                                                                                                                                .DTime (T(n))=\{L(M)\mid \mathcal{O}(T(n)) מ"ט שרצה בזמן M\} אזי T:\mathbb{N}	o\mathbb{N} הגדרה: תהא
                                                                                                                                                                                                                                                טענה: קיים מוודא פולינומי ל־FACTOR.
                                                                                                               מעגלים מעל \Gamma \uplus \Sigma כך
                                                                                                                                                                                                                                                                                                                                                                                                \left\{0^{k}1^{k}\mid k\geq0\right\}\in \mathrm{DTime}\left(n^{2}\right) טענה:
                                                                                                                                                                                   .SUBSETSUM = \{\langle S,k \rangle \mid (S \subseteq \mathbb{N}) \land (\exists T \subseteq S. \sum_{i \in T} i = t)\} הגדרה:
                                                             .C_{	ext{inp}}\left(z
ight)=R_{0}\left(	au_{M,z}
ight) אזי z\in\Sigma\uplus\Gamma יהי
                                                                                                                                                                                                                                         .SUBSETSUM: סענה: קיים מוודא פולינומי
                                                                                                                                                                                                                                                                                                                                                                                   \left\{0^{k}1^{k}\mid k\geq0\right\}\in \mathrm{DTime}\left(n\log\left(n\right)\right) מסקנה:
                                                    אזי i \in \{0, \ldots, T(n) - 1\} ויהי z \in \Sigma \uplus \Gamma יהי •
                                                                                                                                                                                                                                                                                                                                        משפט: תהא L \in \text{DTime}(t(n)) ותהא ותהא t(n) = o(n \log(n)) אזי איז רגולרית.
                                                                                                                                                                                     (\mathcal{L} \in \mathcal{NP}) שפה אזי שפה (\mathcal{L} \in \mathcal{NP}) שפה אזי פולינומי שפט: תהא
                                                                        .C_{\text{next}}\left(R_i\left(\tau_{M,z}\right)\right) = R_{i+1}\left(\tau_{M,z}\right)
                                                                                                                                                                                                                                                                                                                                      \left\{0^k1^k\mid k\geq 0
ight\}
otin \operatorname{DTime}\left(t\left(n
ight)
ight) אזי t\left(n
ight)=o\left(n\log\left(n
ight)
ight) מסקנה: תהא
                                                                                                                                                                                                                            .CLIQUE, IS, FACTOR, SUBSETSUM \in \mathcal{NP} :מסקנה
                                              .C_{	ext{out}}\left(R_{T(n)}\left(	au_{M,z}
ight)
ight)=M\left(z
ight) אזי z\in\Sigma\uplus\Gamma יהי \bullet
                                                                                                                                                                                                                                                    השערה: \mathcal{P} \neq \mathcal{NP} השערה פתוחה
                                                                                                                                                                                                                                                                                                               M כי n\in\mathbb{N} המקיימת לכל n\in\mathbb{N} כי n\in\mathbb{N} בי מונקציה חשיבה בזמן: פונקציה n\in\mathbb{N} עבורה קיימת מ"ט
               .C_{M,n}^{\Sigma \uplus \Gamma}(z) = (C_{	ext{out}} \circ C_{	ext{next}} \circ \ldots \circ C_{	ext{next}} \circ C_{	ext{inp}})(z) אזי z \in \Sigma \uplus \Gamma יהי
                                                                                                                                                        M עבורה קיימת מ"ט f:D	o (\Gamma\backslash\{\sqcup\})^* אזי D\subset\Sigma עבורה קיימת מ"ט
                                                                                                                                                                                                                                                                                                                                                                              \mathcal{O}\left(T\left(n\right)\right) בזמן \left(T\left(n\right)\right)_{2} את מחשבת 1^{n} בזמן
טענה: תהא M מ"ט רצה בזמן באשר T:\mathbb{N} 	o \mathbb{N} ותהא א מענה: תהא א סענה: חשיבה בזמן באשר א חשיבה בזמן א מ
                                                                                                                                                       עוצרת לכל M\left(x\right) א מתקיים כי x\in\Sigma^{*} המקיים כי המקיים לכל p\in\mathbb{N}\left[x\right] עוצרת לכל
                                                                                                                                                                                                                                                                                                                                                T\left(n
ight)=\Omega\left(n
ight) אינה קבועה אזי חשיבה T:\mathbb{N}	o\mathbb{N} חשיבה טענה: תהא
עבורה poly (T\left(n
ight)) אזי אזי \left|C_{M,n}^{\Sigma \uplus \Gamma}
ight| = \mathcal{O}\left(T^{2}\left(n
ight)
ight) וכן קיימת פונקציה T\left(n
ight)
                                                                                                                                                                                                                                                               היותר אחרי p(|x|) צעדים.
                                                                                                                                                                                                                                                                                                              עבורם לכל C \in \mathbb{R} משפט מכונת טיורינג אוניברסלית עם טיימר: קיימת מ"ט אוניברסלית וקיים עם עבורם לכל
                                                                                                              f(1^n) = \langle C_{M,n}^{\Sigma \uplus \Gamma} \rangle
                                                                                                                                                        רדוקציית מיפוי פולינומית: יהיו \Delta,\Delta אלפבייתים באשר באשר באר בא שפה ותהא רדוקציית מיפוי פולינומית: יהיו
                                                                                                                                                                                                                                                                                                               עוצרת על הקלט עוצרת מתקיים מתקיים לאחר tלאחר על הקלט עוצרת על באשר א ולכל Mעוצרת לאחר מ"ט M
T\left(n
ight) ויהי מסקנה: תהא M מ"ט רצה בזמן באשר T:\mathbb{N}	o\mathbb{N} מ"ט רצה בזמן ויהי T
                                                                                                                                                                                                    . שפה אזי רדוקציית מיפוי A מ־A ל־B חשיבה פולינומית B\subset \Delta^*
                                                                                                                                                                                                                                                                                                                                                                                                                         עדים. C \cdot t תוד \langle M, x \rangle
                                                                                    .C_{M,n}^{\Sigma \uplus \Gamma}(z) = M(z) אזי z \in \Sigma \uplus \Gamma
                                                                                                                                                        שפה ותהא B\subset \Delta^* שפה תהא A\subset \Sigma^* תהא תהא באשר באשר באשר אלפבייתים באשר שפה תהא אלפבייתים באשר באשר באשר א
                                                                                                                                                                                                                                                                                                               t\in\mathbb{N} אוניברסלית U וקיים M לכל מ"ט M לכל מ"ט U וקיים U וקיים וועכ U אוניברסלית אוניברסלית ווקיים
טענה: יהי \Pi אלפבית אזי קיימת פונקציה חשיבה פולינומית f עבורה לכל מעגל בוליאני \Omega מתקיים
                                                                                                                                                                                                                  A <_n B רדוקציית מיפוי פולינומית אזי f: \Sigma^* 	o \Delta^*
וכן z \in \{0,1\}^n לכל C(z) = f(C)(z) באשר בסיס דה־מורגן באל בוליאני מעל בוליאני מעל ב
                                                                                                                                                                                                                                                                        .CLIQUE \leq_p IS :טענה
                                                                                                                                                                                                                                                                                                                     \langle M, x, t \rangle אם U מקבלת אזי אזי לאחר לכל היותר א לאחר לכל הקלט אוצרת על הקלט M
                                                                                                                 |f(C)| = \mathcal{O}(|C|)
                                                                                                                                                                                                A \in \mathcal{P} אזי A <_n B וכן B \in \mathcal{P} שפות באשר A, B אזי טענה: תהיינה
                                                                                                                                                                                                                                                                                                                              \langle M, x, t \rangle אם M דוחה את או לא עוצרת לאחר t צעדים אזי או או t או את t
למה: תהא M מ"ט רצה בזמן באשר n < T (n) חשיבה בזמן חשיבה T : \mathbb{N} \to \mathbb{N} תהא
                                                                                                                                                                                                            \mathcal{NPH}=\{\mathcal{L}\mid orall L\in \mathcal{NP}\,(L\leq_{p}\mathcal{L})\} שפה \mathcal{NPH}=\{\mathcal{L}\mid orall L\in \mathcal{NP}\,(L\leq_{p}\mathcal{L})\}
                                                                                                                                                                                                                                                                                                                                                                                          צעדים. C \cdot t \log (t) צעדים U ullet
                                                                                                                                                                                                                                                                                                              משפט היררכיית הזמן: תהא T:\mathbb{N}	o\mathbb{N} חשיבה בזמן ותהא t(n)=o\left(rac{T(n)}{\log(T(n))}
ight) אזי
באשר f\left(1^{n}\right)=\langle C_{M,n}\rangle באשר poly \left(T\left(n\right)\right) באשר חשיבה פונקציה f חשיבה בזמן דעורה רT\left(n\right)
                                                                                                                                                                                                                                    \mathcal{NPC} = \mathcal{NP} \cap \mathcal{NPH} :שפה \mathcal{NP}
M\left(z
ight) מתקיים z \in \{0,1\}^n וכן לכל \left|C_{M,n}
ight| = \mathcal{O}\left(T^2\left(n
ight)
ight) מעגל עבורו C_{M,n}
                                                                                                                                                                                                             (\mathcal{P} = \mathcal{NP}) \Longleftrightarrow (\mathcal{L} \in \mathcal{P}) אזי \mathcal{L} \in \mathcal{NPC} טענה: תהא
                                                                                                                                                                                                                                                                                                                                                                                                             .DTime (t(n)) \subseteq DTime(T(n))
                                                                                                 (C_{M,n}(z)=1) \iffמקבלת).
                                                                                                                                                        ACC_{\mathcal{NP}} = \{\langle M, x, 1^t \rangle \mid בעדים t צעדים אחרי מקבלת אחרי מקבלת M(x, w) בורו w
                                                                                                                                                                                                                                                                                                                                                                      DTime (n^c) \subseteq DTime (n^d) אזי 1 < c < d מסקנה: יהיו
                                                                                                            .CIRSAT \in \mathcal{NPC} :טענה
                                                                                                                                                                                                                                                                                                               T\left(n
ight) אזי דיסרטית שרצה בזמן T\left(n
ight)>n אזי דאשר דיסרטית אזי T\left(n
ight)>n אזי דאשר דיסרטית אזי דיסרטית אזי
                                                                                                                                                                                                                                                                  ACC_{\mathcal{NP}} \in \mathcal{NPC} טענה:
f:\{0,1\}^* 	o \{0,1\} ותהא n < T(n) מסקנה: תהא T:\mathbb{N} 	o \mathbb{N} חשיבה בזמן באשר
                                                                                                                                                                     A,B\in\mathcal{NPC} אזי A\leq_{p}B וכן A\in\mathcal{NPC} שפות באשר A,B\in\mathcal{NP} אזי טענה: תהיינה
                                                                                                                                                                                                                                                                                                                                                    L\left(M\right)=L\left(M'\right) עבורה \mathcal{O}\left(T^{2}\left(n\right)\right) שרצה בזמן M' שרצה מ"ט M'
ניתנת לחישוב על ידי משפחת מעגלים מגודל f אזי f לא ניתנת לחישוב על ידי מ"ט בזמן ניתנת לחישוב על ידי מ
                                                                                                                                                                                                 C\left(x\right)=1 המקיים x\in\{0,1\}^{n} מעגל ספיק: מעגל מעגל עבורו קיים
                                                                                                                                                                                                                                                                                                               טענה: תהא T\left(n
ight) > T באשר אז היימת RAM מודל T\left(n
ight) > T באשר דימו היימת T:\mathbb{N} 
ightarrow \mathbb{N}
                                                                                                                                  \sqrt{T(n)}
                                                                                                                                                        A\in M_{m	imes k}\left(\{p_i\}\cup\{\lnot p_i\}
ight) וקיימת m\in\mathbb{N} עבורה קיים arphi\in \mathrm{CNF} פסוק: k\mathrm{CNF}
                                                                                                                                                                                                                                                                                                                                                               L\left(M\right)=L\left(M'\right) עבורה \mathcal{O}\left(T^{3}\left(n\right)\right) שרצה בזמן M'
                                                                                                           .CIRSAT <_p 3SAT :טענה
                                                                                                                                                                                                                                               \varphi = \bigwedge_{i=1}^{m} \bigvee_{i=1}^{k} (A)_{i,k} המקיימת
                                                                                                                                                                                                                                                                                                              עבורה T:\mathbb{N} 	o \mathbb{N} אזי אזי מטל"ד אזי תהא N עבורה איזי איזי עבונת טיורינג אר־דטרמיניסטית: תהא
                                                                                                    .3SAT \leq_p SUBSETSUM :טענה
                                                                                                                                                                                          .kSAT = \{\langle \varphi \rangle \mid (\varphi \in kCNF) \land (ספיקה) \} אזי k \in \mathbb{N}_+ יהי יהי הגדרה: יהי
                                                                                                                                                                                                                                                                                                                                                   T\left(n
ight) לכל n\in\mathbb{N} בעומק לכל היותר x\in\Sigma^{n} ולכל תלכל היותר
                                                                                                  .SUBSETSUM \in \mathcal{NPC} :מסקנה
                                                                                                                                                                                                                                              .kSAT \in \mathcal{NP} אזי k \in \mathbb{N}_+ טענה: יהי
                                                                                                                                                                                                                                                                                                                                                                                                                   אזי T:\mathbb{N} \to \mathbb{N} אזי תהא
                                                                                                       .3SAT \leq_p HAMPATH :טענה
                                                                                                                                                                                                                                                                              .2SAT \in \mathcal{P} :טענה
                                                                                                                                                                                                                                                                                                                                                         .NTime (T(n)) = \{L(N) \mid \mathcal{O}(T(n)) מטל"ד שרצה בזמן N\}
                                                                                                      .HAMPATH \in \mathcal{NPC} מסקנה:
                                                                                                                                                                                                                                                        .3SAT \in \mathcal{NPC} :משפט קוק־לוין
                                                                                                                                                                                                                                                                                                              טענה: תהא T\left(n
ight) אזי קיימת מ"ט ותהא T\left(n
ight)\geq n אזי קיימת מ"ט די תהא תהא תהא T:\mathbb{N} 
ightarrow \mathbb{N}
                                                                                                                                                                                                                                                                                                                                                                              L\left(N\right)=L\left(M\right) עבורה 2^{\mathcal{O}\left(T\left(n\right)\right)} שרצה בזמן M
                                                                              .co\mathcal{NP}=\left\{L\mid\overline{L}\in\mathcal{NP}
ight\} :co\mathcal{NP} שפה
                                                                                                                                                                                                                 kSAT <_p \ellSAT אזי k < \ell באשר k, \ell \in \mathbb{N}_+ טענה: יהיו
                                                                                    השערה: מתוחה co\mathcal{NP} 
eq \mathcal{NP} השערה פתוחה
                                                                                                                                                                                                                         .kSAT \in \mathcal{NPC} אזי k \in \mathbb{N} \setminus \{0,1,2\} מסקנה: יהי
                                                                                                                                                                                                                                                                                                                                                                                                           \mathcal{P} = \bigcup_{c \in \mathbb{N}} \mathsf{DTime}\left(n^c\right) : \mathcal{P} שפה
                                                                         טענה: תהיינה A \leq_p B שפות באשר A, B אזי
                                                                                                                                                                                                                                                                 .3SAT \leq_p CLIQUE משפט:
                                                                                                                                                                                                                                                                                                                                                             .PATH =\{\langle G,s,t
angle\mid tל מ־s לים מסלול מכוון עם מכוון גרף מכוון G\}
                                                                                    A\in\mathcal{NP} אזי B\in\mathcal{NP} אם
                                                                                                                                                                                                                                                            .CLIQUE, IS \in \mathcal{NPC} מסקנה:
                                                                                                                                                                                                                                                                                                                                                                                                                                    .PATH \in \mathcal{P} :טענה
```

.PRIME  $\in \mathcal{P}$  משפט:

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

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

.HALT  $<_m$  HALT  $_\varepsilon$  טענה:

 $A \leq_m B$  אזי  $B \in \mathcal{P}\left(\Sigma^*\right) \setminus \{\Sigma^*,\varnothing\}$  ותהא  $A \in \mathcal{R}$  אזי

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

v ותהא A  $\in M_{m imes k}\left(\{p_i\}\cup\{\lnot p_i\}
ight)$  השמה אזי

 $N\left(igwedge_{i=1}^{m}igee_{j=1}^{k}(A)_{i,k}\,,v
ight) = \left|\left\{i\in[m]\ \middle|\ \overline{v}\left(igee_{j=1}^{k}(A)_{i,k}
ight) = \operatorname{True}
ight\}
ight|$  .  $C\operatorname{CNF} = \left\{\left\langle arphi,k 
ight
angle\ |\ (arphi\in\operatorname{CNF}) \wedge (\exists v\left(N\left(arphi,v
ight) = k
ight)
ight\}$ 

 $A \in co\mathcal{NP}$  אזי  $B \in co\mathcal{NP}$  •

 $(co\mathcal{NP} = \mathcal{NP}) \iff (\mathcal{L} \in co\mathcal{NP})$  אזי  $\mathcal{L} \in \mathcal{NPC}$  מסקנה: תהא  $\mathcal{P} \subseteq \mathcal{NP} \cap \mathrm{co}\mathcal{NP}$  :טענה

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

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

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

.MATMULT =  $\{\langle A, B, C \rangle \mid (A, B, C \in M_n(\mathbb{Z})) \land (A \cdot B = C)\}$  :הגדרה:  $\mathbb{P}_{r\leftarrow\{0,1\}^n}\left(D\cdot r=0
ight)\leq 0.5$  אזי D
eq 0 באשר באשר  $D\in M_n\left(\mathbb{Z}
ight)$  טענה: תהא מסקנה: קיימת מ"ט M אשר רצה בזמן  $\mathcal{O}\left(n^2\right)$  עבורה

- . דוחה  $M\left(x\right)$  אשר אינו קידוד של שלשת מטריצות  $x\in\left\{ 0,1\right\} ^{*}$
- וכן  $A\cdot B=C$  המקיימות  $A,B,C\in M_n\left(\mathbb{Z}\right)$  עבורו קיימות  $x\in\{0,1\}^*$ מקבלת. מתקיים M(x) מקבלת.  $x = \langle A, B, C \rangle$
- וכן  $A\cdot B \neq C$  המקיימות  $A,B,C\in M_n\left(\mathbb{Z}\right)$  עבורו קיימות  $x\in\{0,1\}^*$  וכן  $\mathbb{P}\left(\mathbf{M}\left(\mathbf{x}\right)\right) < 2^{-100}$  מקבלת  $\mathbf{X} = \langle A, B, C \rangle$

Cנוסחה אריתמטית: יהי  $\mathbb{F}$  שדה ויהי C מעגל מעל  $\mathbb{F}$  עם הבסיס  $\{+, \times\}$  אזי נוסחה ב־  $\varphi\left(x_1\dots x_n\right)=0$  מתקיים  $x_1\dots x_n\in\mathbb{F}$  עבורה לכל

> $\mathsf{ZE}_{\mathbb{F}} = \{\langle \varphi \rangle \mid \varphi \equiv 0 \text{ עבורה } \mathbb{F}$  עבורה אריתמטית אריתמטית מעל  $\overline{ZE_{\mathbb{Z}_2}}\in\mathcal{NPC}$  :טענה

 $2^h$  אזי arphi מעל  $\mathbb F$  אזי arphi מוסחה אריתמטית בעומק h מעל  $\mathbb F$  אזי arphi מחשבת פולינום מדרגה לכל היותר  $\deg\left(f
ight)<|\mathbb{F}|$  באשר  $f\in\mathbb{F}\left[x_{1},\ldots,x_{n}
ight]$  המחשבת מעל  $\mathbb{F}$  באשר אריתמטית מעל  $(\varphi = 0) \iff (f = 0)$  אא

 $ZE_{\mathbb{F}} \in \mathcal{R}$  אינסופי אזי  $\mathbb{F}$  שדה שלכנה: יהי

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

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

- . דוחה  $M\left(x\right)$  מתקיים מעל אינו קידוד של נוסחה אריתמטית מעל  $M\left(x
  ight)$  מתקיים מעל אם וכן  $arphi\equiv 0$  וכן מקיימת מעל אריתמטית הריתמטית מעל • אם איימת arphi מחקיים יום יום אריתמטית מעל
- .poly ( $|\varphi|$ ) מקבלת בזמן
- מתקיים  $x=\langle \varphi \rangle$  מוכו  $\varphi \not\equiv 0$  המקיים מעל  $x=\langle \varphi \rangle$  מרקיים  $\varphi \not\equiv 0$  מתקיים .poly ( $|\varphi|$ ) בזמן  $\mathbb{P}\left( \text{ מקבלת} \right) M\left( x \right) \right) \leq 0.01$

תחלתית עם קונפיגורציה התחלתית מ"ט דו־סרטית תהא חשיבה חשיבה  $T\left(n\right)$  תהא מכונת אקראית: מכונת מיורינג אקראית:  $.r \in \{0,1\}^{T(|x|)}$  באשר x\$r

אקראית מכונת טיורינג אקראית: תהא  $T\left(n
ight)$  חשיבה בזמן ותהא מכונת טיורינג אקראית: אקראית

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

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

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

סימון: תהא M משתנה מקרי לקבלת  $T\left(n\right)$  יהי זמן ריצה מקרי מקרי לקבלת משתנה מהיט אקראית עם מון יהי  $T\left(n\right)$ עבור  $r \in \{0,1\}^{T(|x|)}$  אקראית. M(x;r)

עם אמן ריצה פולינומי מ"ט אקראית M עם אפר עבורה פולינומי שפה  $\mathcal{L}$  ותהא שפה  $\alpha:\mathbb{N} \to [0,1]$  הגדרה: תהא מתקיים  $n \in \mathbb{N}$  ממקום מסויים מחקיימת כי החל המקיימת  $T\left(n\right)$ 

- .  $\mathbb{P}_{r\leftarrow\{0,1\}^{T(n)}}$  (מקבלת  $M\left(x;r
  ight)\geq lpha\left(n
  ight)$  מתקיים  $x\in\mathcal{L}\cap\Sigma^{n}$  לכל  $\mathbb{P}_{r\leftarrow\{0,1\}^{T(n)}}$  (מקבלת) מקבלת  $M\left(x;r
  ight)=0$  מתקיים  $\mathcal{L} \in \mathcal{RP}(\alpha)$  אזי
- $\mathcal{RP}(\beta) \subseteq \mathcal{RP}(\alpha)$  אזי מסויים מסויים  $\alpha < \beta$  באשר  $\alpha, \beta : \mathbb{N} \to [0,1]$  טענה: תהיינה  $\mathcal{RP}(1) = \mathcal{P}$  :טענה

 $\mathcal{RP}\left(lpha
ight)\subset\mathcal{NP}$  אזי מסויים מסויים 0<lpha באשר  $lpha:\mathbb{N} o [0,1]$  עענה: תהא  $\mathrm{co}\mathcal{RP}\left(lpha
ight)=\left\{\overline{L}\mid L\in\mathcal{RP}\left(lpha
ight)
ight\}$  אזי  $lpha:\mathbb{N}
ightarrow\left[0,1
ight]$  הגדרה: תהא M אם"ם קיימת מ"ט אקראית  $\mathcal{L} \in \mathrm{co}\mathcal{RP}\left(lpha
ight)$  אזי שפה lpha אזי  $lpha:\mathbb{N} 
ightarrow [0,1]$  אם lphaעם זמו ריצה פולינומי  $T\left(n
ight)$  המקיימת כי החל ממקום מסויים  $n\in\mathbb{N}$  מתקיים

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

.ZE $_{\mathbb{R}}\in\mathrm{co}\mathcal{RP}\left(0.99
ight)$  :טענה  $\mathcal{RP}\left(n^{-c}
ight)=\mathcal{RP}\left(1-2^{-n^d}
ight)$  איז  $c,d\in\mathbb{N}$  איז  $c,d\in\mathbb{N}$  סענה: סימון:  $\mathcal{RP}=\mathcal{RP}\left(0.5\right)$ 

 $co\mathcal{RP} = co\mathcal{RP} (0.5)$  : סימוו

עם זמן ריצה M עם אקראית מ"ט עבורה  $\mathcal{L}$  עבורה שפה  $lpha, eta: \mathbb{N} o [0,1]$  אהיינה הגדרה: תהיינה פולינומי  $n \in \mathbb{N}$  מתקיים מסויים  $n \in \mathbb{N}$  מתקיים

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

 $\mathbb{P}_{x \leftarrow f(0,1)}^{T(n)}(n)$  מקבלת  $M\left(x;r
ight) \leq lpha\left(n
ight)$  מתקיים  $x \notin \mathcal{L} \cap \Sigma^{n}$  לכל  $\mathcal{L} \in \mathcal{BPP}(\alpha, \beta)$  אזי

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

 $\mathcal{RP}\left(lpha
ight)=\mathcal{BPP}\left(0,lpha
ight)$  אזי  $lpha:\mathbb{N}
ightarrow\left[0,1
ight]$  טענה: תהא

 $\mathrm{co}\mathcal{RP}\left(lpha
ight)=\mathcal{BPP}\left(1-lpha,1
ight)$  אזי  $lpha:\mathbb{N}
ightarrow\left[0,1
ight]$  טענה: תהא

טענה: תהיינה ממקום מסויים אזי  $lpha \leq eta \leq \gamma \leq \delta$  עבורן  $lpha, eta, \gamma, \delta: \mathbb{N} o [0,1]$  טענה: תהיינה  $\mathcal{BPP}(\alpha, \delta) \subset \mathcal{BPP}(\beta, \gamma)$ 

משפט צ'רנוף־הופדינג: יהי  $\delta>0$  יהי  $\delta>0$  יהי אזי איר משפט צ'רנוף־הופדינג:

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

טענה: יהיו  $c,d\in\mathbb{N}$  חשיבה מותהא  $c,d\in\mathbb{N}$  טענה: יהיו החל ממקום מסויים אזי  $n^{-c} \leq lpha\left(n
ight) \leq 1-n^{-c}$ 

 $\mathcal{BPP}\left(\alpha\left(n\right)-n^{-c},\alpha\left(n\right)+n^{-c}\right)\subseteq\mathcal{BPP}\left(2^{-n^{d}},1-2^{-n^{d}}\right)$