```
.prefix (L)=\{y\in \Sigma^*\mid \exists x\in \Sigma^*.yx\in L\} שפת הרישא: תהא L\subseteq \Sigma^* תהא שפת הרישא
                                                         .suffix (L)=\{y\in \Sigma^*\mid \exists x\in \Sigma^*.xy\in L\} שפת הסיפא: תהא L\subseteq \Sigma^* שפת הסיפא:
                                                אלגוריתם מכריע שפה: תהא A:\Sigma^*	o \{	ext{true},	ext{false}\} שפה אזי אלגוריתם L\subset \Sigma^* המקיים
                                                                                                A\left(x\right)= true מקבל: לכל x\in L מתקיים
                                                                                                A\left(x
ight)= false מתקיים x
otin L לכל
                                                                           f:\left\{ 0,1
ight\} ^{n}
ightarrow\left\{ 0,1
ight\} ^{m} אזי n,m\in\mathbb{N} ההיינה בולאנית: תהיינה
                                                          \{f_1\dots f_n\} אזי בסיס פונקציות בוליאניות: תהיינה f_1\dots f_n פונקציות אזי
                                                                                                                  \mathcal{B} = \{\wedge, \vee, \neg\} בסיס דה־מורגן:
                                                                                            הערה: תמיד נוסיף לבסיס את הפונקציות הקבועות.
לכל f_i:\{0,1\}^{k_i}	o\{0,1\} באשר באשר f_1\dots f_n\in\mathcal{B} מעגל בוליאני: יהי f_i:\{0,1\}^{k_i} בסיס פונקציות בוליאניות תהיינה
                        המקיים \{f_1\dots f_n, x_1\dots x_m, y_1\dots y_k\} מעל מכוון אזי גרף אזי גרx_1\dots x_m, y_1\dots y_k\in\{0,1\} ותהיינה ווה
                                                                                                                    .חסר מעגלים מכוונים G
                                                                                                     \deg^-(x_i) = 0 מתקיים i \in [m] לכל
                                                                                                     \deg^-(f_i) = k_i מתקיים i \in [n] לכל
                                                                               \deg^+(y_i)=0 וכן \deg^-(y_i)=1 מתקיים i\in[k] לכל •
                                                                                                             f_1 \dots f_n יהי מעגל בוליאני אזי מעגל
                                                                                                          .E\left( C
ight) יהי מעגל בוליאני אזי מעגל מעגל יהי
                                                                                    \max_{v \in V(C)} \deg^+(v) יהי מעגל בולינארי מעגל :fan-out
                                                                    .\{G \leq C \mid 1 של Gשל fan-out אזי בולינארי מעגל בולינארי יהי מעגל מעגל מעגל מיהי יהי
שערוך מעגל בולינארי על קלט: יהי y_i מעגל בולינאני ויהי v \in \{0,1\}^m אזי שערוך מעגל בולינארי על קלט: יהי מעגל מעגל בולינאני ויהי
                                                                                                 הפונקציות הבוליאניות על הקודקודים הנכנסים.
                                      C\left(v
ight)=\left(y_{1}\ldots y_{k}
ight) הוא C על של אזי השערוך אזי v\in\left\{ 0,1
ight\} ^{m} אזי ויהי מעגל בולינאני ויהי
                                                        C\left(w
ight)=1 עבורו w\in\left\{ 0,1
ight\} ^{n} אזי אזי w\in\left\{ 0,1
ight\} ^{n} עבורו מעגל מקבל מילה: יהי
                                               L\left(C
ight)=\left\{x\in\left\{0,1
ight\}^{n}\mid x שפה של מעגל: יהי C מעגל בעל פלט יחיד אזי C מקבל את מעגל מעגל:
           .C\left(v
ight)=f\left(v
ight) מתקיים v\in\left\{ 0,1
ight\} ^{n} עבורו לכל בולינאני f:\left\{ 0,1
ight\} ^{n}	o\left\{ 0,1
ight\} מתקיים מעגל מחשב פונקציה: תהא
v \in \{0,1\}^m משפט אוניברסליות דה־מורגן: תהא f:\{0,1\}^m 	o \{0,1\}^m 	o \{0,1\}^k משפט אוניברסליות אוניברסליות אויים מעגל פיים מעגל אזי קיים מעגל אוניברסליות אויים מורגן אויים מעגל פיים מעגל בוליאני
                                                                       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
                                     L\left(\mathcal{C}
ight)=\left\{x\in\left\{0,1
ight\}^{*}\mid x\in L\left(\mathcal{C}_{|x|}
ight)
ight\} שפה של משפחת מעגלים: תהא
                                            L\left(\mathcal{C}
ight)=\mathcal{L} משפחה מכריעה שפה: תהא \mathcal{L}\subseteq\left\{ 0,1
ight\} ^{st} עפה אזי משפחה של מעגלים
                                                           . שונה. משפחה של מעגלים \mathcal C עבורה לכל משפחה של משפחה של מעגלים שונה.
```

 $0<|\Sigma|<\aleph_0$ אלפבית: קבוצה Σ המקיימת אלפבית: מילים: יהי Σ אלפבית אזי $\Sigma^*=\bigcup_{n=0}^\infty \Sigma^n$

 $L \subset \Sigma^*$ אלפבית אזי אונ Σ יהי שפה: יהי

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

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

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

 $(w_1\dots w_n)^m=\prod_{i=1}^m \langle w_1\dots w_n
angle$ אזי איזי $(w_1\dots w_n)\in \Sigma^*$ אזי מילה: תהא

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

 $L_1\parallel L_2=L_1L_2=\{w\omega\mid (w\in L_1)\wedge (\omega\in L_2)\}$ שרשור שפות: תהיינה $L_1,L_2\subseteq \Sigma^*$ שפות אזי שרשור שפות: תהיינה

 $L^m=\left\{\prod_{i=1}^k w_i \mid orall i\in [k]\,.w_i\in L
ight\}$ אזי $m\in\mathbb{N}$ שפה ויהי $L\subseteq\Sigma^*$ תהא

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

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

 $L^* = igcup_{k=0}^\infty L^k$ שפה אזי $L \subseteq \Sigma^*$ תהא שפה: תהא

```
(Q, \Sigma, \delta, q, F)
                                                                          Q, \Sigma, \delta, q, F אס"ד אזי אס"ד אזי אס"ד אזי אס"ד אזי אזי אזי אזי
                                                                         \Sigma אס"ד אזי (Q,\Sigma,\delta,q,F) אס"ד אזי דטרמיניסטי: יהי
                                                              .\delta אזי אזי (Q,\Sigma,\delta,q,F) אס"ד אזי דטרמיניסטי: אס"ד אזי אס"ד אזי
                                                                   Q, \Sigma, \delta, q, F אס"ד אזי אס ופי דטרמיניסטי: יהי Q, \Sigma, \delta, q, F אס"ד אזי אזי אזי
                                                                F אזי אזי (Q,\Sigma,\delta,q,F) אס"ד אזי אוי דטרמיניסטי: יהי
וכן לכל \hat{\delta}\left(q,arepsilon
ight)=q מתקיים q\in Q מתקיים המורחבת: יהי (Q,\Sigma,\delta,q_0,F) אס"ד אזי \hat{\delta}:Q	imes\Sigma^*	o Q עבורה לכל
                                                                                       .\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}
                                  \hat{\mathcal{S}}\left(q_0,x
ight)\in F אס"ד אזי x\in\Sigma^* אס"ד אזי אזי אוטומט סופי מקבל מילה: יהי מילה: יהי ערמיניסטי מקבל מילה: יהי
(q_n \in F \ )וכן i \in [n] לכל (q_{i-1}, x_i) = q_i עבורם q_1 \dots q_n \in Q וכן אמקבל את i \in [n] וכן לכל לכל את אס"ד ויהי x \in \Sigma^n טענה: יהי
                                               L\left(A
ight)=\{x\in\Sigma^{st}\mid x אס"ד אזי איזי A מקבל את אם דטרמיניסטי: יהי איזי אס"ד אזי אוי
                                               L\left(A
ight)=\mathcal{L} המקיים A המקיים אס"ד \mathcal{L}\subseteq\Sigma^* עבורה אזי שפה אלפבית אזי שפה הגולרית: יהי
                                                                                                                                     טענה: Ø רגולרית.
                                                                                                                                   .טענה: \{\varepsilon\} רגולרית
                                                                                                       . רגולרית \{x \mid \#_1(x) = 1 \mod 2\} רגולרית
                                                                                          . רגולרית \{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 אזי L \neq \{ \varepsilon \} וכן L \neq \varnothing שפה באשר באשר 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} \bullet
                                                                                                        . רגולרית מתקיים כי n\in\mathbb{N} רגולרית •
                                                                                                                                    . רגולרית L^*
                                                                                                     מסקנה: \{x \mid \#_1(x) = 0 \mod 2\} רגולרית.
אוטומט סופי לא־דטרמיניסטי מינוס (אסלד"ם): תהא Q 
eq \varnothing קבוצה סופית יהי \delta: Q 	imes \Sigma 	o \mathcal{P}(Q) ותהיינה
                                                                                                                      (Q, \Sigma, \delta, S, F) אזי S, F \subseteq Q
                                                          Q אסלד"ם אזי (Q, \Sigma, \delta, S, F) אסלד"ם מינוס: יהי
                                                         \Sigma אסלד"ם אזי (Q, \Sigma, \delta, S, F) אסלד"ם מינוס: יהי
                                              .\delta אטלד"ם איזי (Q,\Sigma,\delta,S,F) איזי מעברים באוטומט סופי לא־דטרמיניסטי מינוס: יהי
                                             F אסלד"ם אזי (Q, \Sigma, \delta, S, F) אסיניסטי מינוס: אסיניסטי סופי לא־דטרמיניסטי מינוס: יהי
\hat{\delta}\left(T,arepsilon
ight)=T מתקיים מתקיים לכל \hat{\delta}:\mathcal{P}\left(Q
ight)	imes\Sigma^*	o\mathcal{P}\left(Q
ight) אסלד"ם אזי מתקיים איז \hat{\delta}:\mathcal{P}\left(Q
ight)	imes\Sigma^*	o\mathcal{P}\left(Q
ight) אסלד"ם אזי
                                                                             \hat{\delta}\left(q,x
ight)=igcup_{q\in\hat{\delta}\left(T,x_{1}...x_{n-1}
ight)}\delta\left(q,x_{n}
ight) מתקיים x\in\Sigma^{n} וכן לכל
```

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

 $\mathcal{O}\left(n\cdot 2^n
ight)$ ענה: תהא $f:\left\{0,1
ight\}^n o\{0,1\}$ אזי קיים מעגל $f:\left\{0,1
ight\}^n o\{0,1\}$ וכן $|C|=\mathcal{O}\left(n\cdot 2^n
ight)$ אזי קיים מעגל C עבורו $|C|=\mathcal{O}\left(n\cdot 2^n
ight)$ בגודל $f:\left\{0,1
ight\}^n o\{0,1\}$ טענה: תהא $f:\left\{0,1
ight\}^n o\{0,1\}$ אזי קיים מעגל $f:\left\{0,1
ight\}^n o\{0,1\}$ וכן $|C|=\mathcal{O}\left(2^n
ight)$ אזי קיים מעגל $|C|=\mathcal{O}\left(2^n
ight)$ וכן $|C|=\mathcal{O}\left(2^n
ight)$

 $\mathcal{O}\left(rac{2^n}{n}
ight)$ אזי שמחשב את f שמחשב או $f:\left\{0,1
ight\}^n o \left\{0,1
ight\}$ משפט לופיאנוב: תהא

 $rac{2^n}{10n}$ טענה שאנון: קיים C בגודל מעגל $f:\{0,1\}^n o\{0,1\}$ שאינה ניתנת לחישוב בעזרת מעגל $n\in\mathbb{N}$

אזי $F\subseteq Q$ אזי $\delta:Q imes \Sigma o Q$ יהי הופית יהי לפבית תהא אופבית עהש"ד): תהא אוטומט סופי דטרמיניסטי (אס"ד): תהא

 $|\mathcal{C}_n| \leq S\left(n
ight)$ אבורה $S: \mathbb{N} o \mathbb{N}$ אזי משפחה של מעגלים: תהא משבחה מעגלים: תהא

C-גודל מעגל: יהי מעגל בוליאני C אזי וודל מעגל: יהי מעגל בוליאני

 $\hat{\delta}\left(S,x
ight)\cap F
eq \varnothing$ אוטומט סופי לא־דטרמיניסטי מינוס מקבל מילה: יהי (Q,Σ,δ,S,F) אסלד"ם אזי $x\in\Sigma^n$ המקיים פוכן $q_0\in S$ וכן $q_0\in S$ אזי $q_i\in\delta\left(q_{i-1},x_i\right)$ אזי ($q_i\in\delta\left(q_{i-1},x_i\right)$

 $L\left(M
ight)=\{x\in\Sigma^*\mid x$ שפה של אוטומט סופי לא־דטרמיניסטי מינוס: יהי M אסלד"ם אזי M מקבל את ארשר באר אוטומט סופי דטרמיניסטי מינוס החזקה: יהי $M=(Q,\Sigma,\delta,S,F)$ אטומט סופי דטרמיניסטי מינוס החזקה: יהי

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

 $\hat{\delta_A}(T,x)=\hat{\delta_M}(T,x)$ אזי $x\in \Sigma^*$ ויהי ויהי $T\subseteq Q_N$ תהא של אס"ד החזקה של אס"ד אס"ד החזקה של מה: יהי א

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

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

 $S,F\subseteq Q$ ותהיינה $\delta:Q imes \Sigma_{arepsilon} o \mathcal{P}\left(Q
ight)$ אלפבית תהא אלפבית הא פופית אסל"ד): תהא אזי $\delta:Q imes \Sigma_{arepsilon} o \mathcal{P}\left(Q
ight)$ אזי $\delta:Q,\Sigma,\delta,S,F$.

Q אסל"ד אזי (Q, Σ, δ, S, F) אסל"ד אזי אסל"ד אזי אסל"ד אזי

 Σ אסל"ד אזי (Q,Σ,δ,S,F) אסל"ד אזי אזי אלפבית באוטומט סופי לא־דטרמיניסטי:

 $.\delta$ אזי אזי (Q,Σ,δ,S,F) אסל"ד אזי אזי אסל"ד אזי אסל"ד אזי אזי אזי אזי

 (Q,Σ,δ,S,F) אסל"ד אאי אוי אסל"ד איזי אסל"ד אאי אסל"ד איזי אוי מצבים התחלתיים באוטומט סופי לא־דטרמיניסטי:

F אסל"ד אזי (Q, Σ, δ, S, F) אסל"ד אזי איזי אסל"ד אזי אסל"ד אזי

 $.E\left(q
ight) = \left\{q' \in Q \mid \exists a \in Q^{k+1}. \left(a_0 = q
ight) \wedge \left(orall i \in [k]. a_i \in \delta\left(a_{i-1}, arepsilon
ight)
ight) \wedge \left(a_k = q'
ight)
ight\}$ אזי $q \in Q$ אזי $q \in Q$

פונקציית המעברים המורחבת: יהי (Q,Σ,δ,S,F) אסל"ד אזי $\hat{\delta}:\mathcal{P}\left(Q\right) imes\Sigma^* o\mathcal{P}\left(Q\right)$ אסל"ד אזי (Q,Σ,δ,S,F) עבורה לכל $\hat{\delta}:\mathcal{P}\left(Q\right) imes\Sigma^* o\mathcal{P}\left(Q\right)$ מתקיים $\hat{\delta}\left(q,x\right)=E\left(\bigcup_{q\in\hat{\delta}\left(T,x_1...x_{n-1}\right)}\delta\left(q,x_n\right)\right)$ מתקיים $\hat{\delta}\left(T,\varepsilon\right)=E\left(T\right)$

 $\hat{\mathcal{S}}(S,x)\cap F
eq arnothing$ המקיים $x\in\Sigma^*$ אוטומט סופי לא־דטרמיניסטי מקבל מילה: יהי (Q,Σ,δ,S,F) אסל"ד אזי

 $x^{\!\!\!/}=\sigma_1\dots\sigma_n$ איי $x=arepsilon^{k_0}\sigma_0arepsilon^{k_1}\sigma_1arepsilon^{k_2}\dots\sigma_narepsilon^{k_n}$ עבורם $x\in\Sigma^k$ יהי $x\in\Sigma^*$ יהי $x\in\Sigma^k$ יהי $x\in\Sigma^k$ יהי $x\in\Sigma^k$ איי $x\in\Sigma^k$ איי $x\in\Sigma^k$ איי $x\in\Sigma^k$ עבורם $x\in\Sigma^k$ עבורם $x\in\Sigma^k$ וכן $x\in\Sigma^k$ איי $x\in\Sigma^k$ איי $x\in\Sigma^k$ איי $x\in\Sigma^k$ איי $x\in\Sigma^k$ וכן $x\in\Sigma^k$ וכן $x\in\Sigma^k$ וכן $x\in\Sigma^k$ וכן $x\in\Sigma^k$ וכן $x\in\Sigma^k$

 $L\left(A
ight)=\{x\in\Sigma^{st}\mid x$ אסל"ד אזי $A\}$ מקבל את A אסל"ד אזי לא־דטרמיניסטי: יהי

 $L\left(N
ight)=L\left(M
ight)$ עבורו M עבורו אזי קיים אסלד אזי איז קיים אסלד אזי יהי אסל"ד אזי אסל

 $L\left(A
ight)=L\left(M
ight)$ עבורו A אסל"ד אזי קיים אס"ד אסל"ד אזי קיים אס אסקנה: יהי N

 $(L(N)=\mathcal{L})$ שפה אזי \mathcal{L} שפה אזי בולרית) אסל"ד N אלפבית ותהא בית שפה אזי \mathcal{L} שפה אזי \mathcal{L}

ביטוי רגולרי (ב"ר): יהי Σ אלפבית אזי

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

שפה נוצרת מביטוי רגולרי: יהי Σ אלפבית אזי

- $L(\varnothing) = \varnothing \bullet$
- $L\left(a
 ight)=\left\{ a
 ight\}$ אזי $a\in\Sigma_{arepsilon}$ יהי יהי
- $L\left(R_{1}\cup R_{2}
 ight)=L\left(R_{1}
 ight)\cup L\left(R_{2}
 ight)$ אזי רגולרים אזי רגולרים אזי רגולרים R_{1},R_{2}
 - $L(R_1R_2) = L(R_1)L(R_2)$ יהיו R_1, R_2 ביטויים רגולרים אזי
 - $L(R^*) = L(R)^*$ יהי R ביטוי רגולרי אזי יהי R

 $R\left(\Sigma
ight)=\left\{r\in\Sigma^{st}\mid$ יהי Σ אלפבית אזי r ביטוי רגולרי א

הערה: קיים סדר פעולות לביטויים רגולריים

```
    סגור קליני.
    שרשור.
    איחוד.
    יהי ∑ אלפ
    ז ניתנת לניפוח:
    ש וכן לכל
    למת הניפוח:
    ע הניפוח:
    תהא
```

 $(L(r)=\mathcal{L})$ שפה אזי (\mathcal{L} רגולרית) \Longleftrightarrow (קיים $r\in R$ עבורו $\mathcal{L}\subseteq \Sigma^*$ שפה עבורו $\mathcal{L}\subseteq \mathcal{L}$ שפה ניתנת לניפוח: שפה \mathcal{L} וקבוע $0>\ell>0$ עבורם לכל $w\in \mathcal{L}$ באשר $w\in \mathcal{L}$ קיימים $x,y,z\in \Sigma^*$

וכן $|xy|\leq \ell$ וכן |y|>0 באשר $x,y,z\in \Sigma^*$ קיימים $\ell\leq |w|$ באשר לכל לכל עבורם לכל עבורם לכל $w\in \mathcal{L}$ באשר לכל א באשר $x,y,z\in \Sigma^*$ באשר $x,y,z\in \mathcal{L}$ מתקיים $x,y,z\in \mathcal{L}$ מתקיים $x,y,z\in \mathcal{L}$ מתקיים א באשר וכן לכל $x,y,z\in \mathcal{L}$

 ℓ ניתנת לניפוח עבורו $\ell>0$ עבורו שפה רגולרית שפה עפה תהא למת הניפוח. עבורו שפה למת הניפוח

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

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

. טענה: $\{0^i1^j \mid i>j\}$ אינה רגולרית

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

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

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

 $.\sim_A=\left\{(x,y)\in (\Sigma^*)^2\;\Big|\; \hat{\delta}\left(q_0,x
ight)=\hat{\delta}\left(q_0,y
ight)
ight\}$ הגדרה: יהי A אס"ד ויהיו $x\sim_{L(A)}y$ עבורם $x\sim_A y$ עבורם $x,y\in \Sigma^*$ אויי א אס"ד ויהיו

 $x\sim_A y$ טענה: יהי A אס"ר ויהיו $x,y\in \Sigma^*$ אא $x\sim_A y$ מסקנה: יהי A אס"ד אזי $|Q|>|\Sigma^*/\sim_A|>|\Sigma^*/\sim_{L(A)}|$ מסקנה: יהי A אס"ד אזי

 $\Sigma^*/_{\sim_L}$ שפה רגולרית אזי ב $\Sigma^*/_{\sim_L}$ סופית.

.(סופית) שפה בייהיל־נרוד: תהא בה בה אזי עם שבה בה בה בה בה $\Sigma^*/\sim_L)$ סופית).

 $y\sim_L x_i$ אזי $y\in \Sigma^*$ ויהי $\Sigma^*/_{\sim_L}$ שפה באשר $y\in \Sigma^*$ סופית תהא קבוצת נציגים של ב $\Sigma^*/_{\sim_L}$ ויהי $y\sim_L x_i$ טופית תהא (Class y=i

אזי אס"ד $\{x_1\dots x_n\}$ אווומט סופי דטרמיניסטי המחלקות: תהא $L\subseteq \Sigma^*$ אווומט סופי דטרמיניסטי המחלקות: תהא עפה באשר באשר באשר ערכה על ערכה על באשר (Q,Σ,δ,q_0,F)

- $.Q = [|\Sigma^*/\sim_L|] \bullet$
- $.\delta\left(i,\sigma
 ight)=\mathrm{Class}\left(x_{i}\sigma
 ight)$
 - $.q_0 = \operatorname{Class}\left(arepsilon
 ight) \,\,ullet$
- $.F = \{i \in Q \mid x_i \in L\} \bullet$

טענה: תהא L אס"ד המחלקות של Δ יהי Σ^*/\sim_L יהי אס"ב אס"ב ענה: $\{x_1\dots x_n\}$ סופית תהא Σ^*/\sim_L טענה: תהא Δ יהי Δ אס"ב באשר אס"ב באשר Δ יהי Δ יהי יהי Δ

 $L\left(N
ight)=\left\{x\in\left[n
ight]^{*}\mid\exists\sigma\in\Sigma.\#_{\sigma}\left(x
ight)=0
ight\}$ עבורו $\left|Q\right|=n$ אזי קיים אסל"ד א מעל תוב אסל"ד ועבורו אזי קיים אסל"ד איי מעל וואסל"ד איי מעל וואסל וואסל"ד איי מעל וואסל"ד איי מעל וואסל וואס

 $|Q|\geq 2^n$ אזי A אזי A אזי A אזי הי A אווי A אזי הי A איזי מענה: יהי A איזי מעל A איזי A איזי

 $q_0,q_a,q_r\in Q$ יהיו יהי $\Sigma\subseteq \Gamma$ וכן אלפבית עבורו $\Sigma\subseteq \Gamma$ יהיו אלפבית יהי אלפבית סופית יהי Ω אלפבית סופית יהי Ω אלפבית יהי Ω אלפבית יהי Ω אלפבית יהי Ω אוי Ω יהיו Ω יחים Ω יהיו Ω יהיו Ω יהיו Ω יהיו Ω יהיו Ω יהיו Ω יחים Ω יהיו Ω יחים Ω יהיו Ω יחים Ω יחים Ω יחי Ω יחי Ω יחים Ω יחים Ω יחים Ω יחים Ω יחים Ω יחים Ω יחים

.Qאזי מ"ט ($Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r$) מייט מיורינג: תהא

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

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

 $.\delta$ אזי מעברים מעברים מיט מיורינג: תהא $(Q,\Sigma,\Gamma,\delta,q_0,q_a,q_r)$ מ"ט מייט מייט מייט מיי

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

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

 $c=q_0v$ המקיימת $v\in\Sigma^*$ עבורה קיים עבורה אזי קונפיגורציה אזי קונפיגורציה אזי קונפיגורציה אזי קונפיגורציה מקבלת: תהא $u,v\in\Sigma^*$ מ"ט אזי קונפיגורציה $c=uq_av$ עבורה קיימים עבורה קיימים $u,v\in\Sigma^*$ המקיימים עבורה קיימים עבורה קיימים $u,v\in\Sigma^*$ המקיימים עבורה קיימים עבורה קיימים עבורה מ"ט אזי קונפיגורציה דוחה: תהא $u,v\in\Sigma^*$ מ"ט אזי קונפיגורציה עבורה קיימים אזי קונפיגורציה דוחה: תהא עבורה קיימים עבורה קיימים עבורה קיימים עבורה עבורה

cעם עם אוי נזהה את מ"ט ותהא קונפיגורציה אזי מ"ט ותהא M

קונפיגורציה c' המקיימת אחד הבאים קונפיגורציה אזי קונפיגורציה M מ"ט תהא מ"ט תהא קונפיגורציה אזי קונפיגורציה אוי

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

 c_i עוברת ל־ c_{i-1} עוברת מקבלת מילה: תהא m מ"ט אזי $a_i \in \mathcal{L}^*$ עבורו קיימות $a_i \in \mathcal{L}^*$ עוברת מקבלת מילה: תהא $a_i \in \mathcal{L}^*$ עוברת ל־ $a_i \in \mathcal{L}^*$

 $L\left(M
ight)=\{x\in\Sigma^{st}\mid x$ שפה של מכונת טיוריגנ: תהא M מ"ט אזי M מקבל את שפה של מכונת טיוריגנ

x את אדוחה אל לא מקבלת אורינג א עוצרת על קלט: תהא מ"ט אזי אזי $x\in \Sigma^*$ עבורו M אזי אוצרת על קלט: תהא

מתקיים M' מסוג M וכן לכל M מסוג M מחקיים מודלים שקולים: מודלים שקולים: מודלים שקולים

- $L\left(A
 ight)=L\left(A'
 ight)$ המקיימת M' מסוג A' המקיימת •
- $L\left(B
 ight) =L\left(B^{\prime}
 ight)$ המקיימת M מסוג B^{\prime}

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

הערה: את כל הפעולות ממכונת טיורינג נכליל בצורה הטבעית עבור מכונת טיורינג נחה.

מסקנה: מכונת טיורינג ומכונת טיורינג נחה הינן מודלים שקולים.

יהיו $\Sigma\subseteq \Gamma$ וכן $\Sigma\subseteq \Gamma$ וכן אלפבית יהי Σ אלפבית יהי Σ אלפבית וכן היה $\Sigma\subseteq \Gamma$ אתהא $\Sigma\subseteq \Gamma$ ההא $\Sigma\subseteq \Gamma$ קבוצה סופית יהי Σ אלפבית יהי $\Sigma\subseteq \Gamma$ ההא $\Sigma\subseteq \Gamma$ ההא Σ היי Σ אוי Σ היי Σ אוי Σ היי ותהא Σ וכן Σ היי ותהא Σ היי ועבור Σ היי ועבור Σ אוי ועבור Σ וכן Σ היי וכן Σ היי וכן Σ היי וכן Σ היי וכן Σ וכן Σ היי וכן Σ היי וכן Σ היי וכן Σ וכן Σ היי וכן Σ היי וכן Σ היי וכן Σ וכן Σ היי ו

הערה: את כל הפעולות ממכונת טיורינג נכליל בצורה הטבעית עבור מכונת טיורינג רב־סרטית.

 $.c_1\$c_2\$\dots\$c_k$ אזי אזי $.c_1\dots c_k\in \Gamma^*Q\Gamma^*$ אזיינה מ"ט רב־סרטית: תהא א מ"ט רב־סרטית: תהא

המקיימת $v\in \Sigma^*$ המקיימת אזי קונפיגורציה c מ"ט רב־סרטית אזי התחלתית במכונת טיורינג רב־סרטית: תהא א מ"ט רב־סרטית אזי קונפיגורציה $c=q_0v$

. מסקנה: יהי $k \in \mathbb{N}_+$ אזי מכונת טיורינג ומכונת טיורינג מסקנה: יהי אזי מכונת טיורינג ומכונת אזי מכונת מסקנה:

 $(k,(\pi_1\dots\pi))$ אזי $\pi_1\dots\pi_p$ ותהיינה $k\in\mathbb{N}$ יהי

k אזי RAM מספר הרגיסטרים במודל RAM: יהי (k,Π) מודל

 Π אזי RAM מודל ויהי (k,Π) יהי יהי

 $T:\mathbb{N} \to \mathbb{N}$ וכן $R_0 \dots R_k \in \mathbb{N}$ וכן PC $\in \mathbb{N}$ אזי מודל RAM מודל מודל אורציה במודל RAM: יהי ובן מודל

.PC מונה התוכנית בקונפיגורציה: יהי (k,Π) מודל (RAM ותהא יהי קונפיגורציה אזי אזי

R ותהא קונפיגורציה אזי (T,R, אותה תהא (R מודל מודל אזי יהי יהי קונפיגורציה: יהי יהי יהי

T אזי אונפיגורציה (T,R,PC) ותהא ותהא מודל (RAM) אור אזי אינרון בקונפיגורציה: יהי

.MIPS זהה לריצת מעבד RAM זהה לריצת מעבד

טענה: מכונת טיורינג ומודל RAM הם מודלים שקולים.

 $\square\in\Gamma\setminus\Sigma$ וכן $\Sigma\subseteq\Gamma$ אלפבית יהי Γ אלפבית אלפבית (מטל"ד): תהא $Q
eq\emptyset$ קבוצה סופית יהי Ω אלפבית יהי Ω אלפבית עבורו Ω וכן Ω וכן Ω וכן Ω באשר Ω באשר Ω ותהא Ω ותהא Ω ותהא Ω ותהא Ω ותהא Ω ותהא Ω אזי Ω איזי Ω איזי Ω ותהא Ω איזי Ω ותהא Ω ותהא Ω ותהא Ω ותהא Ω ותהא Ω באשר Ω באשר Ω קונפיגורציה איי קונפיגורציה איי קונפיגורציה עוברת: תהא Ω מטל"ד תהא Ω מטל"ד והי Ω המקיימת Ω וכן Ω וכן Ω וכן Ω הינה איי עץ קונפיגורציות מתקיים (Ω באצא עץ חישוב: תהא Ω מטל"ד ויהי Ω איי עץ קונפיגורציות ען Ω עם שורש Ω עבורו לכל Ω קונפיגורציות מתקיים (Ω באצא איי עץ קונפיגורציות Ω

 $T_{N,x}$ מכונת טיוריגנ לא־דטרמיניסטית מקבלת מילה: תהא N מטל"ד אזי $x\in \Sigma^*$ עבורו קיים עלה מקבל ב־ $T_{N,x}$ מטל"ד אזי $x\in \Sigma^*$ עבורו מתקבל על ידי $x\in \Sigma^*$ אינו מתקבל על ידי $x\in \Sigma^*$ עבורו מכונת טיוריגנ לא־דטרמיניסטית דוחה מילה: תהא $x\in \Sigma^*$ מטל"ד אזי $x\in \Sigma^*$

 $L(N)=\{x\in\Sigma^*\mid x$ מקבל את א $N\}$ מטל"ד אזי N מטל"ד איזי איזי איזי ארזי נא־דטרמיניסטית: תהא

x את את את אוצרת אל איז איז איז עבורו אז איז איז אוורה את את אוצרת איז אוצרת אוצ

טענה: מכונת טיורינג ומכונת טיורינג לא־דטרמיניסטית הינן מודלים שקולים.

```
xעוצרת על M עוצרת שפה: תהא x\in \Sigma^* מתקיים כי \mathcal{L}=L\left(M
ight) עבורה מכונת טיורינג מכריע שפה: תהא שפה אזי מ"ט M
                               \mathcal{R}=\{\mathcal{L}\subseteq\Sigma^*\mid\mathcal{L} אמכריעה מ"ט M המכריעה איז \Sigma אלפבית איז \Sigma אלפבית איז היי \Sigma
                                                                                                                                   \mathcal{R} \subseteq \mathcal{RE} :מסקנה
                                                            עבורו \Sigma \cup \{\$\} מעל האלפבית שפה אזי מ"ט שפה אזי מונה עבור שפה: תהא ב\mathcal{L} \subseteq \Sigma^*
                                                                                \delta(q,\sigma)=(q',\sigma',R) מתקיים \sigma\in\Gamma ולכל g\in Q לכל
                                                                                                      מקיימת \varepsilon מקיימת על הרצת E הרצת •
                                                           . לכל x \in L מתקיים כיx \in \mathbb{R} על הסרט לאחר מספר סופי של צעדים x \in L
                                                                                 . לעולם אים x \notin L לא על הסרט לעולם x \notin L לכל
                                                                              . טענה: תהא \mathcal{L}\subseteq \Sigma^* שפה אזי (\mathcal{L}\in\mathcal{RE}) שפה ל־\mathcal{L}\subseteq \Sigma^* מונה).
.$y$ לפני
                                                                  . טענה: תהא \mathcal{L}\subseteq \Sigma^* מונה לקסיקוגרפי). שפה אזי שפה אזי ענה: תהא \mathcal{L}\subseteq \Sigma^*
                                                                             \operatorname{co}\mathcal{RE}=\{\mathcal{L}\subseteq\Sigma^*\mid\overline{\mathcal{L}}\in\mathcal{RE}\} יהי \Sigma אלפבית אזי יהי \Sigma אלפבית אזי
                                                                                                                           \mathcal{R} = \mathcal{RE} \cap \mathrm{co}\mathcal{RE} :טענה
                                     . חח"ע עד כדי שינוי שמות. f:\{M\mid מ"ט M\} 	o \{0,1\}^* חח"ע עד כדי שינוי שמות.
                                                                                   M מ"ט אזי \langle M \rangle הינו הקידוד הבינארי של M מ"ט אזי מיט 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 מאותחל עם אינו הקידוד הבינארי של מילה מילה x מילה מילה מילה M מאותחל עם
                                                                          משפט מכונת טיורינג אוניברסלית: קיימת מ"ט U מעל \{0,1\} עבורה
                                       Mנכל מ"ט Mולכל קלט M של M מתקיים (M מקבלת את א ולכל קלט M ולכל קלט M
                                            M את את M ולכל קלט M של M מתקיים (M דוחה את M) ולכל מ"ט M
                             עבור M לא עוצרת עבור M מתקיים (M של M מתקיים (M לא עוצרת עבור M לכל מ"ט M ולכל קלט M של M
                                                                       x \notin \operatorname{Im}(f) באשר x \notin \operatorname{Im}(f) מתקיים כי x \in \{0,1\}^* לכל
                                                                                    L \notin \mathcal{RE} \cup \mathrm{co}\mathcal{RE} טענה: קיימת L \subseteq \{0,1\}^* שפה עבורה
                                                                   ACC = \{ \langle M, x \rangle \mid (מ"ט M) \wedge (מ מילה) \wedge (x את מקבלת את מקבלת מ"ט)
                                                                                                                                   \mathsf{ACC} \in \mathcal{RE} :טענה
                                                            L\left(M
ight)=\left\{ \left\langle N
ight
angle \mid\left\langle N
ight
angle \notin L\left(N
ight)
ight\} עבורה \left\{ 0,1
ight\} עבורה א קיימת מ"ט M מעל
                                        \{\langle N \rangle \mid \langle N \rangle \notin L(N)\} אזי המכריעה את ACC אזי קיימת מ"ט א מ"ט המכריעה את מ"ט המכריעה את
                                                                                                                                     .ACC \notin \mathcal{R} טענה:
                                                                    .HALT = \{\langle M, x \rangle \mid (\alpha"ט) \land (x) \land (x) \land (x) \} הגדרה:
                                                                                                                              .HALT \in \mathcal{RE} \backslash \mathcal{R} :טענה
                                                                                       .EMPTY = \{\langle M \rangle \mid \alpha"0 \mid M \land (L(M) = \varnothing)\} הגדרה:
                                                                                                                                  .EMPTY \notin \mathcal{R} :
```

עוצרת M מתקיים כי M מתקיים כי M מתקיים כי M מחשבת פונקציה: תהא M מ"ט ותהא M מ"ט ותהא M מ"ט ותהא

חשיבה עבורה $f:\Sigma^* o\Delta^*$ שפה איי איז $B\subset\Delta^*$ שפה ותהא $\Sigma\subset\Delta$ תהא באשר באשר באשר Σ . אלפבייתים באשר

סימון: יהיו $f:\Sigma^* o\Delta^*$ אלפבייתים באשר $E\subseteq\Delta^*$ שפה תהא שפה תהא $E\subseteq\Delta^*$ שפה באשר באשר באשר באשר סימון: יהיו

M המחשבת איM בורה קיימת מ"ט M המחשבת איM בורה קיימת M המחשבת איM המחשבת אי

שפות כריעות למחצה/שפות ניתנות למניה רקורסיבית/שפות ניתנות למבלה: יהי Σ אלפבית אזי

 $\mathcal{RE} = \{ \mathcal{L} \subseteq \Sigma^* \mid \mathcal{L} = L(M) \text{ עבורה } M \text{ עבורה} \}$

.EMPTY \in co \mathcal{RE} טענה: $A \in \mathcal{R}$ אזי $A \leq_m B$ וכן $B \in \mathcal{R}$ שפות באשר A, B איזי $A \in \mathcal{R}$

f(x)יש וכן הסרט בסוף הריצה הינו x על x

 $A \leq_m B$

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

```
הערה: יש דבר כזה רדוקציה כללית שמכלילה את רדוקציית המיפוי, לא עברנו על זה פורמלית, מסומן >.
                                                                                                                      \{\langle M \rangle \mid \langle M \rangle \notin L(M)\} \leq ACC מסקנה:
                                                                                                                                             ACC \leq_m HALT מסקנה:
                                                                                                                                              ACC \leq EMPTY מסקנה:
                                                                                                                      .REG = \{\langle M \rangle \mid L(M)\} - הגדרה:
                                                                                                                                                       .REG 
otin \mathcal{R} :טענה
                                                                                                           EQ = \{ \langle M_1, M_2 \rangle \mid L(M_1) = L(M_2) \} :הגדרה
                                                                                                                                                         .EQ \notin \mathcal{R} :טענה
                                                                                                                     .\mathsf{HALT}_{arepsilon} = \{\langle M \rangle \mid arepsilon עוצר על M \} :
                                                                                                                                            .HALT \leq_m HALT_{\varepsilon} :
                                                                                     A \leq_m B אזי B \in \mathcal{P}\left(\Sigma^*\right) \setminus \{\Sigma^*,\varnothing\} ותהא A \in \mathcal{R} אזי
                                               .\overline{B}ל למה: תהיינה A,B שפות ותהא f רדוקציית מיפוי מ־A ל־B לימה: תהיינה שפות ותהא לדוקציית מיפוי מ
                                                                                                               טענה: תהיינה A \leq_m B שפות באשר A,B אזי
                                                                                                                                A \in \mathcal{RE} אזי B \in \mathcal{RE} אם
                                                                                                                          A\in \mathrm{co}\mathcal{RE} אזי B\in \mathrm{co}\mathcal{RE} אם
                                                                                                                            \overline{ACC} \leq_m EQ וכן ACC \leq_m EQ טענה:
                                                                                                                                        .EQ \notin \mathcal{RE} \cup co\mathcal{RE} :מסקנה
                                                                                                             \mathcal{C}\subseteq\mathcal{P}\left(\Sigma^{*}
ight) אלפבית אזי יהי \Sigma אלפבית יהי
                                                                                        L_{\mathcal{C}} = \{\langle M \rangle \mid L\left(M\right) \in \mathcal{C}\} הגדרה: תהא \mathcal{C} תכונה סמנטית אזי
                                                                            L_{\mathcal{C}} 
otin \mathcal{R} משפט רייס: תהא \mathcal{C} \in \mathcal{P}\left(\mathcal{RE}\right) \setminus \{\mathcal{RE},\varnothing\} משפט רייס: תהא
                                                                                                                       L_{\mathcal{C}} \in \mathcal{R} אזי \mathcal{C} \in \{\mathcal{RE}, \varnothing\} טענה: תהא
                                                                                                                                .PRIME = \{(p)_2 \mid p \in \mathbb{P}\} :הגדרה:
                                                                                                                   .2 הערה: קידוד מספרים תמיד יעשה בבסיס
                                                                                                             .EQPRIME = \{\langle M \rangle \mid L(M) = PRIME\} הגדרה:
                                                                                                                                                .EQPRIME \notin \mathcal{R} :
                                                             L_{\mathcal{C}}\notin\operatorname{co}\mathcal{RE} אזי \mathcal{C}\in\mathcal{P}\left(\mathcal{RE}\setminus\{\varnothing\}
ight)\setminus\{\varnothing\} אוי תהא הרחבה ראשונה: תהא
                                                     L_{\mathcal{C}}
otin\mathcal{E} אזי arnothing\in\mathcal{C} באשר \mathcal{C}\in\mathcal{P}\left(\mathcal{RE}
ight)\setminus\{\mathcal{RE}\} עענה משפט רייס הרחבה שנייה: תהא
                                                                                                                                                  .REG \notin \mathcal{RE} מסקנה:
                                                                                                                         ALL = \{\langle M \rangle \mid L(M) = \Sigma^* \} הגדרה:
                                                                                                                                                  \overline{HALT} \leq_m ALL למה:
                                                                                                                                          .ALL \notin \mathcal{RE} \cup \text{co}\mathcal{RE} טענה:
על הקלט M מתקיים כי x\in \Sigma^n ולכל לימן ריצה של מכונת טיורינג: תהא מ"ט אזי T:\mathbb{N} \to \mathbb{N} עבורה לכל מתקיים כי
                                                                                                                               צעדים. T\left(n\right) צעדים x
                                                  .DTime (T\left(n\right))=\{L\left(M\right)\mid\mathcal{O}\left(T\left(n\right)\right) בימן שרצה בימן M\} אזי T:\mathbb{N}\to\mathbb{N} הגדרה: תהא
                                                                                                                         \left\{0^k1^k\mid k\geq 0
ight\}\in \mathrm{DTime}\left(n^2
ight) טענה:
                                                                                                              \left\{ 0^{k}1^{k}\mid k\geq0
ight\} \in DTime \left( n\log\left( n
ight) 
ight) מסקנה:
                                                                        (T(n))_2 את מחשבת את על הקלט M כי M כי n\in\mathbb{N} כי M עבורה קיימת מ"ט M עבורה קיימת מ"ט M המקיימת לכל
                                                                                                                                                        בזמן \mathcal{O}\left(T\left(n\right)\right) בזמן
```

M באשר x ולכל קלט M ולכל מ"ט עבורם לכל מ"ם $C\in\mathbb{R}$ באשר שוניברסלית עם טיימר: קיימת מ"ט אוניברסלית עו וקיים

 $A,B
otin \mathcal{R}$ אזי $A \leq_m B$ וכן $A
otin \mathcal{R}$ אזי A,B מסקנה: תהיינה

 $T\left(n
ight)=\Omega\left(n
ight)$ עענה: תהא $T:\mathbb{N} o\mathbb{N}$ חשיבה בזמן שאינה קבועה אזי

עוצרת על הקלט X לאחר t צעדים מתקיים כי U עוצרת על הקלט x לאחר t צעדים מתקיים כי

משפט: קיימת מ"ט אוניברסלית U וקיים ווכל $C\in\mathbb{R}$ עבורם לכל מ"ט מ"ט אוניברסלית עוכל $C\in\mathbb{R}$ מתקיים

```
\mathcal{P} = igcup_{c \in \mathbb{N}} DTime (n^c): \mathcal{P} שפה
                                                                                             .PATH = \{\langle G, s, t \rangle \mid tל מ־ל מסלול עם מכוון עם מכוון עם מסלול G\}
                                                                                                                                                           .PATH \in \mathcal{P} :טענה
                                                                                                                                                         .PRIME \in \mathcal{P} משפט:
                                                                                                                                \mathcal{NP} = igcup_{c \in \mathbb{N}} \operatorname{NTime}\left(n^c
ight) : \mathcal{NP} שפה
                                                                                                                                                          \mathcal{P} \subseteq \mathcal{NP} :מסקנה
                                                                         .HAMPATH \in \mathcal{NP} :טענה
                                                                                                                           השערה: רוחה השערה: HAMPATH \notin \mathcal{P}
                                                                                                                         \mathcal{EXP} = igcup_{k \in \mathbb{N}} \mathsf{DTime}\left(2^{n^k}\right) : \mathcal{EXP} שפה
                                                                                                                 \mathcal{NEXP}=igcup_{k\in\mathbb{N}} NTime \left(2^{n^k}
ight):\mathcal{NEXP} שפה
                                                                                                                                                 \mathcal{E} \mathcal{X} \mathcal{P} \subseteq \mathcal{N} \mathcal{E} \mathcal{X} \mathcal{P} טענה:
                                                                                                                             \mathcal{P} \subseteq \mathcal{NP} \subseteq \mathcal{EXP} \subseteq \mathcal{NEXP} מסקנה:
                                                                                                                                                           \mathcal{P} \subsetneq \mathcal{EXP} :טענה
                                                                                                                                                    \mathcal{NP} \subsetneq \mathcal{NEXP} טענה:
                                                                                                                      (\mathcal{P} = \mathcal{NP}) \Longrightarrow (\mathcal{EXP} = \mathcal{NEXP}) טענה:
                                                                                         x על M על הינו ריצת M מ"ט ויהי x \in \Sigma^* אזי ויהי M מ"ט ויהי
                                                                      מוודא לשפה: תהא \Sigma \cup \{","\} שפה אזי מ"ט V מעל אלפבית \mathcal{L} \subseteq \Sigma^* המקיים
                                                                                     . מקבלת V\left(x,w\right) עבורו w\in\Sigma^{*} אזי קיים x\in\mathcal{L} מקבלת.
                                                                                 . דוחה V\left(x,w\right) מתקיים כיw\in\Sigma^{*} אזי לכל x
otin\mathcal{L} אזי יהי
                                                                                           \mathcal{L}\subseteq \Sigma^* טענה: תהא \mathcal{L}\subseteq \Sigma^* שפה אזי שפה אזי ל־\mathcal{L}\subseteq \Sigma^*
V\left(x,w
ight) מדווא פולינומי לשפה: תהא x,w\in\Sigma^* שפה אזי מוודא V ל־\mathcal{L} עבורו קיים p\in\mathbb{N}\left[x
ight] המקיים כי לכל
                                                                                                                               עוצרת לכל היותר אחרי p\left(|x|\right) צעדים.
                                                                                      .CLIQUE = \{\langle G, k \rangle \mid k גרף גרף בעל מכוון בעל קליקה מגודל G\}
                                                                                                                                טענה: קיים מוודא פולינומי ל־CLIQUE.
                                           (u,v) \notin E מתקיים בלתי תלויה (ב"ת): יהי G גרף אזי I \subseteq V עבורה לכל u,v \in I מתקיים מתקיים לבוצת צמתים בלתי תלויה (ב"ת):
                                                                                       .IS = \{\langle G, k \rangle \mid k גרף גרף בעל קבוצה ב"ת מגודל א מכוון בעל מכוון גרף גרף לא
                                                                                                                                        טענה: קיים מוודא פולינומי ל־IS.
                                                                                                                 .FACTOR = \{\langle N, k \rangle \mid \exists d \in [k] . (d|N)\} :הגדרה:
                                                                                                                               .FACTOR טענה: קיים מוודא פולינומי
                                                                                 .SUBSETSUM = \{\langle S,t \rangle \mid (S \subseteq \mathbb{N}) \land (\exists T \subseteq S. \sum_{i \in T} i = t)\} הגדרה:
```

. $\langle M,x,t \rangle$ אם U מקבלת אזי איז לאחר לכל היותר לכל לאחר א עוצרת על הקלט א פאר א לאחר לכל היותר או לא עוצרת לאחר א צעדים אזי U דוחה את א או לא עוצרת לאחר U צעדים אזי עוצרת או לא עוצרת לאחר לאחר א צעדים אזי שוחה את א או לא עוצרת לאחר א צעדים איזי שוחה את א או לא עוצרת לאחר א צעדים איזי שוחה את א או לא עוצרת לאחר א צעדים איזי שוחה את א או לא עוצרת לאחר א צעדים איזי שוחה את א או לא עוצרת לאחר א צעדים איזי שוחה את א או לא עוצרת לאחר א צעדים איזי שוחה את א או לא עוצרת לאחר א צעדים איזי שוחה את א או לא עוצרת לאחר לאחר איזי שוחה את או לא עוצרת לאחר לכל היותר את או לא עוצרת לאחר לכל היותר את או לא עוצרת לאחר לכל היותר את או לא עוצרת לאחר לא עוצרת לאחר את או לא עוצרת לאחר לכל היותר את או לא עוצרת לאחר את או לא עוצרת לאחר לא עוצרת לא עוצרת לאחר לא עוצרת לא עוצרת

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

.DTime $(t\left(n
ight))\subsetneq$ DTime $(T\left(n
ight))$ אזי $t\left(n
ight)=o\left(rac{T(n)}{\log(T(n))}
ight)$ חשיבה בזמן ותהא $T:\mathbb{N} o\mathbb{N}$ אזי $T:\mathbb{N} o\mathbb{N}$

 $\mathcal{O}\left(T^{2}\left(n
ight)
ight)$ שרצה בזמן M' שרצה בזמן $T\left(n
ight)>n$ באשר דותהא $T:\mathbb{N} o\mathbb{N}$ שרצה מ"ט רב־סרטית שרצה בזמן דותהא

 $\mathcal{O}\left(T^{3}\left(n
ight)
ight)$ שרצה בזמן M' שרצה מ"ט $T\left(n
ight)$ אזי קיימת מ"ט $T:\mathbb{N} o\mathbb{N}$ שרצה בזמן תהא $T:\mathbb{N} o\mathbb{N}$

מתקיים $x\in \Sigma^n$ אולכל ולכל $T:\mathbb{N} o \mathbb{N}$ עבורה לכל מטל"ד אזי איי תולינג לא־דטרמיניסטית: תהא אול מטל"ד אזי מטל"ד אזי אולכל מיורינג לא־דטרמיניסטית:

עבורה M שרצה בזמן M שרצה בזמן M אזי קיימת מ"ט M שרצה בזמן N ותהא N מטל"ד שרצה N שרצה בזמן N שרצה בזמן N

צעדים. $C \cdot t \log{(t)}$ צעדים $U \bullet$

 $L\left(M
ight)=L\left(M'
ight)$ עבורה

 $L\left(M\right)=L\left(M'\right)$ עבורה

L(N) = L(M)

 $.T\left(n
ight)$ בעומק לכל היותר בעומק כי

.DTime $(n^c) \subsetneq$ DTime (n^d) אזי $1 \le c < d$ מסקנה: יהיו

```
.ACC_{\mathcal{NP}} = \{\langle M, x, 1^t \rangle \mid צעדים t אחרי לכל היותר מקבלת לכל M(x, w) עבורו w קיים w
                                                                                                                                                                    .ACC_{\mathcal{NP}} \in \mathcal{NPC} טענה:
                                                                          A\in\mathcal{NPC} אזי A\leq_p B וכן A\in\mathcal{NPC} שפות באשר A,B\in\mathcal{NP} אזי אזי
                                                                                                    .C\left(x
ight)=1 המקיים x\in\left\{ 0,1
ight\} ^{n} מעגל ספיק: מעגל עבורו קיים
            .arphi = igwedge_{i=1}^migee_{i=1}^k(A)_{i.k} המקיימת A\in M_{m	imes k}\left(\{p_i\}\cup\{\lnot p_i\}
ight) וקיימת וקיים וקיימת m\in\mathbb{N} בסוק arphi\in CNF פסוק: פסוק
                                                                                              .kSAT = \{\langle \varphi \rangle \mid (\varphi \in kCNF) \land (ספיקה) \} אזי k \in \mathbb{N}_+ יהי יהי הגדרה: יהי
                                                                                                                                                .kSAT \in \mathcal{NP} אזי k \in \mathbb{N}_+ טענה: יהי
                                                                                                                                                                               .2SAT \in \mathcal{P} :טענה
                                                                                                                                                         .3SAT \in \mathcal{NPC} :משפט קוק־לוין
                                                                                                                   .kSAT \leq_p \ellSAT אזי k \leq \ell באשר k, \ell \in \mathbb{N}_+ טענה: יהיו
                                                                                                                             .kSAT \in \mathcal{NPC} אזי k \in \mathbb{N} \setminus \{0,1,2\} מסקנה: יהי
                                                                                                                                                                   .3SAT \leq_p CLIQUE משפט:
                                                                                                                                                             .CLIQUE, IS \in \mathcal{NPC} מסקנה:
                                                                                        סימון: תהא v השמה אזי A\in M_{m\times k}\left(\{p_i\}\cup\{\neg p_i\}\right) האז A\in M_{m\times k}\left(\{p_i\}\cup\{\neg p_i\}\right) . N\left(\bigwedge_{i=1}^m\bigvee_{j=1}^k\left(A\right)_{i,k},v\right)=\left|\left\{i\in[m]\;\middle|\;\overline{v}\left(\bigvee_{j=1}^k\left(A\right)_{i,k}\right)=\mathrm{True}\right\}\right| . C-\mathrm{CNF}=\left\{\left\langle\varphi,k\right\rangle\;\middle|\;\left(\varphi\in\mathrm{CNF}\right)\wedge\left(\exists v\left(N\left(\varphi,v\right)=k\right)\right)\right\} הגדרה:
                                                                                                                                                                  .C - \mathtt{CNF} \in \mathcal{NPC} :טענה
                                                                                                                      .DNFSAT = \{\langle \varphi \rangle \mid (\varphi \in DNF) \land (\varphi \in \varphi)\} הגדרה:
                                                                                                                                                                           .DNFSAT \in \mathcal{P} :טענה
                                                                                                C - DNF = \{ \langle \varphi, k \rangle \mid (\varphi \in DNF) \land (\exists v (N (\varphi, v) = k)) \} הגדרה:
                                                                                                                                                          C - CNF \leq_p C - DNF :
                                                                                                                                                               .C-{	t DNF}\in {\cal NPC} מסקנה:
                                                         .PARTITION = \left\{S\subseteq\mathbb{N}\mid (מולטי קבוצה S)\wedge\left(\exists T\subseteq S\left(\sum_{i\in T}i=\sum_{i\in S\setminus T}i\right)\right)
ight\} הגדרה:
                                                                                                                                                               .PARTITION \in \mathcal{NPC} טענה:
                                         (u \in C) \lor (v \in C) מתקיים \{u,v\} \in E עבורה לכל עבורה לכל איז מרטיים: יהי
                                                                                         .VC = \{\langle G,k\rangle\mid k גרף גרף א מכוון בעל כיסוי קודקודים מגודל G\}
                                                                                                                                                                            .VC \in \mathcal{NPC} :טענה
                                                                                                              \mathcal{B}\subseteq igcup_{n=1}^\infty \left(\Sigma^n	o\Sigma
ight) בסיס פונקציות: יהי \Sigma אלפבית אזי
לכל f_i:\Sigma^{k_i}	o\Sigma באשר בסיס פונקציות מעל תהיינה k_1\dots k_n\in\mathbb{N}_+ תהיינה מעל בסיס פונקציות מעל בסיס בסיס פונקציות מעל
                                       המקיים \{f_1\dots f_n, x_1\dots x_m, y_1\dots y_k\} מעל מינה x_1\dots x_m, y_1\dots y_k\in \Sigma ותהיינה i\in [n]
```

 $p\in\mathbb{N}[x]$ פונקציה חשיבה פולינומית: תהא $D\subseteq\Sigma$ אזי $f:D o (\Gamma\backslash\{\sqcup\})^*$ אזי $D\subseteq\Sigma$ אזי חשיבה פולינומית: תהא

f שפה אזי רדוקציית מיפוי $B\subseteq \Delta^*$ שפה ותהא $A\subseteq \Sigma^*$ תהא הא $\Sigma\subseteq \Delta$ אלפבייתים באשר אפבייתים באשר באשר אותהא

.SUBSETSUM טענה: קיים מוודא פולינומי

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

מ־A ל־B חשיבה פולינומית.

 $A \leq_p B$ אזי

.CLIQUE \leq_p IS :טענה

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

 (\mathcal{L}^-) שפה אזי פולינומי מוודא פולינומי ל $(\mathcal{L}\in\mathcal{NP})$ שפה אזי שפט: תהא שפט: תהא

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

 $\mathcal{NPH} = \{\mathcal{L} \mid \forall L \in \mathcal{NP} (L \leq_p \mathcal{L})\}$ שפה \mathcal{NP} יקשה:

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

 $\mathcal{NPC} = \mathcal{NP} \cap \mathcal{NPH}$ שפה \mathcal{NP} שפה

. אעדים $p\left(|x|\right)$ אחרי אחרי לכל עוצרת עוצרת אחרי מתקיים כי מתקיים כי מתקיים כי $M\left(x\right)$ אתקיים כי לכל

```
חסר מעגלים מכוונים. G ullet
```

- $\deg^-(x_i) = 0$ מתקיים $i \in [m]$ לכל
- $\deg^-\left(f_i
 ight)=k_i$ מתקיים $i\in[n]$ לכל
- $\deg^+(y_i)=0$ וכן $\deg^-(y_i)=1$ מתקיים $i\in[k]$ לכל •

הערה: נשמור על הטרמינולוגיה ממעגל בוליאני כהכללה טבעית.

 $z\in \left\{0,1
ight\}^n$ יהי $T\left(n
ight)$ מ"ט שרצה מ"ט שרצה בזמן הא חשיבה בזמן האי חשיבה בזמן הא חשיבה בזמן חשיבה בזמן $T:\mathbb{N} o \mathbb{N}$ יהי $T\left(n
ight)$ יהי הקונפיגורציות/טאבלו: תהא $T:\mathbb{N} o \mathbb{N}$ אזי $T\left(n
ight)$ אזי $T\left(n
ight)$ אזי $T\left(n
ight)$ המקיימת הקיימת בזיער הריצה של $T:\mathbb{N} o \mathbb{N}$ אזי $T\left(n
ight)$ אזי $T\left(n
ight)$ המקיימת בזיער המקיימת הריצה של $T\left(n
ight)$ אזי $T\left(n
ight)$ אזי $T\left(n
ight)$ המקיימת בזיער המקיימת בזיער הריצה של מיי

 $.\delta\left(q_r,\sigma
ight)=\left(q_r,\sigma,R
ight)$ וכן וכן $\delta\left(q_a,\sigma
ight)=\left(q_a,\sigma,R
ight)$ כי נניח כי הקונפיגורציות נניח כי

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

 $\Sigma \uplus \Gamma$ נגדיר מעגלים מעל מ"ט רצה בזמן (T(n) מ"ט רצה בזמן באשר באמן באשר מעל מאט נדיר מעגלים מעל $T:\mathbb{N} \to \mathbb{N}$ נגדיר מעגלים מעל

- $.C_{ ext{inp}}\left(z
 ight)=R_{0}\left(au_{M,z}
 ight)$ אזי $z\in\Sigma\uplus\Gamma$ יהי •
- $.C_{\mathrm{next}}\left(R_{i}\left(au_{M,z}
 ight)
 ight)=R_{i+1}\left(au_{M,z}
 ight)$ איי $i\in\left\{ 0,\ldots,T\left(n
 ight)-1
 ight\}$ ויהי $z\in\Sigma\uplus\Gamma$ יהי יהי
 - $.C_{ ext{out}}\left(R_{T(n)}\left(au_{M,z}
 ight)
 ight)=M\left(z
 ight)$ אזי $z\in\Sigma\uplus\Gamma$ יהי \bullet
 - $.C_{M,n}^{\Sigma \uplus \Gamma}\left(z
 ight) = \left(C_{ ext{out}} \circ C_{ ext{next}} \circ \ldots \circ C_{ ext{next}} \circ C_{ ext{inp}}
 ight)\left(z
 ight)$ אזי $z \in \Sigma \uplus \Gamma$ יהי •

טענה: תהא T(n) אזי איי וכן קיימת T(n) אזי איי וכן קיימת M מ"ט רצה בזמן באשר $T:\mathbb{N} \to \mathbb{N}$ אזי וכן קיימת $f(n) = \left\langle C_{M,n}^{\Sigma \uplus \Gamma} \right\rangle$ עבורה $f(n) = \left\langle C_{M,n}^{\Sigma \uplus \Gamma} \right\rangle$ עבורה עבורה איי ופונקציה f(n)

 $C^{\Sigma \oplus \Gamma}_{M,n}(z)=M\left(z
ight)$ אזי $z\in \Sigma \oplus \Gamma$ וויהי $T\left(n
ight)$ וויהי $T\left(n
ight)$ אזי $T\left(n
ight)$ מסקנה: תהא $T\left(n
ight)$ חשיבה בזמן באשר $T\left(n
ight)$ תהא $T\left(n
ight)$ חשיבה בזמן באשר פולינומית $T\left(n
ight)$ עבורה לכל מעגל בוליאני $T\left(n
ight)$ מעגל בוליאני מעל בוליאני מעל $T\left(n
ight)$ מעגל בוליאני $T\left(n
ight)$ מעגל בוליאני מעל בוליאני מעל בוליאני $T\left(n
ight)$ מעגל בוליאני מעל בוליאני מעל בוליאני באשר $T\left(n
ight)$ לכל $T\left(n
ight)$ בסיס דה־מורגן באשר $T\left(n
ight)$ לכל $T\left(n
ight)$ מעגל בוליאני מעל בוליאני באשר בוליאני מעל בוליאני באשר בוליאני באשר בוליאני בוליאני בוליאני מעל בוליאני מעל בוליאני בוליאני

למה: תהא $T\left(n\right)$ אזי קיימת פונקציה חשיבה t בזמן משיבה t חשיבה t מתקיים (t מתקיי

.CIRSAT $\in \mathcal{NPC}$:טענה

.CIRSAT $\leq_p 3$ SAT :טענה

.3SAT \leq_p SUBSETSUM :טענה

 $\mathsf{SUBSETSUM} \in \mathcal{NPC}$:מסקנה

.3SAT \leq_p HAMPATH :טענה

. HAMPATH $\in \mathcal{NPC}$:מסקנה

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

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

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

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

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

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

 $\mathsf{FACTOR} \in \mathcal{NP} \cap \mathsf{co}\mathcal{NP}$:

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

.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

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

- . דוחה $M\left(x\right)$ אשר אינו קידוד של שלשת מטריצות $x\in\left\{ 0,1\right\} ^{st}$ דוחה לכל
- . מקפינם $M\left(x\right)$ מקבינת $x=\langle A,B,C\rangle$ וכן $A\cdot B=C$ המקיימות $A,B,C\in M_n\left(\mathbb{Z}\right)$ מתקיים $x\in\left\{0,1\right\}^*$ מקבלת.

מתקיים $x=\langle A,B,C \rangle$ וכן $A\cdot B \neq C$ המקיימות $A,B,C \in M_n\left(\mathbb{Z}\right)$ שבורו קיימות $x\in\left\{0,1\right\}^*$ $\mathbb{P}(x) = M(x)$ מקבלת) M(x)

Cנוסחה אריתמטית: יהי $\mathbb F$ שדה ויהי מעגל מעל $\mathbb F$ עם הבסיס אזי נוסחה $\mathbb F$ אזי נוסחה ב־

 $arphi\equiv 0$ אזי $arphi\left(x_1\ldots x_n
ight)=0$ מתקיים $x_1\ldots x_n\in\mathbb{F}$ אזי עבורה לכל עבורה לכל עבורה לכל

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

 $\overline{ZE_{\mathbb{Z}_2}}\in\mathcal{NPC}$:טענה

 2^h טענה: תהא φ נוסחה אריתמטית בעומק מעל $\mathbb F$ מעל מעל אזי פוסחה אריתמטית בעומק סענה:

 $(arphi\equiv 0)\Longleftrightarrow (f=0)$ אזי $\deg(f)<|\mathbb{F}|$ באשר $f\in\mathbb{F}[x_1,\ldots,x_n]$ המחשבת מעל \mathbb{F} המחשבת ענה: תהא φ $\mathsf{ZE}_{\mathbb{F}} \in \mathcal{R}$ מסקנה: יהי \mathbb{F} שדה אינסופי אזי

 $\deg\left(\prod_{i=1}^n x_i^{d_i}
ight) = \sum_{i=1}^n d_i$ איזי $d_1 \dots d_n \in \mathbb{N}$ דרגה טוטאלית של מונום: יהיו

 $\operatorname{deg}\left(\sum_{i=1}^{k}\prod_{j=1}^{n}x_{j}^{d_{i,j}}
ight)=\max\left\{\operatorname{deg}\left(\prod_{j=1}^{n}x_{j}^{d_{i,j}}
ight)\left[i\in[k]
ight\}$ איז $d\in M_{k imes n}\left(\mathbb{N}
ight)$ הדגה טוטאלית של פולינום: תהא $\mathbb{P}_{a_1,\ldots,a_n\leftarrow S}\left(f\left(a_1\ldots a_n
ight)=0
ight)\leq rac{\deg(f)}{|S|}$ סופית אזי f
eq 0 באשר באשר $f\in\mathbb{F}\left[x_1,\ldots,x_n
ight]$ באשר באשר למה שוורץ־זיפל: יהי מסקנה: קיימת מ"ט M עבורה לכל $x \in \{0,1\}^*$ מתקיים

- . דוחה $M\left(x\right)$ מתקיים מעל אינו קידוד של נוסחה אריתמטית אריתמטית x
- .poly (|arphi|) מקבלת בזמן $M\left(x
 ight)$ מתקיים $x=\langlearphi
 angle$ וכן arphi=0 מתקיים מעל π מקבלת בזמן ϕ
- .poly $(|\varphi|)$ בזמן בזמן M(x) מקבלת M(x) בזמן $\varphi \neq 0$ וכן $\varphi \neq 0$ מתקיים $\varphi \neq 0$ מקבלת מעל $\varphi \neq 0$ המקיימת $\varphi \neq 0$ מחשר אריתמטית מעל $\varphi \neq 0$ המקיימת $\varphi \neq 0$ בזמן $\varphi \neq 0$ באשר x\$r איז התחלתית קונפיגורציה תכן איז מ"ט דו־סרטית איז מ"ט דו־סרטית תונפיגורציה התחלתית תהא תחלתית מכונת מיורינג אקראית: $r \in \{0,1\}^{T(|x|)}$

T חסם עליון לזמן ריצה של מכונת טיורינג אקראית: תהא תהא $T\left(n
ight)$ חשיבה בזמן ותהא מכונת טיורינג אקראית אזי $M\left(x;r
ight)=M\left(x\$r
ight)$ אזי $r\in\left\{ 0,1
ight\} ^{T(|x|)}$ ויהי $x\in\left\{ 0,1
ight\} ^{*}$ אזי היצה $T\left(n
ight)$ יהי זמן: תהא M מ"ט אקראית עם זמן ריצה וויהי $T\left(n
ight)$ יהי x אזי $x \in \{0,1\}^{T(|x|)}$ ויהי $x \in \{0,1\}^*$ אזי $x \in \{0,1\}^*$ יהי $x \in \{0,1\}^*$ אזי אזי מכונת טיורינג אקראית: תהא x אזי $x \in \{0,1\}^{T(|x|)}$ יהי $x \in \{0,1\}^*$ יהי יהי אקראית עם אקראית עם מ"ט אקראית: תהא אקראית: $x \in \{0,1\}^{T(|x|)}$ יהי יהי יהי אקראית. $r \in \{0,1\}^{T(|x|)}$ עבור $M\left(x;r
ight)$ משתנה מקרי לקבלת $M\left(x;r
ight)$ עבור $M\left(x;r
ight)$ יהי $M\left(x;r
ight)$ משתנה מקרי לקבלת עם זמן ריצה $M\left(x;r
ight)$ יהי $M\left(x;r
ight)$ משתנה מקרי לקבלת עם זמן ריצה $M\left(x;r
ight)$

המקיימת כי החל ממקום T(n) המקיימת מ"ט אקראית מ"ט אקראית שפה בורה שפה עבורה שפה $\alpha:\mathbb{N} \to [0,1]$ המקיימת מ מסויים $n \in \mathbb{N}$ מתקיים

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

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

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

 $\mathcal{RP}(1) = \mathcal{P}$:טענה

 $\mathcal{RP}\left(lpha
ight)\subseteq\mathcal{NP}$ אזי ממקום מסויים 0<lpha באשר $lpha:\mathbb{N}
ightarrow \left[0,1
ight]$ עענה: תהא

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

טענה: תהא $\alpha:\mathbb{N} o[0,1]$ אזי $\mathcal{L}\in\mathrm{co}\mathcal{RP}\left(lpha
ight)$ אם זיים אקראית \mathcal{L} עם זמן ריצה פולינומי $\alpha:\mathbb{N} o[0,1]$ המקיימת $\alpha:\mathbb{N} o[0,1]$ כי החל ממקום מסויים $n\in\mathbb{N}$ מתקיים

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

 $\mathrm{ZE}_{\mathbb{R}}\in\mathrm{co}\mathcal{RP}\left(0.99
ight)$ טענה: $\mathcal{RP}\left(n^{-c}
ight)=\mathcal{RP}\left(1-2^{-n^d}
ight)$ אזי $c,d\in\mathbb{N}$ טענה: יהיו

 $\mathcal{RP} = \mathcal{RP}\left(0.5
ight): \mathcal{RP}$ שפה

 $\cos \mathcal{RP} = \cos \mathcal{RP} (0.5) : \cos \mathcal{RP}$ שפה

המקיימת כי החל T(n) המקיימת מ"ט אקראית מ"ט אקראית בורה שפה \mathcal{L} המקיימת שפה $\alpha,\beta:\mathbb{N} \to [0,1]$ המקיימת כי החל ממקום מסויים $n\in\mathbb{N}$ מתקיים

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

```
\mathcal{L} \in \mathcal{BPP}(\alpha, \beta) אזי
                                                                                                                                     \mathcal{BPP} = \mathcal{BPP}\left(\frac{1}{2}, \frac{2}{3}\right) : \mathcal{BPP} שפה
                                                                                                       \mathcal{RP}\left(\alpha\right)=\mathcal{BPP}\left(0,\alpha\right) אזי \alpha:\mathbb{N}\rightarrow\left[0,1\right] 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] מענה: תהא
                    \mathcal{BPP}\left(lpha,\delta
ight)\subseteq\mathcal{BPP}\left(eta,\gamma
ight) אזי ממקום מסויים מlpha\leqeta\leq\gamma\leq\delta עבורן lpha,eta,\gamma,\delta:\mathbb{N}	o[0,1]
               \mathbb{P}\left(\left|p-\frac{1}{n}\sum_{i=1}^nA_i\right|\geq\delta
ight)\leq 2^{-\Theta\left(\delta^2n
ight)} אזי A_1,\ldots,A_n\sim \mathrm{Ber}\left(p
ight) ויהיו n\in\mathbb{N} יהי \delta>0 יהי \delta>0
טענה: יהיו n^{-c} \leq lpha\left(n\right) \leq 1-n^{-c} אויים מסויים מסויים מסויים מסויים מסויים מסויים מסויים מסויים מסויים אזי c,d \in \mathbb{N}
                                                                                          \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)
                                                   (c_1\$c_2\$\dots\$c_k)^i=c_i קונפיגורציה אזי קונפיגורציה ותהא מ"ט k־סרטית ותהא מרטית ההא מינפיגורציה אזי מינוני תהא
                                                                          A אזי x \setminus A הינה המחרוזת x \in \Sigma^* ותהא x \in \Sigma^* אזי x \in \Sigma^* הינה המחרוזת אברי
c_0=q_0x באשר באר היבוכיות סיבוכיות בעלת סיבוכיות מקום: תהא או מ"ט תלת־סרטית S:\mathbb{N}	o\mathbb{N} באשר באר מכונת סיורינג בעלת סיבוכיות מקום: תהא
                                                                                                                            וכן i \in [n] לכל לc_i מתקיים מתקיים
                                                                                                   c_i^1 = x \backslash Q סרט לקריאה בלבד: לכל i \in [n] מתקיים •
                                                                                       |c_{i-1}^2| \leq S(n) + 1 מתקיים i \in [n] לכל •
                                             (c_{i-1}^3ackslash Q)_i=\left(c_i^3ackslash Q
ight)_i מתקיים מתקיים j\in\left[\left|c_{i-1}^3
ight|
ight] ולכל i\in[n] ולכל
                                S אזי אוי מקום ריצה של מכונת טיורינג: תהא S:\mathbb{N} 	o \mathbb{N} ותהא של מיש בעלת סיבוכיות מקום אזי ותהא
                                                                                           הערה: נקרא למכונת טיורינג בעלת סיבוכיות מקום מכונט טיורינג.
                                                 .DSpace (S\left(n
ight))=\{L\left(M
ight)\mid\mathcal{O}\left(S\left(n
ight)
ight) במקום שרצה במקום M\} אזי S:\mathbb{N}	o\mathbb{N} הגדרה: תהא
                                                                                                               \mathcal{PSPACE} = \bigcup_{c \in \mathbb{N}} \mathsf{DSpace}\left(n^c\right) : \mathcal{PSPACE} שפה
```

 $(S\left(n
ight))_2$ את משבת את מ"ט א הקלט הקלט איז איז מא המקיימת לכל M כי $n\in\mathbb{N}$ כי M על הקלט את עבורה $S:\mathbb{N} o\mathbb{N}$ מחשבת את פונקציה מיימת מ"ט א

 $\log{(n)}$ פונקציה חשיבה במקום לוגריתמי: תהא $D\subseteq\Sigma$ אזי $D=(\Gamma\setminus\{\sqcup\})^*$ עבורה קיימת מ"ט מ

רדוקציית מיפוי $B\subseteq \Delta^*$ שפה ותהא במקום לוגריתמי: יהיו Σ,Δ אלפבייתים באשר באר Σ,Δ שה תהא במקום לוגריתמי: יהיו

שפה ותהא $A\subset \Sigma^*$ רדוקציית מיפוי במקום $A\subset \Sigma^*$ שפה תהא $\Sigma\subset \Delta$ אלפבייתים באשר Σ רדוקציית מיפוי במקום

.DSpace $(t\left(n\right))\subsetneq$ DSpace $(T\left(n\right))$ איז $t\left(n\right)=o\left(S\left(n\right)\right)$ חשיבה במקום ותהא $S:\mathbb{N} o\mathbb{N}$ חשיבה המקום:

 $\mathcal{LOGSPACE} = \mathsf{DSpace}\left(\log\left(n\right)\right) : \mathcal{LOGSPACE}$ שפה

.DSpace (1) = DSpace $(\log(\log(n))) = \{L \mid L$ רגולרית $L\}$.DTime $(T(n)) \subseteq D$ Space (T(n)) אינה: תהא T חשיבה בזמן אזי

.DSpace $(S(n))\subseteq \operatorname{DTime}\left(2^{\mathcal{O}(S(n))}\right)$ אזי $S\geq \log$ באשר באשר $S:\mathbb{N} \to \mathbb{N}$ מענה: תהא

 $\mathcal{LOGSPACE} = L$:סימון:

 $\mathcal{NP} \subseteq \mathcal{PSPACE}$ טענה:

מסקנה: $\mathcal{PSPACE}\subseteq\mathcal{P}$ מסקנה: $\mathcal{PSPACE}\subseteq\mathcal{EXP}$

מסקנה: מסקנה: $\mathcal{PSPACE} \subsetneq \mathcal{PSPACE}$ מסקנה: לפחות אחד מהבאים נכון $\mathcal{LOGSPACE} \subsetneq \mathcal{P}$ • \mathcal{PSPACE} •

מ־A ל־B חשיבה במקום לוגריתמי.

 $A \leq_{p} B$ אזי $A \leq_{L} B$ טענה: תהיינה A, B שפות עבורן

. $\mathcal{O}\left(S\left(n\right)\right)$ במקום

f את המחשבת

 $A \leq_L B$ לוגריתמי אזי