```
.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\notin 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 גר א וותהיינה מכוון וותהיינה וותהיינה וווi\in[n]
                                                                                                                   .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 אויים מעל בסיס אויים מעגל אזי קיים 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 \mathcal{C} משפחה של מעגלים
                                            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  $\Sigma$  המקיימת אלפבית: מילים: יהי  $\Sigma$  אלפבית אזי  $\Sigma^*=\bigcup_{n=0}^\infty \Sigma^n$ 

 $L \subset \Sigma^*$  אלפבית אזי אונ  $\Sigma$  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:

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

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

 $L^R=\{w^R\mid w\in L\}$  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 עQ, \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 A\} מקבל את אס"ד אזי יהי A אס"ד איזי אס"ד אוטומט סופי דטרמיניסטי: יהי
                                                  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} \bullet
                                                                                                                                       . 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
                                                (Q,\Sigma,\delta,S,F) אסלד"ם איז איז אסלד"ם איז אסלד"ם איז אסלד"ם איז איז אסלד"ם איז איז אסלד"ם איז
                                                   F אסלד"ם אזי אסלד"ם מקבלים באוטומט אסופי לא־דטרמיניסטי מינוס: יהי (Q, \Sigma, \delta, S, F) אסלד"ם אזי
\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

 $\hat{\delta}\left(S,x
ight)\cap F
eq \varnothing$  המקיים אזי  $x\in\Sigma^*$  המקיים אוטומט סופי לא־דטרמיניסטי מינוס מקבל מילה: יהי  $q_i\in\delta\left(q_{i-1},x_i
ight)$  אזי ( $q_i\in\delta\left(q_{i-1},x_i
ight)$ 

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

 $\Sigma_{\varepsilon} = \Sigma \cup \{\varepsilon\}$ אזי אלפבית אזי יהי יהי לפבית אזי יהי

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

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

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

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

F אזי אוי אסל"ד אזי עסל"ד אזי אסל"ד אזי אסל"ד אזי אסל"ד אזי אסל"ד אזי מצבים מקבלים באוטומט סופי לא־דטרמיניסטי: יהי

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

פונקציית המעברים המורחבת: יהי  $(Q,\Sigma,\delta,S,F)$  אסל"ד אזי  $\hat{\delta}:\mathcal{P}\left(Q\right) imes\Sigma^* o\mathcal{P}\left(Q\right)$  אסל"ד אזי  $(Q,\Sigma,\delta,S,F)$  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  $(Q,\Sigma,\delta,S,F)$  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  $x\in\Sigma^k$  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 אסל"ד אזי קיים אס אז אסל"ד אזי קיים אס אס אד N

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

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

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

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

- $L(\varnothing) = \varnothing \bullet$
- $.L\left( a
  ight) =\left\{ a
  ight\}$  אזי  $a\in\Sigma_{arepsilon}$  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

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

הערה: קיים סדר פעולות לביטויים רגולריים

```
. איחוד
                                    (L(r)=\mathcal{L} עבורו r\in R(\Sigma) עבורית)\Longleftrightarrow(קיים L(r)=\mathcal{L} עבורו r\in \mathcal{L} עבורו r\in \mathcal{L} עבורו
שפה ניתנת לניפוח: שפה \mathcal{L} וכן |y|>0 עבורם לכל w\in\mathcal{L} באשר w\in\mathcal{L} עבורם לכל \ell>0 עבורם וכן
                                                                                                       xy^kz\in L מתקיים k\in\mathbb{N} וכן לכל w=xyz
                                                          \ell ניתנת לניפוח עבורו \ell>0 טענה למת הניפוח: תהא שפה רגולרית אזי קיים
                                                                  \min\{\ell\in\mathbb{N}_+\mid\ell ניתנת לניפוח: תהא \mathcal{L} שפה רגולרית אזי \mathcal{L} ניתנת לניפוח: תהא
                                                                                         טענה: \{x \in \{0,1\}^* \mid \#_0(x) = \#_1(x)\} אינה רגולרית.
                                                                                                                  טענה: \{0^i 1^j \mid i > j\} אינה רגולרית.
                                                                                                       . טענה: \{a^p \mid a \in \Sigma, ראשוני p\} אינה רגולרית
                                      . 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 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^* תהא הגדרה: תהא
                                                                                              . טענה: תהא \Sigma^* \subseteq L שפה אזי ליחס שקילות. L \subseteq \Sigma^*
                                                                    |Q|>|\Sigma^*/_{\sim_A}|>|\Sigma^*/_{\sim_{L(A)}}| אס"ד אזי אס"ד אזי ויהי A אס"ד אזי
                                                                                            מסקנה: תהא L \subseteq \Sigma^* סופית. L \subseteq \Sigma^* סופית.
                                                                  .(סופית) בייהיל־נרוד: תהא בה אזי עם האזי L\subseteq \Sigma^* משפט מייהיל־נרוד: תהא בה עם בה עם האזי עם בייהיל־נרוד: תהא
y\sim_L x_i אזי y\in \Sigma^* ויהי \Sigma^*/_{\sim_L} שפה באשר y\in \Sigma^*/_{\sim_L} סופית תהא \{x_1\dots x_n\} קבוצת נציגים של ב\Sigma^*/_{\sim_L} ויהי
                                                                                                                                               .Class (y) = i
אוט אוט סופי דטרמיניסטי המחלקות: תהא \Sigma^*/_{\sim_L} שפה באשר באשר שפה באשר \{x_1\dots x_n\} קבוצת נציגים של ב\Sigma^*/_{\sim_L} אוי אס"ד אוטומט סופי דטרמיניסטי המחלקות:
                                                                                                                                    באשר (Q, \Sigma, \delta, q_0, F)
                                                                                                                                    Q = [|\Sigma^*/\sim_L|] \bullet
                                                                                                                            .\delta(i,\sigma) = \text{Class}(x_i\sigma) \bullet
                                                                                                                                     .q_0 = \operatorname{Class}\left(\varepsilon\right) \bullet
                                                                                                                          .F = \{i \in Q \mid x_i \in L\} \bullet
טענה: תהא L אס"ד המחלקות של \Sigma^*/_{\sim_L} שפה באשר באשר \Sigma^*/_{\sim_L} סופית תהא \Sigma^*/_{\sim_L} סופית תהא באשר באשר באשר אס"ד המחלקות של ויהי
                                                                                                                    \hat{S_A}(q_0,y) = \text{Class}(y) אזי y \in \Sigma^*
               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 מעל מעל N מעל מעל אזי קיים אסל"ד N מעל מעל מעל מעל יהי n\in\mathbb{N}_{+} איי קיים אסל"ד
                          |Q|\geq 2^n אזי L\left(A
ight)=\left\{x\in\left[n
ight]^*\mid\exists\sigma\in\Sigma.\#_{\sigma}\left(x
ight)=0
ight\} אזי מעל n\in\mathbb{N}_{+} אזי n\in\mathbb{N}_{+} טענה: יהי n\in\mathbb{N}_{+} איזי
(Q,\Sigma,\Gamma,\delta,q_0,q_a,q_r) אזי \delta:(Q\setminus\{q_a,q_r\})	imes\Gamma	o Q	imes\Gamma	imes\{L,R\} באשר q_a
eq q_r ותהא
                                                                                Q מ"ט אזי Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r מצבים במכונת טיורינג: תהא
                                                                               \Sigma אזי מ"ט מ"ט (Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r) אלפבית במכונת טיורינג: תהא
                                                                         \Gamma אזי טייט מייט מיי(Q,\Sigma,\Gamma,\delta,q_0,q_a,q_r) אלפבית סרט במכונת טיורינג: תהא
                                                                    .\delta אזי מעברים במכונת טיורינג: תהא (Q,\Sigma,\Gamma,\delta,q_0,q_a,q_r) מ"ט מיט מיט מינקציית מעברים
                                                                        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) מצב מקבל במכונת טיורינג: תהא
                                                                           Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r מ"ט אזיQ, \Sigma, \Gamma, \delta, q_0, q_a, q_r מצב דוחה במכונת טיורינג: תהא
                                                                                                         c \in \Gamma^*Q\Gamma^* מ"ט אזי M מהא M
                            c=q_0v המקיימת v\in\Sigma^* עבורה קיים עבורה מ"ט אזי קונפיגורציה מונפיגורציה מ"ט אזי קונפיגורציה מ"ט מ"ט אזי קונפיגורציה אורציה מחלתית:
                      .c=uq_av המקיימים u,v\in \Sigma^* עבורה קיימים עבורה מונפיגורציה מיט אזי קונפיגורציה מקבלת: תהא u,v\in \Sigma^* המקיימים עבור
                         c=uq_rv אזי המקיימים u,v\in \Sigma^* עבורה קיימים עבורה קיימים אזי קונפיגורציה M מ"ט אזי קונפיגורציה c\in \Gamma^*Q\Gamma^*
                                                                               cעם עם cעם אזי נזהה אזי נזהה dעם מ"ט ותהא d
```

סגור קליני.שרשור.

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  $q,q'\in Q$  וכן  $u,v\in\Gamma^*$  וכן  $a,b,b'\in\Gamma$ 
  - c'=q'b'v וכן  $\delta\left(q,b
    ight)=\left(q',b',L
    ight)$  וכן c=qbv עבורם  $q,q'\in Q$  וקיימים  $u,v\in\Gamma^*$  וקיימים  $b,b'\in\Gamma$
  - 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' היימת  $\bullet$
- $L\left( B
  ight) =L\left( B^{\prime}
  ight)$  המקיימת  $B^{\prime}$  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  $\Sigma$  אלפבית יהי  $\Sigma$  אלפבית וכן היה  $\Sigma\subseteq \Gamma$  אתהא  $\Sigma\subseteq \Gamma$  ההא  $\Sigma\subseteq \Gamma$  קבוצה סופית יהי  $\Sigma$  אלפבית יהי  $\Sigma\subseteq \Gamma$  ההא  $\Sigma\subseteq \Gamma$  ההא  $\Sigma$  היי  $\Sigma$  אוי  $\Sigma$  היי  $\Sigma$  אוי  $\Sigma$  היי ותהא  $\Sigma$  וכן  $\Sigma$  היי ותהא  $\Sigma$  היי ותהא  $\Sigma$  אוי  $\Sigma$  היי וער איי  $\Sigma$  היי וער הא  $\Sigma$  וכן  $\Sigma$  היי וכן

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

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

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 אזי מכונת טיורינג ומכונת טיורינג מכונת אזי מכונת אזי מכונת אזי מכונת אזי מכונת מסקנה: יהי אזי מכונת טיורינג ומכונת אזי מכונת מסקנה: יהי אזי מכונת מכונת מכונת 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 וודל  $(k,\Pi)$  מודל

 $\Pi$  אזי RAM מודל ויהי $(k,\Pi)$  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 אורציה במודל RAM: יהי ורציה מודל

.PC אוי קונפיגורציה:  $(T,R,\operatorname{PC})$  ותהא מודל ( $k,\Pi$ ) אוי יהי יהי קונפיגורציה: יהי מונה התוכנית בקונפיגורציה:

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 הערה: ריצת מודל

טענה: מכונת טיורינג ומודל RAM הם מודלים שקולים.

 $\square\in\Gamma\setminus\Sigma$  מכונת טיוריגנ לא־דטרמיניסטית (מטל"ד): תהא  $Q
eq\emptyset$  קבוצה סופית יהי  $\Sigma$  אלפבית יהי  $\Gamma$  אלפבית עבורו  $\Sigma\subseteq\Gamma$  וכן  $\Sigma\subseteq\Gamma$  וכן  $\Sigma\subseteq\Gamma$  אזי  $\Sigma$  ( $\Sigma$  אזי  $\Sigma$  באשר  $\Sigma$  ותהא  $\Sigma$  ( $\Sigma$  ותהא  $\Sigma$  וכן  $\Sigma$  וכן  $\Sigma$  וכן  $\Sigma$  וכן  $\Sigma$  וכן  $\Sigma$  וכן  $\Sigma$  אזי עץ קונפיגורציות מתקיים שורש  $\Sigma$  עבורו לכל  $\Sigma$  קונפיגורציות מתקיים ( $\Sigma$  צאצא עורבת  $\Sigma$  עורבת  $\Sigma$ 

 $x \in \Sigma^*$  עבורו קיים עלה מקבל ב־ $x \in \Sigma^*$  אזי אזי אזי מטל"ד מילה: תהא מקבל מילה: תהא

x אינו מתקבל על ידי אינו טיוריגנ לא־דטרמיניסטית דוחה מילה: תהא א מטל"ד אזי  $x \in \Sigma^*$  עבורו מטוריגנ לא־דטרמיניסטית דוחה מילה:

 $L\left(N
ight)=\left\{x\in\Sigma^{*}\mid x$  אזי מקבל אזי מטל"ד מיוריגנ לא־דטרמיניסטית: תהא א מטל"ד מיוריגנ ארדטרמיניסטית: תהא אוי

x את את אדת אלא מקבלת לא מטר"ד אזי איזי איזי אזי אוורינג אוצרת על קלט: תהא את אוצרת על קלט: תהא אוורינג איזירינג ארדטרמיניסטית איז עוצרת על קלט: תהא

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
                                                                                 לא על הסרט לעולם. x$ מתקיים כי x$ לא על הסרט לעולם.
                                                                              . 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 \mathcal{L}\subseteq \Sigma^* מונה לקסיקוגרפי).
                                                                                  \mathrm{co}\mathcal{RE}=\{\mathcal{L}\subseteq\Sigma^*\mid\overline{\mathcal{L}}\in\mathcal{RE}\} אלפבית אזי 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
                                       Mולכל קלט M של M מתקיים (M מקבלת את את אונכל קלט M מקבלת את M
                                            (x) את את M ולכל קלט M של M מתקיים M מתקיים M של 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\}^*
                                                                                    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\left(N
ight)\} מ"ט א המכריעה את ACC מהנכריעה את M מ"ט ממכריעה את
                                                                                                                                    .ACC \notin \mathcal{R} טענה:
                                                        .HALT = \{\langle M, x \rangle \mid \langle M, x \rangle \mid (w"ט) \land (x) \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 עוצרת מכונת טיורינג מחשבת פונקציה: תהא

חשיבה עבורה  $f:\Sigma^* o\Delta^*$  שפה איי איז  $B\subset\Delta^*$  שפה ותהא  $\Sigma\subset\Delta$  תהא באשר באשר באשר  $\Sigma$ . 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 לקבלה: יהי  $\Sigma$  אלפבית אזי

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

f(x)יים אינו בסוף הסרט בסוף x וכן הסרט בסוף אינו

 $A \leq_m B$ 

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

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

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

```
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 לישה: 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 אזי
                                                                                        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{\text{HALT}} \leq_m \text{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
```

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

בזמן  $\mathcal{O}\left(T\left(n\right)\right)$  בזמן

 $T\left(n
ight)=\Omega\left(n
ight)$  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

```
\langle M, x, t \rangle אם M דוחה את x או לא עוצרת לאחר t צעדים אזי t דוחה את t
                                                                                                               צעדים. C \cdot t \log{(t)} צעדים U ullet
            .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}
                                                                                              .DTime (n^c) \subsetneq DTime (n^d) אזי 1 \le c < d מסקנה: יהיו
\mathcal{O}\left(T^2\left(n
ight)
ight) איז קיימת מ"ט M שרצה בזמן T\left(n
ight)>n איז בימן T:\mathbb{N}	o\mathbb{N} שרצה בזמן T:\mathbb{N}	o\mathbb{N} איז קיימת מ"ט T
                                                                                                                                     L\left(M
ight)=L\left(M'
ight) עבורה
\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}
                                                                                                                                     L\left(M\right)=L\left(M'\right) עבורה
x\in \Sigma^n אחרינג לא־דטרמיניסטית: תהא א מטל"ד אזי T:\mathbb{N}	o\mathbb{N} עבורה לכל ולכל x\in \Sigma^n מתקיים תליון לזמן ריצה של מכונת טיורינג לא־דטרמיניסטית: תהא
                                                                                                                           .T\left( n
ight) בעומק לכל היותר בעומק כי
                                             .NTime (T(n))=\{L(N)\mid \mathcal{O}(T(n)) מטל"ד שרצה בזמן N\} אזי T:\mathbb{N}\to\mathbb{N} הגדרה: תהא
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
                                                                                                                                                .L(N) = L(M)
                                                                                                                            \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}} DTime \left(2^{n^k}
ight) :\mathcal{EXP} שפה
                                                                                                        \mathcal{NEXP} = igcup_{k \in \mathbb{N}} NTime \left(2^{n^k}
ight): \mathcal{NEXP} שפה
                                                                                                                                     \mathcal{E} \dot{\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:
                                                                                  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 שפה בהא המקיים מוודא לשפה:
                                                                              . מקבלת V\left(x,w\right) עבורו w\in\Sigma^{*} אזי קיים x\in\mathcal{L} מקבלת.
                                                                           . דוחה V\left(x,w\right) אזי לכל w\in\Sigma^{*} מתקיים כי x
otin\mathcal{L} דוחה.
                                                                                   \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(|x|) צעדים.
                                                                               .CLIQUE = \{\langle G, k \rangle \mid k גרף גרף לא מכוון בעל קליקה מגודל G\} הגדרה:
                                                                                                                     .CLIQUE טענה: קיים מוודא פולינומי
                                                                              \mathsf{LIS} = \{\langle G, k \rangle \mid k גרף גרף לא מכוון בעל קבוצה בת"ל מגודל G\} גרף גרף גרף הגדרה:
                                                                                                                            טענה: קיים מוודא פולינומי ל־IS.
                                                                                                       .FACTOR = \{\langle N, k \rangle \mid \exists d \in [k] . (d|N)\} :הגדרה:
                                                                                                                    .FACTOR טענה: קיים מוודא פולינומי
```

 $\langle M, x, t \rangle$  אם M עוצרת על הקלט x לאחר לכל היותר t צעדים אזי M מקבלת את M

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

 $\mathcal{L}\subseteq \Sigma^*$  משפט: תהא  $\mathcal{L}\subseteq \Sigma^*$  שפה אזי שפה אזי ( $\mathcal{L}\in\mathcal{NP}$ ) שפה משפט

.SUBSETSUM טענה: קיים מוודא פולינומי

```
A \in \mathcal{NPC} אזי A \leq_p B וכן A \in \mathcal{NPC} שפות באשר A, B \in \mathcal{NP} 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 m\in\mathbb{N} אבורה קיים וארכה arphi \in \mathbb{N}
                                                                                                                                                       .kSAT =\{\langle arphi 
angle \mid (arphi \in kCNF) \land (ספיקה) 
angle \mid k \in \mathbb{N}_+ הגדרה: יהי k \in \mathbb{N}_+ אזי k \in \mathbb{N}_+
                                                                                                                                                                                                                                        .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 איזי 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 A \in M_{m 	imes k}\left(\{p_i\} \cup \{\lnot p_i\}
ight) השמה אזי
                                                                                                                                             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\}
                                                                                                                                                                                                                                                                             .CCNF \in \mathcal{NPC} :טענה
                                                                                                                                                                                             .DNFCNF = \{\langle \varphi \rangle \mid (\varphi \in DNF) \land (\varphi \in \varphi)\} הגדרה:
                                                                                                                                                                                                                                                                                 .DNFCNF \in \mathcal{P} :טענה
                                                                 (u \in C) \lor (v \in C) מתקיים \{u,v\} \in E מבורה לכל עבורה לכל איז מכוון אזי C \subseteq V מרקיים גרף לא מכוון אזי
                                                                                                                                                VC = \{\langle G, k \rangle \mid k גרף גרף לא מכוון בעל כיסוי קודקודים מגודל G\} גרף גרף לא
                                                                                                                                                                                                                                                                                     .VC \in \mathcal{NPC} :טענה
                                                                                                                                                                                \mathcal{B}\subseteq igcup_{n=1}^\infty \left(\Sigma^n	o\Sigma
ight) בסיס פונקציות: יהי אלפבית אזי בסיס ביסיס ביסיס ביסיס ביסיס אלפבית אזי
לכל f_i:\Sigma^{k_i}	o\Sigma בסיס פונקציות מעל f_i:\Sigma^{k_i}	o\Sigma תהיינה היינה לות תהיינה מעל בסיס פונקציות מעל בסיס מעגל: יהי
                                                            ותהיינה \{f_1\dots f_n, x_1\dots x_m, y_1\dots y_k\} אזי גרף מכוון i\in [n] המקיים i\in [n]
                                                                                                                                                                                                                                                        . חסר מעגלים מכוונים G ullet
                                                                                                                                                                                                                       \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] לכל
                                                                                                                                                                        הערה: נשמור על הטרמינולוגיה ממעגל בוליאני כהכללה טבעית.
z\in\left\{ 0,1
ight\} ^{n} יהי T\left( n
ight) מ"ט שרצה בזמן הא M מ"ט שרצה הזמן באשר האיט חשיבה בזמן האי היא T\left( n
ight) יהי
                                                         R_i\left(	au_{M,z}
ight)=c_i המקיימת 	au_{M,z}\in M_{T(n)+1}\left(\Sigma \uplus \Gamma
ight) אזי אזי M\left(z
ight) אזי הריצה של פינפיגורציות הריצה של הריצה של אזי אזי אזי המקיימת הריצה של חיינה הריצה של הריצה של חיינה אזי המקיימת הריצה של חיינה הריצה של חיינה הריצה של חיינה הריצה של הריצה של חיינה הריצה של הריצה הריצה של הריצה הריצה של הריצה של
```

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

f שפה אזי רדוקציית מיפוי  $B\subseteq \Delta^*$  שפה ותהא  $A\subseteq \Sigma^*$  תהא  $\Sigma\subseteq \Delta$  אלפבייתים באשר אור בדוקציית מיפוי

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

. אעדים פי  $p\left(|x|\right)$  אחרי אחרי לכל אוצרת עוצרת אוצר מתקיים כי  $x\in\Sigma^*$  אעדים מתקיים כי לכל

 $ACC_{\mathcal{NP}} = \{\langle M, x, 1^t \rangle \mid$  צעדים t צעדים לכל היותר מקבלת לכל מקבלת M(x, w) מקבלת t

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

 $\mathcal{NPH}=\{\mathcal{L}\mid orall L\in \mathcal{NP}\,(L\leq_p\mathcal{L})\}$  שפה  $\mathcal{NP}$ ־קשה:

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

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

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

מ־A ל־B חשיבה פולינומית.

 $A \leq_p B$  אזי

.CLIQUE  $\leq_p$  IS :טענה

 $\mathsf{ACC}_{\mathcal{NP}} \in \mathcal{NPC}$  טענה:

```
.\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 הקונפיגורציות נניח כי
                                                                                       כך \Sigma \uplus \Gamma מעלים מעל T\left(n\right) נגדיר מיט רצה מיט מעל מ"ט רצה בזמן באשר מעלים מעל T\left(n\right) כך הגדרה: תהא
                                                                                                                                                               .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) אזי i\in\{0,\ldots,T\left(n
ight)-1\} ויהי z\in\Sigma\uplus\Gamma 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 •
                                                                                                       .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) איהי z \in \Sigma \uplus \Gamma יהי
טענה: תהא T:\mathbb{N} 	o \mathbb{N} אזי אזי C_{M,n}^{\Sigma \uplus \Gamma} = \mathcal{O}\left(T^{2}\left(n\right)\right) אזי אזי אזי רצה בזמן מ"ט אזי n \leq T\left(n\right) וכן קיימת T:\mathbb{N} 	o \mathbb{N}
                                                                                                                                 f\left(1^{n}
ight)=\left\langle C_{M,n}^{\Sigma\uplus\Gamma}
ight
angle עבורה poly \left(T\left(n
ight)
ight) פונקציה שיבה בזמן
C_{M,n}^{\Sigma \uplus \Gamma}(z) = M(z) אזי z \in \Sigma \uplus \Gamma ויהי T(n) ויהי מסקנה: תהא n \leq T(n) חשיבה בזמן באשר T: \mathbb{N} \to \mathbb{N} ויהי
טענה: יהי f\left(C
ight) מתקיים כי f\left(C
ight) מעגל בוליאני עבורה לכל מעגל פולינומית פונקציה חשיבה פולינומית עבורה לכל מעגל פולינומית f\left(C
ight) מעגל בוליאני מעגל פולינומית איז קיימת פונקציה חשיבה פולינומית אוויים ביימות פונקציה חשיבה פולינומית אוויים ביימות פונקציה חשיבה פולינומית אוויים ביימות פונקציה חשיבה פולינומית פונקציה פולינומית פולינומית פונקציה פולינומית פונקציה פולינומית פונקציה פולינומית פולינומית פולינומית פונקציה פולינומית פולימית פולימי
                                                                                         |f\left(C
ight)|=\mathcal{O}\left(|C|
ight) וכן z\in\left\{ 0,1
ight\} ^{n} לכל C\left(z
ight)=f\left(C
ight)\left(z
ight) בסיס דה־מורגן באשר
למה: T\left(n
ight) אזי קיימת פונקציה חשיבה T\left(n
ight) מ"ט רצה בזמן באשר איי קיימת פונקציה חשיבה T:\mathbb{N} 	o \mathbb{N} אהי
(C_{M,n}(z)=1) \iffמקבלת).
                                                                                                                                                                                                                .CIRSAT \in \mathcal{NPC} :
מסקנה: תהא f:\{0,1\}^*	o \{0,1\} ותהא ווהא n\leq T(n) חשיבה בזמן באשר די משפחת מעגלים מסקנה: תהא
                                                                                                                       \sqrt{T\left(n
ight)} אזי f לא ניתנת לחישוב על ידי מ"ט בזמן אזי f אזי לא מגודל מגודל
                                                                                                                                                                                                               .CIRSAT \leq_p 3SAT :טענה
                                                                                                                                                                                                     .3SAT \leq_n SUBSETSUM :טענה
                                                                                                                                                                                                   .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\} :co\mathcal{NP} שפה
                                                                                                                                                                                 השערה פתוחה .co\mathcal{NP} \neq \mathcal{NP} : השערה
                                                                                                                                                                    טענה: תהיינה A \leq_p B שפות באשר A \leq_p B אזי
                                                                                                                                                                                         A \in \mathcal{NP} אזי B \in \mathcal{NP} אם ullet
                                                                                                                                                                                 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 \mathcal{L}\in\mathcal{NPC} מסקנה: תהא
                                                                                                                                                                                                          \mathcal{P} \subseteq \mathcal{NP} \cap \mathrm{co}\mathcal{NP} :טענה
                                                                                                                                                                       השערה: \mathcal{P} \neq \mathcal{NP} \cap \mathrm{co}\mathcal{NP} השערה
                                                                                                                                                                                              \mathsf{FACTOR} \in \mathcal{NP} \cap \mathsf{co}\mathcal{NP} :
                                                                                                                                                                       השערה פתוחה \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
                                                                                                                                                    \mathcal{O}\left(n^{2}
ight) אשר רצה בזמן \mathcal{O}\left(n^{2}
ight) עבורה מסקנה: קיימת מ"ט M
                                                                                                             . דוחה M\left(x\right) אשר אינו קידוד של שלשת מטריצות x\in\left\{ 0,1\right\} ^{*}
        . מקבלת. M\left(x\right) מתקיים 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\} ^{*} לכל
                                        עבורו קיימות x=\langle A,B,C \rangle וכן A\cdot B \neq C המקיימות A,B,C \in M_n\left(\mathbb{Z}\right) מתקיים x\in\{0,1\}^*
                                                                                                                                                                                         \mathbb{P}\left(M\left(x\right)\right) \leq 2^{-100} מקבלת
                                                                                   Cנוסחה אריתמטית: יהי \mathbb{F} שדה ויהי C מעגל מעל \mathbb{F} עם הבסיס \{+, \times\} 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 arphi עבורה לכל
                                                                                                                            .ZE_{\mathbb{F}}=\{\langle \varphi \rangle \mid \varphi\equiv 0 עבורה אריתמטית אריתמטית אריתמטית עבורה אריתמטית ק
```

 $.2^h$  טענה: תהא arphi נוסחה אריתמטית בעומק שמעל  $\mathbb F$  מעל מעל מעל היותר לכל היותר  $\varphi$ 

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

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

 $\deg\left(\prod_{i=1}^n x_i^{d_i}
ight) = \sum_{i=1}^n d_i$  אזי  $d_1 \dots d_n \in \mathbb{N}$  אזי מונום: יהיו  $\deg\left(\sum_{i=1}^{k}\prod_{j=1}^{n}x_{j}^{d_{i,j}}
ight)=\max\left\{\deg\left(\prod_{j=1}^{n}x_{j}^{d_{i,j}}
ight)\left[\ i\in[k]
ight\}$  איי  $d\in M_{k imes n}\left(\mathbb{N}
ight)$  ההא מוטאלית 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  $S\subseteq\mathbb{F}$  חתהא ותהא f
eq 0 באשר באשר באשר  $f\in\mathbb{F}\left[x_1,\ldots,x_n
ight]$ 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(x) מתקיים  $x=\langle arphi \rangle$  וכן  $arphi \equiv 0$  המקיימת מעל  $\mathbb R$  המקיימת arphi המקיימת  $arphi \equiv 0$
- .poly (|arphi|) בזמן  $\mathbb{P}(|arphi|) \leq 0.01$  מתקיים מתקיים  $x = \langle arphi \rangle$  וכן  $arphi \not\equiv 0$  מתקיים אריתמטית מעל  $\mathbb{R}$  המקיימת  $\varphi \not\equiv 0$  וכן באשר x\$r איז התחלתית קונפיגורציה התחלתית מכונת מיורינג אקראית: תהא תחלתית מ"ט דו־סרטית מכונת מיורינג אקראית: תהא  $r \in \{0,1\}^{T(|x|)}$

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

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

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

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

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

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

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

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

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

המקיימת כי החל T(n) המקיימת מ"ט אקראית M עם זמן ריצה פולינומי  $\alpha,\beta:\mathbb{N} o [0,1]$  המקיימת כי החל הגדרה: ממקום מסויים  $n\in\mathbb{N}$  מתקיים

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

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

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

 $\mathcal{BPP}\left(lpha,\delta
ight)\subseteq\mathcal{BPP}\left(eta,\gamma
ight)$  אזי ממקום מסויים מיים  $lpha\leqeta\leq\gamma\leq\delta$  עבורן עבורן  $lpha,eta,\gamma,\delta:\mathbb{N} o[0,1]$  $\mathbb{P}\left(\left|p-rac{1}{n}\sum_{i=1}^nA_i
ight|\geq\delta
ight)\leq 2^{-\Theta\left(\delta^2n
ight)}$  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  $n^{-c} \leq lpha\left(n\right) \leq 1-n^{-c}$  חשיבה בזמן פולינומי מסויים מסויים  $lpha: \mathbb{N} \to [0,1]$  החל ממקום מסויים אזי  $c,d \in \mathbb{N}$  יהיו  $c,d \in \mathbb{N}$  יהיו  $c,d \in \mathbb{N}$  הריל ממקום מסויים אזי  $\mathcal{BPP}\left(lpha\left(n\right)-n^{-c},lpha\left(n\right)+n^{-c}\right) \subseteq \mathcal{BPP}\left(2^{-n^d},1-2^{-n^d}\right)$ 

 $(c_1\$c_2\$\dots\$c_k)^i=c_i$  קונפיגורציה אזי ק $(c_1\$c_2\$\dots\$c_k)^i=c_1$  קונפיגורציה אזי מ"ט M מ"ט M

A אברי x ללא אברי x הינה המחרוזת אוי  $x \in \Sigma^*$  ותהא אברי  $x \in \Sigma^*$  הינה המחרוזת אברי

 $c_0=q_0x$  באשר באר סינור לכל קונפיגורציות עבורה מיט תלת־סרטית אזי מ"ט תלת־סרטית האא  $S:\mathbb{N} o\mathbb{N}$  באשר באשר מכונת סיורינג בעלת סיבוכיות מקום: תהא אזי מ"ט תלת־סרטית עבורה לכל  $c_i=1$  מתקיים וכן  $c_i=1$  עוברת ל־ $c_i=1$  לכל מתקיים

- $c_i^1=xackslash Q$  מתקיים  $i\in[n]$  לכל לקריאה בלבד: לכל •
- $.\left|c_{i-1}^{2}\right|\leq S\left(n\right)+1$ מתקיים  $i\in\left[n\right]$ לכל לכל במקום: סרט סרט סרט לכל
- $.ig(c_{i-1}^3ackslash Qig)_i=ig(c_i^3ackslash Qig)_i$  מתקיים מתקיים  $j\inig[ig|c_{i-1}ig|ig]$  ולכל ולכתיבה חד־פעמית: לכל

S אזי אינ מקום חיבוכיות מיט בעלת מ"ט אזי איזי אזי אזי מיט מיט מיט מיט מיט מיורינג: תהא אור אזי אזי אזי מיט מיט מיט מיורינג

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

 $\mathcal{PSPACE} = igcup_{c \in \mathbb{N}} \operatorname{DSpace}\left(n^c
ight) : \mathcal{PSPACE}$  שפה

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

 $\mathcal{LOGSPACE} = L$  סימון:

.DSpace (1) = DSpace  $(\log (\log (n))) = \{L \mid L \mid L\}$  :

.DTime  $(T(n))\subseteq D$ Space (T(n)) אזי חשיבה בזמן חשיבה T חשיבה מענה:

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

.DSpace  $(S(n))\subseteq ext{DTime }(2^{\mathcal{O}(S(n))})$  אזי  $S\geq \log$  באשר באשר  $S:\mathbb{N} o \mathbb{N}$  טענה: תהא

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

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

 $(S\left(n
ight))_2$  את מחשבת  $1^n$  מחשבת מחשבה לכל  $n\in\mathbb{N}$  כי  $n\in\mathbb{N}$  מחשבת מ"ט  $S:\mathbb{N}\to\mathbb{N}$  מחשבת פונקציה חשיבה במקום: פונקציה  $S:\mathbb{N}\to\mathbb{N}$  מחשבת את במקום במקום  $O\left(S\left(n
ight)\right)$ .

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

 $\mathcal{LOGSPACE} \subseteq \mathcal{PSPACE}$  מסקנה:

מסקנה: לפחות אחד מהבאים נכון

- $\mathcal{LOGSPACE} \subseteq \mathcal{P}$ 
  - $\mathcal{P} \subseteq \mathcal{PSPACE} \bullet$

 $\log{(n)}$  מקום מיט M בעלת מייט  $f:D o (\Gamma \setminus \{ \sqcup \})^*$  אזי אזי  $D \subseteq \Sigma$  אזי אזי מקום לוגריתמי: תהא  $f:D o (\Gamma \setminus \{ \sqcup \})^*$  אזי אזי מקום לוגריתמי: תהא

רדוקציית מיפוי במקום לוגריתמי: יהיו  $\Sigma,\Delta$  אלפבייתים באשר  $\Sigma\subseteq\Delta$  תהא שפה ותהא שפה אזי רדוקציית מיפוי מיפוי במקום לוגריתמי.  $A\subseteq\Sigma$  אלפבייתים באשר  $A\subseteq\Sigma$  תהא היא רדוקציית מיפוי לוגריתמי.

 $A \leq_p B$  אזי  $A \leq_L B$  טענה: תהיינה A, B שפות עבורן