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

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

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

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

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

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

חזקה של מילה: תהא $\langle w_1\dots w_n\rangle\in\Sigma^*$ ויהי $m\in\mathbb{N}$ אזי $\langle w_1\dots w_n\rangle^m=\prod_{i=1}^{m}\langle w_1\dots w_n\rangle$.

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

שפה: יהי Σ אלפבית אזי $L\subseteq\Sigma^*$.

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

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

חזקה של שפה: תהא $L\subseteq\Sigma^*$ שפה ויהי $m\in\mathbb{N}$ אזי $L^m=\left\{\prod_{i=1}^{k}w_i\mid\forall i\in[k].w_i\in L\right\}$.

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

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

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

אלגוריתם מכריע שפה: תהא $L\subseteq\Sigma^*$ שפה אזי אלגוריתם $A:\Sigma^*\to\{\text{true},\text{false}\}$ המקיים

- מקבל: לכל $x\in L$ מתקיים $A(x)=\text{true}$.
- דוחה: לכל $x\notin L$ מתקיים $A(x)=\text{false}$.

פונקציה בולאנית: תהיינה $n,m\in\mathbb{N}$ אזי $f:\{0,1\}^n\to\{0,1\}^m$.

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

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

הערה: תמיד נוסיף לבסיס את הפונקציות הקבועות.

מעגל בוליאני: יהי $\mathcal{B}$ בסיס פונקציות בוליאניות תהיינה $k_1\dots k_n\in\mathbb{N}_+$ תהיינה $f_1\dots f_n\in\mathcal{B}$ באשר $f_i:\{0,1\}^{k_i}\to\{0,1\}$ לכל $i\in[n]$ ותהיינה $x_1\dots x_m,y_1\dots y_k\in\{0,1\}$ אזי גרף מכוון G מעל $\{f_1\dots f_n,x_1\dots x_m,y_1\dots y_k\}$ המקיים

- G חסר מעגלים מכוונים.
- לכל $i\in[m]$ מתקיים $\deg^-(x_i)=0$.
- לכל $i\in[n]$ מתקיים $\deg^-(f_i)=k_i$.
- לכל $i\in[k]$ מתקיים $\deg^-(y_i)=1$ וכן $\deg^+(y_i)=0$.

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

חוטים: יהי C מעגל בוליאני אזי $E(C)$.

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

נוחסאות: יהי C מעגל בולינארי אזי $\{G\le C\mid 1$ הוא G של ה־fan-out$\}$.

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

סימון: יהי C מעגל בולינאני ויהי $v\in\{0,1\}^m$ אזי השערוך של C על v הוא $C(v)=(y_1\dots y_k)$.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

טענה שאנון: קיים $n\in\mathbb{N}$ עבורו קיימת $f:\{0,1\}^n\to\{0,1\}$ שאינה ניתנת לחישוב בעזרת מעגל C בגודל קטן מאשר $\frac{2^n}{10n}$.

אוטומט סופי דטרמיניסטי (אס"ד): תהא $Q\neq\varnothing$ קבוצה סופית יהי Σ אלפבית תהא $\delta:Q\times\Sigma\to Q$ יהי $q\in Q$ ותהא $F\subseteq Q$ אזי (Q,Σ,δ,q,F).

מצבים באוטומט סופי דטרמיניסטי: יהי (Q,Σ,δ,q,F) אס"ד אזי Q.

אלפבית באוטומט סופי דטרמיניסטי: יהי (Q,Σ,δ,q,F) אס"ד אזי Σ.

פונקציית מעברים באוטומט סופי דטרמיניסטי: יהי (Q,Σ,δ,q,F) אס"ד אזי δ.

מצב התחלתי באוטומט סופי דטרמיניסטי: יהי (Q,Σ,δ,q,F) אס"ד אזי q.

מצבים מקבלים באוטומט סופי דטרמיניסטי: יהי (Q,Σ,δ,q,F) אס"ד אזי F.

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

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

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

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

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

טענה: $\varnothing$ רגולרית.

טענה: $\{\varepsilon\}$ רגולרית.

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

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

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

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

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

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

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

אוטומט סופי לא־דטרמיניסטי מינוס (אסלד"ם): תהא $Q\neq\varnothing$ קבוצה סופית יהי Σ אלפבית תהא $\delta:Q\times\Sigma\to\mathcal{P}(Q)$ ותהיינה $S,F\subseteq Q$ אזי (Q,Σ,δ,S,F).

מצבים באוטומט סופי לא־דטרמיניסטי מינוס: יהי (Q,Σ,δ,S,F) אסלד"ם אזי Q.

אלפבית באוטומט סופי לא־דטרמיניסטי מינוס: יהי (Q,Σ,δ,S,F) אסלד"ם אזי Σ.

פונקציית מעברים באוטומט סופי לא־דטרמיניסטי מינוס: יהי (Q,Σ,δ,S,F) אסלד"ם אזי δ.

מצבים התחלתיים באוטומט סופי לא־דטרמיניסטי מינוס: יהי (Q,Σ,δ,S,F) אסלד"ם אזי S.

מצבים מקבלים באוטומט סופי לא־דטרמיניסטי מינוס: יהי (Q,Σ,δ,S,F) אסלד"ם אזי F.

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

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

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

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

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

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

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

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

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

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

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

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

פונקציית מעברים באוטומט סופי לא־דטרמיניסטי: יהי (Q,Σ,δ,S,F) אסל"ד אזי δ.

מצבים התחלתיים באוטומט סופי לא־דטרמיניסטי: יהי (Q,Σ,δ,S,F) אסל"ד אזי S.

מצבים מקבלים באוטומט סופי לא־דטרמיניסטי: יהי (Q,Σ,δ,S,F) אסל"ד אזי F.

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

סביבת ε: יהי N אסל"ד ויהי $T\subseteq Q$ אזי $E(T)=\bigcup_{q\in T}E(q)$.

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

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

סימון: יהי $x\in\Sigma^*$ יהיו $\sigma_1\dots\sigma_n\in\Sigma\backslash\{\varepsilon\}$ ויהיו $k_0\dots k_n\in\mathbb{N}$ עבורם $x=\varepsilon^{k_0}\sigma_0\varepsilon^{k_1}\sigma_1\varepsilon^{k_2}\dots\sigma_n\varepsilon^{k_n}$ אזי $x^{\not\varepsilon}=\sigma_1\dots\sigma_n$.

טענה: יהי A אסל"ד ויהי $x\in\Sigma^n$ אזי (A מקבל את x)$\iff$(קיימים $q_0\dots q_n\in Q$ עבורם $q_0\in S$ וכן $q_i\in\delta\left(q_{i-1},x_i^{\not\varepsilon}\right)$ לכל $i\in[n]$ וכן $q_n\in F$).

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

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

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

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

ביטוי רגולרי (ב"ר): יהי Σ אלפבית אזי

- $\varnothing$.
- יהי $a\in\Sigma_\varepsilon$ אזי a.
- יהיו R_1,R_2 ביטויים רגולרים אזי $R_1\cup R_2$.
- יהיו R_1,R_2 ביטויים רגולרים אזי R_1R_2.
- יהי R ביטוי רגולרי אזי R^*.

שפה נוצרת מביטוי רגולרי: יהי Σ אלפבית אזי

- $L(\varnothing)=\varnothing$.
- יהי $a\in\Sigma_\varepsilon$ אזי $L(a)=\{a\}$.
- יהיו R_1,R_2 ביטויים רגולרים אזי $L(R_1\cup R_2)=L(R_1)\cup L(R_2)$.
- יהיו R_1,R_2 ביטויים רגולרים אזי $L(R_1R_2)=L(R_1)L(R_2)$.
- יהי R ביטוי רגולרי אזי $L(R^*)=L(R)^*$.

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

הערה: קיים סדר פעולות לביטויים רגולריים

- סגור קליני.
- שרשור.
- איחוד.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

משפט מייהיל־נרוד: תהא $L \subseteq \Sigma^*$ שפה אזי (L רגולרית)$\Longleftrightarrow$(${}^{\Sigma^*}/_{\sim_L}$ סופית).

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

אוטומט סופי דטרמיניסטי המחלקות: תהא $L \subseteq \Sigma^*$ שפה באשר ${}^{\Sigma^*}/_{\sim_L}$ סופית ותהא $\{x_1 \ldots x_n\}$ קבוצת נציגים של ${}^{\Sigma^*}/_{\sim_L}$ אזי אס"ד $(Q, \Sigma, \delta, q_0, F)$ באשר

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

קונפיגורציה עוברת/צעד: תהא M מ"ט תהא c קונפיגורציה אזי קונפיגורציה c' המקיימת אחד הבאים
- קיימים $a,b,b'\in\Gamma$ וקיימים $u,v\in\Gamma^*$ וקיימים $q,q'\in Q$ עבורם $c=uaqbv$ וכן $\delta(q,b)=(q',b',L)$ וכן $c'=uq'ab'v$.
- קיימים $b,b'\in\Gamma$ וקיימים $u,v\in\Gamma^*$ וקיימים $q,q'\in Q$ עבורם $c=qbv$ וכן $\delta(q,b)=(q',b',L)$ וכן $c'=q'b'v$.
- קיימים $b,b'\in\Gamma$ וקיימים $u,v\in\Gamma^*$ וקיימים $q,q'\in Q$ עבורם $c=uqbv$ וכן $\delta(q,b)=(q',b',R)$ וכן $c'=ub'q'v$.

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

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

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

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

מודלים שקולים: מודלים M,M' עבורם לכל A מסוג M וכן לכל B מסוג M' מתקיים
- קיימת A' מסוג M' המקיימת $L(A)=L(A')$.
- קיימת B' מסוג M המקיימת $L(B)=L(B')$.

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

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

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

מסקנה: מכונת טיורינג ומכונת טיורינג נחה הינן מודלים שקולים.

מכונת טיוריגנ רב־סרטית: יהי $k\in\mathbb{N}_+$ תהא $Q\neq\varnothing$ קבוצה סופית יהי Σ אלפבית יהי Γ אלפבית עבורו $\Sigma\subseteq\Gamma$ וכן $\sqcup\in\Gamma\backslash\Sigma$ יהיו $q_0,q_a,q_r\in Q$ באשר $q_a\neq q_r$ ותהא $\delta:(Q\backslash\{q_a,q_r\})\times\Gamma^k\to Q\times\Gamma^k\times\{L,R\}^k$ אזי $(k,Q,\Sigma,\Gamma,\delta,q_0,q_a,q_r)$.

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

קונפיגורציה במכונת טיוריגנ רב־סרטית: תהא M מ"ט רב־סרטית ותהיינה $c_1\dots c_k\in\Gamma^*Q\Gamma^*$ אזי $c_1\$c_2\$\dots\$c_k$.

קונפיגורציה התחלתית במכונת טיוריגנ רב־סרטית: תהא M מ"ט רב־סרטית אזי קונפיגורציה c עבורה קיים $v\in\Sigma^*$ המקיימת $c=q_0v\sqcup\$q_0\sqcup\$\dots\$q_0\sqcup$.

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

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

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

פקודות במודל RAM: יהי (k,Π) מודל RAM אזי Π.

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

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

רגיסטרים בקונפיגורציה: יהי (k,Π) מודל RAM ותהא (T,R,PC) קונפיגורציה אזי R.

זיכרון בקונפיגורציה: יהי (k,Π) מודל RAM ותהא (T,R,PC) קונפיגורציה אזי T.

הערה: ריצת מודל RAM זהה לריצת מעבד MIPS.

טענה: מכונת טיורינג ומודל RAM הם מודלים שקולים.

מכונת טיוריגנ לא־דטרמיניסטית (מטל"ד): תהא $Q\neq\varnothing$ קבוצה סופית יהי Σ אלפבית יהי Γ אלפבית עבורו $\Sigma\subseteq\Gamma$ וכן $\sqcup\in\Gamma\backslash\Sigma$ יהיו $q_0,q_a,q_r\in Q$ באשר $q_a\neq q_r$ ותהא $\delta:(Q\backslash\{q_a,q_r\})\times\Gamma\to\mathcal{P}(Q\times\Gamma\times\{L,R\})$ אזי $(Q,\Sigma,\Gamma,\delta,q_0,q_a,q_r)$.

קונפיגורציה עוברת: תהא N מטל"ד תהא $q\in Q$ ותהא $b\in\Gamma$ ותהיינה $u,v\in\Gamma^*$ באשר $uqbv$ קונפיגורציה אזי קונפיגורציה c' עבורה קיימת $\delta':(Q\backslash\{q_a,q_r\})\times\Gamma\to Q\times\Gamma\times\{L,R\}$ המקיימת $\delta'(q,b)\in\delta(q,b)$ וכן $uqbv$ הינה δ'־עוברת ל־c'.

עץ חישוב: תהא N מטל"ד ויהי $x\in\Sigma^*$ אזי עץ קונפיגורציות $T_{N,x}$ עם שורש $q_0x\sqcup$ עבורו לכל c,c' קונפיגורציות מתקיים (c' צאצא של c)$\Longleftrightarrow$(c' עוברת ל־c).

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

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

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

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

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

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

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

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

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

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

- לכל $q\in Q$ ולכל $\sigma\in\Gamma$ מתקיים $\delta(q,\sigma)=(q',\sigma',R)$.
- הרצת E על הקונפיגורציה ε מקיימת
  - לכל $x\in L$ מתקיים כי $\$x\$$ על הסרט לאחר מספר סופי של צעדים.
  - לכל $x\notin L$ מתקיים כי $\$x\$$ לא על הסרט לעולם.

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

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

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

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

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

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

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

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

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

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

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

- לכל מ"ט M ולכל קלט x של M מתקיים (U מקבלת את $\langle M,x\rangle$)$\Longleftrightarrow$(M מקבלת את x).
- לכל מ"ט M ולכל קלט x של M מתקיים (U דוחה את $\langle M,x\rangle$)$\Longleftrightarrow$(M דוחה את x).
- לכל מ"ט M ולכל קלט x של M מתקיים (U לא עוצרת עבור $\langle M,x\rangle$)$\Longleftrightarrow$(M לא עוצרת עבור x).
- לכל $x\in\{0,1\}^*$ באשר $x\notin\text{Im}(f)$ מתקיים כי U דוחה את x.

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

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

טענה: $\text{ACC}\in\mathcal{RE}$.

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

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

טענה: $\text{ACC}\notin\mathcal{R}$.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

מסקנה: $\text{ACC}\leq \text{EMPTY}$.

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

טענה: $\text{REG}\notin\mathcal{R}$.

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

טענה: $\text{EQ}\notin\mathcal{R}$.

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

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

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

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

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

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

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

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

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

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

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

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

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

הערה: קידוד מספרים תמיד יעשה בבסיס 2.

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

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

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

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

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

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

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

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

חסם עליון לזמן ריצה של מכונת טיורינג: תהא M מ"ט אזי $T:\mathbb{N}\to\mathbb{N}$ עבורה לכל $n\in\mathbb{N}$ ולכל $x\in\Sigma^n$ מתקיים כי M על הקלט x מבצעת לכל היותר $T(n)$ צעדים.

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

טענה: $\{0^k1^k \mid k\geq 0\}\in\text{DTime}(n^2)$.

מסקנה: $\{0^k1^k \mid k\geq 0\}\in\text{DTime}(n\log(n))$.

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

מסקנה: תהא $t(n)=o(n\log(n))$ אזי $\{0^k1^k \mid k\geq 0\}\notin\text{DTime}(t(n))$.

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

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

משפט מכונת טיורינג אוניברסלית עם טיימר: קיימת מ"ט אוניברסלית U וקיים $C\in\mathbb{R}$ עבורם לכל מ"ט M ולכל קלט x באשר M עוצרת על הקלט x לאחר t צעדים מתקיים כי U עוצרת על הקלט $\langle M,x\rangle$ תוך $C\cdot t$ צעדים.

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

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

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

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

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

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

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

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

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

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

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

טענה: $\text{PATH}\in\mathcal{P}$.

משפט: $\text{PRIME}\in\mathcal{P}$.

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

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

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

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

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

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

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

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

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

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

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

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

מוודא לשפה: תהא $\mathcal{L}\subseteq\Sigma^{*}$ שפה אזי מ"ט V מעל אלפבית $\Sigma\cup\left\{ ","\right\}$ המקיים
- שלמות: יהי $x\in\mathcal{L}$ אזי קיים $w\in\Sigma^{*}$ עבורו $V\left(x,w\right)$ מקבלת.
- נאותות: יהי $x\notin\mathcal{L}$ אזי לכל $w\in\Sigma^{*}$ מתקיים כי $V\left(x,w\right)$ דוחה.

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

מדווא פולינומי לשפה: תהא $\mathcal{L}\subseteq\Sigma^{*}$ שפה אזי מוודא V ל־$\mathcal{L}$ עבורו קיים $p\in\mathbb{N}\left[x\right]$ המקיים כי לכל $x,w\in\Sigma^{*}$ מתקיים כי $V\left(x,w\right)$ עוצרת לכל היותר אחרי $p\left(\left|x\right|\right)$ צעדים.

הגדרה: $\text{CLIQUE}=\left\{ \left\langle G,k\right\rangle \mid k\text{ גרף לא מכוון בעל קליקה מגודל }G\right\}$.

טענה: קיים מוודא פולינומי ל־CLIQUE.

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

טענה: קיים מוודא פולינומי ל־IS.

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

טענה: קיים מוודא פולינומי ל־FACTOR.

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

טענה: קיים מוודא פולינומי ל־SUBSETSUM.

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

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

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

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

רדוקציית מיפוי פולינומית: יהיו Σ, Δ אלפבייתים באשר $\Delta \subseteq \Sigma$ תהא $A \subseteq \Sigma^*$ שפה ותהא $B \subseteq \Delta^*$ שפה אזי רדוקציית מיפוי f מ־A ל־B חשיבה פולינומית.

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

טענה: $\text{CLIQUE} \leq_p \text{IS}$.

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

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

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

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

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

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

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

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

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

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

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

טענה: $2\text{SAT} \in \mathcal{P}$.

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

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

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

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

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

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

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

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

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

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

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

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

טענה: $\text{VC} \in \mathcal{NPC}$.

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

מעגל: יהי Σ אלפבית יהי $\mathcal{B}$ בסיס פונקציות מעל Σ תהיינה $k_1 \ldots k_n \in \mathbb{N}_+$ תהיינה $f_1 \ldots f_n \in \mathcal{B}$ באשר $f_i : \Sigma^{k_i} \to \Sigma$ לכל $i \in [n]$ ותהיינה $x_1 \ldots x_m, y_1 \ldots y_k \in \Sigma$ אזי גרף מכוון G מעל $\{f_1 \ldots f_n, x_1 \ldots x_m, y_1 \ldots y_k\}$ המקיים

- G חסר מעגלים מכוונים.
- לכל $i \in [m]$ מתקיים $\deg^-(x_i) = 0$.
- לכל $i \in [n]$ מתקיים $\deg^-(f_i) = k_i$.
- לכל $i \in [k]$ מתקיים $\deg^-(y_i) = 1$ וכן $\deg^+(y_i) = 0$.

הערה: נשמור על הטרמינולוגיה ממעגל בוליאני כהכללה טבעית.

מטריצת הקונפיגורציות/טאבלו: תהא $T : \mathbb{N} \to \mathbb{N}$ חשיבה בזמן באשר $n \leq T(n)$ תהא M מ"ט שרצה בזמן $T(n)$ יהי $z \in \{0,1\}^n$ ותהיינה $c_1 \ldots c_i$ קונפיגורציות הריצה של $M(z)$ אזי $\tau_{M,z} \in M_{T(n)+1}(\Sigma \uplus \Gamma)$ המקיימת $R_i(\tau_{M,z}) = c_i$.

הערה: במטריצת הקונפיגורציות נניח כי $\delta\left(q_{a},\sigma\right)=\left(q_{a},\sigma,R\right)$ וכן $\delta\left(q_{r},\sigma\right)=\left(q_{r},\sigma,R\right)$.

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

הגדרה: תהא $T:\mathbb{N}\to\mathbb{N}$ חשיבה בזמן באשר $n\le T\left(n\right)$ ותהא M מ״ט רצה בזמן $T\left(n\right)$ נגדיר מעגלים מעל $\Sigma\uplus\Gamma$ כך

- יהי $z\in\Sigma\uplus\Gamma$ אזי $C_{\text{inp}}\left(z\right)=R_{0}\left(\tau_{M,z}\right)$.
- יהי $z\in\Sigma\uplus\Gamma$ ויהי $i\in\left\{ 0,\ldots,T\left(n\right)-1\right\}$ אזי $C_{\text{next}}\left(R_{i}\left(\tau_{M,z}\right)\right)=R_{i+1}\left(\tau_{M,z}\right)$.
- יהי $z\in\Sigma\uplus\Gamma$ אזי $C_{\text{out}}\left(R_{T\left(n\right)}\left(\tau_{M,z}\right)\right)=M\left(z\right)$.
- יהי $z\in\Sigma\uplus\Gamma$ אזי $C_{M,n}^{\Sigma\uplus\Gamma}\left(z\right)=\left(C_{\text{out}}\circ C_{\text{next}}\circ\ldots\circ C_{\text{next}}\circ C_{\text{inp}}\right)\left(z\right)$.

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

מסקנה: תהא $T:\mathbb{N}\to\mathbb{N}$ חשיבה בזמן באשר $n\le T\left(n\right)$ תהא M מ״ט רצה בזמן $T\left(n\right)$ ויהי $z\in\Sigma\uplus\Gamma$ אזי $C_{M,n}^{\Sigma\uplus\Gamma}\left(z\right)=M\left(z\right)$.

טענה: יהי Π אלפבית אזי קיימת פונקציה חשיבה פולינומית f עבורה לכל מעגל בוליאני C מתקיים כי $f\left(C\right)$ מעגל בוליאני מעל בסיס דה־מורגן באשר $C\left(z\right)=f\left(C\right)\left(z\right)$ לכל $z\in\{0,1\}^{n}$ וכן $\left|f\left(C\right)\right|=\mathcal{O}\left(\left|C\right|\right)$.

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

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

מסקנה: תהא $T:\mathbb{N}\to\mathbb{N}$ חשיבה בזמן באשר $n\le T\left(n\right)$ ותהא $f:\{0,1\}^{*}\to\{0,1\}$ לא ניתנת לחישוב על ידי משפחת מעגלים מגודל $\mathcal{O}\left(T\left(n\right)\right)$ אזי f לא ניתנת לחישוב על ידי מ״ט בזמן $\sqrt{T\left(n\right)}$.

טענה: $\text{CIRSAT}\le_{p}3\text{SAT}$.

טענה: $3\text{SAT}\le_{p}\text{SUBSETSUM}$.

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

טענה: $3\text{SAT}\le_{p}\text{HAMPATH}$.

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

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

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

טענה: תהיינה A,B שפות באשר $A\le_{p}B$ אזי

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

מסקנה: תהא $\mathcal{L}\in\mathcal{NPC}$ אזי $\left(\mathcal{L}\in\text{co}\mathcal{NP}\right)\Longleftrightarrow\left(\text{co}\mathcal{NP}=\mathcal{NP}\right)$.

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

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

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

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

הגדרה: $\text{MATMULT}=\left\{ \left\langle A,B,C\right\rangle \mid\left(A,B,C\in M_{n}\left(\mathbb{Z}\right)\right)\wedge\left(A\cdot B=C\right)\right\}$.

טענה: תהא $D\in M_{n}\left(\mathbb{Z}\right)$ באשר $D\ne0$ אזי $\mathbb{P}_{r\leftarrow\{0,1\}^{n}}\left(D\cdot r=0\right)\le0.5$.

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

- לכל $x\in\{0,1\}^{*}$ אשר אינו קידוד של שלשת מטריצות $M\left(x\right)$ דוחה.
- לכל $x\in\{0,1\}^{*}$ עבורו קיימות $A,B,C\in M_{n}\left(\mathbb{Z}\right)$ המקיימות $A\cdot B=C$ וכן $x=\left\langle A,B,C\right\rangle$ מתקיים $M\left(x\right)$ מקבלת.
- לכל $x\in\{0,1\}^{*}$ עבורו קיימות $A,B,C\in M_{n}\left(\mathbb{Z}\right)$ המקיימות $A\cdot B\ne C$ וכן $x=\left\langle A,B,C\right\rangle$ מתקיים $\mathbb{P}\left(M\left(x\right)\text{ מקבלת}\right)\le2^{-100}$.

נוסחה אריתמטית: יהי $\mathbb{F}$ שדה ויהי C מעגל מעל $\mathbb{F}$ עם הבסיס $\left\{ +,\times\right\}$ אזי נוסחה ב־C.

סימון: תהא φ נוסחה אריתמטית מעל $\mathbb{F}$ עבורה לכל $x_{1}\ldots x_{n}\in\mathbb{F}$ מתקיים $\varphi\left(x_{1}\ldots x_{n}\right)=0$ אזי $\varphi\equiv0$.

הגדרה: $\text{ZE}_{\mathbb{F}}=\left\{ \left\langle \varphi\right\rangle \mid\varphi\equiv0\text{ עבורה } \mathbb{F} \text{ נוסחה אריתמטית מעל } \varphi\right\}$.

טענה: $\overline{\text{ZE}_{\mathbb{Z}_{2}}}\in\mathcal{NPC}$.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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