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 $\langle w_1\ldots w_n\rangle\in\Sigma^*$ אזי $\langle w_1\ldots w_n\rangle^R=\langle w_n\ldots w_1\rangle$.

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

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

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

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 $\text{prefix}(L)=\left\{y\in\Sigma^*\mid\exists x\in\Sigma^*.yx\in L\right\}$.

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

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

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

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

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

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

הערה: תמיד נוסיף לבסיס את הפונקציות הקבועות.

מעגל בוליאני: יהי $\mathcal{B}$ בסיס פונקציות בוליאניות תהיינה $k_1\ldots k_n\in\mathbb{N}_+$ תהיינה $f_1\ldots f_n\in\mathcal{B}$ באשר $f_i:\{0,1\}^{k_i}\to\{0,1\}$ לכל $i\in[n]$ ותהיינה $x_1\ldots x_m,y_1\ldots y_k\in\{0,1\}$ 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 $\deg^+(y_i)=0$.

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

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 $\{G\le C\mid$ ה־fan-out של G הוא $1\}$.

שערוך מעגל בולינארי על קלט: יהי C מעגל בולינאני ויהי $v\in\{0,1\}^m$ אזי $v=(x_1\ldots x_m)$ 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 $C(v)=(y_1\ldots y_k)$.

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 $L(C)=\left\{x\in\{0,1\}^n\mid C\text{ מקבל את }x\right\}$.

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 מעגל בוליאני C אזי $|C|$ מספר השערים ב־C.

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

טענה: תהא $f:\{0,1\}^n\to\{0,1\}$ אזי קיים מעגל C שמחשב את f בגודל $\mathcal{O}(n\cdot2^n)$.

מסקנה: תהא $\mathcal{L}\subseteq\{0,1\}^n$ אזי קיים מעגל C עבורו $L(C)=\mathcal{L}$ וכן $|C|=\mathcal{O}(n\cdot2^n)$.

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 $\hat{\delta}(q,x)=\delta\left(\hat{\delta}\left(q,x_1\ldots x_{n-1}\right),x_n\right)$.

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 $\delta\left(q_{i-1},x_i\right)=q_i$ לכל $i\in[n]$ וכן $q_n\in F$).

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

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.
- $L\parallel\mathcal{L}$ 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 $\hat{\delta}(q,x)=\bigcup_{q\in\hat{\delta}\left(T,x_1\ldots x_{n-1}\right)}\delta(q,x_n)$.

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)$\Longleftrightarrow$(קיימים $q_0\ldots q_n\in Q$ עבורם $q_0\in S$ וכן $q_i\in\delta\left(q_{i-1},x_i\right)$ לכל $i\in[n]$ וכן $q_n\in F$).

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

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

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

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

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

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

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 $\hat{\delta}(q,x)=E\left(\bigcup_{q\in\hat{\delta}\left(T,x_1\ldots x_{n-1}\right)}\delta(q,x_n)\right)$.

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 $\sigma_1\ldots\sigma_n\in\Sigma\backslash\{\varepsilon\}$ ויהיו $k_0\ldots k_n\in\mathbb{N}$ עבורם $x=\varepsilon^{k_0}\sigma_0\varepsilon^{k_1}\sigma_1\varepsilon^{k_2}\ldots\sigma_n\varepsilon^{k_n}$ אזי $x^\varepsilon=\sigma_1\ldots\sigma_n$.

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

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

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)$\Longleftrightarrow$(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 $L\left(R^*\right)=L(R)^*$.

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

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

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

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

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

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

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

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

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

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

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

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

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

סימון: תהא $L\subseteq\Sigma^*$ שפה באשר $\Sigma^*/\sim_L$ סופית תהא $\{x_1\ldots x_n\}$ 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,Σ,δ,q_0,F) באשר

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

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 $|Q|\ge2^n$.

מכונת טיורינג (מ"ט): תהא $Q\neq\varnothing$ קבוצה סופית יהי Σ אלפבית יהי Γ אלפבית עבורו $\Sigma\subseteq\Gamma$ וכן $␣\in\Gamma\backslash\Sigma$ 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 $c=q_0v$.

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

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

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

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

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

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

מכונת טיורינג דוחה מילה: תהא M מ"ט אזי $x\in\Sigma^*$ עבורו קיימות $c_0\ldots c_n$ 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 טיורינג: תהא M מ"ט אזי $L(M)=\left\{x\in\Sigma^*\mid M\text{ מקבל את }x\right\}$.

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

מודלים שקולים: מודלים M,M' עבורם לכל A מסוג M וכן לכל B מסוג M' מתקיים

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

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

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

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

מסקנה: מכונת טיורינג ומכונת טיורינג נחה הינן מודלים שקולים.

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

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

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

קונפיגורציה התחלתית במכונת טיורינג רב־סרטית: תהא M מ"ט רב־סרטית אזי קונפיגורציה c עבורה קיים $v \in \Sigma^*$ המקיימת $c = q_0 \text{⊔}\$q_0 v \text{⊔}\$ \dots$.

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

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

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 $R_0 \dots R_k \in \mathbb{N}$ וכן $T : \mathbb{N} \to \mathbb{N}$ וכן $\text{PC} \in \mathbb{N}$.

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 טיורינג לא־דטרמיניסטית (מט"ד): תהא $Q \neq \varnothing$ קבוצה סופית יהי Γ אלפבית עבורו $\Sigma \subseteq \Gamma \setminus \{\text{⊔}\}$ וכן $\text{⊔} \in \Gamma \setminus \Sigma$ יהיו $q_0, q_a, q_r \in Q$ באשר $q_a \neq q_r$ ותהא $\delta : (Q \setminus \{q_a, q_r\}) \times \Gamma \to \mathcal{P}(Q \times \Gamma \times \{L, R\})$ אזי $(Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r)$.

קונפיגורציה עוברת: תהא N מט"ד תהא $q \in Q$ ותהא $b \in \Gamma$ ותהיינה $u, v \in \Gamma^*$ באשר $ubqbv$ קונפיגורציה אזי קונפיגורציה c' עבורה קיימת $\delta' : (Q \setminus \{q_a, q_r\}) \times \Gamma \to Q \times \Gamma \times \{L, R\}$ סופי וכן x אינו מתקבל על ידי N.

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

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

מכונת טיורינג לא־דטרמיניסטית לא עוצרת על קלט: תהא N מט"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 $\mathcal{RE} = \{\mathcal{L} \subseteq \Sigma^* \mid \mathcal{L} = L(M) \text{ עבורה מ"ט } M\}$ (קיימת מ"ט M עבורה $\mathcal{L} = L(M)$).

מכונת טיורינג מכריע שפה: תהא $\mathcal{L} \subseteq \Sigma^*$ שפה אזי מ"ט M עבורה $\mathcal{L} = L(M)$ ובנוסף 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 $\delta(q, \sigma) = \left(q', \sigma', R\right)$.
- 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 $\mathcal{L} \in \mathcal{RE} \iff$(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 $x \leq_{\text{lex}} y$ מתקיים כי $\$x\$$ רשום על הסרט לפני $\$y\$$.

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

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

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

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

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 $\{\langle N \rangle \mid \langle N \rangle \notin L(N)\}$.

שפה $\mathcal{R}$: $\text{ACC} \notin \mathcal{R}$.

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

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

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

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

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

פונקציית חשיבה: תהא $\Sigma \subseteq D$ אזי $f : D \to (\Gamma \setminus \{\text{⊔}\})^*$ עבורה קיימת מ"ט M המחשבת את f.

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

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

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

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

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

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

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

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

מסקנה: $\text{EMPTY} \leq \text{ACC}$.

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

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

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

טענה: $\text{EQ} \notin \mathcal{R}$.

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

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

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

למה: תהיינה A, B רדוקציות 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 $A \in \text{co}\mathcal{RE}$ אזי $B \in \text{co}\mathcal{RE}$.

טענה: $\text{EQ} \leq_m \text{ACC}$ 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 $\mathcal{C} \in \mathcal{P}(\mathcal{RE}) \setminus \{\mathcal{RE}, \varnothing\}$ תכונה סמנטית אזי $L_{\mathcal{C}} \notin \mathcal{R}$.

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

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

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 $\{\varnothing\} \subsetneq \mathcal{C} \subsetneq \mathcal{P}(\mathcal{RE} \setminus \{\varnothing\})$ אזי $L_{\mathcal{C}} \notin \text{co}\mathcal{RE}$.

טענה משפט רייס הרחבה שנייה: תהא $\{\mathcal{RE}\} \subsetneq \mathcal{C} \subsetneq \mathcal{P}(\mathcal{RE}) \setminus \{\varnothing\}$ באשר $\varnothing \notin \mathcal{C}$ 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: $\text{DTime}\left(n^2\right) \ni \left\{0^k 1^k \mid k \geq 0\right\}$.

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

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

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

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

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

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

משפט: קיימת מ"ט אוניברסלית U וקיים $C \in \mathbb{R}$ עבורם לכל מ"ט M לכל קלט x ולכל $t \in \mathbb{N}$ מתקיים
- אם M עוצרת על הקלט x לאחר לכל היותר t צעדים אזי U מקבלת את $\langle M, x, t \rangle$.
- אם M דוחה את x או לא עוצרת לאחר t צעדים אזי U דוחה את $\langle M, x, t \rangle$.
- U עוצרת לאחר $C \cdot t \log(t)$ צעדים.

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

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

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

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

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

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

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

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

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

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

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

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

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

טענה: $(\mathcal{EXP} = \mathcal{NEXP}) \implies (\mathcal{P} = \mathcal{NP})$.

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

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

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

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

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

טענה: קיים מוודא פולינומי ל־CLIQUE.

קבוצת צמתים בלתי תלויה (ב"ת): יהי G גרף אזי $I \subseteq V$ עבורה לכל $u, v \in I$ מתקיים $(u, v) \notin E$.

הגדרה: $\text{IS} = \{\langle G, k \rangle \mid G \text{ גרף לא מכוון בעל קבוצה ב"ת מגודל } k\}$.

טענה: קיים מוודא פולינומי ל־IS.

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

טענה: קיים מוודא פולינומי ל־FACTOR.

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

טענה: קיים מוודא פולינומי ל־SUBSETSUM.

משפט: תהא $\mathcal{L} \subseteq \Sigma^*$ שפה אזי $\mathcal{L} \in \mathcal{NP} \iff$(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 $\Sigma \subseteq D$ אזי $f : D \to (\Gamma \setminus \{\text{⊔}\})^*$ 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 Δ, Σ אלפביתים 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 Δ, Σ אלפביתים באשר $\Delta \subseteq \Sigma$ תהא $A \subseteq \Sigma^*$ שפה ותהא $B \subseteq \Delta^*$ שפה אזי $f : \Sigma^* \to \Delta^*$ 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 $\mathcal{NPH}$-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 $(\mathcal{P} = \mathcal{NP}) \iff (\mathcal{L} \in \mathcal{P})$.

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

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

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

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 $k \in \mathbb{N} \setminus \{0,1,2\}$ 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: $C - \text{CNF} = \{\langle \varphi, k \rangle \mid (\varphi \text{ CNF}) \wedge (\exists v \,(N(\varphi, v) = k))\}$.

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

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

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

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

טענה: $C - \text{CNF} \leq_p C - \text{DNF}$.

מסקנה: $C - \text{DNF} \in \mathcal{PC}$.

הגדרה: $\text{PARTITION} = \left\{\left\langle \left\{\sum_{i \in T} i = \sum_{i \in S \setminus T} i\right\}_{T \subseteq S} S \right\rangle \wedge \left(\exists T \subseteq S \left(\sum_{i \in T} i = \sum_{i \in S \setminus T} i\right)\right) \mid (S \text{ מולטי קבוצה}) \wedge (S \subseteq \mathbb{N})\right\}$.

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

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

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 $k_1 \dots k_n \in \mathbb{N}_+$ $f_1 \dots f_n \in \mathcal{B}$ באשר $f_i : \Sigma^{k_i} \to \Sigma$ לכל $i \in [n]$ ותהיינה $x_1 \dots x_m, y_1 \dots y_k \in \Sigma$ אזי גרף מכוון G מעל $\{f_1 \dots f_n, x_1 \dots x_m, y_1 \dots y_k\}$ המקיים
- G חסר מעגלים מכוונים.
- לכל $i \in [m]$ מתקיים $\deg^-(x_i) = 0$.
- לכל $i \in [n]$ מתקיים $\deg^-(f_i) = k_i$.
- לכל $i \in [k]$ מתקיים $\deg^-(y_i) = 1$ וכן $\deg^+(y_i) = 0$.

הערה: נשמור על הטרמינולוגיה ממעגל בוליאני כהכללה טבעית.

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

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

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

הגדרה: תהא $T : \mathbb{N} \to \mathbb{N}$ חשיבה בזמן באשר $n \leq T(n)$ ותהא M מ"ט רצה בזמן $T(n)$ נגדיר מעגלים מעל $\Sigma \uplus \Gamma$ כך
- יהי $z \in \Sigma \uplus \Gamma$ אזי $C_{\text{inp}}(z) = R_0(\tau_{M,z})$.
- יהי $z \in \Sigma \uplus \Gamma$ ויהי $i \in \{0, \dots, T(n) - 1\}$ אזי $C_{\text{next}}(R_i(\tau_{M,z})) = R_{i+1}(\tau_{M,z})$.

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

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

משקנה: תהא $T : \mathbb{N} \to \mathbb{N}$ חשיבה בזמן באשר $n \leq T\left(n\right)$ ותהא M מ"ט רצה בזמן $T\left(n\right)$ ויהי $z \in \Sigma \uplus \Gamma$ אזי $C^{\Sigma \uplus \Gamma}_{M,n}\left(z\right) = M\left(z\right)$.

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 $z \in \{0,1\}^n$ לכל $C\left(z\right) = f\left(C\right)\left(z\right)$ וכן $|f\left(C\right)| = \mathcal{O}\left(|C|\right)$.

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

טענה: $\text{3SAT} \in \mathcal{NPC}$.

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

טענה: $\text{3SAT} \leq_p \text{CIRSAT}$.

טענה: $\text{3SAT} \leq_p \text{SUBSETSUM}$.

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

טענה: $\text{3SAT} \leq_p \text{HAMPATH}$.

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

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

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

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

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

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

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

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

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

הגדרה: $\text{MATMULT} = \{(A, B, C) \mid (A, B, C \in M_n\left(\mathbb{Z}\right)) \wedge (A \cdot B = C)\}$

טענה: תהא $D \in M_n\left(\mathbb{Z}\right)$ באשר $D \neq 0$ אזי $\mathbb{P}_{r \leftarrow \{0,1\}^n}\left(D \cdot r = 0\right) \leq 0.5$

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

נוסחה אריתמטית: יהי $\mathbb{F}$ שדה ויהי C מעגל מעל $\mathbb{F}$ עם הבסיס $\{+, \times\}$ 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 $\varphi \equiv 0$.

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

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

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

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

דרגה טוטאלית של פולינום: תהא $d \in M_{k \times n}\left(\mathbb{N}\right)$ אזי

$$\deg\left(\sum_{i=1}^k \prod_{j=1}^n x_j^{d_{i,j}}\right) = \max\left\{\deg\left(\prod_{j=1}^n x_j^{d_{i,j}}\right) \;\middle|\; i \in [k]\right\}$$

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

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

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

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

חסם עליון לזמן ריצה של מכונת טיורינג אקראית: תהא $T\left(n\right)$ חשיבה בזמן ותהא M מכונת טיורינג אקראית אזי T.

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

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

סימון: תהא M מ"ט אקראית עם זמן ריצה $T\left(n\right)$ יהי x קלט אזי $M\left(x\right)$ משתנה מקרי לקבלת $M\left(x;r\right)$ 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 $T\left(n\right)$ המקיימת כי החל ממקום מסויים $n \in \mathbb{N}$ מתקיים

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

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

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

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

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

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

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

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

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

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

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

שפה $\text{co}\mathcal{RP}$: $\text{co}\mathcal{RP} = \text{co}\mathcal{RP}\left(0.5\right)$.

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

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

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

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

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

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

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

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

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