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 $\deg^+(y_i)=0$.

שערים במעגל בוליאני: יהי C מעגל בוליאני אזי $f_1\dots f_n$.

קלטים במעגל בוליאני: יהי C מעגל בוליאני אזי $x_1\dots x_m$.

פלטים במעגל בוליאני: יהי C מעגל בוליאני אזי $y_1\dots y_k$.

חוטים במעגל בוליאני: יהי C מעגל בוליאני אזי $E(C)$.

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

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

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

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

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 $L\left(\mathcal{C}\right)=\mathcal{L}$.

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

הערה 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 ומספר הקלטים ב־C.

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

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

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

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

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

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 $Q\ne\varnothing$ קבוצה סופית יהי Σ אלפבית תהא $\delta:Q\times\Sigma\to Q$ יהי $q\in Q$ ותהא $F\subseteq Q$ אזי $\left(Q,\Sigma,\delta,q,F\right)$.

מצבים באוטומט סופי דטרמיניסטי: יהי $\left(Q,\Sigma,\delta,q,F\right)$ אס"ד אזי Q.

אלפבית באוטומט סופי דטרמיניסטי: יהי $\left(Q,\Sigma,\delta,q,F\right)$ אס"ד אזי Σ.

פונקציית מעברים באוטומט סופי דטרמיניסטי: יהי $\left(Q,\Sigma,\delta,q,F\right)$ אס"ד אזי δ.

מצב התחלתי באוטומט סופי דטרמיניסטי: יהי $\left(Q,\Sigma,\delta,q,F\right)$ אס"ד אזי q.

מצבים מקבלים באוטומט סופי דטרמיניסטי: יהי $\left(Q,\Sigma,\delta,q,F\right)$ אס"ד אזי F.

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

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

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 $L\left(A\right)=\{x\in\Sigma^*\mid x \text{ מקבל את } A\}$.

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

טענה: $\varnothing$ רגולרית.

טענה: $\{\varepsilon\}$ רגולרית.

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

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

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

טענה: תהא $L\subseteq\Sigma^*$ שפה באשר $L\ne\varnothing$ וכן $L\ne\{\varepsilon\}$ 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: $\{x\mid\#_1\left(x\right)=0\mod 2\}$ רגולרית.

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

מצבים באוטומט סופי לא־דטרמיניסטי מינוס: יהי $\left(Q,\Sigma,\delta,S,F\right)$ אסלד"ם אזי Q.

אלפבית באוטומט סופי לא־דטרמיניסטי מינוס: יהי $\left(Q,\Sigma,\delta,S,F\right)$ אסלד"ם אזי Σ.

פונקציית מעברים באוטומט סופי לא־דטרמיניסטי מינוס: יהי $\left(Q,\Sigma,\delta,S,F\right)$ אסלד"ם אזי δ.

מצבים התחלתיים באוטומט סופי לא־דטרמיניסטי מינוס: יהי $\left(Q,\Sigma,\delta,S,F\right)$ אסלד"ם אזי S.

מצבים מקבלים באוטומט סופי לא־דטרמיניסטי מינוס: יהי $\left(Q,\Sigma,\delta,S,F\right)$ 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)$\Longleftrightarrow$(קיימים $q_0\ldots q_n\in Q$ 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 $L(M)=\{x\in\Sigma^*\mid x \text{ מקבל את } M\}$.

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

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 $x\in\Sigma^*$ ויהיו $\sigma_1\ldots\sigma_n\in\Sigma\backslash\{\varepsilon\}$ 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 $x^{\not\varepsilon}=\sigma_1\ldots\sigma_n$.

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 $q_i\in\delta\left(q_{i-1},x_i^{\not\varepsilon}\right)$ לכל $i\in[n]$ וכן $q_n\in F$).

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

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 $L(R^*)=L(R)^*$.

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

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 $r\in R\left(\Sigma\right)$ עבורו $L\left(r\right)=\mathcal{L}$).

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 $xy^{k}z\in L$.

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

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

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

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

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

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

הגדרה: יהי A אס"ד אזי $\sim_{A}=\left\{ \left(x,y\right)\in\left(\Sigma^{*}\right)^{2}\mid\hat{\delta}\left(q_{0},x\right)=\hat{\delta}\left(q_{0},y\right)\right\}$.

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

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

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 $\left\{ x_{1}\ldots x_{n}\right\}$ קבוצת נציגים של ${}^{\Sigma^{*}}/_{\sim_{L}}$ ויהי $y\in\Sigma^{*}$ עבורו $x_{i}\sim_{L}y$ אזי $\text{Class}\left(y\right)=i$.

אוטומט סופי דטרמיניסטי המחלקות: תהא $L\subseteq\Sigma^{*}$ שפה באשר ${}^{\Sigma^{*}}/_{\sim_{L}}$ סופית ותהא $\left\{ x_{1}\ldots x_{n}\right\}$ קבוצת נציגים של ${}^{\Sigma^{*}}/_{\sim_{L}}$ אזי אס"ד $\left(Q,\Sigma,\delta,q_{0},F\right)$ באשר

- $Q=\left[|{}^{\Sigma^{*}}/_{\sim_{L}}|\right]$.
- $\delta\left(i,\sigma\right)=\text{Class}\left(x_{i}\sigma\right)$.
- $q_{0}=\text{Class}\left(\varepsilon\right)$.
- $F=\left\{ i\in Q\mid x_{i}\in L\right\}$.

טענה: תהא $L\subseteq\Sigma^{*}$ שפה באשר ${}^{\Sigma^{*}}/_{\sim_{L}}$ סופית תהא $\left\{ x_{1}\ldots x_{n}\right\}$ קבוצת נציגים של ${}^{\Sigma^{*}}/_{\sim_{L}}$ יהי A אס"ד המחלקות של L ויהי $y\in\Sigma^{*}$ אזי $\hat{\delta_{A}}\left(q_{0},y\right)=\text{Class}\left(y\right)$.

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

טענה: יהי $n\in\mathbb{N}_{+}$ ויהי A אס"ד מעל $[n]$ עבורו $L\left(A\right)=\left\{ x\in\left[n\right]^{*}\mid\exists\sigma\in\Sigma.\#_{\sigma}\left(x\right)=0\right\}$ 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 $\sqcup\in\Gamma\backslash\Sigma$ יהיו $q_{0},q_{a},q_{r}\in Q$ באשר $q_{a}\neq q_{r}$ ותהא $\delta:\left(Q\backslash\left\{ q_{a},q_{r}\right\} \right)\times\Gamma\to Q\times\Gamma\times\left\{ L,R\right\}$ אזי $\left(Q,\Sigma,\Gamma,\delta,q_{0},q_{a},q_{r}\right)$.

מצבים במכונת טיורינג: תהא $\left(Q,\Sigma,\Gamma,\delta,q_{0},q_{a},q_{r}\right)$ מ"ט אזי Q.

אלפבית במכונת טיורינג: תהא $\left(Q,\Sigma,\Gamma,\delta,q_{0},q_{a},q_{r}\right)$ מ"ט אזי Σ.

אלפבית סרט במכונת טיורינג: תהא $\left(Q,\Sigma,\Gamma,\delta,q_{0},q_{a},q_{r}\right)$ מ"ט אזי Γ.

פונקציית מעברים במכונת טיורינג: תהא $\left(Q,\Sigma,\Gamma,\delta,q_{0},q_{a},q_{r}\right)$ מ"ט אזי δ.

מצב התחלתי במכונת טיורינג: תהא $\left(Q,\Sigma,\Gamma,\delta,q_{0},q_{a},q_{r}\right)$ מ"ט אזי q_{0}.

מצב מקבל במכונת טיורינג: תהא $\left(Q,\Sigma,\Gamma,\delta,q_{0},q_{a},q_{r}\right)$ מ"ט אזי q_{a}.

מצב דוחה במכונת טיורינג: תהא $\left(Q,\Sigma,\Gamma,\delta,q_{0},q_{a},q_{r}\right)$ 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 $c=uq_{a}v$.

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

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

מכונת טיורינג מקבלת מילה: תהא M מ"ט אזי $x\in\Sigma^{*}$ עבורו קיימות קונפיגורציות $c_{0}\ldots c_{n}$ באשר $c_{0}=q_{0}x$ וכן c_{i-1} עוברת ל־c_{i} לכל $i\in\left[n\right]$ וכן c_{n} קונפיגורציה מקבלת.

מכונת טיורינג דוחה מילה: תהא M מ"ט אזי $x\in\Sigma^{*}$ עבורו קיימות קונפיגורציות $c_{0}\ldots c_{n}$ באשר $c_{0}=q_{0}x$ וכן c_{i-1} עוברת ל־c_{i} לכל $i\in\left[n\right]$ וכן c_{n} קונפיגורציה דוחה.

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

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

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 $\sqcup\in\Gamma\backslash\Sigma$ יהיו $q_{0},q_{a},q_{r}\in Q$ באשר $q_{a}\neq q_{r}$ ותהא $\delta:\left(Q\backslash\left\{ q_{a},q_{r}\right\} \right)\times\Gamma\to Q\times\Gamma\times\left\{ L,R,S\right\}$ אזי $\left(Q,\Sigma,\Gamma,\delta,q_{0},q_{a},q_{r}\right)$.

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 $\sqcup\in\Gamma\backslash\Sigma$ יהיו $q_{0},q_{a},q_{r}\in Q$ באשר $q_{a}\neq q_{r}$ ותהא $\delta:\left(Q\backslash\left\{ q_{a},q_{r}\right\} \right)\times\Gamma^{k}\to Q\times\Gamma^{k}\times\left\{ L,R\right\} ^{k}$ אזי $\left(k,Q,\Sigma,\Gamma,\delta,q_{0},q_{a},q_{r}\right)$.

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

קונפיגורציה במכונת טיורינג רב־סרטית: תהא M מ"ט k־סרטית ותהיינה $c_{1}\ldots c_{k}\in\Gamma^{*}Q\Gamma^{*}$ באשר $c_{i}\cap Q=c_{j}\cap Q$ לכל $i,j\in\left[k\right]$ 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 $c=q_{0}v\sqcup\$q_{0}\sqcup\$\ldots\$q_{0}\sqcup$.

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

מודל RAM: יהי $k\in\mathbb{N}$ ותהיינה $\pi_{1}\ldots\pi_{p}:\mathbb{N}\to\mathbb{N}$ אזי $\left(k,\left(\pi_{1}\ldots\pi_{p}\right)\right)$.

מספר הרגיסטרים במודל RAM: יהי $\left(k,\Pi\right)$ מודל RAM אזי k.

פקודות במודל RAM: יהי $\left(k,\Pi\right)$ מודל RAM אזי Π.

קונפיגורציה במודל RAM: יהי $\left(k,\Pi\right)$ מודל RAM יהיו $R_{0}\ldots R_{k}\text{PC}\in\mathbb{N}$ ותהא $T:\mathbb{N}\to\mathbb{N}$ אזי $\left(T,\left\{ R_{1}\ldots R_{k}\right\} ,\text{PC}\right)$.

מונה התוכנית בקונפיגורציה: יהי $\left(k,\Pi\right)$ מודל RAM ותהא $\left(T,R,\text{PC}\right)$ קונפיגורציה אזי PC.

רגיסטרים בקונפיגורציה: יהי $\left(k,\Pi\right)$ מודל RAM ותהא $\left(T,R,\text{PC}\right)$ קונפיגורציה אזי R.

זיכרון בקונפיגורציה: יהי $\left(k,\Pi\right)$ מודל RAM ותהא $\left(T,R,\text{PC}\right)$ קונפיגורציה אזי T.

קונפיגורציה עוברת במודל RAM: יהי $\left(k,\Pi\right)$ מודל RAM ותהא $\left(T,R,\text{PC}\right)$ קונפיגורציה אזי קונפיגורציה $\left(T',R',\text{PC}'\right)$ באשר

- $\text{PC}'=\text{PC}+1$.
- קיים $i\in\left[k\right]$ עבורו לכל $j\in\left[k\right]\backslash\left\{ i\right\}$ מתקיים $R'_{j}=R_{j}$ וכן קיים $\pi\in\Pi\cup\left\{ \text{Id}\right\}$ המקיים $R'_{i}=\pi\left(R_{i}\right)$.
- קיים $i\in\mathbb{N}$ עבורו לכל $j\in\mathbb{N}\backslash\left\{ i\right\}$ מתקיים $T'\left(j\right)=T\left(j\right)$ וכן קיים $\pi\in\Pi\cup\left\{ \text{Id}\right\}$ המקיים $T'\left(i\right)=\pi\left(T\left(i\right)\right)$.

אלגוריתם במודל RAM: יהי $\left(k,\Pi\right)$ מודל RAM אזי פונקציה δ מקונפיגורציות לקונפיגורציות עבורה לכל קונפיגורציה C מתקיים C עוברת ל־$\delta\left(C\right)$.

סימון: יהי $\left(k,\Pi\right)$ מודל RAM ויהי $x\in\mathbb{N}$ נגדיר $T:\mathbb{N}\to\mathbb{N}$ כך $T\left(n\right)=\left\{ \begin{smallmatrix}x & n=0\\ 0 & \text{else} \end{smallmatrix}\right.$ אזי $\text{Start}_{x}=\left(T,\left\{ 0\right\} ,0\right)$.

סימון: יהי $\left(k,\Pi\right)$ מודל RAM יהי A אלגוריתם ויהי $x\in\mathbb{N}$ אזי $A_{\text{stop}}=\min\left\{ n\in\mathbb{N}\mid A^{\left(n+1\right)}\left(\text{Start}_{x}\right)=A^{\left(n\right)}\left(\text{Start}_{x}\right)\right\}$.

ריצה של מודל RAM: יהי $\left(k,\Pi\right)$ מודל RAM יהי A אלגוריתם ויהי $n\in\mathbb{N}$ אזי $A^{\left(A_{\text{stop}}\right)}\left(\text{Start}_{x}\right)$.

הערה: ריצת מודל RAM זהה לריצת מעבד MIPS.

טענה: מכונת טיורינג ומודל RAM הם מודלים שקולים.

מכונת טיוריג 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 $q_0 x \sqcup$ 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 $\mathcal{RE} = \{\mathcal{L} \subseteq \Sigma^* \mid \mathcal{L} = L(M) \text{ עבורה } M \text{ קיימת מ"ט}\}$.

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 $\mathcal{R} = \{\mathcal{L} \subseteq \Sigma^* \mid \mathcal{L} \text{ המכריעה את } M \text{ קיימת מ"ט}\}$.

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 $x \leq_{\text{lex}} y$ מתקיים כי $\$x\$$ רשום על הסרט לפני $\$y\$$.

טענה: תהא $\mathcal{L} \subseteq \Sigma^*$ שפה אזי ($\mathcal{L} \in \mathcal{R}$)$\Longleftrightarrow$(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 $f : \{M \mid M \text{ מ"ט}\} \to \{0,1\}^*$ 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: $\text{ACC} = \{\langle M, x \rangle \mid (M \text{ מ"ט}) \wedge (x \text{ מילה}) \wedge (M \text{ מקבלת את } x)\}$.

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

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

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

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

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

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

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

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

רדוקציית מיפוי: יהיו Σ,Δ אלפבייתים 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 $\left(x\in A\right)\Longleftrightarrow\left(f\left(x\right)\in B\right)$.

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 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 $A\le_{m}B$ אזי $B\notin\mathcal{R}$.

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

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

מסקנה: $\text{HALT}\le_{m}\text{ACC}$.

מסקנה: $\text{EMPTY}\le\text{ACC}$.

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

טענה: $\text{REG}\notin\mathcal{R}$.

הגדרה: $\text{EQ}=\left\{ \left\langle M_{1},M_{2}\right\rangle \mid L\left(M_{1}\right)=L\left(M_{2}\right)\right\}$.

טענה: $\text{EQ}\notin\mathcal{R}$.

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

טענה: $\text{HALT}\le_{m}\text{HALT}_{\varepsilon}$.

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

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 $A\le_{m}B$ 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: $\text{ACC}\le_{m}\text{EQ}$ וכן $\overline{\text{ACC}}\le_{m}\text{EQ}$.

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

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

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

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

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

הגדרה: $\text{PRIME}=\left\{ \left(p\right)_{2}\mid p\in\mathbb{P}\right\}$.

הערה: קידוד מספרים תמיד יעשה בבסיס 2.

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

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

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

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

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

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

למה: $\overline{\text{HALT}}\le_{m}\text{ALL}$.

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 $T\left(n\right)$ צעדים.

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

טענה: $\left\{ 0^{k}1^{k}\mid k\geq0\right\} \in\text{DTime}\left(n^{2}\right)$.

מסקנה: $\left\{ 0^{k}1^{k}\mid k\geq0\right\} \in\text{DTime}\left(n\log\left(n\right)\right)$.

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

מסקנה: תהא $t\left(n\right)=o\left(n\log\left(n\right)\right)$ אזי $\left\{ 0^{k}1^{k}\mid k\geq0\right\} \notin\text{DTime}\left(t\left(n\right)\right)$.

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 $\left(T\left(n\right)\right)_{2}$ בזמן $\mathcal{O}\left(T\left(n\right)\right)$.

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

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 $\left\langle M,x\right\rangle$ 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 $\left\langle M,x,t\right\rangle$.
- אם M דוחה את x או לא עוצרת לאחר t צעדים אזי U דוחה את $\left\langle M,x,t\right\rangle$.
- 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 $1\leq c<d$ אזי $\text{DTime}\left(n^{c}\right)\subsetneq\text{DTime}\left(n^{d}\right)$.

טענה: תהא $T:\mathbb{N}\to\mathbb{N}$ באשר $T\left(n\right)\geq n$ 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 $T\left(n\right)\geq n$ 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 $T\left(n\right)\geq n$ 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: $\mathcal{NP}\subsetneq\mathcal{NEXP}$.

טענה: $\left(\mathcal{P}=\mathcal{NP}\right)\Longrightarrow\left(\mathcal{EXP}=\mathcal{NEXP}\right)$.

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 $V(x,w)$ 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 $(\mathcal{L} \in \mathcal{RE})\Longleftrightarrow$(קיים מוודא ל־$\mathcal{L}$).

מוודא פולינומי לשפה: תהא $\mathcal{L} \subseteq \Sigma^*$ שפה אזי מוודא V ל־$\mathcal{L}$ 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: $\text{FACTOR} = \{\langle N, k\rangle \mid \exists d \in [k] . (d|N)\}$.

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 $(\mathcal{L} \in \mathcal{NP})\Longleftrightarrow$(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 $(\mathcal{L} \in \mathcal{P}) \Longleftrightarrow (\mathcal{P} = \mathcal{NP})$.

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: יהי $k \in \mathbb{N}_+$ אזי 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: $\text{CLIQUE}, \text{IS} \in \mathcal{NPC}$.

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

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

טענה: $C-\text{CNF}\in\mathcal{NPC}$.

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

טענה: $\text{DNFSAT}\in\mathcal{P}$.

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

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

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

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

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

טענה: $\text{VC}\in\mathcal{NPC}$.

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

מעגל: יהי Σ אלפבית יהי $\mathcal{B}$ בסיס פונקציות מעל Σ תהיינה $k_{1}\dots k_{n}\in\mathbb{N}_{+}$ תהיינה $f_{1}\dots f_{n}\in\mathcal{B}$ 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 $\deg^{-}\left(x_{i}\right)=0$.
- לכל $i\in[n]$ מתקיים $\deg^{-}\left(f_{i}\right)=k_{i}$.
- לכל $i\in[k]$ מתקיים $\deg^{-}\left(y_{i}\right)=1$ וכן $\deg^{+}\left(y_{i}\right)=0$.

הערה: נשמור על הטרמינולוגיה ממעגל בוליאני כהכללה טבעית.

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

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

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

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

טענה: תהא $T:\mathbb{N}\to\mathbb{N}$ חשיבה בזמן באשר $n\le T(n)$ ותהא M מ"ט רצה בזמן $T(n)$ 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 $n\le T(n)$ תהא M מ"ט רצה בזמן $T(n)$ 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 $n\le T(n)$ ותהא M מ"ט רצה בזמן $T(n)$ 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 ($M\left(z\right)$ מקבלת)$\Longleftrightarrow$($C_{M,n}\left(z\right)=1$).

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

מסקנה: תהא $T:\mathbb{N}\to\mathbb{N}$ חשיבה בזמן באשר $n\le T(n)$ 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: $\text{co}\mathcal{NP} \neq \mathcal{NP}$. 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 $A \in \text{co}\mathcal{NP}$.

מסקנה: 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: $\text{MATMULT} = \{\langle A, B, C\rangle \mid (A, B, C \in M_n(\mathbb{Z})) \wedge (A \cdot B = C)\}$.

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

מסקנה: קיימת מ"ט M אשר רצה בזמן $\mathcal{O}(n^2)$ עבורה
- לכל $x \in \{0,1\}^*$ אשר אינו קידוד של שלשת מטריצות $M(x)$ דוחה.
- לכל $x \in \{0,1\}^*$ עבורו קיימות $A, B, C \in M_n(\mathbb{Z})$ המקיימות $A \cdot B = C$ וכן $x = \langle A, B, C\rangle$ מתקיים $M(x)$ מקבלת.
- לכל $x \in \{0,1\}^*$ עבורו קיימות $A, B, C \in M_n(\mathbb{Z})$ המקיימות $A \cdot B \neq C$ וכן $x = \langle A, B, C\rangle$ מתקיים $\mathbb{P}(\text{מקבלת } M(x)) \leq 2^{-100}$.

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 $\varphi(x_1 \ldots x_n) = 0$ אזי $\varphi \equiv 0$.

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

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 $\text{ZE}_{\mathbb{F}} \in \mathcal{R}$.

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 $d \in M_{k \times n}(\mathbb{N})$ 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 $f \in \mathbb{F}[x_1, \ldots, x_n]$ 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 $\mathbb{P}(\text{מקבלת } M(x)) \leq 0.01$ בזמן $\text{poly}(|\varphi|)$.

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

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

טענה: תהיינה $\alpha, \beta : \mathbb{N} \to [0,1]$ באשר $\beta \leq \alpha$ 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 $\mathbb{P}_{r\leftarrow\{0,1\}^{T(n)}}(M(x;r)=1$ מקבלת$)$.
- לכל $x\notin\mathcal{L}\cap\Sigma^n$ מתקיים $\mathbb{P}_{r\leftarrow\{0,1\}^{T(n)}}(M(x;r)\le 1-\alpha(n)$ מקבלת$)$.

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

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

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

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

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

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

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

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

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

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

סימון: תהא M מ"ט k־סרטית ותהא $c_1\$c_2\$\ldots\$c_k$ קונפיגורציה אזי $(c_1\$c_2\$\ldots\$c_k)^i=c_i$.

סימון: תהא $x\in\Sigma^*$ ותהא $A\subseteq\Sigma^*$ אזי $x\backslash A$ הינה המחרוזת x ללא אברי A.

מכונת טיורינג בעלת סיבוכיות מקום: תהא $S:\mathbb{N}\to\mathbb{N}$ אזי מ"ט תלת־סרטית M עבורה לכל קונפיגורציות $c_0\ldots c_n$ באשר $c_0=q_0x$ וכן c_{i-1} עוברת ל־c_i לכל $i\in[n]$ מתקיים

- סרט לקריאה בלבד: לכל $i\in[n]$ מתקיים $c_i^1=x\backslash Q$.
- סרט חסום במקום: לכל $i\in[n]$ מתקיים $\left|c_{i-1}^2\right|\le S(n)+1$.
- סרט לכתיבה חד־פעמית: לכל $i\in[n]$ ולכל $j\in\left[\left|c_{i-1}^3\right|\right]$ מתקיים $\left(c_{i-1}^3\backslash Q\right)_j=\left(c_i^3\backslash Q\right)_j$.

חסם עליון למקום ריצה של מכונת טיורינג: תהא $S:\mathbb{N}\to\mathbb{N}$ ותהא M מ"ט בעלת סיבוכיות מקום S אזי S.

הערה: נקרא למכונת טיורינג בעלת סיבוכיות מקום מכונת טיורינג.

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

שפה PSPACE: $\text{PSPACE}=\bigcup_{c\in\mathbb{N}}\text{DSpace}(n^c)$.

שפה LOGSPACE: $\text{LOGSPACE}=\text{DSpace}(\log(n))$.

סימון: $\text{LOGSPACE}=\text{LSPACE}=\mathcal{L}$.

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

טענה: תהא T חשיבה בזמן אזי $\text{DTime}(T(n))\subseteq\text{DSpace}(T(n))$.

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

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

מסקנה: $\text{LSPACE}\subseteq\mathcal{P}$.

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

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

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

מסקנה: $\text{LSPACE}\subsetneq\text{PSPACE}$.

מסקנה: לפחות אחד מהבאים נכון

- $\text{LSPACE} \subsetneq \mathcal{P}$.
- $\mathcal{P} \subsetneq \text{PSPACE}$.

השערה: $\text{LSPACE} \subsetneq \mathcal{P}$. השערה פתוחה

השערה: $\mathcal{P} \subsetneq \text{PSPACE}$. השערה פתוחה

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

רדוקציית מיפוי במקום לוגריתמי: 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 במקום לוגריתמי.

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 במקום לוגריתמי אזי $A \le_L B$.

טענה: תהיינה A, B שפות עבורן $A \le_L B$ אזי $A \le_p B$.

שפה $\mathcal{P}$־קשה: $\mathcal{PH} = \{\mathcal{L} \mid \forall L \in \mathcal{P}\,(L \le_L \mathcal{L})\}$.

שפה $\mathcal{P}$־שלמה: $\mathcal{PC} = \mathcal{P} \cap \mathcal{PH}$.

טענה: תהא f חשיבה במקום $S : \mathbb{N} \to \mathbb{N}$ תהא g חשיבה במקום $R : \mathbb{N} \to \mathbb{N}$ ותהא $m : \mathbb{N} \to \mathbb{N}$ עבורה לכל $n \in \mathbb{N}$ ולכל $x \in \Sigma^n$ מתקיים $|f(x)| \le m(n)$ אזי $g \circ f$ חשיבה במקום $\mathcal{O}(S(n) + \log(m(n)) + R(m(n)))$.

טענה: תהיינה A, B שפות באשר $B \in \text{LSPACE}$ וכן $A \le_L B$ אזי $A \in \text{LSPACE}$.

מסקנה: תהיינה A, B, C שפות באשר $A \le_L B$ וכן $B \le_L C$ אזי $A \le_L C$.

טענה: תהא $A \in \mathcal{PC} \cap L$ אזי $\mathcal{P} = \text{LSPACE}$.

הגדרה: $\text{CVAL} = \{\langle C, x\rangle \mid (C \text{ מעגל בוליאני}) \wedge (C(x) = 1)\}$.

למה קוק־לוין: תהא M מ"ט רצה בזמן פולינומי אזי קיימת פונקציה חשיבה f במקום לוגריתמי עבורה $f(1^n) = \langle C_{M,n}\rangle$ באשר $C_{M,n}$ מעגל עבורו לכל $z \in \{0,1\}^n$ מתקיים ($M(z)$ מקבלת)$\Longleftrightarrow$($C_{M,n}(z) = 1$).

טענה: $\text{CVAL} \in \mathcal{PC}$.

סימון: תהא M מטל"ד k־סרטית ותהא $c_1\$c_2\$\ldots\$c_k$ קונפיגורציה אזי $(c_1\$c_2\$\ldots\$c_k)^i = c_i$.

מכונת טיורינג לא דטרמיניסטית בעלת סיבוכיות מקום: תהא $S : \mathbb{N} \to \mathbb{N}$ אזי מטל"ד תלת־סרטית M עבורה לכל קונפיגורציות $c_0 \ldots c_n$ באשר $c_0 = q_0 x$ וכן c_{i-1} עוברת ל־c_i לכל $i \in [n]$ מתקיים
- סרט לקריאה בלבד: לכל $i \in [n]$ מתקיים $c_i^1 = x\backslash Q$.
- סרט חסום במקום: לכל $i \in [n]$ מתקיים $|c_{i-1}^2| \le S(n) + 1$.
- סרט לכתיבה חד־פעמית: לכל $i \in [n]$ ולכל $j \in [|c_{i-1}^3|]$ מתקיים $(c_{i-1}^3\backslash Q)_j = (c_i^3\backslash Q)_j$.

חסם עליון למקום ריצה של מכונת טיורינג לא דטרמיניסטית: תהא $S : \mathbb{N} \to \mathbb{N}$ ותהא M מטל"ד בעלת סיבוכיות מקום S אזי S.

הערה: נקרא למכונת טיורינג לא דטרמיניסטית בעלת סיבוכיות מקום מכונת טיורינג לא דטרמיניסטית.

הגדרה: תהא $S : \mathbb{N} \to \mathbb{N}$ אזי $\text{NSpace}(S(n)) = \{L(M) \mid \mathcal{O}(S(n)) \text{ מטל"ד הרצה במקום } M\}$.

שפה NPSPACE: $\text{NPSPACE} = \bigcup_{c \in \mathbb{N}} \text{NSpace}(n^c)$.

שפה $\mathcal{NL}$: $\mathcal{NL} = \text{NSpace}(\log(n))$.

השערה: $\text{LSPACE} = \mathcal{NL}$. השערה פתוחה

סימון: תהא M מ"ט יהיו $x, y \in \Gamma^*$ ויהי $q \in Q$ אזי $\text{find}_Q(xqy) = |x| + 1$.

מוודא במקום לוגריתמי: תהא $A \subseteq \Sigma^*$ שפה אזי מ"ט תלת־סרטית V עבורה לכל קונפיגורציות $c_0 \ldots c_n$ באשר $c_0 = q_0 x$ וכן c_{i-1} עוברת ל־c_i לכל $i \in [n]$ מתקיים
- סרט לקריאה בלבד: לכל $i \in [n]$ מתקיים $c_i^1 = x\backslash Q$.
- סרט עד: לכל $i \in [n]$ מתקיים $\text{find}_Q(c_{i-1}^2) \le \text{find}_Q(c_i^2)$.
- סרט עבודה: לכל $i \in [n]$ מתקיים $|c_{i-1}^3| \le S(n) + 1$.

וכן לכל $x \in \Sigma^*$ מתקיים ($x \in A$)$\Longleftrightarrow$(קיים $w \in \Sigma^*$ עבורו $V(x\$w)$ מקבלת).

סימון: תהא $A \subseteq \Sigma^*$ שפה יהי V מוודא בזמן לוגריתמי ויהיו $x, w \in \Sigma^*$ אזי $V(x, w) = V(x\$w)$.

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

הגדרה: $\text{STCON} = \{\langle G, s, t\rangle \mid (G \text{ גרף מכוון}) \wedge (\text{קיים מסלול מ־} s \text{ ל־} t)\}$.

טענה: $\text{STCON} \in \mathcal{NL}$.

שפה $\mathcal{NL}$-קשה: $\mathcal{NLH} = \{\mathcal{L} \mid \forall L \in \mathcal{NL}\,(L \le_L \mathcal{L})\}$.

שפה $\mathcal{NL}$-שלמה: $\mathcal{NLC} = \mathcal{NL} \cap \mathcal{NLH}$.

טענה: $\text{STCON} \in \mathcal{NLC}$.

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

אלגוריתם לקיום מסלול עם חסם לאורכו בגרף מכוון: יהי G גרף מכוון יהיו $s, t \in V$ ויהי $\ell \in \mathbb{N}_+$ אזי

```
function Reach(G, s, t, ℓ):
    if ℓ = 1 then
        if (s, t) ∈ E then return True
        return False
    for v ∈ V do
        b1 ← Reach(G, s, v, ⌈ℓ/2⌉)
        b2 ← Reach(G, v, t, ⌊ℓ/2⌋)
        if b1 ∧ b2 then return True
    end
    return False
```

טענה: יהי G גרף מכוון יהיו $s, t \in V$ ויהי $\ell \in \mathbb{N}_+$ אזי $(\text{Reach}(G,s,t,\ell) = \text{True}) \Longleftrightarrow$(קיים מסלול מ־$s$ ל־t באורך לכל היותר ℓ).

משפט סאביץ': $\text{STCON} \in \text{DSpace}\left(\log(n)^2\right)$.

מסקנה: $\mathcal{NL} \subseteq \text{DSpace}\left(\log(n)^2\right)$.

מסקנה: תהא $S : \mathbb{N} \to \mathbb{N}$ חשיבה במקום באשר $S \ge \log$ אזי $\text{NSpace}(S(n)) \subseteq \text{DSpace}\left(S^2(n)\right)$.

מסקנה: $\text{PSPACE} = \text{NPSPACE}$.

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

משפט אימרמן־סלפצ'ני: $\overline{\text{STCON}} \in \mathcal{NL}$.

מסקנה: $\mathcal{NL} = \text{co}\mathcal{NL}$.

פסוק EkCNF: יהי $k \in \mathbb{N}_+$ אזי 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 $\varphi = \bigwedge_{i=1}^{m} \bigvee_{j=1}^{k} (A)_{i,k}$ וכן $\left|\text{FV}\left(\bigvee_{j=1}^{k} (A)_{i,k}\right)\right| = k$ לכל $i \in [m]$.

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

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

טענה: יהי $k \in \mathbb{N}_+$ תהא $\varphi \in \text{E}k\text{SAT}$ אזי $\mathbb{P}_{v:\{p_i\} \to \{\text{True},\text{False}\}}(\overline{v}(\varphi) = \text{True}) = \frac{k}{8}$.

יחס הפסוקיות המסופקות: יהיו $k, m \in \mathbb{N}_+$ תהא $A \in M_{m \times k}(\{p_i\} \cup \{\neg p_i\})$ ותהא v השמה אזי $\text{RCl}\left(\bigwedge_{i=1}^{m} \bigvee_{j=1}^{k} (A)_{i,k}, v\right) = \frac{1}{m} \cdot \text{Cl}\left(\bigwedge_{i=1}^{m} \bigvee_{j=1}^{k} (A)_{i,k}, v\right)$.

משפט PCP: קיימת רדוקציה פולינומית f מ־3CNF ל־E3CNF המקיימת

- תהא $\varphi \in 3\text{CNF}$ ספיקה אזי $f(\varphi)$ ספיקה.
- תהא $\varphi \in 3\text{CNF}$ לא ספיקה ותהא v השמה אזי $\text{RCl}(f(\varphi), v) \le \frac{7.01}{8}$.

מסקנה: תהא f רדוקציה פולינומית מ־3CNF ל־E3CNF עבורה $f(\varphi)$ ספיקה לכל $\varphi \in 3\text{CNF}$ ספיקה וכן קיימת $\varphi \in 3\text{CNF}$ לא ספיקה וקיימת השמה v עבורן $\text{RCl}(f(\varphi), v) > \frac{7.01}{8}$ אזי $\mathcal{P} = \mathcal{NP}$.