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: תהא X קבוצה אזי $f:X\to\{0,1\}$.

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

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

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

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

חוטים: יהי C מעגל בוליאני אזי $E(C)$.

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

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

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

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

משפחה מכריעה שפה: תהא $L\subseteq\{0,1\}^*$ שפה אזי משפחה של מעגלים $\{C_n\}_{n\in\mathbb{N}}$ עבורה לכל $n\in\mathbb{N}$ ולכל $x\in\{0,1\}^n$ מתקיים $(C_n(x))\Longleftrightarrow(x\in L)$.

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

מודל יוניפורמי: משפחה של מעגלים $\{C_n\}_{n\in\mathbb{N}}$ 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 $\{C_n\}_{n\in\mathbb{N}}$ משפחה של מעגלים אזי $S:\mathbb{N}\to\mathbb{N}$ עבורה $|C_n|\le S(n)$.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

טענה: $\varnothing$ רגולרית.

טענה: $\{\varepsilon\}$ רגולרית.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

טענה: יהי M אסלד"ם ויהי $x\in\Sigma^n$ אזי (M מקבל את x)$\Longleftrightarrow$(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 $L(M)=\{x\in\Sigma^*\mid x$ 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 $\hat{\delta}(q,x)=R\left(\bigcup_{q\in\hat{\delta}(T,x_1\ldots x_{n-1})}\delta(q,x_n)\right)$.

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

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 $R(\Sigma)=\{r\in\Sigma^*\mid$ ביטוי רגולרי $r\}$.

הערה: קיים סדר פעולות לביטויים רגולריים

- סגור קליני.
- שרשור.
- איחוד.

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

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

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

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

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

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

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

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