מעגלים בוליאניים

הגדרה (מעגל בוליאני): תהי B קבוצה של פונקציות בוליאניות. מעגל בוליאני מעל B עם ביטי קלט $x_1,\ldots,x_n$ וביטי פלט $y_1,\ldots,y_m$ הוא גרף מכוון וחסר מעגלים שמקיים את התכונות הבאות: • כל צומת מסומן ע"י ביט קלט x_i, ביט פלט y_i, או $g\in B$ • לכל ביט פלט y_i, בדיוק צומת אחד מסומן ע"י y_i עם דרגת כניסה 1 ודרגת יציאה 0 • דרגת הכניסה של כל צומת קלט - 0 • לכל צומת המסומן בפונקציה $g\in B$ אם g מוגדרת על $\{0,1\}^k$ אז דרגת הכניסה k. כל צומת נכנסת מקבלת אינדקס.

צומת שמסומן בפונקציה נקרא "שער" וקשתות "חוטים". ה־**fan-out** של המעגל הוא דרגת היציאה המקסימלית. מעגלים עם fan-out=1 נקראים "נוסחאות".

טענה: יש תהליך שהופך מעגל לנוסחה, אבל צריך כמה עותקים של הקלטים.

טענה: כל $f:\{0,1\}^n\to\{0,1\}$ חשיבה מעל דה מורגן $(\neg,\wedge,\vee)$.

הגדרה (משפחה של מעגלים): $\mathcal{C}=\{c_n\}_{n\in\mathbb{N}}$, c_n מוגדר על קלטים באורך n.
$\mathcal{C}$ מכריעה שפה $L\subseteq\{0,1\}^*$ אם לכל $n\in\mathbb{N}$ ולכל $x\in\{0,1\}^n$, $c_n(x)=1\iff x\in L$

הגדרה (גודל): גודל של מעגל הוא מספר השערים בו.

הגדרה: נגיד ש $L\in SIZE(O(f(n)))$ אם קיימת משפחה של מעגלים $\mathcal{C}=\{c_n\}_{n\in\mathbb{N}}$ שמכריעה את L וגם $|c_n|\le f(n)$

טענה (מתרגול): $f:\{0,1\}^n\to\{0,1\}$ ניתנת לחישוב ע"י מעגל בגודל $O(2^n)$.

טענה (מתרגול): $f:\{0,1\}^n\to\{0,1\}$ ניתנת לחישוב ע"י מעגל בגודל $O\left(\frac{2^n}{n}\right)$.

טענה (שאנון): עבור n גדול מספיק קיימות פונקציות שלא ניתנות לחישוב ע"י מעגלים בגודל $s<\frac{2^n}{10n}$.

אוטומטיים סופיים

הגדרה (אס"ד): אס"ד הוא חמישיה $A=(Q,\Sigma,\delta,q_0,F)$
• Q קבוצה סופית של מצבים • Σ אלפאבית • $\delta:Q\times\Sigma\to Q$ פונקציית המעברים • q_0 מצב תחילי • $F\subseteq Q$ קבוצת המצבים המקבלים.

פונקציית המעברים המורחבת $\hat{\delta}:Q\times\Sigma^*\to Q$ מוגדרת באינדוקציה:
$$\hat{\delta}(q,\varepsilon)=q,\ \ \hat{\delta}(q,x_1,\ldots,x_n)=\delta\left(\hat{\delta}(x_1,\ldots,x_{n-1}),x_n\right)$$
האוטומט מקבל מילה $x\in\Sigma^*$ אם $\hat{\delta}(q_0,x)\in F$.
שפה נקראת רגולרית אם קיים אס"ד שמקבל אותה.

תכונות סגירות: • איחוד • חיתוך • משלים • שרשור • חזקה • סגור קליני

סגור קליני: $V^0=\{\varepsilon\},V^{i+1}=\{wv\mid w\in V^i,v\in V\},V^*=\bigcup_{i\ge0}V^i$

טענה (מתרגול): L רגולרית אמ"מ $\{w^R\mid w\in L\}$ רגולרית

טענה (מתרגול): L רגולרית אז גם $\{w_1w_2\mid w_1,w_2\in\Sigma^*\wedge\exists\sigma\in\Sigma:w_1\sigma w_2\in L\}$ רגולרית

טענה (משיעורי הבית): L רגולרית אז $\left\{x_1x_2...x_k\ \middle|\ \begin{array}{c}k\in\mathbb{N},x_1,...,x_k\in\Sigma,\exists y_1,...,y_{2k}\in\Sigma:\\ x_1y_1y_2,....,x_ky_{2k-1}y_{2k}\in L\end{array}\right\}$ רגולרית

טענה (משיעורי הבית): L רגולרית אז $\{xy\mid yx\in L\}$ רגולרית

טענה (משיעורי הבית): L רגולרית אז לכל L' $\{x\in\Sigma^*\mid\exists y\in L',xy\in L\}$ רגולרית

הגדרה (אסל"ד): אסל"ד הוא חמישיה $N=(Q,\Sigma,\delta,S,F)$
• Q קבוצה סופית של מצבים • Σ אלפאבית • $\delta:Q\times(\Sigma\cup\{\varepsilon\})\to2^Q$ פונקציית המעברים • $S\subseteq Q$ מצבים תחיליים • $F\subseteq Q$ מצבים מקבלים.

כדי להגדיר את $\hat{\delta}:2^Q\times\Sigma^*\to2^Q$ נגדיר סביבת אפסילון $E(q)$ להיות:
$$E(q)=\{q'\in Q\mid\exists q_0,\ldots,q_k\in Q.q_0=q,\forall i.\delta(q_{i-1},q_i)=\varepsilon,q_k=q'\}$$
$$\hat{\delta}(Q',w)=\begin{cases}E(Q') & w=\varepsilon\\ E\left(\bigcup_{r\in\hat{\delta}(Q')}\delta(r,w_n)\right) & n=|w|\ge1\end{cases}$$
האסל"ד מקבל מילה $x\in\Sigma^*$ אם $\hat{\delta}(S,x)\cap F\neq\emptyset$

משפט: לכל אסל"ד קיים אס"ד כך ש־$L(A)=L(B)$. (הוכחה: כל מצב מייצג קבוצה של מצבים)

ביטויים רגולרים: $a\in\Sigma,\ \varepsilon,\ \emptyset,\ (R_1\cup R_2),\ (R_1R_2),\ (R^*)$

טענה: שפה רגולרית $\iff$ קיים לה ביטוי רגולרי.

טענה (מתרגול): לכל שני ביטווים רגולרים r,s מתקיים $L((r^*s^*)^*)=L((r\cup s)^*)$

למת הניפוח: לכל שפה רגולרית $\mathcal{L}$ קיים $0<\ell$ כך שלכל $s\in\mathcal{L}$ עם $|s|\ge\ell$, $s=xyz$ כך ש: • $xy^iz\in\mathcal{L}$ לכל $0\le i$ • $|y|>0$ • $|xy|\le\ell$
אבל, לא כל שפה שמקיימת את למת הניפוח היא רגולרית. למשל, $\mathcal{L}=\{a^ib^nc^n\mid n\ge0,i\ge1\}\cup\{b^nc^m\mid n,m\ge0\}$

מיהיל־נרוד: נאמר ש־$x\overset{\mathcal{L}}{\sim}y$ אם לכל $z\in\Sigma^*$, $xz\in\mathcal{L}\iff yz\in\mathcal{L}$. אז, $\mathcal{L}$ רגולרית $\iff$ יש כמות סופית של מחלקות שקילות של ב־$\overset{\mathcal{L}}{\sim}$.

משפט: $\mathcal{L}$ רגולרית אז $\mathcal{L}\in Size(O(n))$

מכונות טיורינג וכריעות

הגדרה (מכונת טיורינג): מכונת טיורינג היא שביעייה $(Q,\Sigma,\Gamma,\delta,q_0,q_a,q_r)$
• Q קבוצה סופית • Γ אלפאבית סרט, $\llcorner\in\Gamma$. • $\Sigma\subset\Gamma$ אלפאבית קלט, $\llcorner\notin\Sigma$ • $\delta:(Q\setminus\{q_a,q_r\})\times\Gamma\to Q\times\Gamma\times\{L,R\}$ פונקציית מעברים • $q_0\in Q$ מצב התחלתי, $q_a\in Q$ מצב מקבל, $q_r\in Q$ מצב דוחה $q_r\neq q_a$

הגדרה (מטל"ד): מ"ט לא דטרמיניסטית־ מטל"ד היא שביעייה $(Q,\Sigma,\Gamma,\delta,q_0,q_a,q_r)$
• Q קבוצת מצבים סופית • Γ אלפאבית סרט, $\llcorner\in\Gamma$. • $\Sigma\subset\Gamma$ אלפאבית קלט, $\llcorner\notin\Sigma$ • $\delta:(Q\setminus\{q_a,q_r\})\times\Gamma\to2^{Q\times\Gamma\times\{L,R\}}$ פונקציית מעברים • $q_0\in Q$ מצב התחלתי, $q_a\in Q$ מצב מקבל, $q_r\in Q$ מצב דוחה $q_r\neq q_a$

טענה: המודלים של מ"ט ומטל"ד שקולים. הרעיון: לסרוק את עץ החישוב ולבדוק האם עלה כלשהו מקבל.

הגדרה (קונפיגורציה): קונפיגורציה מייצגת את המצב של מ"ט ברגע מסוים. למשל $1011q_70111$ אומר שהתוכן של הסרט הוא 10110111, שהמצב הוא q_7, ושהמ"ט נמצאת בתא החמישי של הסרט (על 0). הקונפיגורציה ההתחלתית עבור קלט w היא q_0w.

הגדרה: M מקבלת/דוחה קלט $x\in\Sigma^*$ אם קיימת סדרת קונפיגורציות $c_0,\ldots,c_t$ כך ש־$c_0=q_0x$, c_{i-1} עוברת ל־c_i, ו־c_t מקבלת/דוחה, ונסמן ב־$\mathcal{L}(M)$ את כל המילים ש־M מקבלת.

הגדרה ($\mathcal{R}$): שפה $\mathcal{L}$ כריעה אם קיימת מ"ט שעוצרת לכל קלט x, ומקבלת $\iff x\in\mathcal{L}$. $\mathcal{R}$ אוסף השפות הכריעות.

הגדרה ($\mathcal{RE}$): שפה $\mathcal{L}$ כריעה למחצה אם קיימת מ"ט שמקבלת $\iff x\in\mathcal{L}$. $\mathcal{RE}$ אוסף השפות הכריעות למחצה.

הגדרה שקולה: מ"ט E הינה מונה עבור $L\subseteq\Sigma^*$ אם:
• ל־E יש סרט פלט לכתיבה חד פעמית • הא"ב של סרט הפלט הוא $\Sigma\cup\{\$\}$
• בריצה על הקלט הריק: לכל $x\in\mathcal{L}$ המחרוזת $\$x\$$ תופיע בפלט ואם $x\notin\mathcal{L}$ אז $\$x\$$ לא תופיע. $\mathcal{L}\in\mathcal{RE}\iff$ קיים מונה.

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

משפט: קיימת מ"ט שמסמלצת מכונות טיורינג ויש לה מספר מצבים <100.

טענה: קיימת שפה $\mathcal{L}\subseteq\{0,1\}^*$ שאינה כריעה. כי $\aleph_0\le|\text{TMs}|\le|\mathcal{RE}|$ ו־$|\mathcal{L}|=\aleph$.

הוכחה ש־$\text{ACC}\notin\mathcal{R}$: נניח בשלילה שמ"ט A מכריעה את ACC. נשתמש ב־A ונבנה מ"ט חדשה: $\text{Flip}(\langle M\rangle)$. אם A דוחה Flip מקבלת ואם A מקבלת Flip דוחה. אבל, $\text{Flip}(\langle\text{Flip}\rangle)$ מקבלת $\iff$ $A(\langle\text{Flip},\langle\text{Flip}\rangle\rangle)$ דוחה $\iff$ $\text{Flip}(\langle\text{Flip}\rangle)$ לא מקבלת. סתירה.

הגדרה (פונקציה חשיבה): יהיו M מ"ט, $D\subseteq\Sigma^*$, $f:D\to\Gamma^*\setminus\{\llcorner\}$. M מחשבת את f אם לכל קלט $x\in D$, M עוצרת ובסוף הריצה על הסרט כתוב $f(x)\llcorner$.

רדוקציית מיפוי: יהיו $A,B\subseteq\Sigma^*$. רדוקציית מיפוי מ־A ל־B היא פונקציה חשיבה $f:\Sigma^*\to\Sigma^*$ כך שלכל $x\in\Sigma^*$, $x\in A\iff f(x)\in B$, ונסמן $A\le_m B$. אם $A\le_m B$ אז,
• $A\in\mathcal{R}\Longleftarrow B\in\mathcal{R}$ • $A\in\mathcal{RE}\Longleftarrow B\in\mathcal{RE}$ • $A\in co\mathcal{RE}\Longleftarrow B\in co\mathcal{RE}$

משפט רייס: יהיו $\mathcal{C}\subseteq\mathcal{RE}$ אוסף שפות כך ש־$\emptyset\neq\mathcal{C}\neq\mathcal{RE}$. אז:
$$\mathcal{L}_\mathcal{C}=\{\langle M\rangle\mid\mathcal{L}(M)\in\mathcal{C},M\text{ is a TM}\}\notin\mathcal{R}$$
הרחבה 1: $\emptyset\subsetneq\mathcal{C}\subseteq\mathcal{RE}\setminus\{\emptyset\}$ אז $\mathcal{L}_\mathcal{C}\notin co\mathcal{RE}$ **הרחבה 2:** $\emptyset\in\mathcal{C}\subsetneq\mathcal{RE}$ אז $\mathcal{L}_\mathcal{C}\notin\mathcal{RE}$ **הרחבה 3:** $\emptyset\subsetneq\mathcal{C}\subsetneq\mathcal{RE}\setminus\{\Sigma^*\}$ אז $\mathcal{L}_\mathcal{C}\notin\mathcal{RE}$ **הרחבה 4:** $\Sigma^*\in\mathcal{C}\subseteq\mathcal{RE}$ אז $\mathcal{L}_\mathcal{C}\notin co\mathcal{RE}$

הגדרה (מוודא): תהי v מ"ט עם א"ב קלט $\{,\}\cup\Sigma$ ותהי $\mathcal{L}\subseteq\Sigma^*$. v מוודא עבור $\mathcal{L}$ אם:
• שלמות: לכל $x\in\mathcal{L}$ קיים $w\in\Sigma^*$ כך ש־$v(x,w)$ מקבל • נאותות: לכל $x\notin\mathcal{L}$ ולכל $w\in\Sigma^*$, $v(x,w)$ דוחה. w נקראת עד.

טענה: $\mathcal{L}\in RE\iff$ ל־$\mathcal{L}$ קיים מוודא פולינומי.

סיבוכיות זמן

הגדרה (זמן ריצה): תהי $T:\mathbb{N}\to\mathbb{N}$, M רצה בזמן $T(n)$ אם M מבצעת לכל היותר $T(n)$ לפני שהיא עוצרת עבור קלט באורך n.
$$\text{DTime}(T(n))=\{\mathcal{L}(M)\mid M\text{ runs in time }O(T(n))\}$$

משפט היררכיית הזמן: $T:\mathbb{N}\to\mathbb{N}$ חשיבה בזמן אם קיימת מ"ט שבהנתן 1^n מחשבת את $T(n)$ בזמן $O(T(n))$. תהי $T(n)$ חשיבה בזמן ו־$t(n)$ שמקיימת $t(n)\log t(n)=o(T(N))$, אז $\text{DTime}(t(n))\subsetneq\text{DTime}(T(n))$.

רעיון הוכחה: מקבל קלט w. מחשב את $T(n)$. דוחה אם w לא מהצורה $\langle M,0^k\rangle$ או אם $|\langle M\rangle|>\log T(n)$. מריץ $T(n)$ צעדים של $U(\langle M,w\rangle)$ (נותנים ל־M בתור קלט את עצמה!). אם U עצרה וקיבלה, Flip דוחה, אחרת Flip מקבל. נשים לב שלכל מ"ט M ש־Flip הריץ עד הסוף, Flip יפלוט פלט שונה ממנה, ולכן הוא שונה מכל מ"ט כזו.

משפט: אם $\mathcal{L}\in\text{DTime}(o(n\log n))$ אז $\mathcal{L}$ רגולרית.

דוגמה לזמן ריצה שונה במ"ט דו סרטית: השפה היא מחרוזות עם אותה כמות של אפסים ואחדים. $O(n)$ בדו סרטית (סרט שנעתיק אליו את האפסים, ואז נעבור על שני הסרטים), אבל $\Omega(n\log n)$ בחד סרטית (צריך לספור איכשהו).

משפט (סימולציה של רב־סרטית): מ"ט רב־סרטית בעלת זמן ריצה $n\le T(n)$ ניתנת לסימולציה ע"י מ"ט חד־סרטית בעלת זמן ריצה $O(T^2(n))$.

משפט (סימולציה של חד־סרטית): קיימת מ"ט אוניברסלית U כך שלכל M,x אם $M(x)$ עוצרת תוך t צעדים, אזי $U(\langle M,x\rangle)$ עוצרת תוך $O(|\langle M\rangle|^3t\log t)$ צעדים.
הפער של $\log t$ נובע מהתקורה של סימולציה אוניברסלית על מ"ט חד־סרטית. עבור מ"ט רב־סרטית ניתן לסמלץ בזמן לינארי.

הגדרה (זמן ריצה לא דטרמיניסטי): תהי $t:\mathbb{N}\to\mathbb{N}$ ו־N מטל"ד. N רצה בזמן $t(n)$ אם לכל $n\in\mathbb{N}$ ולכל קלט x באורך n, עץ הקונפיגורציות $T_{N,x}$ בעומק לכל היותר $t(n)$.
$$\text{NTime}(T(n))=\{\mathcal{L}(N)\mid N\text{ runs in time }O(T(n))\}$$

טענה: כל מטל"ד בעלת זמן ריצה $t(n)$ ניתנת לסימולציה ע"י מ"ט דטרמיניסטית בזמן $2^{O(t(n))}$.

הגדרה: $\mathsf{P}=\bigcup_{c\in\mathbb{N}}\text{DTime}(n^c)$, $\mathsf{NP}=\bigcup_{c\in\mathbb{N}}\text{NTime}(n^c)$

הגדרה (מוודא פולינומי): תהי v מ"ט עם א"ב קלט $\{,\}\cup\Sigma$ ותהי $\mathcal{L}\subseteq\Sigma^*$. v מוודא פולינומי עבור $\mathcal{L}$ אם:
• שלמות: לכל $x\in\mathcal{L}$ קיים $w\in\Sigma^*$ כך ש־$v(x,w)$ מקבל • נאותות: לכל

$x \notin \mathcal{L}$ ולכל $w \in \Sigma^*$, $v(x,w)$ דוחה • <u>יעילות:</u> קיים פולינום $p(n)$ כך שלכל $x,w \in \Sigma^*$ זמן הריצה של $v(x,w)$ לכל היותר $p(|x|)$. <u>w נקראת עד</u>.

טענה: $\mathcal{L} \in \mathsf{NP} \iff$ ל-$\mathcal{L}$ קיים מוודא פולינומי.

הגדרה (רדוקציית מיפוי פולינומית): יהיו Σ_A, Σ_B אלפאביתים, $A \subseteq \Sigma_A^*, B \subseteq \Sigma_B^*$. רדוקציית מיפוי פולינומית מ-A ל-B היא פונקציה $f : \Sigma_A^* \to \Sigma_B^*$ חשיבה בזמן פולינומי כך שלכל $x \in \Sigma_A$, $f(x) \in B \iff x \in A$. <u>סימון:</u> $A \leq_p B$.
אם $A \leq_p B$ ו-$B \in \mathsf{P}$ אז $A \in \mathsf{P}$.
אם $A \leq_p B$ ו-$B \in \mathsf{NP}$ ו-$A \in \mathsf{NPC}$ אז $B \in \mathsf{NPC}$

הגדרה (בעיה NP-שלמה): $\mathcal{L}_0$ נקראת NP-שלמה אם: • $\mathcal{L}_0 \in \mathsf{NP}$ • לכל $\mathcal{L} \in \mathsf{NP}$, $\mathcal{L} \leq_p \mathcal{L}_0$. המחלקה של NP-שלמות היא NPC.

דוגמה: $\mathrm{ACC}_{\mathsf{NP}} = \left\{\left\langle M, x, 1^t\right\rangle \mid \exists w. M(x,w) \text{ accepts in time } t\right\}$. $\mathrm{ACC}_{\mathsf{NP}} \in \mathsf{NPC}$.

הגדרה: נוסחת 3CNF $\Phi(x_1,\ldots,x_n)$ הינה מהצורה $\bigwedge_{j\in[k]} c_i$ כאשר כל c_i מהצורה $c_i = (z_{i,1} \vee z_{i,2} \vee z_{i,3})$ כאשר $z_{i,j} \in \{x_1,\ldots,x_n,\overline{x_1},\ldots,\overline{x_n}\}$.

הגדרה: $3\mathrm{SAT} = \{\langle\Phi\rangle \mid \Phi \text{ is satisfiable 3CNF}\}$. **משפט:** $3\mathrm{SAT} \in \mathsf{NPC}$.

הלב של קוק-לוין: תהי $n \leq t(n)$ חשיבה בזמן ותהי M מ"ט הרצה ב-$t(n)$. קיימת פונקציה חשיבה בזמן $\mathrm{poly}(t(n))$ שבהנתן 1^n מחשבת (קידוד) מעגל $\mathcal{C}_{m,n} : \{0,1\}^N \to \{0,1\}$ המקיים:
• לכל $z \in \{0,1\}^n$, $M(z)$ מקבלת $\iff \mathcal{C}_{m,n}(z) = 1$ • $|\mathcal{C}_{m,n}| = O\left(t^2(n)\right)$

רעיון הוכחה: לבנות מעגל שמעביר מקונפיגורציה אחת לבאה ואז לחבר $t(n)$ כאלה זה לזה.

מסקנה: אם $f : \{0,1\}^* \to \{0,1\}$ אינה ניתנת לחישוב ע"י משפחת מעגלים בגודל $O(s(n))$ אז לא ניתנת לחישוב ע"י מ"ט בזמן $\sqrt{s(n)}$.

מסקנה: $\mathrm{CIRSAT} \in \mathsf{NPC}$ **מסקנה:** $3\mathrm{SAT} \in \mathsf{NPC}$ (רדוקציה מ-CIRSAT ל-3SAT).

<u>אקראיות בחישוב</u>

הגדרה: מ"ט אקראית עם זמן ריצה $t(n)$ הינה מ"ט דו-סרטית: הסרט הראשון מאכלס בתחילת הריצה את הקלט x ומשמש בסרט עבודה. הסרט השני הינו "סרט אקראיות" ומאותחל בתחילת הריצת למחרוזת $r \in \{0,1\}^{t(|x|)}$. $M(x;r)$ מסמנת ריצה על קלט x עם אקראיות r. נתייחס ל-$M(x)$ בתור משתנה מקרי $M(x;r)$.

הגדרה: תהי $\alpha(n) \in [0,1]$, $\mathcal{L} \in \mathrm{RP}(\alpha(n))$ אם קיימת מ"ט אקראית M הרצה בזמן פולינומי $p(n)$ כך שלכל n מספיק גדול, ו-$x \in \{0,1\}^n$:
• אם $x \in \mathcal{L}$, $\Pr_{r \leftarrow \{0,1\}^{p(n)}}[M(x;r) = 1] \geq \alpha(n)$
• אם $x \notin \mathcal{L}$, $\Pr_{r \leftarrow \{0,1\}^{p(n)}}[M(x;r) = 1] = 0$

הגדרה: $\mathrm{coRP} = \left\{L \mid \overline{L} \in \mathrm{RP}(\alpha(n))\right\}$ (לעולם לא טועים עבור $x \in \mathcal{L}$).

מוסכמה: $\mathrm{RP} = \mathrm{RP}(1/2)$, $\mathrm{coRP} = \mathrm{coRP}(1/2)$.

טענה: לכל $c,d \in \mathbb{N}$, $\mathrm{RP}(n^{-c}) = \mathrm{RP}\left(1 - 2^{-n^d}\right)$. מריצים n^{c+d} פעמים ומקבלים אם אחת הריצות קיבלה.

טענה: $\mathsf{NP} = \bigcup_{c>0} \mathrm{RP}\left(2^{-n^c}\right)$

הגדרה: יהיו $\alpha(n), \beta(n) \in [0,1]$, $\mathcal{L} \in \mathrm{BPP}(\alpha(n), \beta(n))$ אם קיימת מ"ט אקראית M הרצה בזמן פולינומי $p(n)$ כך שלכל n גדול מספיק ו-$x \in \{0,1\}^n$,
• אם $x \in \mathcal{L}$, $\Pr_{r \leftarrow \{0,1\}^{p(n)}}[M(x;r) = 1] \geq \beta(n)$
• אם $x \notin \mathcal{L}$, $\Pr_{r \leftarrow \{0,1\}^{p(n)}}[M(x;r) = 1] \leq \alpha(n)$

ניתן לומר ש-$\mathrm{RP} = \mathrm{BPP}\left(0, \frac{1}{2}\right)$ ו-$\mathrm{coRP} = \mathrm{BPP}\left(\frac{1}{2}, 1\right)$.

מוסכמה: $\mathrm{BPP} = \mathrm{BPP}(1/3, 2/3)$

טענה: לכל $c,d \in \mathbb{N}$ ו-$\alpha(n)$ חשיבה בזמן $\mathrm{poly}(n)$ כך שלכל n גדול מספיק $\left(\alpha(n) - n^{-c}, \alpha(n) + n^{-c}\right) \subseteq [0,1]$, מתקיים:

$$\mathrm{BPP}\left(\alpha(n) - n^{-c}, \alpha(n) + n^{-c}\right) \subseteq \mathrm{BPP}\left(2^{-n^d}, 1 - 2^{-n^d}\right)$$

משפטים בהסתברות:

צ'רנוף-הופדינג: יהיו $A_1,\ldots,A_s$ משתני ברנולי ב"ת עם תוחלת זהה $E[A_i] = p$, אזי:

$$\Pr\left[\left|p - \frac{1}{s}\sum_{i=1}^{s} A_i\right| \geq \delta\right] \leq 2^{-\Omega\left(\delta^2 s\right)}$$

<u>סיבוכיות מקום</u>

המודל: סרט קלט - לקריאה בלבד, אפשר לעבור עליו לשני הכיוונים.
סרט עבודה: קריאה/כתיבה, אפשר לעבור עליו לשני הכיוונים, מקום מוגבל.
סרט פלט: כתיבה חד פעמית, אפשר לעבור עליו רק בכיוון אחד.
נאמר ש-M רצה במקום $s(n)$ אם לכל $n \in \mathbb{N}$ ולכל קלט x באורך n, M משתמשת בלכל היותר $s(n)$ תאים על סרט העבודה בטרם עוצרת (בפרט תמיד עוצרת).

הגדרה: $\mathrm{DSpace}(s(n)) = \{\mathcal{L}(M) \mid M \text{ is a TM, space } O(s(n))\}$
$\mathsf{PSPACE} = \bigcup_{c\in\mathbb{N}} \mathrm{DSpace}(n^c)$
$\mathsf{L} = \mathsf{LOGSPACE} = \mathrm{DSpace}(\log(n))$
$\mathrm{DSpace}(O(1)) = \mathrm{DSpace}(o(\log\log(n))) = \{\mathcal{L} \mid \mathcal{L} \text{ is regular}\}$

טענה: תהי $s(n) \geq \log(n)$, אז $\mathrm{DSpace}(s(n)) \subseteq \mathrm{DTime}\left(2^{O(s(n))}\right)$.
בפרט $\mathsf{L} \subseteq \mathsf{P}$.
(רעיון: מספר הקונפיגורציות אליהן $M(x)$ יכולה להגיע חסום)

הגדרה: $s : \mathbb{N} \to \mathbb{N}$ הינה פונקציה חשיבה במקום אם קיימת מ"ט שבהנתן 1^n מחשבת את הקידוד הבינארי של $s(n)$ במקום $O(s(n))$.

משפט: תהי $s(n) \leq \log(n)$ פונקציה חשיבה במקום, אזי: $\mathrm{DSpace}(o(s(n))) \subsetneq \mathrm{DSpace}(s(n))$.

מסקנה: $\mathsf{L} \subsetneq \mathsf{PSPACE}$ ולכן לפחות אחד מהבאים נכון: .1 $\mathsf{L} \subsetneq \mathsf{P}$ .2 $\mathsf{P} \subsetneq \mathsf{PSPACE}$

הגדרה: יהיו Σ_A, Σ_B אפלאבתים, $A \subseteq \Sigma_A^*$, $B \subseteq \Sigma_B^*$. רדוקציית מיפוי במקום לוגריתמי מ-A ל-B היא פונקציה $f : \Sigma_A^* \to \Sigma_B^*$ חשיבה במקום לוגריתמי כך שלכל $x \in \Sigma_A$, $x \in A \iff f(x) \in B$. סימון: $A \leq_L B$.
אם $A \leq_L B$ ו-$B \in \mathsf{L}$ אז $A \in \mathsf{L}$
אם $A \leq_L B$ ו-$B \leq_L C$ אז $A \leq_L C$

טענה: יהיו f,g חשיבות במקום $s_f(n), s_g(n)$ בהתאמה ויהי $m_f(n)$ חסם על אורך הפלט של f, אז <u>$g(f)$ ניתנת לחישוב במקום</u> $O(s_f(n) + \log m_f(n) + s_g(m_f(n)))$.

הגדרה (בעיה P-שלמה): שפה A_0 P-שלמה אם: • $\mathcal{L}_0 \in \mathsf{P}$ • לכל $\mathcal{L} \in \mathsf{P}$, $\mathcal{L} \leq_l \mathcal{L}_0$.

טענה: CVAL (מעגל בוליאני עם ערך 1) בעיה P-שלמה. **קוק-לוין מנוסחת מחדש:** תהי M מ"ט פולינומית. קיימת פונ' חשיבה <u>במקום לוגריתמי</u> שבהנתן 1^n מחשבת (קידוד) מעגל $\mathcal{C}_{m,n} : \{0,1\}^n \to \{0,1\}$ כך שלכל $z \in \{0,1\}^n$, $M(z)$ מקבלת $\iff \mathcal{C}_{m,n}(z) = 1$.

הגדרה (סיבוכיות מקום לא-דטרמיניסטית): תהי $s : \mathbb{N} \to \mathbb{N}$ ו-M מטל"ד תלת-סרטית עם סרט .... M רצה במקום $s(n)$ אם לכל $n \in \mathbb{N}$ ולכל קלט x באורך n, ובכל ענף בעץ החישוב $T_{M,x}$, M משתמשת בלכל היותר $s(n)$ תאים על סרט העבודה בטרם עוצרת (תמיד עוצרת).

הגדרה: $\mathrm{NSpace}(s(n)) = \{\mathcal{L}(N) \mid N \text{ runs in space } O(s(n))\}$
הגדרה: $\mathsf{NL} = \mathrm{NSpace}(\log(n))$

הגדרה: v מוודא במקום לוגריתמי עבור שפה A אם v מ"ט 4-סרטית: • סרט קלט לקריאה בלבד • <u>סרט עד לקריאה חד פעמית</u> • סרט עבודה. לכל עד וכל x באורך n, v משתמש בלכל היותר $O(\log(n))$ תאים בסרט העבודה ו-$x \in A \iff$ קיים עד w כך ש-$v(x;w)$ מקבל.

טענה: $A \in \mathsf{NL} \iff$ קיים מוודא במקום לוגריתמי עבור A.

בעיות NL-שלמות: A_0 NL-שלמה אם: • $A_0 \in \mathsf{NL}$ • לכל $A \in \mathsf{NL}$, $A \leq_L A_0$.

טענה: STCON בעיה NL-שלמה. בנוסף $\mathsf{NL} \subseteq \mathsf{P}$ כי אם $A \in \mathsf{NL}$ אז $A \leq_L \mathrm{STCON}$ ולכן $A \leq_p \mathrm{STCON}$ ובגלל ש-$\mathrm{STCON} \in \mathsf{P}$, $A \in \mathsf{P}$.

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

הוכחה: <u>$\mathrm{Reach}(G,u,v,\ell)$</u> (האם קיים מסלול באורך $\leq \ell$ מ-u ל-v)
1. אם $\ell = 1$ נקבל $\iff (u,v) \in E$
2. לכל $w \in V$, נחשב $\mathrm{Reach}(G,u,w,\lceil \ell/2 \rceil)$ ו-$\mathrm{Reach}(G,w,v,\lfloor \ell/2 \rfloor)$.
3. נקבל אם שניהם קיבלו עבור w כלשהו אחר נדחה.

מסקנות: $\mathsf{NL} \subseteq \mathrm{DSpace}\left(\log^2 n\right)$. באופן כללי יותר גם $\mathrm{NSpace}(s(n)) \subseteq \mathrm{DSpace}\left(s^2(n)\right)$ ובפרט <u>$\mathsf{PSPACE} = \mathsf{NPSPACE}$</u>.

משפט (אימרמן-שלפיסני): $\overline{\mathrm{STCON}} \in \mathsf{NL}$ (כלומר, $\mathsf{NL} = \mathsf{coNL}$).

<u>בעיות</u>

$A \leq_L B$: פונקציה חשיבה במקום לוגריתמי, $x \in A \iff f(x) \in B$
אם $A \leq_L B$ ו-$B \in \mathsf{L}$ אז $A \in \mathsf{L}$
אם $A \leq_L B$ ו-$B \leq_L C$ אז $A \leq_L C$
$A \leq_p B$: פונקציה חשיבה בזמן פולינומי, $x \in A \iff f(x) \in B$
אם $A \leq_p B$ ו-$B \in \mathsf{P}$ אז $A \in \mathsf{P}$.
אם $A \leq_p B$ ו-$B \in \mathsf{NP}$ ו-$A \in \mathsf{NPC}$ אז $B \in \mathsf{NPC}$

הגדרה (NPC): $\mathcal{L}_0$ NP-שלמה אם: • $\mathcal{L}_0 \in \mathsf{NP}$ • לכל $\mathcal{L} \in \mathsf{NP}$, $\mathcal{L} \leq_p \mathcal{L}_0$.
הגדרה (PC): $\mathcal{L}_0$ P-שלמה אם: • $\mathcal{L}_0 \in \mathsf{P}$ • לכל $\mathcal{L} \in \mathsf{P}$, $\mathcal{L} \leq_L \mathcal{L}_0$.
הגדרה (NLC): $\mathcal{L}_0$ NL-שלמה אם: • $\mathcal{L}_0 \in \mathsf{NL}$ • לכל $\mathcal{L} \in \mathsf{NL}$, $\mathcal{L} \leq_L A_0$.

ACC	$\mathcal{RE} \setminus \mathcal{R}$	$\langle M, x\rangle$ כך ש-$M(x)$ מקבלת
HALT	$\mathcal{RE} \setminus \mathcal{R}$	$\langle M, x\rangle$ כך ש-$M(x)$ עוצרת
EMPTY	$co\mathcal{RE} \setminus \mathcal{R}$	$\langle M\rangle$ כך ש-$\mathcal{L}(M)$ ריקה
REG	$\overline{\mathcal{RE} \cup co\mathcal{RE}}$	$\langle M\rangle$ כך ש-$\mathcal{L}(M)$ רגולרית
EQ	$\overline{\mathcal{RE} \cup co\mathcal{RE}}$	$\langle M_1, M_2\rangle$ כך ש-$\mathcal{L}(M_1) = \mathcal{L}(M_2)$
L_∞	$\overline{\mathcal{RE} \cup co\mathcal{RE}}$	$\langle M\rangle$ כך ש-$\mathcal{L}(M)$ אינסופית
HAMPATH	NPC	$\langle G, s, t\rangle$ בגרף המכוון G יש מסלול המילטוני מ-s ל-t
CLIQUE	NPC	$\langle G, k\rangle$ כך ש-G גרף לא מכוון עם קליקה בגודל k
IS	NPC	G גרף לא מכוון שיש קב' כך שאין קשת בין כל שניים בגודל k
IS∧CLIQUE	NPC	$\langle G, k\rangle$ כך ש-G גרף לא מכוון עם קליקה בגודל k וגם קב' כדשאין קשת בין כל שניים בגודל k
IS∧CLIQUE	NPC	$\langle G, k\rangle$ כך ש-G גרף לא מכוון עם קליקה בגודל k וגם קב' כדשאין קשת בין כל שניים בגודל k
3SAT	NPC	האם נוסחאת 3CNF ספיקה (מוגדר ב"סיבוכיות זמן")
CIRSAT	NPC	$\langle \mathcal{C}, x\rangle$ מעגל בוליאני וקיים $w \in \{0,1\}^*$ כך ש $\mathcal{C}(x,w) = 1$
C-CNF	NPC	$\langle \varphi, k\rangle$ נוסחת CNF, ומספר טבעי כך שיש השמה שמספקת בדיוק k ליטרלים בנוסחה
C-DNF	NPC	$\langle \varphi, k\rangle$ נוסחת DNF, ומספר טבעי כך שיש השמה שמספקת בדיוק k ליטרלים בנוסחה
SUBSETSUM	NPC	$s_1,\ldots,s_k,t \in \mathbb{N}. \exists I \subseteq [k] . \sum_{i\in I} s_i = t$
CVAL	PC	$\langle \mathcal{C}, x\rangle$ $\mathcal{C}$ מעגל בוליאני ו-$\mathcal{C}(x) = 1$
STCON	NLC	G מכוון, קיים מסלול מ-s ל-t
VC	NPC	קבוצה של k צמתים הנוגעת בכל הקשתות
E3SAT	NPC	Φ היא 3-CNF עם בדיוק שלושה ליטרלים שונים בכל פסוקית