



1 מעגלים בוליאניים

הגדרה (קונפיגורציה): קונפיגורציה מייצגת את המצב של מ"ט ברגע מסוים. למשל 1011q70111 אומר שהתוכן של הסרט הוא 10110111, התמצב הוא q7, ושהמ"ט נמצאת בתא החמישי של הסרט (על 0). הקונפיגורציה ההתחלית עבור קלט x היא q_0w .

הגדרה: מקבלת/דוחה קלט $x \in \Sigma^*$ אם קיימת סדרת קונפיגורציות c_0, \dots, 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 (R): שפה \mathcal{L} כריעה אם קיימת מ"ט שעוצרת לכל קלט x , ומקבלת $\iff x \in \mathcal{L}$.

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

הגדרה (coRE): שפה \mathcal{L} כריעה למחצה. אוסף השפות הכריעות למחצה.

הגדרה שקולה: מ"ט E הינה מונה עבור $L \subseteq \Sigma^*$ אם:

- E^{-1} יש סרט פלט לכתיבה חד פעמית • הא"ב של סרט הפלט הוא $\Sigma \cup \{\$ \}$
- $\$x\$$ איז $x \notin L$ המחרוזת $\$x\$$ תופיע בפלט ואם $x \in L$ אז $\$x\$$ לא תופיע.

טענה: $\mathcal{R} = \text{coRE} \iff \mathcal{L} \subseteq \{0, 1\}^*$ קיימת מ"ט שמסמלת מכונות טיורינג ויש לה מספר מצבים ≤ 100 (לסמלץ מ"ט זה פולינומיאלי).

טענה: קיימת שפה $\mathcal{L} \subseteq \{0, 1\}^*$ שאינה כריעה. כי $|\mathcal{R}| \leq |\text{TMs}| \leq \aleph_0$.

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

רדוקציית מופוי: יהיו $A, B \subseteq \Sigma^*$. רדוקציית מופוי מ- A ל- B היא פונקציה חשיבה $f: \Sigma^* \rightarrow \Sigma^*$ כך שלכל $x \in A$, $x \in \Sigma^* \iff f(x) \in B$ ונסמן $A \leq_m B$.

אם $A \leq_m B$ אז $A \in \text{coRE} \iff B \in \text{coRE}$.

משפט רייס: יהיו $C \subseteq \text{RE}$ אוסף שפות כך $\emptyset \neq C \neq \text{RE}$ אז:

הרחבה 1: $\emptyset \subseteq C \subseteq \text{RE} \setminus \{ \emptyset \}$ או $C \subseteq \text{coRE}$ או $C \subseteq \text{RE}$.

הרחבה 2: $\emptyset \subseteq C \subseteq \text{RE}$ או $C \subseteq \text{coRE}$.

הרחבה 3: $\emptyset \subseteq C \subseteq \text{RE} \setminus \{ \emptyset \}$ או $C \subseteq \text{coRE}$.

הרחבה 4: $\emptyset \subseteq C \subseteq \text{RE}$ או $C \subseteq \text{coRE}$.

הגדרה (מוודא): תהי v מ"ט עם א"ב קלט $\Sigma \cup \{ _ \}$ ותהי $L \subseteq \Sigma^*$ מוודא עבור L אם:

• שלמות: לכל $x \in L$ קיים $w \in \Sigma^*$ כך ש- $v(x, w)$ מקבל • נאותות: לכל $x \notin L$ ולכל $w \in \Sigma^*$, $v(x, w)$ דוחה. w נקראת עד.

טענה: $L \in \text{RE} \iff L \in \text{coRE}$ וגם $L \in \text{RE} \cup \text{coRE}$.

4 סיבוכיות זמן

הגדרה (זמן ריצה): תהי $T: \mathbb{N} \rightarrow \mathbb{N}$ רצה בזמן $T(n)$ אם M מבצעת לכל היותר $T(n)$ לפני שהיא עוצרת עבור קלט באורך n .

משפט היררכיית הזמן: $T: \mathbb{N} \rightarrow \mathbb{N}$ 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 $DTime(T(n)) \subseteq DTime(t(n))$ אז $t(n) \log t(n) = o(T(n))$.

רעיון הנוכח: מאכשב את $T(n)$. דוחה אם לא מהצורה $\langle M, 0^k \rangle$.

או אם $\log T(n) > |M|$. מריץ $T(n)$ צעדים של $U(\langle M, w \rangle)$ ונתונים ל- M בתור קלט עם צמזמא. אם U עזרה וקיבלה, $Flip$ דוחה, אחרת $Flip$ מקבל. נשים לב שלכל מ"ט M $Flip$ הרץ עד הסוף, $Flip$ יפלט פלט שונה ממנה, ולכן הוא שונה מכל מ"ט כזו.

משפט: אם $L \in DTime(o(n \log n))$ אז 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 כל האפסים, ואז נעבור על שניהם ונבדוק שכמות האחדים שווה לכמות האפסים), אבל $\Omega(n \log n)$ בחד סרטית (צריך לספור איכשהו).

משפט (סימולציה של רבי-סרטית): מ"ט רבי-סרטית בעלת זמן ריצה $n \leq T(n)$ 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 עוצרת תוך t צעדים, אזי $U(\langle M, x \rangle)$ עוצרת תוך $O(|\langle M \rangle|^3 t \log t)$ צעדים.

הפעל על $\log t$ נובע מהתקורה של סימולציה אוניברסלית על מ"ט חד-סרטית. עבור מ"ט רבי-סרטית ניתן לסמלץ בזמן לינארי.

הגדרה (זמן ריצה לא דטרמיניסטי): תהי $t: \mathbb{N} \rightarrow \mathbb{N}$ 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 $t(n)$.

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

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

הגדרה (מוודא פולינומי): תהי v מ"ט עם א"ב קלט $\Sigma \cup \{ _ \}$ ותהי $L \subseteq \Sigma^*$ מוודא פולינומי עבור L אם:

• שלמות: לכל $x \in L$ קיים $w \in \Sigma^*$ כך ש- $v(x, w)$ מקבל • נאותות: לכל $x \notin L$ ולכל $w \in \Sigma^*$, $v(x, w)$ דוחה • עילנות: קיים פולינום $p(n)$ כך שלכל $x, w \in \Sigma^*$ זמן הריצה של $v(x, w)$ לכל היותר $p(|x|)$. w נקראת עד.

טענה: $L \in \text{NP} \iff L \in \text{coNP}$ קיים מוודא פולינומי.

הגדרה (רדוקציית מופוי פולינומית): יהיו Σ_A, Σ_B אלפאביטים, $A \subseteq \Sigma_A^*$, $B \subseteq \Sigma_B^*$ רדוקציית מופוי פולינומית מ- A ל- B היא פונקציה $f: \Sigma_A^* \rightarrow \Sigma_B^*$ חשיבה בזמן פולינומי כך שלכל $x \in A$, $x \in \Sigma_A \iff f(x) \in B$.

אם $A \leq_p B$ אז $A \in \text{NP}$ או $A \in \text{coNP}$ או $A \in \text{P}$.

אם $A \leq_p B$ ו- $B \in \text{NP}$ אז $A \in \text{NP}$.

אם $A \leq_p B$ ו- $B \in \text{coNP}$ אז $A \in \text{coNP}$.

הגדרה (בעיה NP-שלמה): נקראת NP-שלמה אם: $L_0 \in \text{NP}$ • לכל $L \in \text{NP}$, $L \leq_p L_0$.

המחלקה של NP-שלמות היא NPC.

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

$\text{ACC}_{\text{NP}} \in \text{NP}$.

הגדרה: נוסחת 3CNF $\Phi(x_1, \dots, x_n)$ 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 $z_{i,j} \in \{x_1, \dots, x_n, \bar{x}_1, \dots, \bar{x}_n\}$.

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

3 מכונות טיורינג וכריעות

הגדרה (מכונת טיורינג): מכונת טיורינג היא שבעייה $(Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r)$ קבוצת מצבים סופית Γ אלפאבית סרט, $\Sigma \subseteq \Gamma$ אלפאבית קלט, $q_0 \in Q$ 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 דטרמיניסטי מטל"ד היא שבעייה $(Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r)$ קבוצת מצבים סופית Γ אלפאבית סרט, $\Sigma \subseteq \Gamma$ אלפאבית קלט, $q_0 \in Q$ 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: לטרוק את עץ החישוב ולבדוק האם עלה כלשהו מקבל.

הגדרה (מכונת טיורינג): מכונת טיורינג היא שבעייה $(Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r)$ קבוצת מצבים סופית Γ אלפאבית סרט, $\Sigma \subseteq \Gamma$ אלפאבית קלט, $q_0 \in Q$ 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: לטרוק את עץ החישוב ולבדוק האם עלה כלשהו מקבל.



הגדרה: $DSPACE(s(n)) = \{ \mathcal{L}(M) \mid M \text{ is a TM, space } O(s(n)) \}$
 $PSPACE = \bigcup_{c \in \mathbb{N}} DSPACE(c \log n)$
 $L = LOGSPACE = DSPACE(\log n)$
 $DSPACE(O(1)) = DSPACE(o(\log \log(n))) = \{ \mathcal{L} \mid \mathcal{L} \text{ is regular} \}$
טענה: $DSPACE(s(n)) \subseteq DTIME(2^{O(s(n))})$ אז $s(n) \geq \log(n)$ וזו לחבר $t(n)$ כאלה זה לזה.
 $L \subseteq P$

רעיון: מספר הקונפיגורציות אליהן $M(x)$ יכולה להגיע (חסום)
הגדרה: $s: \mathbb{N} \rightarrow \mathbb{N}$ הינה פונקציה חשיבה במקום אם קיימת מ"ט שבהנתן 1^n מחשבת את הקידוד הבינארי של $s(n)$ במקום $O(s(n))$.
משפט: תהי $\log(n) \leq s(n)$ פונקציה חשיבה במקום, אזי: $DSPACE(o(s(n))) \subsetneq DSPACE(s(n))$.
מסקנה: $P \subsetneq L \subsetneq PSPACE$ ולכן לפחות אחד מהבאים נכון: 1. $L \subsetneq P$ 2. $P \subsetneq L$.

הגדרה: יהיו Σ_A, Σ_B אפלאבטים, $A \subseteq \Sigma_A^*, B \subseteq \Sigma_B^*$. רדוקציית מייפו במקום לוגריתמי מ A ל B היא פונקציה $f: \Sigma_A^* \rightarrow \Sigma_B^*$ חשיבה במקום לוגריתמי כך שלכל $A \leq_L B$ סימון: $f(x) \in B \iff x \in A, x \in \Sigma_A$
 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 $g(f)$ ניתנת לחישוב במקום $O(s_f(n) + \log m_f(n) + s_g(m_f(n)))$.

הגדרה (בעיה P-שלמה): שפה A_0 P-שלמה אם: $L_0 \in P$ לכל $\mathcal{L} \in P$
טענה: CVAL (מעגל בוליאני עם ערך 1) בעיה P-שלמה. **קוק-ליון מנוסחת מחדש:** תהי M מ"ט פולינומית. קיימת פונ' חשיבה במקום לוגריתמי שבהנתן 1^n מחשבת (קידוד) מעגל $\{0, 1\}^n \rightarrow \{0, 1\}^n$ כך שלכל $C_{m,n}: \{0, 1\}^n \rightarrow \{0, 1\}^n$
 $C_{m,n}(z) = 1 \iff M(z) = 1$

הגדרה (סיבוכיות מקום לא-דטרמיניסטית): תהי $s: \mathbb{N} \rightarrow \mathbb{N}$ מ-1 מטל"ד תלת-סרטיית עם סרט M רצה במקום $s(n)$ אם לכל $n \in \mathbb{N}$ ולכל קלט x באורך n , ובכל ענף בעץ החישוב $M, T_{M,x}$ משתמשת בכלל היותר $s(n)$ תאים על סרט העבודה בטרם עוצרת (תמיד עוצרת).
הגדרה: $NSpace(s(n)) = \{ \mathcal{L}(N) \mid N \text{ runs in space } O(s(n)) \}$
הגדרה: $NL = NSpace(\log n)$

הגדרה: v מודא במקום לוגריתמי עבור שפה A אם v מ"ט 4-סרטיית: סרט קלט לקריאה בלבד • סרט עד לקריאה חד פעמית • סרט עבודה. לכל עד וכל x באורך n , משתמש בכלל היותר $O(\log n)$ תאים בטרם העבודה ו- $x \in A$ קיים עד w כך ש- $(x; w)$ מקבל.
טענה: $A \in NL \iff$ קיים מודא במקום לוגריתמי עבור A .

בעיות NL-שלמות: $A_0 \in NL$ לכל $A_0 \in NL$ • $A \leq_L A_0$ לכל $A \in NL$
טענה: STCON בעיה NL-שלמה. בנוסף $NL \subseteq P$ אם $A \in NL$ או $A \leq_L A$ • STCON ולכן $STCON \in P$ ובגלל $A \leq_P STCON$ • $A \in P$, $STCON \in P$
משפט (סאביץ'): $STCON \in DSPACE(\log^2 n)$

הוכחה: האם קיים מסלול באורך $\geq \ell$ מ- u ל- v
 1. אם $\ell = 1$ נקבל $(u, v) \in E \iff$
 2. לכל $w \in V$, נחשב $Reach(G, u, w, \lceil \ell/2 \rceil)$ ו- $Reach(G, w, v, \lfloor \ell/2 \rfloor)$.
 3. נקבל אם שניהם קיבלו עבור w כלשהו אחר נדחה.
הערה: $Reach(G, u, v, \ell) \in \log n \log \ell$ אבל אסור להשתמש בזה בלי להוכיח n חסם על שכנים, l חסם על צעדים).
טענה: אלא הרץ במקום $S(n)$ אפשר לחשב בעזרת מעגלים בוליאניים בעומק $\log^2(n)$
מסקנות: $NSpace(\log^2 n) \subseteq DSPACE(\log^2 n)$. באופן כללי יותר גם $NSpace(s(n)) \subseteq DSPACE(s^2(n))$
 $PSPACE = NPSPACE$ ובפרט $DSPACE(s^2(n))$

משפט (אימרמן-שלפיסיני): $STCON \in NL$ (כלומר, $NL = coNL$).
טענה: DNF ב- P
טענה: תהיינה f, g חשיבות במקום $S_f(n), S_g(n)$, בהתאמה ויהי $m_f(n)$ חסם על אורך הקלט של f , אז $g(f)$ ניתנת לחישוב במקום $O(S_f(n) + \log m_f(n) + S_g(m_f(n)))$

7 בעיות

$A \leq_L B$: פונקציה חשיבה במקום לוגריתמי, $x \in A \iff f(x) \in B$
 אם $A \leq_L B$ ו $B \leq_L C$ אז $A \leq_L C$
טענה: $A \leq_P B \iff$ פונקציה חשיבה בזמן פולינומי, $x \in A \iff f(x) \in B$
 אם $A \leq_P B$ אז $B \in P$ או $A \in P$
 אם $A \leq_P B$ אז $B \in NP$ או $A \in NP$
 אם $A \leq_P B$ ו $B \in NPC$ אז $A \in NPC$
הגדרה (NPC): $L_0 \in NPC$ -שלמה אם: $L_0 \in NP$ • לכל $L_0 \in NP$ לכל $\mathcal{L} \leq_P L_0$
הגדרה (PC): $L_0 \in PC$ -שלמה אם: $L_0 \in P$ • לכל $\mathcal{L} \leq_L L_0$
הגדרה (NLC): $L_0 \in NLC$ -שלמה אם: $L_0 \in NL$ • לכל $\mathcal{L} \leq_L A_0$

8 טריקים ושטיקים

- מחלקות סיבוכיות נוספות שאולי יופיעו: $ZPP = RP \cap coRP$ וגם $RP, coRP \subseteq BQP \subseteq PP \subseteq PSPACE$
- אפשר להפוך מודא למכריע על-ידי מעבר על כל העדים האפשריים
- אוטומטים לא יכולים לזכור הרבה, בפרט $\{x \mid |x| = 2023^k\}$ וכל מיני דברים כאלה כנראה לא יהיו רגולריים.
- מ"ט היא מטל"ד עם מסלול חישוב יחיד.
- מקדם של x^M כלשהו של $(a_1 + b_1x^{k_1})(a_2 + b_2x^{k_2}) \dots (a_n + b_nx^{k_n})$ קשור ל-SUBSETSUM כי צריך $k_{i_1} + \dots + k_{i_r}$
- עוצמות: $|\mathcal{R}| = |\mathcal{R}| = \dots = \aleph_0$ ו- $|Size(O(1))| = \aleph$

הלב של קוק-ליון: תהי $n \leq t(n)$ חשיבה בזמן ותהי M מ"ט הרצה ב- $t(n)$. קיימת פונקציה חשיבה בזמן $poly(t(n))$ שבהנתן 1^n מחשבת (קידוד) מעגל: $C_{m,n}: \{0, 1\}^n \rightarrow \{0, 1\}^n$ המקיים:
 • לכל $M(z), z \in \{0, 1\}^n$ מקבלת $M(z) = 1 \iff C_{m,n}(z) = 1$
רעיון הוכחה: לבנות מעגל שמעביר מקונפיגורציה אחת לבהא וזו לחבר $t(n)$ כאלה זה לזה.
מסקנה: אם $f: \{0, 1\}^* \rightarrow \{0, 1\}^*$ אינה ניתנת לחישוב ע"י משפחת מעגלים בגודל $O(\sqrt{s(n)})$ אז לא ניתנת לחישוב ע"י מ"ט בזמן $\sqrt{s(n)}$.
מסקנה: $CIRSAT \in NPC$ **מסקנה:** $3SAT \in NPC$ (רדוקציה מ- $CIRSAT$ ל- $3SAT$).
טענה: $P \subseteq NP \subseteq EXP \subseteq NEXP$, אבל $P \subseteq NP \subseteq EXP \subseteq NEXP$.

5 אקראיות בחישוב

הגדרה: מ"ט אקראית עם זמן ריצה $t(n)$ הינה מ"ט דו-סרטיית: הסרט הראשון מאכלס בתחילת הריצה את הקלט x ומשמש בסרט עבודה. הסרט השני הינו "סרט אקראיות" ומאוחל בתחילת הריצה למחרוזת $r \in \{0, 1\}^{t(n)}$. $M(x; r)$ מסמנת ריצה על קלט x עם אקראיות r . נתייחס ל- $M(x)$ בתור משתנה מקרי $M(x; r)$.
הגדרה: תהי $\alpha(n) \in [0, 1]$, $\alpha(n) \in RP(\alpha(n))$ אם קיימת מ"ט אקראית M הרצה בזמן פולינומי $p(n)$ כך שלכל n מספיק גדול, ו- $x \in \{0, 1\}^n$
 • $\Pr_{r \leftarrow \{0, 1\}^{p(n)}} [M(x; r) = 1] \geq \alpha(n), x \in \mathcal{L}$
 • אם $x \notin \mathcal{L}$ אז $\Pr_{r \leftarrow \{0, 1\}^{p(n)}} [M(x; r) = 1] = 0$

הגדרה: $coRP = \{L \mid \bar{L} \in RP(\alpha(n))\}$ (לעולם לא טועים עבור $x \in \mathcal{L}$).
מוסקמה: $coRP = coRP(1/2), RP = RP(1/2)$
טענה: לכל $c, d \in \mathbb{N}$, $RP(1/2) = RP(n^{-c}) = RP(1 - 2^{-n^d})$. מריצים n^{c+d} פעמים ומקבלים אם אחת הריצות קיבלה.

טענה: $NP = \bigcup_{c>0} RP(2^{-n^c})$
הגדרה: יהיו $\alpha(n), \beta(n) \in [0, 1]$, $\alpha(n), \beta(n) \in BPP(\alpha(n), \beta(n))$ אם קיימת מ"ט אקראית M הרצה בזמן פולינומי $p(n)$ כך שלכל n גדול מספיק ו- $x \in \{0, 1\}^n$
 • $\Pr_{r \leftarrow \{0, 1\}^{p(n)}} [M(x; r) = 1] \geq \beta(n), x \in \mathcal{L}$
 • $\Pr_{r \leftarrow \{0, 1\}^{p(n)}} [M(x; r) = 1] \leq \alpha(n), x \notin \mathcal{L}$

ניתן לומר ש- $RP(1/2) = BPP(0, 1/2)$
מוסקמה: $BPP = BPP(1/3, 2/3)$
טענות לגבי השפות: $P \subseteq RP \subseteq NP, BPP$
טענה: לכל $c, d \in \mathbb{N}$ ו- $\alpha(n)$ חשיבה בזמן $poly(n)$ כך שלכל n גדול מספיק $(\alpha(n) - n^{-c}, \alpha(n) + n^{-c}) \subseteq [0, 1]$ מתקיים:
 $coRP = BPP(1/2, 1)$

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

הגדרה: נוסחה אריתמטית היא נוסחה (מעגל עם fan-out 1) עם שערי $+, \times, 0, 1$
הגדרה: עבור שדה \mathbb{F} נגדיר $ZE_{\mathbb{F}} = \{ \phi \mid \forall x \in \mathbb{F}, \phi(x) = 0 \wedge \phi \text{ is AF} \}$
טענות מהשב: $NP \subseteq \bigcup BPP(1/2, 1/2 + \frac{1}{2n^c})$, $ZPP = RP \cap coRP$
למה(שוורץ-יפול): יהי $p \in \mathbb{F}[x_1, \dots, x_n]$ פולינום bn משתנים מעל \mathbb{F} , אז אם p הוא לא זהותית 0, מדרגה טוטלית d אז לכל $S \subseteq \mathbb{F}$ תת קבוצה סופית מתקיים כי

$$\Pr_{(x_1, \dots, x_n) \leftarrow S^n} [P(x_1, \dots, x_n) = 0] \leq \frac{d}{|S|}$$

משפט: $ZE_{\mathbb{F}} \in BPP$
משפטים בהסתברות:

אי שוויון מרקוב: יהי X משתנה מקרי בעל תוחלת אזי לכל $a > 0$:

$$\Pr[|X| \geq a] \leq \frac{E(|X|)}{a}$$

אי שוויון צ'בישב: יהי X משתנה מקרי בעל תוחלת אזי לכל $C > 0$:

$$\Pr[|X - E(X)| \geq C] \leq \frac{Var(X)}{C^2}$$

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

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

אי שוויון קולמגורוב: יהיו X_1, \dots, X_N משתנים מקריים ב"ת עם תוחלת אפס והשונוות של כולם סופית. נסמן $S_k = \sum_{i=1}^k X_k$ אזי לכל $\lambda > 0$ מתקיים:

$$\Pr \left[\max_{1 \leq k \leq n} |S_k| \geq \lambda \right] \leq \frac{1}{\lambda^2} Var(S_n) = \frac{1}{\lambda^2} \sum_{i=1}^k Var(X_k)$$

6 סיבוכיות מקום

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 בכלל היותר $s(n)$ תאים על סרט העבודה בטרם עוצרת (בפרט תמיד עוצרת).



$\langle M, x \rangle$ כך ש- $M(x)$ מקבלת	$\mathcal{RE} \setminus \mathcal{R}$	ACC
$\langle M, x \rangle$ כך ש- $M(x)$ עוצרת	$\mathcal{RE} \setminus \mathcal{R}$	HALT
$\langle M \rangle$ כך ש- $M(x)$ עוצרת על אפסילון	$\mathcal{RE} \setminus \mathcal{R}$	HALT $_{\epsilon}$
$\langle M \rangle$ כך ש- $\mathcal{L}(M)$ ריקה	$co\mathcal{RE} \setminus \mathcal{R}$	EMPTY
$\langle M \rangle$ כך ש- $\mathcal{L}(M)$ היא Σ^*	$\overline{\mathcal{RE}} \cup co\mathcal{RE}$	ALL
$\langle M \rangle$ כך ש- $\mathcal{L}(M)$ רגולרית	$\overline{\mathcal{RE}} \cup co\mathcal{RE}$	REG
$\mathcal{L}(M_1) = \mathcal{L}(M_2)$ כך ש- (M_1, M_2)	$\overline{\mathcal{RE}} \cup co\mathcal{RE}$	EQ
$\langle M \rangle$ כך ש- $\mathcal{L}(M)$ אינסופית	$\overline{\mathcal{RE}} \cup co\mathcal{RE}$	L_{∞}
$\langle M, x, 1^t \rangle$ כך ש- w קיים כך ש- $M(x, w)$ מקבלת בזמן t	NPC	ACC $_{NP}$
$\langle G, s, t \rangle$ בגרף המכוון G יש מסלול המילטוני מ- s ל- t	NPC	HAMPATH
$\langle G, k \rangle$ כך ש- G גרף לא מכוון עם קליקה בגודל k	NPC	CLIQUE
גרף לא מכוון שיש קב' כך שאין קשת בין כל שניים בגודל k	NPC	IS
$\langle G \rangle$ בגרף המכוון G יש מעגל המילטוני	NPC	HAMCYCLE
$\langle G, k \rangle$ כך ש- G גרף לא מכוון עם קליקה בגודל k וגם קב' כך שאין קשת בין כל שניים בגודל k	NPC	IS \wedge CLIQUE
$\langle G, k \rangle$ כך ש- G גרף לא מכוון עם קליקה בגודל k או קב' כך שאין קשת בין כל שניים בגודל k	NPC	IS \vee CLIQUE
האם נוסחת 3CNF ספיקה (מוגדר ב"סיבוכיות זמן")	NPC	3SAT
$\langle C, x \rangle$ מעגל בוליאני וקיים $w \in \{0, 1\}^*$ כך ש- $C(x, w) = 1$	NPC	CIRSAT
$\langle \varphi, k \rangle$ נוסחת CNF, ומספר טבעי כך שיש השמה שמספקת בדיוק k ליטרלים בנוסחה	NPC	C-CNF
$\langle \varphi, k \rangle$ נוסחת DNF, ומספר טבעי כך שיש השמה שמספקת בדיוק k ליטרלים בנוסחה	NPC	C-DNF
$\sum_{i \in I} s_i = t$ שמקיים $I \subseteq [k]$ ש- $s_1, \dots, s_k, t \in \mathbb{N}$	NPC	SUBSETSUM
קבוצה של k צמתים הנוגעת בכל הקשתות	NPC	VC
Φ היא 3-CNF עם בדיוק שלושה ליטרלים שונים בכל פסוקית עם השמה מקבלת	NPC	E3SAT
$\langle C, x \rangle$ מעגל בוליאני ו- $C(x) = 1$	PC	CVAL
G מכוון, קיים מסלול מ- s ל- t	NLC	STCON
Φ היא 2-CNF עם השמה מקבלת	$DSPACE(\log^2(n))$	2SAT
$\langle G, P \rangle$ בגרף המכוון G יש $(u, v) \in P$ כך שקיים מסלול מ- u ל- v ולהפך	NLC	PCON
$\langle M, q \rangle$ כך ש- M עוברת ב- q לפחות פעמיים בריצה ל- ϵ	\mathcal{R}^c	L visits twice
$\langle M \rangle$ כך ש- $L(M) \in \mathcal{R}$	$\mathcal{RE} \setminus \mathcal{R}$	L_R
$\langle G, s, t \rangle$ בגרף הלא מכוון G יש מסלול המילטוני מ- s ל- t	NPC	UNHAMPATH
$\langle M, q, q' \rangle$ כך ש- M עוברת ב- q וב- q' אותה כמות פעמים בריצה על ϵ , תרגיל 4	$\overline{\mathcal{RE}} \cup co\mathcal{RE}$	L visits same amount
$\langle M \rangle$ כך ש- $ L(M) > 1$, תרגיל 4	$\overline{\mathcal{RE}} \setminus \mathcal{R}$	L size > 1
$\langle A_1, \dots, A_n, k \rangle$ קבוצות כך שקיימות k מהן שזרות בזוגות, תרגיל 5	NPC	Disjoint sets
$\langle A_1, \dots, A_n, k \rangle$ קבוצות כך שקיימות k מהן שחיתוך כל 2 אינו זר, תרגיל 5	NPC	Joint sets
G מכוון, לא קיים מסלול מ- s ל- t (או קידוד לא חוקי של גרף)	NL	STCON
$\langle G, k \rangle$ גרף לא מכוון, קיימת קבוצה של k צמתים כך שהם נוגעים בכל הקשתות	NPC	IS \cap CLIQUE
$\langle G, D \rangle$, G גרף מכוון עם קוטר עד D (אורך המסלול המינימלי בין כל 2 קודקודים בגרף הוא עד D)	NPC	VERTEXCOVER
$\langle G, P \rangle$ קב' קודקודים בגרף מכוון, האם קיים מסלול מכל קודקוד ב- P לכל קודקוד ב- P	$DSPACE(\log n \log D)$	DIAMETER
	NL	PCON

הערה: אפשר לעשות רדוקציה בקלות מ- $PCON$ ל- $STCON$, $PCON \in NLC$.