מודלים חישוביים (0368-2200)

נכתב על ידי רון גולדמן
מבוסס על רשימות של ד״ר אורי שטמר, בית הספר למדעי המחשב ובינה מלאכותית, אוניברסיטת תל אביב

9 ביולי 2025

תוכן העניינים

חלק I

מבוא

פרק 1

מושגים בסיסיים

הגדרה 1.1. **אלפבית** היא קבוצה סופית (לא ריקה) של תווים. נסמן ב-Σ.

הגדרה 1.2. **מילה** מעל אלפבית Σ היא שרשור של מספר סופי של תווים מ-Σ.

סימון 1.1. נסמן:

- Σ^* - **קבוצת כל המילים** מעל Σ.
- Σ^n - קבוצת כל המילים **באורך** $\boldsymbol{n}$ מעל Σ.
- ε - **המילה הריקה**.

הגדרה 1.3. **שפה** מעל אלפבית Σ היא תת קבוצה של Σ^*.

הגדרה 1.4 (חצי פורמלית).
נאמר ש"אלגוריתם" **מכריע** שפה $L \subseteq \Sigma^*$ אם לכל $x \in L$ האלגוריתם מחזיר "כן" (נאמר שהאלגוריתם "מקבל" את x) ולכל $x \notin L$ האלגוריתם מחזיר "לא" (נאמר שהאלגוריתם "דוחה" את x).

הערה 1.1. לא כל הבעיות שמעניינות אותנו הן בעיות הכרעה. למשל בעיית חיפוש: "בהינתן p שאינו ראשוני, מצאו את גורמיו הראשוניים". מסתבר שבהרבה מקרים יש קשרים מאוד הדוקים בין בעיות הכרעה לבעיות חיפוש (יתבהר בהמשך הקורס).

פרק 2

מעגלים בוליאניים

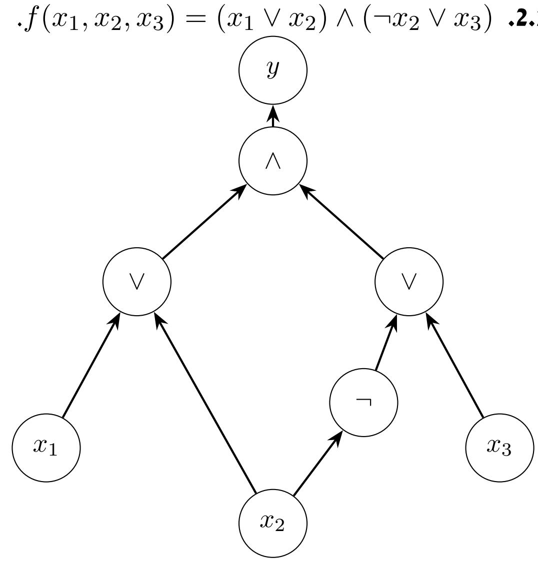
הגדרה 2.1. תהי B קבוצה של פונקציות בוליאניות (כלומר מעל $\{0,1\}$). **מעגל בוליאני** מעל B עם ביטי קלט $x_1,\dots,x_n$ וביטי פלט $y_1,\dots,y_m$ הוא גרף מכוון וחסר מעגלים כאשר:

- כל צומת מסומן על ידי: פונקציה $g \in B$, או קלט x_i, או פלט y_i.
- לכל ביט פלט y_i יש בדיוק צומת אחד המסומן ב-y_i. דרגת הכניסה של צומת זה היא 1 ודרגת היציאה שלו היא 0.
- דרגת הכניסה של כל צומת המסומן בביט קלט x_i היא 0.
- לכל צומת המסומן בפונקציה $g \in B$, אם g מוגדרת על $\{0,1\}^k$ אז ישנן k קשתות הנכנסות לצומת עם סדר המסומן $1,2,\dots,k$. עבור פונקציה $g \in B$ **סימטרית** (כלומר סדר הקלטים לא משנה) אין צורך בסימון סדר הקשתות הנכנסות.

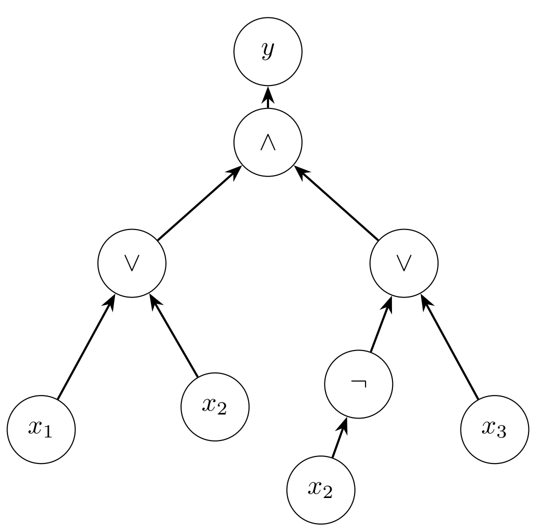
<u>**מונחים:**</u>

- צומת המסומן בפונקציה $g \in B$ נקרא **שער** (gate).
- הקשתות נקראות **חוטים** (wires).
- ה**fan-out** של מעגל הוא דרגת היציאה המקסימלית של שער כלשהו במעגל.
- תת הקבוצה של המעגלים בהן הfan-out הוא 1 נקראים גם **נוסחאות**.

דוגמה 2.1. $f(x_1,x_2,x_3) = (x_1 \vee x_2) \wedge (\neg x_2 \vee x_3)$.



מעגל: fan-out=2



נוסחה: fan-out=1

2.1 חישוב פונקציות על ידי מעגלים

הגדרה 2.2 (שערוך מעגל על קלט)**.**
בהינתן מעגל C עם n ביטי קלט וקלט $v \in \{0,1\}^n$, מציבים ערכים לחוטים באופן איטרטיבי:

- צעד ראשון: לכל $i \in [n]$ מציבים את ערך v_i לחוטים היוצאים מצומת הקלט המסומן ב-x_i.
- צעד איטרטיבי: מוצאים שער שכל הכניסות שלו חושבו (והיציאה טרם חושבה), ומחשבים את הפונק' g המתאימה על ערכי הכניסה ומציבים לחוט היציאה.
- חוזרים על הצעד האיטרטיבי כל עוד אפשר.
- הפלט $C(v)$ הנו הערכים שהוצבו לכניסות של $y_1, \dots, y_m$.

טענה 2.1. התהליך מוגדר היטב, כלומר לכל חוט הצבה אחת ויחידה.

הגדרה 2.3. נאמר כי מעגל C **מחשב פונקציה** $f : \{0,1\}^n \to \{0,1\}^m$ אם לכל קלט $v \in \{0,1\}^n$ מתקיים $C(v) = f(v)$.

טענה 2.2. ניתן לממש שער "וגם" של n משתנים ע"י שערי "וגם" של שני משתנים (על ידי עץ). אותה טענה נכונה לשערי "או".

משפט 2.1 (אוניברסליות של דה-מורגן)**.**
לכל פונקציה $f : \{0,1\}^n \to \{0,1\}^m$ קיים מעגל מעל בסיס דה-מורגן $B = \{\wedge, \vee, \neg\}$ המחשב אותה.

2.2 סיבוכיות מעגלים (על קצה המזלג)

הגדרה 2.4. **משפחה של מעגלים** $\mathcal{C} = \{C_n\}_{n\in\mathbb{N}}$ היא אוסף אינסופי של מעגלים, כך ש-C_n מוגדר על קלטים באורך n, לכל $n \in \mathbb{N}$.

הגדרה 2.5. תהי $\mathcal{C} = \{C_n\}_{n\in\mathbb{N}}$ משפחת מעגלים עם ביט פלט יחיד ותהי $L \subseteq \{0,1\}^*$ שפה. נאמר כי $\mathcal{C}$ **מכריעה את** L אם לכל $n \in \mathbb{N}$ ולכל $x \in \{0,1\}^n$ מתקיים $C_n(x) = 1$ אם ורק אם $x \in L$.

הערה 2.1. על מנת ש-$\mathcal{C}$ תהיה מוגדרת גם במקרה $n = 0$ (כלומר הקלט הריק ε), נרשה שערים קבועים ZERO,ONE.

הגדרה 2.6 (סיבוכיות מעגלים)**.**

- **גודל מעגל** C הוא מספר השערים ב-C, מסומן ב-$|C|$.
- עבור משפחת מעגלים $\mathcal{C} = \{C_n\}_{n\in\mathbb{N}}$ ועבור פונקציה $S : \mathbb{N} \to \mathbb{N}$ נאמר **שגודל משפחת המעגלים** הוא לכל היותר S אם לכל $n \in \mathbb{N}$ מתקיים $|C_n| \le S(n)$.

טענה 2.3. כל פונקציה $f : \{0,1\}^n \to \{0,1\}$ ניתן לחשב ע"י מעגל בגודל $O(n \cdot 2^n)$.

משפט 2.2 (לופיאנוב)**.**
כל פונקציה $f : \{0,1\}^n \to \{0,1\}$ ניתן לחשב ע"י מעגל בגודל $O\left(\frac{2^n}{n}\right)$.

טענה 2.4 (שאנון).
עבור n גדול מספיק, קיימות פונקציות שלא ניתנות לחישוב ע"י מעגלים בגודל $S < \frac{2^n}{10n}$.

משפט 2.3 (חצי פורמלי)**.**
אם $f : \{0,1\}^* \to \{0,1\}$ אינה ניתנת לחישוב ע"י אף משפחת מעגלים $\mathcal{C} = \{C_n\}_{n\in\mathbb{N}}$ בגודל $2^{o(n)}$ אז f אינה ניתנת לחישוב ע"י אף אלגוריתם הרץ בזמן $2^{o(n)}$ (למשל בפייתון).

חלק II

חישוביות

פרק 3

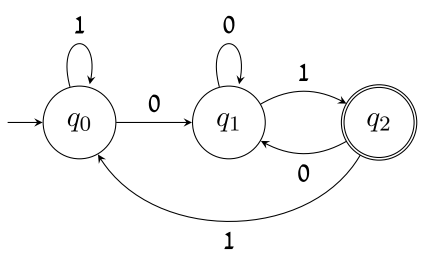
אוטומטים סופיים

3.1 אוטומט סופי דטרמיניסטי

דוגמה 3.1. נרצה להכריע את השפה של מילים בינאריות המסתיימות ב-01:

$$\mathcal{L}_1 = \{w01 : \ w \in \{0,1\}^*\}$$

נתאר תוכנית כזאת באופן סכמטי:



הגדרה 3.1. אוטומט סופי דטרמיניסטי (אס"ד) הוא חמישיה $A = (Q, \Sigma, \delta, q_0, F)$ כאשר:

- Q קבוצה סופית (לא ריקה) של מצבים,
- Σ אלפאבית,
- $\delta : Q \times \Sigma \to Q$ פונקציית מעברים,
- $q_0 \in Q$ מצב תחילי,
- $F \subseteq Q$ קבוצת מצבים מקבלים.

דוגמה 3.2 נתאר את האוטומט עבור $\mathcal{L}_1$ מדוגמה 3.1 כאס"ד $A_1 = (Q, \Sigma, \delta, q_0, F)$, כאשר:

- $Q = \{q_0, q_1, q_2\}$,
- $\Sigma = \{0, 1\}$,
- לכל $x \in \{0, 1\}$:

$$\delta(x, q_0) = \begin{cases} q_0 & x = 1 \\ q_1 & x = 0 \end{cases},$$
$$\delta(x, q_1) = \begin{cases} q_2 & x = 1 \\ q_1 & x = 0 \end{cases},$$
$$\delta(x, q_2) = \begin{cases} q_0 & x = 1 \\ q_1 & x = 0 \end{cases}$$

- $F = \{q_2\}$.

הגדרה 3.2 יהי $A = (Q, \Sigma, \delta, q_0, F)$ אס"ד. **פונקציית המעברים המורחבת** $\hat{\delta} : Q \times \Sigma^* \to Q$ מוגדרת בצורה רקורסיבית:

- עבור המילה הריקה ε, לכל מצב $q \in Q$ מתקיים $\hat{\delta}(q, \varepsilon) = q$,
- לכל $n \geq 1$ ולכל מילה $x \in \Sigma^n$ מתקיים $\hat{\delta}(q, x) = \delta\Big(\hat{\delta}(q, x_1, \ldots, x_{n-1}), x_n\Big)$.

הגדרה 3.3 אס"ד A **מקבל מילה** $x \in \Sigma^*$ אם ורק אם $\hat{\delta}(q_0, x) \in F$.
באופן שקול: A מקבל מילה $x \in \Sigma^n$ אם ורק אם קיימים $q_1, \ldots, q_n \in Q$ כך ש-

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

הגדרה 3.4 השפה של A היא אוסף המילים ש-A מקבל. מסומנת כ-$L(A)$.

הגדרה 3.5 שפה היא **רגולרית** אם קיים אוטומט סופי דטרמיניסטי המקבל אותה.

דוגמה 3.3 השפה של $\mathcal{L}_1$ מדוגמה 3.1 היא רגולרית, כי יש אוטומט שמקבל אותה. נוכיח נכונות של האוטומט A_1:

הוכחה. עבור $w = w_1 \ldots w_n$ מתקיים (נובע מההגדרה של $\hat{\delta}$):

$$\hat{\delta}(q, w_1 \ldots w_n) = \begin{cases} q_0 & w_{n-1}w_n = 11 \\ q_1 & w_{n-1}w_n \in \{00, 10\} \\ q_2 & w_{n-1}w_n = 01 \end{cases}$$

כלומר $w_{n-1}w_n = 01 \iff w \in L(A_1)$, כלומר $w \in \mathcal{L}_1 \iff w \in L(A_1)$, לכן $L(A_1) = \mathcal{L}_1$. ■

3.1.1 תכונות סגירות של שפות רגולריות

הגדרה 3.6. יהי Σ אלפאבית ויהיו $L, L^{'} \subseteq \Sigma^*$ שפות. נגדיר:

- **איחוד**:
$$L \cup L^{'} = \left\{ x \in \Sigma^* : \ x \in L \vee x \in L^{'} \right\}$$

- **חיתוך**:
$$L \cap L^{'} = \left\{ x \in \Sigma^* : \ x \in L \wedge x \in L^{'} \right\}$$

- **משלים** (מוגדר ביחס ל-Σ):
$$\overline{L} = \Sigma^* \setminus L = \left\{ x \in \Sigma^* : \ x \in \Sigma^* \wedge x \notin L^{'} \right\}$$

- **שרשור**:
$$L||L^{'} = LL^{'} = \left\{ xy : \ x \in L \wedge y \in L^{'} \right\}$$

- **חזקה**:
$$L^0 = \{\varepsilon\}, \qquad \text{and } \forall i \geq 1. \ L^i = LL^{i-1}$$

- **סגור קליני**:
$$L^* = \bigcup_{i \geq 0} L^i$$

משפט 3.1. אוסף השפות הרגולריות סגור לכל הפעולות הנ"ל.

3.2 אוטומט סופי לא-דטרמיניסטי

הגדרה 3.7. **אוטומט סופי לא-דטרמיניסטי** (אסל"ד) הוא חמישייה $N = (Q, \Sigma, \delta, S, F)$ כאשר:

- Q קבוצה סופית (לא ריקה) של מצבים,
- Σ אלפאבית,
- $\delta : Q \times \Sigma_\varepsilon \to 2^Q$,
- $S \subseteq Q$ קבוצת מצבים תחיליים,
- $F \subseteq Q$ קבוצת מצבים מקבלים.

הגדרה 3.8. יהי $N = (Q, \Sigma, \delta, S, F)$ אסל"ד.

- עבור $q \in Q$, **ε-סביבת** של q מוגדרת להיות

$$E(q) = \left\{ q^{'} : \ \exists k \geq 0. \exists q = q_0, \ldots, q_k \in Q. \ (\forall i \in [k]. q_i \in \delta(q_{i-1}, \varepsilon)) \wedge q_k = q^{'} \right\}$$

הגדרה 3.9. יהי $N = (Q, \Sigma, \delta, S, F)$ אסל"ד. **פונקציית המעברים המורחבת** $\hat{\delta} : 2^Q \times \Sigma^* \to 2^Q$ מוגדרת בצורה רקורסיבית:

- עבור המילה הריקה ε, לכל $T \subseteq Q$ מתקיים $\hat{\delta}(T, \varepsilon) = E(T)$,
- לכל $n \geq 0$, $x \in \Sigma^n$, $\sigma \in \Sigma$, $T \subseteq Q$ מתקיים

$$\hat{\delta}(T, x\sigma) = E\left(\bigcup_{q \in \hat{\delta}(T,x)} \delta(q, \sigma)\right)$$

הגדרה 3.10. אסל"ד $N = (Q, \Sigma, \delta, S, F)$ **מקבל מילה** $x \in \Sigma^*$ אם ורק אם $\hat{\delta}(S, x) \cap F \neq \emptyset$.
באופן שקול: N מקבל $x \in \Sigma^*$ אם ורק אם קיים $k \geq 0$ וקיים $\tilde{x} \in \Sigma_\varepsilon^k$ כך ש-x מתקבל מ-$\tilde{x}$ ע"י מחיקת כל ה-ε-ים וקיימים $q_0, q_1, \ldots, q_k \in Q$ כך ש-

- $q_0 \in S$,
- לכל $i \in [k]$ מתקיים $q_i \in \delta(q_{i-1}, \tilde{x}_i)$,
- $q_k \in F$.

הגדרה 3.11. **השפה של N** היא אוסף המילים ש-N מקבל. מסומנת כ-$L(N)$.

משפט 3.2 לכל אסל"ד N קיים אס"ד A כך ש-$L(N) = L(A)$. בפרט, שפה היא רגולרית אם ורק אם קיים אסל"ד המקבל אותה.

רעיון ההוכחה. באסל"ד, בכל פעם שקוראים אות עוברים **מקבוצת** מצבים נוכחית לקבוצה אחרת (לפעמים ריקה). בהתאם נוכל לבנות אס"ד שמצביו הם תתי קבוצות של מצבי האסל"ד. ■

3.3 ביטויים רגולריים

הגדרה 3.12. ביטויים רגולריים (ב"ר) מוגדרים בצורה רקורסיבית:

אורך הביטוי n	ביטוי רגולרי R	שפה $L(R)$ שהביטוי מייצג
$n = 1$	$\emptyset$	$\emptyset$
	ε	$\{\varepsilon\}$
	a עבור $a \in \Sigma$	$\{a\}$
$n > 1$	$(R_1 \cup R_2)$ עבור ב"ר R_1, R_2	$L(R_1) \cup L(R_2)$
	$(R_1 R_2)$ עבור ב"ר R_1, R_2	$L(R_1)L(R_2)$
	(R^*) עבור ב"ר R	$(L(R))^*$

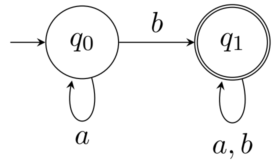
סימון 3.1. $R(\Sigma)$ כל הביטויים הרגולריים מעל Σ.

הערה 3.1. ניתן להשמיט סוגריים לפי סדר הקדימות הבא:

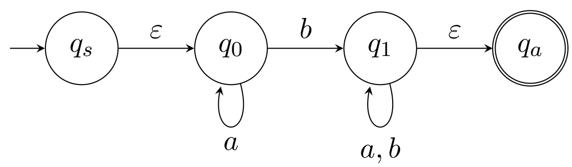
- * קודם לכל (אנלוגי לחזקה),
- אח"כ שרשור (אנלוגי לכפל),
- לבסוף איחוד (אנלוגי לחיבור).

משפט 3.3 שפה ניתנת לתיאור ע"י ביטוי רגולרי אם ורק אם היא רגולרית.

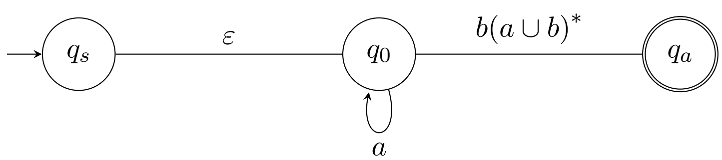
אלגוריתם 3.1 (בניית ביטוי רגולרי מתוך אס"ד)**.** בהינתן אס"ד, נהפוך אותו בשלבים ל-"אסלד מוכלל" אשר על הקשתות שלו נוכל לרשום גם ביטויים רגולריים ולא רק תווים:



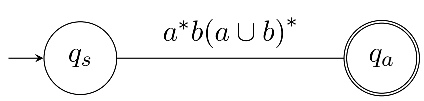
נוסיף שני מצבים:
מצב תחילי q_s עם מעבר ε ממנו לתחילי הקודם,
מצב מקבל q_a עם מעברי ε אליו מכל מצב מקבל קודם.



אחד אחרי השני, "ניפטר" מכל מצב $q \in Q \setminus \{q_a, q_b\}$, על ידי כך שנמחוק אותו ואז "נתקן" את האוטומט על ידי שינוי הביטויים הרגולריים במעברים אליו וממנו.



ואז



בצורה יותר כללית, כאשר אנחנו רוצים להיפטר ממצב $q \in Q \setminus \{q_a, q_b\}$, לכל $q_i, q_j \in Q \setminus \{q\}$ נסמן:
R_1 הביטוי הרגולרי עבור המעבר מ-q_i ל-q (ייתכן $R_1 = \emptyset$),
R_2 הביטוי הרגולרי עבור המעבר מ-q לעצמו (ייתכן $R_2 = \emptyset$),
R_3 הביטוי הרגולרי עבור המעבר מ-q ל-q_j (ייתכן $R_3 = \emptyset$),
R_4 הביטוי הרגולרי עבור המעבר ישירות מ-q_i ל-q_j (שלא דרך q, ייתכן $R_4 = \emptyset$).
לאחר מחיקת המצב q, נתקן את המעבר מ-q_i ל-q_j להיות הביטוי הרגולרי $(R_1)(R_2)^*(R_3) \cup (R_4)$.
בסופו של דבר נשאר עם "אוטומט מוכלל" כזה המכיל רק את שני המצבים q_a, q_b. הביטוי הרגולרי שמופיע על הקשת היחידה שמחברת בין שני המצבים האלה הוא הביטוי הרגולרי שמתאים לאוטומט שהתחלנו ממנו.

3.4 מגבלות של אוטומטים סופיים

3.4.1 למת הניפוח

למה 3.1. תהי L שפה רגולרית. אזי קיים $\ell > 0$ כך שלכל $w \in L$ באורך $|w| \geq \ell$ קיים פירוק $w = xyz$ כאשר:

1. לכל $k \geq 0$ מתקיים $xy^k z \in L$ מתאפשר ניפוח, או "כיווץ" אם נבחר $k = 0$
2. $|y| > 0$ הניפוח הוא לא טריוויאלי, כלומר y הוא לא המחרוזת הריקה
3. $|xy| \leq \ell$ זה תנאי טכני שלפעמים יהיה שימושי. הוא אומר לנו שהחלק של המילה אותו אפשר לנפח הוא יחסית בתחילת המילה (ב-ℓ התווים הראשונים)

הגדרה 3.13. ה-ℓ המינימלי עבורו מתקיימת למת הניפוח (3.1) נקרא **קבוע הניפוח** של L.

למה 3.2. יהי $A = (Q, \Sigma, \delta, q_0, F)$ אס"ד. אז לכל $q \in Q, w_1, w_2 \in \Sigma^*$ מתקיים $\hat{\delta}(q, w_1 w_2) = \hat{\delta}\left(\hat{\delta}(q, w_1), w_2\right)$.

הוכחת למת הניפוח (3.1). יהי $A = (Q, \Sigma, \delta, q_0, F)$ אס"ד המקבל את L, ונגדיר $\ell = |Q|$. יהי $w \in L$ כך ש-$|w| \geq \ell$.
לכל $i \in [\ell]$ נגדיר $q_i = \delta(q_{i-1}, w_i)$.
קיבלנו $|Q| = \ell < \ell + 1$ מצבים $q_0, \ldots, q_\ell \in Q$, ולכן מעיקרון שובך היונים קיימים $m, n \in [\ell] \cup \{0\}$ שונים כך ש-$q := q_m = q_n$.
בה"כ נניח $m < n$, ונגדיר $x = \prod_{i=1}^{m} w_i, y = \prod_{i=m+1}^{n} w_i, z = \prod_{i=n+1}^{\ell}$ (כאשר $\prod$ זה שרשור מוכלל, עבור קבוצת אינדקסים ריקה השרשור הוא ε). מתקיים:

$$\hat{\delta}(q_0, x) = q, \hat{\delta}(q, z) = \hat{\delta}(q_0, w) \in F$$

מתקיים $|y| \geq n - m > 0$, וכן $|xy| = n \leq \ell$ ולכן נותר להוכיח כי לכל $k \geq 0$:

$$\hat{\delta}\left(q_0, xy^k z\right) \in F$$

מלמה 3.2 מתקיים:

$$\hat{\delta}\left(q_0, xy^k z\right) = \hat{\delta}\left(\hat{\delta}\left(\hat{\delta}(q_0, x), y^k\right), z\right) = \hat{\delta}\left(\hat{\delta}\left(q, y^k\right), z\right)$$

ולכן מספיק להוכיח כי לכל $k \geq 0$ מתקיים $\hat{\delta}(q, y^k) = q$ ואז $\hat{\delta}(q_0, xy^k z) = \hat{\delta}\left(\hat{\delta}(q, y^k), z\right) = \hat{\delta}(q, z)$.
נוכיח באינדוקציה על k, עבור $k = 0$ מתקיים $y^0 = \varepsilon$ ולפי הגדרת פונקציית המעברים המורחבת $\hat{\delta}(q, \varepsilon) = q$.
יהי $k \geq 0$ ונניח כי לכל $j \leq k$ מתקיים $\hat{\delta}(q, y^j) = q$, אז לפי למה והנחת האינדוקציה

$$\hat{\delta}(q, y^{k+1}) = \hat{\delta}\left(\hat{\delta}(q, y^k), y\right) = \hat{\delta}(q, y) = q$$

■

אלגוריתם 3.2 (הוכחת אי-רגולריות באמצעות למת הניפוח)**.** נשתמש בלמת הניפוח () כדי להראות ששפות מסויימות אינן רגולריות:
בהינתן שפה L שאנחנו רוצים להראות שאינה רגולרית, נראה כי L אינה מקיימת את למת הניפוח. ספציפית, נראה כי לכל קבוע ℓ קיימת מילה $|w| \geq \ell$ שלא מקיימת את תנאי הלמה.

3.4.2 מחלקות שקילות

הגדרה 3.14 תהי $L \subseteq \Sigma^*$ שפה. מילים $x, y \in \Sigma^*$ נקראות **L-שקולות** אם לכל $z \in \Sigma^*$ מתקיים $xz \in L$ אם ורק אם $yz \in L$. אם x, y L-שקולות נסמן $x \sim_L y$.

הגדרה 3.15 יהי $A = (Q, \Sigma, \delta, q_0, F)$ אס"ד. מילים $x, y \in \Sigma^*$ נקראות **A-שקולות** אם $\hat{\delta}(q_0, x) = \hat{\delta}(q_0, y)$. אם x, y A-שקולות נסמן $x \sim_A y$.

טענה 3.1 לכל שפה $L \subseteq \Sigma^*$ מתקיים כי $\sim_L$ הוא יחס שקילות. לכל $x \in \Sigma^*$ נסמן:

$$[x]_L := [x]_{\sim_L}$$

טענה 3.2 לכל אס"ד $A = (Q, \Sigma, \delta, q_0, F)$ מתקיים כי $\sim_A$ הוא יחס שקילות. לכל $x \in \Sigma^*$ נסמן:

$$[x]_A := [x]_{\sim_A}$$

טענה 3.3 יהי A אס"ד, יהיו $x, y \in \Sigma^*$, ונסמן $L = L(A)$. אם $x \sim_A y$ אז $x \sim_L y$. כלומר $\sim_A$ הוא עידון של $\sim_L$.

מסקנה 3.1 אם $A = A = (Q, \Sigma, \delta, q_0, F)$ אס"ד ו-$L = L(A)$, אזי:

$$|Q| \geq \left|{}^{\Sigma^*}/_{\sim_A}\right| \geq \left|{}^{\Sigma^*}/_{\sim_L}\right|$$

כלומר מספר מחלקות השקילות ב-$\sim_L$ חסום על ידי מספר המצבים בכל אוטומט (או באוטומט המינימלי) שמקבל את L.

מסקנה 3.2 אם L רגולרית אז ${}^{\Sigma^*}/_{\sim_L}$ סופית.

משפט 3.4 (מייהיל-נרוד). L רגולרית אם ורק אם ${}^{\Sigma^*}/_{\sim_L}$ סופית.

הוכחת מייהיל-נרוד. $\Leftarrow$: נובע ממסקנה .

$\Rightarrow$: נניח כי קבוצת המנה סופית, אז קיימת מערכת נציגים סופית שנתארה עם פונקצייה $f: {}^{\Sigma^*}/_{\sim_L} \to \Sigma^*$, כך שלכל $x \in \Sigma^*$ מתקיים $f(x) \in [x]_L$ והיא אינה תלויה בנציג, כלומר:

$$|f([x]_L)| = 1$$

נגדיר אס"ד $A = (Q, \Sigma, \delta, q_0, F)$ שמקבל את L, כאשר:

- $Q = f\left({}^{\Sigma^*}/_{\sim_L}\right)$ מערכת הנציגים הסופית,
- Σ האלפבית ש-L מעליו,
- $\forall q \in Q, \sigma \in \Sigma.\ \delta(q, \sigma) = f([q\sigma]_L)$,
- $q_0 = f([\varepsilon]_L)$,
- $F = Q \cap L$.

טענת עזר: לכל $y \in \Sigma^*$ מתקיים $\hat{\delta}(q_0, y) = f([y]_L)$.

קבוצת המצבים המקבלים של האוטומט היא $Q \cap L$, לכן מטענת העזר לכל $x \in \Sigma^*$:

$$\hat{\delta}(q_0, x) \in F \iff f([x]_L) \in Q \cap L \iff f([x]_L) \in L$$

אם $f([x]_L) \in [x]_L$ בשפה, אז מהגדרת מחלקת השקילות של x, עבור $z = \varepsilon$:

$$f([x]_L)\varepsilon \in L \iff x\varepsilon \in L \iff x \in L$$

מכאן כי $x \in L(A) \iff x \in L$.

הוכחת טענת העזר: נוכיח באינדוקציה על $|y|$, עבור $|y| = 0$ מתקיים $\hat{\delta}(q_0, y) = \hat{\delta}(q_0, \varepsilon) = q_0 = f([\varepsilon]_L) = f([y]_L)$.
נניח כי לכל $|z| = n$ מתקיים $\hat{\delta}(q_0, z) = f([z]_L)$, ויהי $|y| = n + 1$, נסמן $y = z\sigma$, אז לפי הגדרת פונקציית המעברים המורחבת והנחת האינדוקציה:

$$\hat{\delta}(q_0, y) = \delta\Big(\hat{\delta}(q_0, z), \sigma\Big) = \delta(f([z]_L), \sigma) = f\big([f([z]_L)\sigma]_L\big) = f([z\sigma]_L) = f([y]_L)$$

■

פרק 4

מכונות טיורינג

4.1 מכונת טיורינג חד-סרטית

הגדרה 4.1. מכונת טיורינג (מ"ט) היא שביעייה $M = (Q, \Sigma, \Gamma, \delta, q_0 . q_a . q_r)$ כאשר:

- Q קבוצת מצבים סופית $q_0, q_a, q_r \in Q$
- Σ אלפאבית קלט
- Γ אלפאבית סרט כך ש-$\Sigma \subseteq \Gamma$, $\sqcup \in \Gamma \setminus \Sigma$
- δ פונקציית מעברים כך ש-$\delta : (Q \setminus \{q_a, a_r\}) \times \Gamma \to Q \times \Gamma \times \{L, R\}$
- q_0 מצב תחילי
- q_a מצב מקבל
- q_r מצב דוחה, $q_a \neq q_r$

אלגוריתם 4.1 (חישוב של מ"ט).

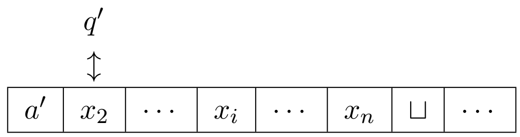
- בתחילת החישוב:
  - הקלט $x \in \Sigma^*$ בתחילת הסרט
  - שאר הסרט מאותחל בסימני $\sqcup$
  - הראש בתחילת הסרט (צד שמאל)
  - המצב הוא q_0

q_0

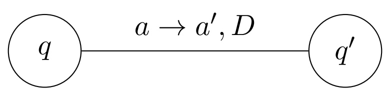
$\updownarrow$

x_1	x_2	$\cdots$	x_i	$\cdots$	x_n	$\sqcup$	$\cdots$

- צעד חישוב:
  - אם המצב הפנימי הוא $q \in Q \setminus \{q_a, q_r\}$ והראש קורא $a \in \Gamma$
  - מחשבים $\delta(q,a) = (q', a', D)$
  - הראש כותב $a^{'}$ (במקום a)
  - עובר למצב $q^{'}$
  - זז צעד ימינה אם $D = R$ ושמאלה אם $D = L$
    (אם $D = L$ והראש בתחילת הסרט אז הוא נותר במקום)
- ברגע שהגענו ל-q_a או q_r החישוב מסתיים.
- בהמשך לתמונה הקודמת, אם $\delta(q, x_1) = (q', a', R)$ אז נקבל



סימון 4.1. עבור $\delta(q,a) = (q', a', D)$ נסמן



אם $q' = q_r$ ניתן להשמיט את הקשת.
אם $a' = a$ ניתן להשמיט a' ולכתוב $a \to D$.

דוגמה 4.1. מ"ט המקבלת קלט x ומסיטה אותו "שיפט אחד ימינה" תוך שבתא השמאלי ביותר מוסיפה תו מיוחד #.

הגדרה 4.2. יהי Σ אלפאבית. בהינתן $>$ יחס סדר חזק טוטאלי על Σ, **סידור לקסיקוגרפי** של Σ^* הוא הסדר חזק הטוטאלי על Σ^* שמוגדר לכל $x = x_1 \ldots x_n, y = y_1 \ldots y_m$ לפי:

$$x <_l y \iff n < m \vee (n = m \wedge \exists k \in [n].\ (\forall i \in [k-1].\ x_i = y_i) \wedge x_k < y_k)$$

דוגמה 4.2. מונה לקסיקוגרפי.
<u>קלט:</u> $\#x$ עבור $x \in \Sigma^*$.
<u>פלט:</u> $\#x'$ כאשר x' הוא העוקב של x בסידור הלקסיקוגרפי (נניח כי נתון סדר על Σ).

בהגדרות הבאות $M = (Q, \Sigma, \Gamma, \delta, q_0 . q_a . q_r)$ מ"ט ונניח בה"כ $Q \cap \Gamma = \emptyset$.

הגדרה 4.3 קונפיגורציה של M היא מחרוזת $c \in \Gamma^* Q \Sigma^*$.
<u>פרשנות:</u> עבור $q \in Q$, $u, v \in \Gamma^*$ נפרש את uqv באופן הבא:

- תוכן הסרט הנוכחי הוא $uv\sqcup^\infty$
- המצב הפנמי הוא q
- הראש נמצא מעל התו הראשון של v

הערה 4.1. נתחייס ל-c ול-$c\sqcup$ כאותה קונפיגורציה.

הגדרה 4.4. תהי c קונפיגורציה.

- c **התחלתית** אם ורק אם $c = q_0v$ עבור $v \in \Sigma^*$
- c **מקבלת** אם ורק אם $c = uq_av$ עבור $u, v \in \Gamma^*$
- c **דוחה** אם ורק אם $c = uq_rv$ עבור $u, v \in \Gamma^*$

הגדרה 4.5. קונפיגורציה c **δ-עוברת** ל-c' אם ורק אם מתקיים אחד מהתנאים הבאים עבור איזשהם $q, q' \in Q$, $u, v \in \Gamma^*$, $a, b, b' \in \Gamma$:

$$c = uaqbv, \qquad \delta(q,b) = (q', b', L), \qquad c' = uq'ab'v \tag{4.1}$$
$$c = qbv, \qquad \delta(q,b) = (q', b', L), \qquad c' = q'b'v \tag{4.2}$$
$$c = uqbv, \qquad \delta(q,b) = (q', b', R), \qquad c' = ub'q'v \tag{4.3}$$

הגדרה 4.6 M **מקבלת/דוחה** קלט $x \in \Sigma^*$ אם קיימת סדרת קונפיגורציות $c_0, \dots, c_t$ כך ש-

1. $c_0 = q_0x$
2. c_{i-1} עוברת ל-c_i לכל $i \in [t]$
3. c_t קונפיגורציה מקבלת/דוחה

סימון 4.2. $L(M)$ אוסף המילים ש-M מקבלת.

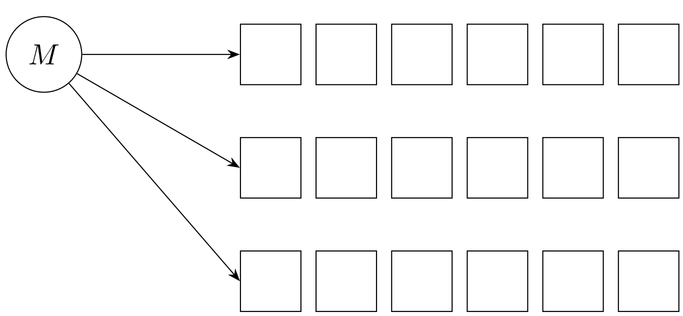
4.2 מודלים שקולים

הגדרה 4.7 (חצי פורמלית). נאמר כי שני **מודלים שקולים** אם כל אחד מהם יכול לסמלץ את השני. כלומר לכל מכונה M במודל אחד קיימת מכונה M' במודל השני שמקבלת/דוחה/לא-עוצרת בדיוק על אותם קלטים.

דוגמה 4.3. המודל של מ"ט עם ראש קורא-כותב שיכול להישאר במקום שקול למ"ט חד-סרטית.

4.2.1 מכונה רב-סרטית

הכללה של המודל של מ"ט כפי שראינו אותו. עכשיו יש לנו גישה ל- k סרטים בעזרת k ראשים קוראים/כותבים:



- **בתחילת החישוב** הקלט נמצא על הסרט הראשון והשאר ריקים ($\sqcup^\infty$) , ובכל סרט הראש מופיע בקצה השמאלי.

- **בכל צעד חישוב** המכונה קוראת k-איה של תווים (תו מתחת לכל ראש) ועפ"י ה- k-איה הנ"ל והמצב הפנימי מחליטה:
  1. איזה תו לרשום תחת כל ראש
  2. לאן להזיז כל ראש
  3. לאיזה מצב פנימי לעבור
- **כלומר פונקציית המעברים** נראית כך: $\delta : (Q \setminus \{q_a, q_r\}) \times \Gamma^k \to Q \times \Gamma^k \times \{L, R\}^k$
- **קונפיגורציה k-סרטית** היא מחרוזת מהצורה $c = c_1\$c_2\$\ldots\#c_k$ כאשר כל c_i היא קונפ' חד-סרטית. בפרט, קונפ' התחלתית נראית כך $q_0x \sqcup \$q_0 \sqcup \$\ldots\$q_0\sqcup$.

טענה 4.1 לכל קבוע $k \in \mathbb{N}$, מ"ט k-סרטית שקולה למ"ט חד-סרטית.

רעיון ההוכחה. בהינתן מ"ט k-סרטית נבנה מ"ט חד-סרטית M' שמסמלצת אותה:

- נשמור את תכני k הסרטים של M באופן משורשר (על הסרט היחיד של M'), מופרדים ב-#
- מיקומי הראשים ייוצגו ע"י סימון bar, למשל $\overline{a}$

סימולטור חד-סרטי M' למ"ט k-סרטית M:

שלב האתחול: בהינתן קלט $x = x_1 \ldots x_n$, נרשום על הסרט

$$\#\overline{x_1}x_2\ldots x_n\#\overline{\sqcup}\#\overline{\sqcup}\#\ldots\#\overline{\sqcup}\sqcup\sqcup\ldots$$

כדי לסמלץ כל צעד של M:

1. נסרוק את הסרט על מנת לקרוא את k התווים מתחת לראשים (שמופיעים עם bar). נזכור מידע זה בעזרת המצב של M' (ניתן לזכור מידע זה כי הוא בגודל קבוע – יש $|\Gamma|^k$ אפשרויות)
2. נסרוק פעם שניה את הסרט על מנת לעדכן את התווים תחת הראשים הווירטואליים ואת מיקום הראשים הווירטואליים (מיקום סמני bar) בהתאם לפונק' המעברים של M.

הערה 4.2 אם ראש וירטואלי כלשהו אמור לזוז ימינה למקום שבו יש #, כלומר למקום "לא מאותחל" בסרט הווירטואלי (בסרט המקורי מגיעים ל-$\sqcup$ מסדרת ה-$\sqcup$ האינסופית), אזי $M\prime$ תסיט את כל סיפת הסרט תא אחד ימינה תוך שבמקום הנוכחי נכתוב $\sqcup$.

מהי סיבוכיות הסימולציה? כלומר אם M מבצעת T_x פעולות חישוב על קלט x, כמה פעולות חישוב תבצע M' על x?
לשם פשטות נניח כי $T_x \geq |x|$ ולכן נוכל להתעלם משלב האתחול שלוקח $|x| + k$ צעדים.
כל צעד בסימולציה (כלומר צעד ששקול לפעולה יחידה של M) לוקח לכל היותר k מעברים על הסרט כולו. ומה אורך הסרט (החלק הפעיל)? הוא לכל היותר k פעמים אורך הסרט הארוך היותר בשלב המקביל בחישוב M על x שהוא חסום ע"י T_x. לכן, מס' הפעולות ש-M' מבצעת בצעד סימולציה יחיד הוא לכל היותר

$$k \cdot k \cdot T_x$$

בסה"כ זמן הריצה של M' על x הוא

$$O(T_x \cdot k^2 T_x) = O(T_x^2)$$

■

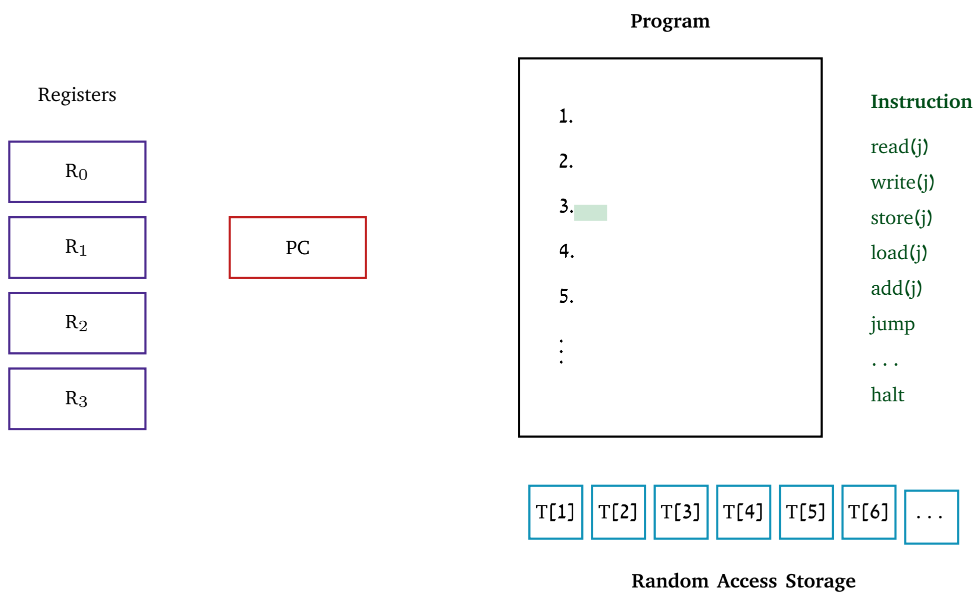
4.2.2 מכונת RAM (Random Access Machine/Memory)

זה מודל שתופס בצורה יותר טובה את מה שבאמת קורה במחשבים שלנו. במקום לעבוד עם אלפבית סופי כמו מ"ט, במודל ה-RAM נעבוד עם ערכים שלמים אי-שליליים (לא חסומים). במודל הזה יש לנו:

- "רגיסטרים" (בהם נחזיק ערכים מספריים עליהם נרצה לבצע פעולות בסיסיות)
- "מערך" זיכרון אינסופי, אנלוגי לסרט הזיכרון האינסופי במ"ט. ישנם 2 הבדלים עיקריים בין הזיכרון הזה לבין הסרט של מ"ט:
  1. כל תא במערך הזה מחזיק **מספר**
  2. יש לנו גישה ישירה לכל תא במערך הזה, ללא צורך לסרוק את הזיכרון בצורה סדרתית כמו במ"ט
- בנוסף לזיכרון ולרגיסטרים, מכונה במודל ה-RAM גם מכילה "תוכנית לביצוע" (=סדרה של פקודות). כדי שנדע "איפה אנחנו" בקריאת התוכנית הזאת, אחד הרגיסטרים במכונה הוא רגיסטר יעודי לשם כך, נקרא "מונה תוכנית" (program counter, Pc) . המונה הזה זוכר את האינדקס של הפקודה הבאה שעלינו לבצע.
- כל פקודה בתוכנית הזאת היא אחת מתוך אוסף סופי של פקודות אפשריות אשר מאוד דומות לפקודות באסמבלי. למשל:

Instruction	Operand	הסבר
read	j	$R_0 \leftarrow T[j]$
write	j	$T[j] \leftarrow R_0$
store	j	$R_j \leftarrow R_0$
load	j	$R_0 \leftarrow R_j$
add	j	$R_0 \leftarrow R_0 + R_j$
jump		PC $\leftarrow R_0$
...	...	...
halt		פקודת סיום ריצה. נחליט על קבלה/דחיה לפי הערך של R_0

בציור:



הגדרה 4.8.

- מכונה במודל RAM הא זוג סדור (k, Π) כאשר:
  - $k \in \mathbb{N}$ מציין את מספר הרגיסטרים
  - $\Pi = (\pi_1, \pi_2, \dots \pi_p)$ היא סדרה של פקודות
- קונפיגורציה במודל זה מוגדרת ע"י:
  1. הערך של מונה התוכנית PC
  2. ערכים ברגיסטרים $R_0, R_1, \dots, R_k \in \mathbb{N} \cup \{0\}$
  3. ערכים במערך הזיכרון $T : \mathbb{N} \to (\mathbb{N} \cup \{0\})$

  בתחילת הריצה כל המערך מאותחל לאפסים. שימו לב שבכל רגע נתון במהלך הריצה, ישנן מספר סופי של תאים המכילים ערכים ששונים מאפס.

טענה 4.2. מכונות טיורינג שקולות ל-RAM.

מימוש מ"ט ע"י RAM

- את הסרט נסמלץ ע"י מערך הזיכרון
- בכל רגע נזכור את מיקום הראש באחד הרגיסטרים, נניח ב-R_1
- את פונקציית המעברים נממש בעזרת "תוכנית פקודות" מתאימה

מימוש מכונת RAM ע"י מ"ט רב-סרטית

- יהיו לנו $k + 3$ סרטים:

1. יהיה לנו סרט אחד לכל רגיסטר אשר יכיל את הערך באותו רגיסטר
2. יהיה לנו סרט נוסף שישמש כזיכרון זמני, למשל כדי לזכור את המספר 271 בפקודה

$$R_0 \leftarrow R_0 + 271$$

3. יהיו לנו סרט נוסף שעליו יהיה כתוב הקלט בתחילת הריצה (נניח שעל אותו סרט גםנכתוב את הפלט, אם צריך, בסיום הריצה)
4. וסרט נוסף אשר יסמלץ את מערך הזיכרון של מכונת ה-RAM במהלך הריצה. אנחנו צריכים לזכור גם את תוכן התאים הלא ריקים ממערך הזיכרון וגם את הכתובות שלהם, ולכן יהיה נח לתחזק את זה כרשימת זוגות מהצורה $(m, T[m])$.

- את "התוכנית" של מכונת ה-RAM נסמלץ בעזרת המצבים ופ' המעברים של המ"ט שלנו. כדי לעשות את זה אנחנו צריכים תת-שגרה (או תת-מ"ט) עבור כל פקודה בתוכנית. למשל, כדי לסמלץ פקודה אשר מערבת קריאה ממערך הזיכרון בתא m, נסרוק את הסרט המתאים ונמצא את הזוג עם האינדקס m, ואז נקרא או נכתוב את הערך המתאים בזוג הזה. (אם לא מצאנו זוג עם אינדקס מתאים, אז הערך שחיפשנו לא אותחל עדיין ולכן ערכו אפס). אחרי שסיימנו לטפל בפקודה הנוכחית, נעבור למצב שמתאים לתחילת הפקודה הבאה (זה אנלוגי להגדלת ה-PC).

הערה 4.1 (תזת צ'רץ'-טיורינג). כל מודל חישוב "סביר" ניתן לסמלץ ע"י מ"ט.

4.3 מכונות טיורינג לא-דטרמיניסטיות

הגדרה 4.9. מכונת טיורינג לא-דטרמיניסטית (מטל"ד) היא שביעייה $N = (Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r)$ כאשר:

- Q קבוצת מצבים סופית $q_0, q_a, q_r \in Q$
- Σ אלפאבית קלט
- Γ אלפאבית סרט כך ש-$\Sigma \subseteq \Gamma$, $\sqcup \in \Gamma \setminus \Sigma$
- δ פונקציית מעברים כך ש-$\delta : (Q \setminus \{q_a, a_r\}) \times \Gamma \to 2^{Q \times \Gamma \times \{L,R\}}$
- q_0 מצב תחילי
- q_a מצב מקבל
- q_r מצב דוחה, $q_a \neq q_r$

הגדרה 4.10. קונפיגורציה של מטל"ד $N = (Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r)$ היא מחרוזת $c \in \Gamma^* Q \Sigma^*$.

הגדרה 4.11. תהי c קונפיגורציה של מטל"ד $N = (Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r)$.

- c **התחלתית** אם ורק אם $c = q_0 v$ עבור $v \in \Sigma^*$
- c **מקבלת** אם ורק אם $c = u q_a v$ עבור $u, v \in \Gamma^*$
- c **דוחה** אם ורק אם $c = u q_r v$ עבור $u, v \in \Gamma^*$

הגדרה 4.12. קונפיגורציה c של מטל"ד $N = (Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r)$ **δ-עוברת** ל-c' אם ורק אם מתקיים לפחות אחד מהתנאים הבאים עבור איזשהם $q, q' \in Q$, $u, v \in \Gamma^*$, $a, b, b' \in \Gamma$:

$$c = uaqbv, \qquad (q', b', L) \in \delta(q, b), \qquad c' = uq'ab'v \tag{4.4}$$
$$c = qbv, \qquad (q', b', L) \in \delta(q, b), \qquad c' = q'b'v \tag{4.5}$$
$$c = uqbv, \qquad (q', b', R) \in \delta(q, b), \qquad c' = ub'q'v \tag{4.6}$$

הגדרה 4.13. תהי $N = (Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r)$ מטל"ד ויהי $x \in \Sigma^*$.
עץ החישוב של N על x, שנסמנו $T_{N,x}$ הוא עץ מושרש שבו כל צומת היא קונפיגורציה כאשר:

- השורש הוא הקונפיגורציה ההתחלתית $q_0 x \sqcup$
- לכל צומת c, ילדיו הם הקונפיגורציות אליהן הקונפיגורציה c עוברת
- צומת הוא עלה אמ"מ הוא קונפ' מקבלת/דוחה או שאינו עובר לאף קונפ', כלומר $\delta(a, b) = \emptyset$

הגדרה 4.14. תהי $N = (Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r)$ מטל"ד.

- N **מקבלת** את $x \in \Sigma^*$ אמ"מ ב-$T_{N,x}$ יש עלה מקבל
- N **דוחה** אמ"מ $T_{N,x}$ סופי וללא עלים מקבלים
- אחרת ($T_{N,x}$ אינסופי ואין עלים מקבלים), N **אינה עוצרת**.

טענה 4.3. המודלים של מ"ט ומטל"ד שקולים.

הוכחה. מ"ט היא בבירור מקרה פרטי של מטל"ד. ביכוון השני נרצה להראות שכל מטל"ד $N = (Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r)$ אפשר לסמלץ ע"י מ"ט M.

נניח בה"כ שלכל $\gamma \in \Gamma$ ולכל $q \in Q \setminus \{q_a, q_r\}$ מתקיים

$$|\delta(q,\gamma)| = C_N \coloneqq |Q| \cdot |\Gamma| \cdot 2$$

(בה"כ כי נוכל להוסיף מעברים למצב q_r, q_a)

כעת, בהינתן q, γ נניח סדר (לקסיקוגרפי) על המעברים האפשריים, כלומר על השלשות:

$$\delta(q,\gamma) = \left\{ \left(q^1, \gamma^1, D^1\right), \ldots, \left(q^{C_N}, \gamma^{C_N}, D^{C_N}\right) \right\}$$

כך בהינתן העץ $T_{N,x}$ הגדרנו סידור על הבנים של כל קודקוד uqv בעץ.

עתה, כל מחרוזת $\alpha \in [C_N]^k$ מגדירה מסלול בעץ $T_{N,x}$ באורך k (=חישוב של M על x ב-k צעדים).

נבנה את M בשני שלבים:

1. נבנה מ"ט L שתשמש את M כתת-פרוצדורה אשר מקבלת x ומחרוזת בחירות α ומסמלצת את ריצת N על x עפ"י α
2. נבנה את M שתחזיק מונה בבסיס C_N שישמש כקלט (יחד עם x) ל-L

בניית L: L היא מ"ט דטר' שמצביה הם בדיוק המצבים של N.
L תשתמש בשלושה סרטים: על סרט הקלט תהיה רשומה המילה x. על הסרט השני תהיה רשומה מחרוזת בחירות α (באורך סופי).
בסרט השלישי נשתמש בשביל לבדוק האם עץ החישוב הוא סופי וכבר סרקנו את כולו.

ריצת L:

- בכל שלב בחישוב, L קוראת בסרט 1 תו נוכחי γ וקוראת בסרט 2 תו "בחירות" c. בהינתן שהמצב הנוכחי הוא q, מבצעת את המעבר ה-c בסידור של $\delta(q,\gamma)$.
- אם לא ניתן לבצע את המעבר, כלומר נתקלנו בעלה (כלומר $\delta(q,\gamma) = \emptyset$ או ש-$q \in \{q_a, q_r\}$) אז נעצור ונענה בהתאם לעלה
- אם בסרט 2 מגיעים לתו ריק אז נכתוב על הסרט השלישי "לא סופי" **ונעצור ונדחה** (אחרת נמשיך בסימולציה).

בניית M: Mתהיה מ"ט עם 4 סרטים:
סרט 1 יהי סרט הקלט שאף פעם לא נשנה את תוכנו (עליו יופיע x)
סרטים $2,3,4$ יהיו הסרטים שישמשו גם את L:

- בכל הרצה של L, המ"ט M תכתוב מחדש את x על סרט 2
- בסרט 3 נתחזק מונה לקסיקוגרפי בבסיס C_N שישמש כמחרוזת הבחירות של L
- בעזרת סרט 4 נסמן לעצמנו האם עת החישוב הוא סופי וכבר סרקנו את כולו.

פעולת M על קלט $x \in \Sigma^*$

אתחול: אתחל את סרט 3 ל-"1" ואתחל את סרט 4 ל-"אולי סופי".

בצע לנצח:

1. מחק את סרט 2 והעתק את x לסרט 2
2. הרץ את L על סרטים $2,3,4$. אם L קיבלה, **עצור וקבל**
3. אם המונה בסרט 3 הוא מהצורה C_n^* אז:
   - אם בסרט 4 רשום "אולי סופי" אז **עצור ודחה** (המשמעות של זה היא שאף אחת מהריצות של L לא שינתה את תוכן הסרט הזה ל-"לא סופי", ולכן כל הענפים שסרקנו היו סופיים)
   - אחרת רשום על סרט 4 "אולי סופי"
4. הגדל את המונה בסרט 3 ב-1 וחזור ל-(1)

■

פרק 5

כריעות

5.1 שפות מתקבלות ושפות מוכרעות ע"י מ"ט

הגדרה 5.1. נגדיר את המחלקה

$$\mathrm{RE} := \{L \subseteq \Sigma^* : \text{there exists a TM } M \text{ such that } L = L(M)\}$$

הגדרה 5.2. נאמר שמ"ט M **מכריעה** (decides) שפה $L \subseteq \Sigma^*$ אם מתקיים:

1. $L = L(M)$
2. לכל $w \in \Sigma^*$ מתקיים ש-M עוצרת על w

את **מחלקת השפות הכריעות** נסמן:

$$\mathrm{R} := \{L \subseteq \Sigma^* : \text{there exists a TM } M \text{ that decides } L\}$$

הגדרה 5.3. מ"ט E הינה **מונה עבור שפה** $L \subseteq \Sigma^*$ אם:

- ל-E סרט פלט לכתיבה חד-פעמית (תא אשר המכונה מאתחלת לא משתנה)
- א"ב פלט $\Sigma \cup \{\$\}$ כאשר בה"כ $\$ \notin \Sigma$
- בריצה של E על הקלט הריק:
  - לכל $x \in L$, המחרוזת $\$x\$$ כתובה על סרט הפלט לאחר מספר סופי של צעדים
  - לכל $x \notin L$, המחרוזת $\$x\$$ לעולם לא כתובה בפלט

טענה 5.1. $L \in \mathrm{RE}$ אמ"מ קיים עבורה מונה.

הוכחה: יהי $\sigma_1, \sigma_2, \ldots$ סידור לקסיקוגרפי של Σ^*.

כיוון ראשון - בהינתן מונה E עבור L נראה כי $L \in \mathrm{RE}$ נבנה מ"ט M המקבלת את L באופן הבא: $M(x)$ מריצה את המונה E ומקבלת אם וכאשר $\$x\$$ מופיע על סרט הפלט.

כיוון שני - בהינתן מ"ט M המקבלת את L נבנה מונה עבור L נבנה מונה E באופן הבא:

- כותב \$ בתא הפלט הראשון לאתחול הרשימה.
- לכל $i \geq 1$:
  - מריץ את M על כל אחד מהקלטים $\sigma_1, \ldots, \sigma_i$ במשך i צעדים
  - בכל פעם שמתקבלת מילה σ_j בתהליך, מוסיפים את σ_j\$ לסרט הפלט

מתקיים:

- אם \$$\sigma_j$\$ נכתב לסרט אז אחת הריצות של M קיבלה את σ_j ולכן $\sigma_j \in L(M)$
- אם $\sigma_j \in L(M)$ ומתקבלת תוך t צעדים של M אזי באיטרציה $i = \max\{j, t\}$ נקבל ש-\$$\sigma_j$\$ תכתב לסרט הפלט

■

הגדרה 5.4 מ"ט E הינה **מונה לקסיקוגרפי עבור שפה** $L \subseteq \Sigma^*$ אם:

- E הוא מונה עבור L
- בריצה של E על הקלט הריק, בנוסף לדרישות של מונה:
  - לכל $x \in L$, אם היא כתובה על הסרט בפעם הראשונה אחרי t צעדים, אז לכל $y \in L$ כך ש-$y < x$ בסדר הלקסיקוגרפי מתקיים כי y כתובה על הסרט בפעם הראשונה אחרי $k > t$ צעדים.

טענה 5.2 $L \in \mathrm{R}$ אמ"מ קיים עבורה מונה לקסיקוגרפי.

__הוכחה:__ יהי $\sigma_1, \sigma_2, \ldots$ סידור לקסיקוגרפי של Σ^*.

כיוון ראשון - בהינתן מונה לקסיקוגרפי E עבור L נראה כי $L \in \mathrm{R}$ נבנה מ"ט M המכריעה את L באופן הבא:
$M(x)$ מריצה את המונה E ומקבלת אם \$$x$\$ מופיע על סרט הפלט, ודוחה אם \$$y$\$ מופיע על סרט הפלט לכל $x > y$ בסדר הלקסיקוגרפי.

כיוון שני - בהינתן מ"ט M המכריעה את L נבנה מונה לקסיקוגרפי עבור L נבנה מונה לקסיקוגרפי E באופן הבא:

- כותב \$ בתא הפלט הראשון לאתחול הרשימה.
- לכל $i \geq 1$:
  - מריץ את $M(\sigma_i)$
  - אם מקבל אז כותב σ_i\$

מתקיים:

- אם \$$\sigma_i$\$ נכתב לסרט אז M קיבלה את σ_i ולכן $\sigma_i \in L(M)$
- אם $\sigma_i \in L(M)$ אזי באיטרציה ה-i נקבל ש-\$$\sigma_i$\$ תכתב לסרט הפלט

■

הגדרה 5.5. נגדיר את המחלקה

$$coRE := \left\{ L \subseteq \Sigma^* : \overline{L} \in \mathrm{RE} \right\}$$

טענה 5.3. R סגורה למשלים.

טענה 5.4. $\mathrm{R} = \mathrm{RE} \cap co\mathrm{RE}$.

הוכחה:

כיוון ראשון - $\mathrm{R} \subseteq \mathrm{RE} \cap co\mathrm{RE}$ $\mathrm{R} \subseteq \mathrm{RE}$ ולכן מספיק להראות $\mathrm{R} \subseteq co\mathrm{RE}$.
תהא $L \in \mathrm{R}$, אזי גם $\overline{L} \in \mathrm{R}$ ולכן גם $\overline{L} \in \mathrm{RE}$.
אז $L \in co\mathrm{RE}$.

כיוון שני - $\mathrm{RE} \cap co\mathrm{RE} \subseteq \mathrm{R}$ תהא $L \in \mathrm{RE} \cap co\mathrm{RE}$, אז קיימות מכונות M_1, M_2 כך ש-$L(M_1) = L, L(M_2) = \overline{L}$.
נגדיר מכונה M שמכריעה את L באופן הבא:

- עבור קלט $x \in \Sigma^*$
- הרץ את $M_1(x), M_2(x)$ במקביל (למשל עם מכונה דו-סרטית)
- אם $M_1(x)$ עוצרת ומקבלת, קבל
- אם $M_2(x)$ עוצרת ומקבלת, דחה

מתקיים:

- אם $M_1(x)$ עוצרת ומקבלת, אז $x \in L$
- אם $M_2(x)$ עוצרת ומקבלת, אז $x \notin L$

אם $x \in L$ אז בהכרח $M_1(x)$ עוצרת ומקבלת, ולכן $M(x)$ מקבלת
אם $x \notin L$ אז בהכרח $M_2(x)$ עוצרת ומקבלת, ולכן $M(x)$ דוחה ■

5.1.1 מ"ט אוניברסליות וקידוד של מ"ט

הגדרה 5.6 קידוד (בינארי) של מ"ט הוא מיפוי חח"ע שלכל מ"ט M מתאים מחרוזת $\langle M \rangle \in \{0,1\}^*$.

סימון 5.1. עבור מ"ט M וקלט x עבורה נסמן ב-$\langle M, x \rangle$ קידוד בינארי של M ושל הקלט x.

דוגמה 5.1. לשם פשטות נראה עכשיו קידוד "כמעט בנארי" שיהיה קל לתיאור.
תהי M מ"ט עם מצבים $Q = \{q_0, q_1, \ldots, q_n\}$ כאשר בה"כ q_0, q_1, q_2 מצבים תחילי/מקבל/דוחה בהתאמה, ועם אלפאבית עבודה $\Gamma = \{\sqcup, 0, 1, 2, \ldots, m\}$ כאשר $0,1$ הם תווי הקלט. לשם פשטות נניח כי $\Sigma = \{0,1\}$.

- נקודד מצב $q_k \in Q$ על ידי המחרוזת qw כאשר w הוא הייצוג הבינארי של k. למשל נייצג את q_3 על ידי $q011$.
- נקודד תו $k \in \Gamma$ על ידי המחרוזת aw כאשר w הוא הייצוג הבינארי של k.

כעת כדי לתאר/לקודד את המכונה M הנתונה, כל מה שאנחנו צריכים לעשות זה לתאר/לקודד את פונק' המעברים של המכונה.
נוכל לרשום זאת ע"י חמישיות כאשר כל חמישייה מתארת את אחד המעברים של פונק' המעברים.

משפט 5.1 קיימת מ"ט U אשר בהינתן קידוד $\langle M, x\rangle$ של מ"ט וקלט, מקבלת/דוחה/לא-עוצרת אם $M(x)$ מקבלת/דוחה/לא-עוצרת.

הערה 5.1. בהינתן קלט שאינו קידוד חוקי, U דוחה.

הערה 5.2. מספר המצבים וגודל האלפאבית של U קבוע (קטן מ-100).

אינטואיציה לבניית U:

- למכונה יהיו 3 סרטים. בתחילת הריצה על סרט 1 מופיע קידוד של הקלט $\langle x\rangle$, על סרט 2 מופיע הקידוד של המ"ט אותה עלינו לסמלץ $\langle M\rangle$, ועל סרט 3 מופיע הקידוד של המצב ההתחלתי, כלומר מחרוזת מהצורה $q000$.
- במהלך הריצה, סרט 1 יסמלץ את הסרט של M בריצה על x (כולל מיקום הראש), וסרט 3 יחזיק את המצב הנוכחי של M.
- בכל שלב בסימולציה, נקרא את קידוד התו עליו מצביע הראש בסרט 1 ואת קידוד המצב הכתוב בסרט 3, ונחפש בסרט 2 חמישייה המתאימה לתו+מצב האלה. אם לא מצאנו אז נעצור ונדחה. אחרת נבצע את השינויים המתאימים בסרטים $2+1$.

5.1.2 האם יש בעיות שתוכניות מחשב לא יכולות לפתור?

טענה 5.5. קיימת $L \in \{0,1\}^*$ כך ש-$L \notin \mathrm{RE} \cup co\mathrm{RE}$. בפרט L אינה כריעה (כלומר אינה ב-R).

הוכחה: שיקולי ספירה:

- יש $\aleph_0$ מחרוזות בינאריות ומספר תתי הקבוצות שלהם הוא $2^{\aleph_0} = \aleph$. כלומר:

$$\left|2^{\{0,1\}^*}\right| = \aleph$$

- לכל שפה ב-$\mathrm{RE} \cup co\mathrm{RE}$ יש מ"ט שמקבלת אותה או את המשלים שלה. לכן

$$|\mathrm{RE} \cup co\mathrm{RE}| = |\{L : L \in \mathrm{RE} \cup co\mathrm{RE}\}| \leq |\{M : M \text{ is a TM}\}| \leq |\{\langle M\rangle : \langle M\rangle \in \{0,1\}^* \text{ is an encoding}\}| = \aleph_0$$

■

הגדרה 5.7. נגדיר את **בעיית הקבלה**

$$\mathrm{ACC} := \{\langle M, x\rangle : \langle M, x\rangle \text{ is an encoding such that } M(x) \text{ accepts}\}$$

טענה 5.6. $\mathrm{ACC} \in \mathrm{RE}$.

הוכחה: $\mathrm{ACC} = L(U)$ כאשר U המכונה האוניברסלית. ■

טענה 5.7. $\mathrm{ACC} \notin \mathrm{R}$.

הוכחה: נגדיר את השפה $F = \{\langle M\rangle : \langle M\rangle \notin L(M)\}$.

למה 5.1 לא קיימת מ"ט M כך ש-$F = L(M)$, כלומר $F \notin \mathrm{RE}$.

הוכחת למה 5.1: נניח בשלילה שקיימת מ"ט M המקבלת את F.
נריץ את M על $\langle M\rangle$:

- אם היא לא מקבלת, אז $\langle M\rangle \notin L(M)$, לכן $\langle M\rangle \in F$ וזו סתירה כי $F = L(M)$.
- אם היא מקבלת אז $\langle M\rangle \in L(M)$, לכן $\langle M\rangle \notin F$ וזו סתירה כי $F = L(M)$.

בכל מקרה $F \neq L(M)$

למה 5.2. אם קיימת מ"ט M_A המכריעה את ACC אז קיימת מ"ט M_F המכריעה את F.

הוכחת למה 5.2: נניח כי קיימת מ"ט M_A המכריעה את ACC, נגדיר מ"ט M_F המכריעה את F באופן הבא:

- עבור קלט $\langle M\rangle \in \{0,1\}^*$, אם הקלט לא קידוד אז דחה.
- הרץ את $M_A(\langle M, \langle M\rangle\rangle)$ וענה הפוך ממנה.

אז משום ש-M_A מכריעה את ACC, M_F תמיד עוצרת, ומקבלת אמ"מ $\langle M\rangle \notin L(M)$.

מסקנה 5.1. לא קיימת מ"ט M_A המכריעה את ACC.

■

הגדרה 5.8 (חצי פורמלית)**.** קיימת **רדוקציה** מבעיית הכרעה A לבעיית הכרעה B אם ניתן להשתמש בכל מכריע עבור B על מנת להכריע את A.

סימון 5.2. $A \leq B$. פרשנות: "B יותר קשה להכרעה מ-A".

בפרט, זה גורר שאם A לא ניתנת להכרעה אז גם B לא ניתנת להכרעה.

הערה 5.3 (אי-יוניפורמיות). ראינו כי ACC לא ניתנת להכרעה ע"י מ"ט. האם ACC ניתנת להכרעה ע"י משפחת מעגלים?
כן! ראינו שלכל שפה יש משפחת מעגלים שמכריעה אותה.
בפרט מעגלים יכולים לפתור בעיות לא כריעות.

הגדרה 5.9. נגדיר את **בעיית העצירה**

$$\mathrm{HALT} := \{\langle M, x\rangle : \langle M, x\rangle \text{ is an encoding such that } M(x) \text{ halts}\}$$

טענה 5.8. $\mathrm{HALT} \in \mathrm{RE} \setminus \mathrm{R}$.

<u>הוכחה:</u> $\mathrm{HALT} \in \mathrm{RE}$ כי ניתן לבדוק האם מכונה עוצרת על קלט באמצעות המ"ט האוניברסלית.

נראה כי $\mathrm{ACC} \leq \mathrm{HALT}$ ובכך נקבל כי $\mathrm{HALT} \notin \mathrm{R}$ תהי H מ"ט המכריעה את HALT. ויהי נבנה מ"ט A שמכריעה את ACC:

- עבור קלט $\langle M, x\rangle \in \{0,1\}^*$ קידוד חוקי, אם הקלט לא קידוד חוקי אז דחה.
- הרץ את $H(\langle M, x\rangle)$, אם מקבלת אז ענה כמו $U(\langle M, x\rangle)$ (היא תעצור כי H קיבלה).
- אם H דוחה אז דחה.

■

הגדרה 5.10. נגדיר את הבעייה

$$\text{EMPTY} := \{\langle M\rangle : \langle M\rangle \text{ is an encoding such that } L(M)=\emptyset\}$$

טענה 5.9. $\text{EMPTY}\notin \text{R}$.

הוכחה: נראה רדוקציה $\text{ACC}\le\text{EMPTY}$.
לכל מ"ט M וקלט עבורה $x\in\Sigma^*$ נגדיר מ"ט M_x באופן הבא:

- עבור קלט $y\in\Sigma^*$
- הרץ את $M(x)$ וקבל אמ"מ M מקבלת

אז $L(M_x)\neq\emptyset \iff x\in L(M)$.
כעת, בהינתן מכריע E עבור EMPTY, נגדיר מכריע A עבור ACC:

- עבור קידוד חוקי $\langle M,x\rangle$
- הרץ את $E(\langle M_x\rangle)$ וקבל אמ"מ דוחה

■

5.2 רדוקציות ואי-כריעות

הגדרה 5.11.

$$\text{REG}=\{\langle M\rangle : \langle M\rangle \text{ is an encoding of a TM } M \text{ such that } L(M) \text{ is regular}\}$$

טענה 5.10. $\text{REG}\notin\text{R}$.

הוכחה: נראה כי $\text{ACC}\le\text{REG}$.
לכל מ"ט M וקלט $x\in\Sigma^*$ נגדיר מ"ט M_x^{01} באופן הבא:

M_x^{01} בהינתן קלט $y\in\Sigma^*$:

- אם y הוא מהצורה 0^n1^n אז נקבל
- אחרת נריץ את $M(x)$ ונקבל אמ"מ M מקבלת

נשים לב שמתקיים:

1. אם $M(x)$ מקבלת אז $L(M_x^{01})=\Sigma^*$ ובפרט $L(M_x^{01})$ רגולרית.
2. אם $M(x)$ לא מקבלת אז $L(M_x^{01})=\{0^n1^n : n\in\mathbb{N}\}$ ובפרט $L(M_x^{01})$ אינה רגולרית.

כעת, בהינתן מכריע G עבור REG, נגדיר מכריע A עבור ACC עבור קלט $z\in\Sigma^*$:

- אם z לא קידוד חוקי של $\langle M,x\rangle$, כאשר M מ"ט ו-$x\in\Sigma^*$ אז נדחה.
- אחרת, נחשב את הקידוד של M_x^{01}, ונריץ $G(\langle M_x^{01}\rangle)$.

- נקבל אם ורק אם מקבלת.

G מכריעה את REG, ו-$L(M_x^{01})$ רגולרית אם ורק אם $M(x)$ מקבלת, לכן A מכריעה את ACC. ■

הגדרה 5.12.

$$\text{EQ} = \{\langle M_1, M_2\rangle : \langle M_1, M_2\rangle \text{ is an encoding of 2 TM's } M_1, M_2 \text{ such that } L(M_1) = L(M_2)\}$$

טענה 5.11. $\text{EQ} \notin \text{R}$.

__הוכחה:__ נראה כי $\text{EMPTY} \leq \text{EQ}$.

בהינתן A מכריע עבור EQ, ומכונה T שמקבלת את השפה הריקה $T = (Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r)$ כאשר לכל $\sigma \in \Gamma, q \in Q \setminus \{q_a, q_r\}$:

$$\delta(q, \sigma) = (q_r, \sqcup, R)$$

נגדיר מכריע E עבור EMPTY עבור קלט $x \in \Sigma^*$ באופן הבא:

- אם x אינו קידוד חוקי $\langle M\rangle$ של מ"ט אז נדחה
- אחרת, הרץ את $A(\langle M, T\rangle)$ וקבל אמ"מ מקבל

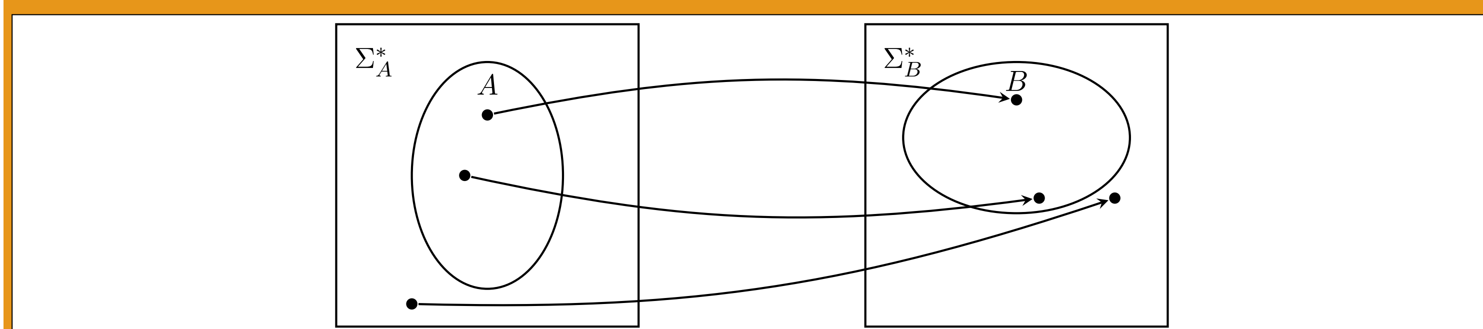
A מכריעה את EQ ו-$\langle M, T\rangle \in \text{EQ}$ אמ"מ $L(M) = \emptyset$ שזה אמ"מ $\langle M\rangle \in \text{EMPTY}$ ולכן E מכריעה את EMPTY. ■

5.2.1 רדוקציות מיפוי

הגדרה 5.13. תהי $M = (Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r)$ מ"ט, תהי $D \subseteq \Sigma^*$ תת קבוצה של Σ^*, ותהי $f : D \to \Gamma^* \setminus \{\sqcup\}$ פונק'.
נאמר כי M **מחשבת את הפונקציה** f אם לכל קלט $x \in D$ מתקיים ש-$M(x)$ עוצרת ובסיום הריצה על הסרט כתוב $f(x)\sqcup^\infty$.
נאמר שפונקציה f היא **חשיבה** אם קיימת מ"ט המחשבת אותה.

הגדרה 5.14. יהיו Σ_A, Σ_B אלפאביתים ויהיו $A \subseteq \Sigma_A^*, B \subseteq \Sigma_B^*$ שפות. **רדוקציית מיפוי** מ-A ל-B היא פונקציה חשיבה $f : \Sigma_A^* \to \Sigma_B^*$ כך שלכל $x \in \Sigma_A^*$ מתקיים:

$$x \in A \iff f(x) \in B$$



סימון 5.3. אם קיימת רדוקציית מיפוי מ-A ל-B נסמן $A \leq_m B$.

טענה 5.12. אם B $A \leq_m B$ ו-$B \in \mathrm{R}$ אז $A \in \mathrm{R}$.

הוכחה: תהי M_B מ"ט המכריעה את B, תהא $f : \Sigma_A^* \to \Sigma_B^*$ רדוקצית מיפוי מ-A ל-B, ותהא M_f מ"ט המחשבת את f.
נגדיר מ"ט M_A המכריעה את A עבור קלט $x \in \Sigma_A^*$:

- נחשב את $f(x)$ באמצעות הרצת $M_f(x)$
- נענה כמו $M_B(f(x))$

M_B מכריעה את B וכן $f(x) \in B \iff x \in A$ ולכן M_A מכריעה את A. ■

הגדרה 5.15.

$$\mathrm{HALT}_\varepsilon = \{\langle M \rangle : \langle M \rangle \text{ is an encoding of a TM where } M(\varepsilon) \text{ halts}\}$$

טענה 5.13. $\mathrm{HALT} \leq_m \mathrm{HALT}_\varepsilon$.

הוכחה: כאשר M_x מוגדרת כמו בהוכחת טענה 5.9, נראה פונק' חשיבה f מתאימה:

- אם w לא קידו חוקי אז נחזיר $z \notin \mathrm{HALT}_\varepsilon$ כלשהו
- אם $w = \langle M, x \rangle$ קידוד חוקי אז נחזיר את הקידוד $\langle M_x \rangle$

f חשיבה. בנוסף, לכל קידוד חוקי $w = \langle M, x \rangle$ מתקיים:
$w \in \mathrm{HALT}$ אמ"מ $M(x)$ עוצרת אמ"מ $M_x(\varepsilon)$ עוצרת אמ"מ $f(w) = \langle M_x \rangle \in \mathrm{HALT}_\varepsilon$.
קידוד לא חוקי איננו ב-HALT וממופה ל-$z \notin \mathrm{HALT}_\varepsilon$. ■

טענה 5.14. אם $A \in \mathrm{R}$ אז לכל $B \in 2^{\Sigma^*} \setminus \{\emptyset, \Sigma^*\}$ מתקיים $A \leq_m B$.

הוכחה: נראה רדוקציה $f : \Sigma_A^* \to \Sigma_B^*$ מ-A ל-B.
B אינה טריוויאלית, אז קיימים $b_0 \notin B, b_1 \in B$ מעל Σ_B.
תהא M_A מ"ט המכריעה את A, נגדיר את f עבור קלט $x \in \Sigma_A^*$:

$$f(x) = b_{M_A(x)}$$

כלומר b_1 אם $M_A(x)$ מקבלת או b_0 אם $M_A(x)$ דוחה.
בבירור f חשיבה, ומשום ש-M_A מכריעה את A אז $f(x) \in B \iff x \in A$.

■

טענה 5.15. אם $A \in \mathrm{R}$ וגם $B \notin \mathrm{R}$ אז $A \leq_m B$ וגם $B \not\leq_m A$.

הוכחה: נניח בשלילה כי $B \leq_m A$, אז מטענה 5.12 מתקיים כי $B \in \mathrm{R}$ וזו סתירה.
אם $B \in \{\emptyset, \Sigma^*\}$ אז היא רגולרית בפרט כריעה, לכן מטענה 5.14 מתקיים $A \leq_m B$. ■

5.2.2 רדוקציות מיפוי ו-RE

טענה 5.16. יהי Σ אלפבית ויהיו $A, B \subseteq \Sigma^*$ שפות כך ש-$B \leq_m A$. אזי:

1. אם $B \in \text{RE}$ אז $A \in \text{RE}$
2. אם $B \in co\text{RE}$ אז $A \in co\text{RE}$

הוכחה: בה"כ נוכיח רק את 1 (אם $B \leq_m A$ אז גם $\overline{B} \leq_m \overline{A}$ ולכן זו למעשה אותה טענה).
תהינא $B \leq_m A$ שפות מעל Σ כך ש-$B \in \text{RE}$, אז קיימת מ"ט M_B שמקבלת את B וקיימת פונקציה חשיבה $f : \Sigma^* \to \Sigma^*$ כך שלכל $x \in \Sigma^*$:

$$x \in A \iff f(x) \in B$$

נגדיר מ"ט M_A שמקבלת את A עבור קלט $x \in \Sigma^*$, שפשוט תריץ את $M_B(f(x))$ ותענה כמוה.
M_B מקבלת את B ו-f רדוקציית מיפוי בין A ל-B ולכן לכל $x \in \Sigma^*$:

$$x \in A \iff f(x) \in B \iff f(x) \in L(M_B) \iff x \in L(M_A)$$

ולכן $A = L(M_A)$. ■

טענה 5.17. $\text{EQ} \notin \text{RE} \cup co\text{RE}$.

5.2.3 משפט רייס

משפט 5.2 יהי $\mathcal{C} \subseteq \text{RE}$ אוסף שפות ב-RE ("תכונה סמנטית") כך ש-$\emptyset \neq \mathcal{C} \neq \text{RE}$ ("לא טריוויאלית"). אזי השפה

$$L_{\mathcal{C}} \coloneqq \{\langle M \rangle : L(M) \in \mathcal{C}\}$$

לא כריעה, כלומר $L_{\mathcal{C}} \notin \text{R}$.
בפרט:

- לכל $\mathcal{C} \subseteq \text{RE}$ לא טריוויאלית כך ש-$\emptyset \notin \mathcal{C}$ מתקיים $L_{\mathcal{C}} \notin co\text{RE}$.
- לכל $\mathcal{C} \subseteq \text{RE}$ לא טריוויאלית כך ש-$\emptyset \in \mathcal{C}$ מתקיים $L_{\mathcal{C}} \notin \text{RE}$.

הוכחת משפט רייס: תהי $\mathcal{C} \subseteq \text{RE}$ תכונה סמנטית לא טריוויאלית. נפריד לשני מקרים:

מקרה א: $\emptyset \notin \mathcal{C}$ נראה $\text{HALT} \leq_m L_{\mathcal{C}}$.
תהי $A \in \mathcal{C}$ ותהי M_A מ"ט המקבלת את A.
לכל מ"ט M וקלט x נגדיר מ"ט $M_x^{\mathcal{C}}$ בהינתן קלט y באופן הבא:

1. מריצה את $M(x)$
2. מריצה את $M_A(y)$ ומקבלת אמ"מ מקבלת

מתקיים:

(א) אם $M(x)$ לא-עוצרת אזי $L\left(M_x^{\mathcal{C}}\right)=\emptyset\notin\mathcal{C}$

(ב) אם $M(x)$ עוצרת אזי $L\left(M_x^{\mathcal{C}}\right)=L(M_A)=A\in\mathcal{C}$

כעת נגדיר רדוקציית מיפוי $f:\Sigma^*\to\Sigma^*$ מ-HALT ל-$L_{\mathcal{C}}$ בהינתן קלט $w\in\Sigma^*$:

- אם w אינו קידוד חוקי של $\langle M,x\rangle$ אז החזר $f(w)=\varepsilon$
- אחרת, אם $w=\langle M,x\rangle$ קידוד חוקי כאשר M מ"ט ו-$x\in\Sigma^*$, נחזיר את הקידוד $f(\langle M,x\rangle)=\left\langle M_x^{\mathcal{C}}\right\rangle$

f חשיבה, ולכל $w\in\Sigma^*$ מתקיים:

$$w\in\mathrm{HALT}\iff f(w)=\langle T\rangle\wedge L(T)\in\mathcal{C}\iff f(w)\in L_{\mathcal{C}}$$

לכן משום ש-$\mathrm{R}\notin\mathrm{HALT}$ לפי טענה $L_{\mathcal{C}}\notin\mathrm{R}$.

<u>מקרה ב:</u> $\emptyset\in\mathcal{C}$ במקרה זה נראה ש-$L_{\mathcal{C}}\notin\mathrm{RE}$ נשים לב שהתכונה $\overline{\mathcal{C}}=\mathrm{RE}\setminus\mathcal{C}$ גם אינה טריוויאלית ומתקיים $\emptyset\notin\overline{\mathcal{C}}$.
לכן, על פי מקרה t מתקיים $L_{\overline{\mathcal{C}}}\notin co\mathrm{RE}$ או לחילופין $\overline{L_{\overline{\mathcal{C}}}}\notin\mathrm{RE}$.
אם נסמן ב-INVALID את שפת כל המחרוזות שאינן קידוד חוקי של מ"ט אז מתקיים:

$$\overline{L_{\overline{\mathcal{C}}}}=\left\{\langle M\rangle:\ L(M)\notin\overline{\mathcal{C}}\right\}\cup\mathrm{INVAIID}=L_{\mathcal{C}}\cup\mathrm{INVALID}$$

ומכיוון ש-$\mathrm{INVALID}\in\mathrm{R}$ נובע שגם $L_{\mathcal{C}}\notin\mathrm{RE}$. ■

הגדרה 5.16. יהי Σ אלפבית.

$$\mathrm{ALL}=\left\{\langle M\rangle:\ L(M)=\Sigma^*\right\}$$

טענה 5.18. $\mathrm{ALL}\notin\mathrm{RE}\cup co\mathrm{RE}$.

<u>הוכחה:</u> השפה ALL מוגדרת לפי תכונה סמנטית לא טריוויאלית $\mathcal{C}$ כך ש-$\emptyset\notin\mathcal{C}$, ולכן $\mathrm{ALL}\notin co\mathrm{RE}$.

<u>הוכחה ש-$\mathrm{ALL}\notin\mathrm{RE}$:</u> נראה ש-$\overline{\mathrm{HALT}}\leq_m\mathrm{ALL}$, ולכן מכיוון שאנחנו כבר יודעים ש-$\overline{\mathrm{HALT}}\notin\mathrm{RE}$, אז מטענה נקבל $\mathrm{ALL}\notin\mathrm{RE}$.
לכל מ"ט M וקלט x נגדיר מ"ט $B_{M,x}$ באופן הבא עבור קלט $y\in\Sigma^*$:

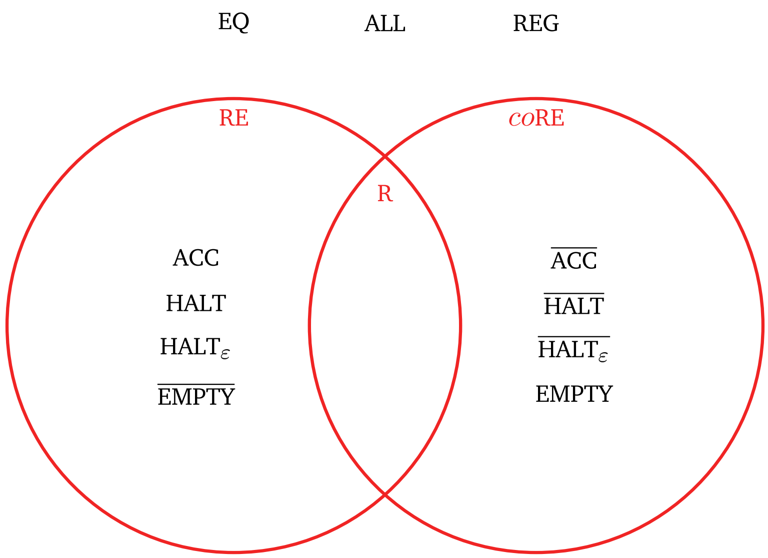
- נריץ את $M(x)$ במשך $|y|$ צעדים ונקבל אמ"מ M לא עצרה.
  מתקיים:
  - אם $M(x)$ לא עוצרת, אז $L(B_{M,x})=\Sigma^*$
  - אם $M(x)$ עוצרת לאחר k צעדים אז $L(B_{M,x})=\{y\in\Sigma^*:\ |y|<k\}$

כעת נגדיר רדוקציית מיפוי $f:\Sigma^*\to\Sigma^*$ מ-$\overline{\mathrm{HALT}}$ ל-ALL עבור קלט $w\in\Sigma^*$ באופן הבא:

- אם w לא קידוד חוקי של מ"ט+קלט אז נחזיר $z\in\mathrm{ALL}$ כלשהו
- אם $w=\langle M,x\rangle$ קידוד חוקי אז נחזיר את הקידוד $\langle B_{M,x}\rangle$

הפונקציה f חשיבה ולכל w מתקיים $w\notin\mathrm{HALT}$ אמ"מ $f(w)\in\mathrm{ALL}$. ■

סיכום ביניים - ציור של תמונת העולם שלנו:



חלק III

סיבוכיות

פרק 6

היררכיית זמן

הגדרה 6.1. תהי $T:\mathbb{N}\to\mathbb{N}$ ותהי M מ"ט דטרמיניסטית. נאמר כי M רצה בזמן $T(n)$ אם לכל $n\in\mathbb{N}$ ולכל קלט $x\in\Sigma^n$ מתקיים ש-$M(x)$ מבצעת לכל היותר $T(n)$ מעברי δ בטרם עוצרת.

הגדרה 6.2. לכל פונקציה $T:\mathbb{N}\to\mathbb{N}$ נסמן:

$$\text{DTime}(T(n))=\{L(M):\ M \text{ is a one tape deterministic TM running in } T(n)\}$$

משפט 6.1. אם $L\in\text{DTime}(o(n\log n))$ אז L רגולרית.

הגדרה 6.3. פונקציה $T:\mathbb{N}\to\mathbb{N}$ היא **פונקצה חשיבה בזמן** אם קיימת מ"ט שבהינתן 1^n מחשבת את הקידוד הבינארי של $T(n)$ בזמן $O(T(n))$.

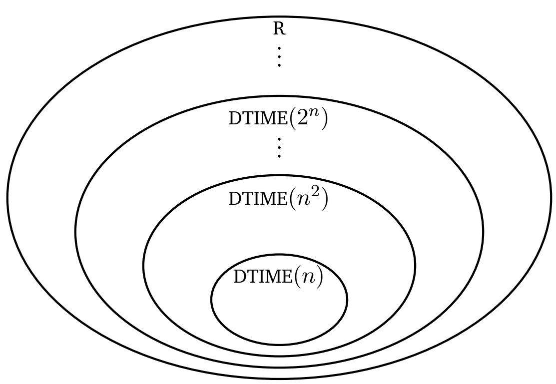
משפט 6.2 (משפט היררכית הזמן). תהיינה $T,t:\mathbb{N}\to\mathbb{N}$. אם T חשיבה בזמן וגם $t(n)=o\left(\frac{T(n)}{\log T(n)}\right)$ אזי:

$$\text{DTime}(t(n))\subsetneq\text{DTime}(T(n))$$

מסקנה 6.1. לכל $1\le c<d$ מתקיים:

$$\text{DTime}(n^c)\subsetneq\text{DTime}\left(n^d\right)$$

בציור:



משפט 6.3 קיימת מ"ט חד-סרטית אוניברסלית U כך שלכל מ"ט חד-סרטית M וקלט $x \in \Sigma^*$, אם $M(x)$ עוצרת תוך t צעדים אז $U(\langle M, x\rangle)$ עוצרת תוך לכל היותר $c_M \cdot t$ צעדים, כאשר c_M תלוי בקידוד $\langle M\rangle$ בלבד.

משפט 6.4 קיימת מ"ט חד-סרטית U_{timer} כך שבהינתן קלטים $t \geq 0$ בייצוג בינארי וקידוד $\langle M, x\rangle$ מתקיים:

- אם $M(x)$ מקבלת תוך t צעדים אז $U_{\text{timer}}(t, \langle M, x\rangle)$ מקבלת
- אם $M(x)$ דוחה או לא עוצרת תוך t צעדים אז $U_{\text{timer}}(t, \langle M, x\rangle)$ דוחה

בנוסף, $U_{\text{timer}}(t, \langle M, x\rangle)$ עוצרת תוך $c_M \cdot t \log t$ צעדים, כאשר c_M תלוי בקידוד $\langle M\rangle$ בלבד.

מסקנה 6.2 עבור קלטים $t \geq 0$ בייצוג בינארי וקידוד $\langle M, x\rangle$, כאשר מפעילים את $U_{\text{timer}}(t, \langle U, \langle M, x\rangle\rangle)$:

- אם $M(x)$ מקבלת תוך $\frac{t}{c_M}$ צעדים אז $U(\langle M, x\rangle)$ מקבלת תוך t צעדים ואז U_{timer} מקבלת
- אם $M(x)$ דוחה או לא עוצרת תוך $\frac{t}{c_M}$ צעדים אז $U(\langle M, x\rangle)$ דוחה או לא עוצרת תוך t צעדים ואז U_{timer} דוחה.

בנוסף, U_{timer} עוצרת תוך $c_U \cdot t \log t = O(t \log t)$ צעדים לכל היותר.

__**הוכחת משפט היררכיית הזמן:**__ תהינה $T, t : \mathbb{N} \to \mathbb{N}$ כך ש-T חשיבה בזמן ו-$t(n) = o\left(\frac{T(n)}{\log(T(n))}\right)$, נגדיר מ"ט בשם Flip אשר בהינתן קלט $w \in \Sigma^n$:

1. נחשב את $\bar{t}(n) = \frac{T(n)}{\log(T(n))}$.
2. אם $w = \left\langle M, 0^k\right\rangle$ עבור מ"ט M ו-$k \in \mathbb{N}$ אז נמשיך, אחרת נדחה.
3. נריץ את $U_{\text{timer}}\left(\bar{t}(n), \left\langle U, \left\langle M, 0^k\right\rangle\right\rangle\right)$ ונקבל אמ"מ U_{timer} דוחה.

טענה 6.1 $L(\text{Flip}) \in \text{DTime}(T(n))$.

הוכחת טענה 6.1:

1. צעד 1 דורש $O(T(n))$ זמן כי T חשיבה בזמן.
2. צעד 2 דורש $O(n)$ זמן.
3. צעד 3 דורש $O(T(n)) = O\left(\bar{t}(n) \cdot \log\left(\bar{t}(n)\right)\right)$ לפי מסקנה 6.2.

טענה 6.2 $L(\text{Flip}) \notin \text{DTime}(t(n))$.

הוכחת טענה 6.2: תהא מ"ט A הרצה בזמן $O(t(n))$, ויהי $k \in \mathbb{N}$.
נתבונן בקלט $w = \left\langle A, 0^k\right\rangle$. זהו קלט באורך $n = |w| = w = \Theta(|\langle A\rangle| + k)$.
נראה כי עבור k גדול מספיק מתקיים (6.1):

$$w = \left\langle A, 0^k\right\rangle \notin L(\text{Flip}) \iff w = \left\langle A, 0^k\right\rangle \in L(A) \tag{6.1}$$

ולכן בפרט $L(A) \neq L(\text{Flip})$, ולכן $\text{Flip} \notin \text{Dtime}(t(n))$.
לשם כך נראה כי עבור k גדול מספיק מתקיים ש-$U\left(\left\langle A, 0^k\right\rangle\right)$ עוצרת תוך $\bar{t}(n)$ צעדים, כי אז:

- אם $\left\langle A, 0^k\right\rangle \in L(A)$ אז בצעד 3 של Flip נקבל ש-U_{timer} עוצרת ואומרת "כן" ולכן Flip אומרת "לא" ולכן $\left\langle A, 0^k\right\rangle \notin L(\text{Flip})$.

- אם $\langle A, 0^k \rangle \notin L(A)$ אז בצעד 3 של Flip נקבל ש-U_{timer} עוצרת ואומרת "לא" ולכן Flip אומרת "כן" ולכן $\langle A, 0^k \rangle \in L(\text{Flip})$.

$U(\langle A, 0^k \rangle)$ עוצרת תוך $O(\bar{t}(n))$ צעדים כי $A(0^k)$ עוצרת תוך $O(t(n))$ צעדים. ■

6.1 תלות זמן הריצה במודל החישוב

משפט 6.5 יהי $T : \mathbb{N} \to \mathbb{N}$. אז לכל מ"ט רב-סרטית M הרצה בזמן $T(n) \geq n$ קיימת מ"ט חד-סרטית M' המסמלצת אותה ורצה בזמן $O(T^2(n))$.

הגדרה 6.4 תהי $t : \mathbb{N} \to \mathbb{N}$ פונקציה ותהי N מטל"ד חד-סרטית. N רצה בזמן $t(n)$ אם לכל $n \in \mathbb{N}$ ולכל $x \in \Sigma^n$, עץ הקונפיגורציות $T_{N,x}$ הוא בעומק $t(n)$ לכל היותר.

הגדרה 6.5 תהי $t : \mathbb{N} \to \mathbb{N}$. נסמן:

$$\text{NTime}(t(n)) \coloneqq \{ L(M) : M \text{ is a one tape NTM that runs in } O(t(n)) \}$$

טענה 6.3. לכל $t : \mathbb{N} \to \mathbb{N}$ מתקיים:

$$\text{NTime}(t(n)) \subseteq \text{DTime}\left(2^{O(t(n))}\right)$$

פרק 7

המחלקות P ו-NP

הגדרה 7.1.

$$\mathrm{P} := \bigcup_{c\in\mathbb{N}} \mathrm{DTime}(n^c)$$

הגדרה 7.2.

$$\mathrm{STCON} = \{\langle G,s,t\rangle : G \text{ is a directed graph where there is a path between s and } t \text{ in } G\}$$

טענה 7.1. $\mathrm{STCON} \in \mathrm{P}$.

הגדרה 7.3.

$$\mathrm{PRIME} = \{p \in \mathbb{N} : p \text{ is prime}\}$$

טענה 7.2. $\mathrm{PRIME} \in \mathrm{P}$.

הגדרה 7.4.

$$\mathrm{NP} := \bigcup_{c\in\mathbb{N}} \mathrm{NTime}(n^c)$$

טענה 7.3. $\mathrm{P} \subseteq \mathrm{NP}$.

הגדרה 7.5. מסלול המילטוני בגרף מכוון G הוא מסלול שמבקר **בכל** צומת **בדיוק** פעם אחת.

הגדרה 7.6.

$$\mathrm{HAMPATH} = \{\langle G,s,t\rangle : G \text{ is a directed graph with an hamiltonian path from } s \text{ to } t\}$$

טענה 7.4. $\mathrm{HAMPATH} \in \mathrm{NP}$.

7.1 NP ווידאו פולינומי

הגדרה 7.7. תהי V מ"ט עם א"ב קלט $\Sigma \cup \{,\}$ ותהי $L \subseteq \Sigma^*$. נאמר ש-V הוא **מוודא פולינומי** עבור L אם:

- **נכונות:**
  - **שלמות:** לכל $x \in L$ קיים $w \in \Sigma^*$ כך ש-$V(x,w)$ מקבל.
  - **נאותות:** לכל $x \notin L$ ולכל $w \in \Sigma^*$ מתקיים ש-$V(x,w)$ דוחה.
- **יעילות:** קיים פולינום $p(n)$ כך שלכל $x,w \in \Sigma^*$ זמן הריצה של $V(x,w)$ הוא לכל היותר $p(|x|)$.

טענה 7.5. $L \in \mathrm{NP}$ אמ"מ קיים ל-L מוודא פולינומי.

__הוכחת הטענה:__

כיוון ראשון: נניח כי $L \in \mathrm{NP}$, אז קיימת מטל"ד N שמכריעה את L בזמן פולינומי, ויהי $p(n)$ פולינום החוסם את זמן הריצה של N. בה"כ נניח כי לכל $x \in \Sigma^*$, עץ החישוב $T_{N,x}$ הוא עץ $|\Sigma|$-י מלא, בעומק $p(|x|)$, כלומר כל קונפיגורציה שאינה מקבלת/דוחה/לא עוצרת δ-עוברת ל-$|\Sigma|$ קונפיגורציות, והמכונה עובדת בדיוק בזמן $p(n)$. בדומה להוכחת טענה 4.3, נניח את אותו סדר לקסיקוגרפי בעץ החישוב.

נגדיר מוודא פולינומי V עבור L באופן הבא:

- לכל $x \in \Sigma^*$, $w \in \Sigma^*$, אם $|w| \neq p(|x|)$ נדחה ($p(n)$ חשיבה בזמן כפולינום).
- אחרת, נסמלץ את $N(x)$ על ענף החישוב שמתואר על ידי $w = w_1 \cdots w_{p(n)}$ ונענה כמוה, כאשר בקונפיגורציה ה-c_i בחישוב, נעבור לקונפיגורציה שהיא הבן ה-w_i שלה בעץ $T_{N,x}$.

שלמות: אם $x \in L$ אז קיים עלה מקבל ב-$T_{N,x}$ ולכן קיים $w \in \Sigma^{p(|x|)}$ כך ש-$V(x,w)$ מקבל.

נאותות: אם $x \notin L$ אז לא קיים עלה מקבל ב-$T_{N,x}$ ולכן לכל $w \in \Sigma^{p(|x|)}$ $V(x,w)$ דוחה.

זמן הריצה של V פולינומי כי הוא רץ בזמן $p(|x|) = |w|$. לכן V מוודא פולינומי עבור L.

כיוון שני: נניח כי קיים מוודא פולינומי V עבור L זרץ בזמן $p(n)$, נגדיר מטל"ד N שמכריעה את L בזמן $p(n)$.

- לכל $x \in \Sigma^*$, ננחש $w \in \Sigma^{p(|x|)}$, ונסמלץ את $V(x,w)$.

הסימלוץ נעשה בזמן $p(|x|)$ ב-$|\Sigma|^{p(|x|)}$ ענפי חישוב במקביל.
משום ש-V רצה בזמן $p(n)$ אז לכל $x \in L$ קיים $w \in \Sigma^{p(|x|)}$ כך ש-$V(x,w)$ מקבל. ולכן יש ב-$T_{N,x}$ עלה מקבל.
אם $x \notin L$ אז לכל $w \in \Sigma^*$ $V(x,w)$ דוחה ולכן ב-$T_{N,x}$ אין עלה מקבל.
קיבלנו כי $x \in L(N)$ אמ"מ $x \in L$ ולכן $L \in \mathrm{NP}$. ■

7.1.1 דוגמאות לבעיות ב-NP

הגדרה 7.8. יהי $G = (V,E)$ גרף לא מכוון. קבוצה $C \subseteq V$ היא **קליקה** ב-G אם לכל $u \neq v \in C$ מתקיים $\{u,v\} \in E$.

הגדרה 7.9.

$$\text{CLIQUE} = \{\langle G, k\rangle : G \text{ is an undirected graph with a clique of size } k\}$$

טענה 7.6. $\text{CLIQUE} \in \text{NP}$.

רעיון ההוכחה: העד ל-$\text{CLIQUE} \in \langle G,k\rangle$ הוא קידוד של קליקה C בגודל k ב-G. ■

הגדרה 7.10. יהי $G=(V,E)$ גרף לא מכוון. קבוצה $I \subseteq V$ היא **בלתי תלויה** ב-G אם לכל $u,v \in I$ מתקיים $\{u,v\} \notin E$.

הגדרה 7.11.

$$\text{IS} = \{\langle G, k\rangle : G \text{ is an undirected graph with an independent set of size } k\}$$

טענה 7.7. $\text{IS} \in \text{NP}$.

רעיון ההוכחה: העד ל-$\text{IS} \in \langle G,k\rangle$ הוא קידוד של קבוצה בלתי תלויה I בגודל k ב-G. ■

הגדרה 7.12.

$$\text{FACTOR} = \{\langle N, k\rangle : \exists 1 < d \leq k.\ d | N\}$$

טענה 7.8. $\text{FACTOR} \in \text{NP}$.

רעיון ההוכחה: העד ל-$\text{FACTOR} \in \langle N,k\rangle$ הוא $1 < d \leq k$ שמחלק את N. ■

7.2 NP-hardness

הגדרה 7.13. נאמר שרדוקציית מיפוי f היא **פולינומית** אם היא חשיבה בזמן פולינומי.

סימון 7.1. אם יש רדוקציית מיפוי פולינומית מ-A ל-B אז נסמן $A \leq_p B$.

הגדרה 7.14. יהי $G=(V,E)$ גרף לא מכוון. **הגרף המשלים** של G הוא הגרף $\overline{G} = \left(V, \overline{E}\right)$ כאשר

$$\overline{E} = \{\{u,v\} : u,v \in V \wedge \{u,v\} \notin E\}$$

טענה 7.9. $\text{IS} \leq_p \text{CLIQUE}$.

הוכחת הטענה: נתאר רדוקציית מיפוי פולינומית מ-IS ל-CLIQUE:

$f(x)$:

- אם x לא קידוד חוקי $x = \langle G,k\rangle$ אז נחזיר $f(x) = x$.
- אם $x = \langle G=(V,E),k\rangle$ קידוד חוקי אז נחזיר $\left\langle \overline{G} = \left(V,\overline{E}\right), k\right\rangle$.

נכונות הרדוקציה נכונה משום שיש ב-G קבוצה בלתי תלויה בגודל k אמ"מ יש ב-$\overline{G}$ קליקה בגודל k. הרדוקציה בבירור חשיבה ופולינומית. ■

טענה 7.10. אם $A \leq_p B$ אז:

1. אם $B \in \mathrm{P}$ אז $A \in \mathrm{P}$.
2. אם $B \in \mathrm{NP}$ אז $A \in \mathrm{NP}$.

הגדרה 7.15. תהא $L \subseteq \Sigma^*$.

1. L היא **NP-קשה** אם לכל $L' \in \mathrm{NP}$ מתקיים $L' \leq_p L$. נסמן $L \in \mathrm{NPH}$.
2. L היא **NP-שלמה** אם היא NP-קשה וגם $L \in \mathrm{NP}$. נסמן $L \in \mathrm{NPC}$.

מסקנה 7.1 (מטענה 7.10). אם $\mathrm{NPC} \cap \mathrm{P} \neq \emptyset$ אז $\mathrm{P} = \mathrm{NP}$.

7.2.1 שפה ראשונה ב-NPC

הגדרה 7.16.

$$\mathrm{ACC}_{\mathrm{NP}} = \left\{ \left\langle M, x, 1^t \right\rangle : M \text{ is TM} \wedge \exists w \in \Sigma^*.\ M(x,w) \text{ accepts in } t \text{ time} \right\}$$

טענה 7.11. $\mathrm{ACC}_{\mathrm{NP}} \in \mathrm{NPC}$.

<u>הוכחה:</u> $\mathbf{ACC_{NP} \in NPH}$:

תהי $L \in \mathrm{NP}$, ויהי V_L מוודא פולינומי עבור L עם זמן ריצה $p(n)$.

נגדיר

$$f(x) = \left\langle V_L, x, 1^{p(|x|)} \right\rangle$$

f חשיבה בזמן פולינומי כי V_L ניתנת לקידוד לתוך בטן המכונה שמחשבת את f, $\left\langle x, 1^{p(|x|)} \right\rangle$ פולינומי ב-$|x|$.

מתקיים כי $x \in L$ אמ"מ קיים $w \in \Sigma^*$ כך ש-$V_L(x,w)$ מקבלת ב-t זמן. לכן

$$x \in L \iff f(x) = \left\langle V_L, x, 1^{p(|x|)} \right\rangle \in \mathrm{ACC}_{\mathrm{NP}}$$

$\mathbf{ACC_{NP} \in NP}$:

נגדיר מוודא V של $\mathrm{ACC}_{\mathrm{NP}}$:

- עבור קלט $w \in \Sigma^*, z \in \Sigma^*$, $V(z,w)$ מקבל אמ"מ קיימת מ"ט M, $x \in \Sigma^*$ ו-$t \in \mathbb{N}$ כך ש-$z = \left\langle M, x, 1^t \right\rangle$ ו-$M(x,w)$ מקבלת תוך t צעדים.

■

טענה 7.12. אם $A \leq_p B$ ו-$A \in \mathrm{NPH}$ אז $B \in \mathrm{NPH}$.

7.2.2 השפה SAT

הגדרה 7.17. פסוק CNF מעל משתנים $x_1, \ldots, x_n$ מוגדר באופן הבא:

- **ליטרל** = משתנה או שלילתו
- **פסוקית** = $\vee$ בין ליטרלים

- **פסוק CNF** = $\wedge$ בין פסוקיות

הגדרה 7.18. פסוק CNF הוא **ספיק** אם קיימת השמה בוליאנית למשתניו כך שערך הנוסחה הוא 1.

הגדרה 7.19.

$$\text{SAT} = \left\{ \langle \phi \rangle : \phi \text{ is a satisfiable CNF formula} \right\}$$

הגדרה 7.20. **נוסחת kCNF** היא נוסחת CNF בה בכל פסוקית יש k ליטרלים.

הגדרה 7.21.

$$\text{kSAT} = \left\{ \langle \phi \rangle : \phi \text{ is a kCNF satisfiable formula} \right\}$$

טענה 7.13. $\text{SAT} \leq_p \text{3SAT}$.

הוכחה: נראה רדוקציה המקבלת פסוק CNF ϕ ומחזירה פסוק 3CNF ψ.

תיאור פורמלי של הרדוקציה:

בהינתן פסוק

$$\phi = c_1 \wedge c_2 \wedge \cdots \wedge c_m$$

כאשר

$$c_i = \ell_{i,1} \vee \ell_{i,2} \vee \cdots \vee \ell_{i,n_i}$$

נבנה פסוק

$$\psi = \bigwedge_i \psi_i$$

כאשר כל ψ_i הוא פסוק 3CNF המוגדר לפי:

$$\psi_i = (\ell_{i,1} \vee \ell_{i,2} \vee t_{i,1}) \wedge \left(\bar{t}_{i,1} \vee \ell_{i,3} \vee t_{i,2}\right) \wedge \left(\bar{t}_{i,2} \vee \ell_{i,4} \vee t_{i,3}\right) \wedge \cdots \wedge \left(\bar{t}_{i,n_i-3} \vee \ell_{i,n_i-1} \vee \ell_{i,n_i}\right)$$

כאשר $t_{i,1}, t_{i,2}, \ldots, t_{i,n_i-3}$ הם משתנים חדשים המופיעים רק ב-ψ_i.

ניתן לבנות את ψ בזמן פולינומי בבירור.

נכונות: כיוון 1: נניח $\phi \in \text{SAT}$ כלומר קיימת הצבה המספקת את ϕ ובפרט מספקת כל פסוקית c_i של ϕ.

נרחיב את ההצבה הזאת להצבה שתספק כל ψ_i ולכן תספק את $\psi = \bigwedge_i \psi_i$.

מכיוון שכל משתנה חדש מופיע ב-ψ_i יחיד, אז אפשר לטפל בכל ψ_i בנפרד.

ההצבה מספקת את c_i כלומר מספקת לפחות ליטרל אחד $\ell_{i,j}$ ב-c_i.

נגדיר הצבה מורחבת באופן הבא:

- $t_{i,s} = T$ לכל $s \in [j-2]$
- $t_{i,s} = F$ לכל $s \in [n_i-2] \setminus [j-2]$

ההצבה הזאת מספקת את $\left(\bar{t}_{i,j-2} \vee \ell_{i,j} \vee t_{i,j-1}\right)$ כי $\ell_{i,j}$ מסתפק. כל הפסוקיות עם אינדקס קטן יותר מסתפקות כי $t_{i,s}$ מסתפק.
כל הפסוקיות עם אינדקס גדול יותר מסתפקות כי $\bar{t}_{i,s}$ מסתפק.

לכן $f(\phi) = \psi \in \text{3SAT}$.

כיוון 2: נניח $f(\phi)=\psi\in 3\text{SAT}$ כלומר קיימת הצבה למשתני ψ המספקת ψ.
מספיק להראות שהיא מספקת כל c_i ולכן מספקת את $\phi=\bigwedge_i c_i$:

- אם $t_{i,1}=F$ אזי $\ell_{i,1}\vee\ell_{i,2}=T$. כלומר ההצבה מספקת את c_i
- אם $t_{i,n_i-3}=T$ אזי $\ell_{i,n_i-1}\vee\ell_{i,n_i}=T$ ושוב ההצבה מספקת את c_i
- אחרת $t_{i,1}=T$ וגם $t_{i,n_i-3}=F$. לכן קיים אינדקס j כך ש-$t_{i,j}=T$ וגם $t_{i,j+1}=F$.
- נסתכל על הפסוקית (שמסתפקת):

$$\left(\bar{t}_{i,j}\vee\ell_{i,j+2}\vee t_{i,j+1}\right)$$

  לכן $\ell_{i,j+2}=T$ ושוב הפסוקית c_i מסתפקת.
- כלומר בשלושת המקרים c_i מסתפקת ולכן כל ϕ מסתפק ולכן $\phi\in 3\text{SAT}$.

■

7.2.3 SAT היא NP-קשה

משפט 7.1 (קוק-לוין). $\text{SAT}\in\text{NPC}$.

הוכחה: תהי שפה $A\in\text{NP}$, נראה כי $A\leq_p\text{SAT}$.
יהי $V=(Q,\Sigma,\Gamma,\delta,q_0,q_a,q_r)$ מוודא פולינומי של A החסום על ידי פולינום $p(n)$.
יהיו x,w קלטים עבור V. נסמן $t=p(|x|)+1$. נייצג חישוב של V על (x,w) ע"י הטבלה:

	$j=0$	$j=1$									$j=t$
$i=0$	#	q_0	x_1	x_2	$\cdots$	x_n	,	w_1	w_2	$\cdots$	w_ℓ
$i=1$	#	c_1									
$i=2$	#	c_2									
$\vdots$		$\vdots$									
$i=t$	#	c_t									

- השורה הראשונה בטבלה הזאת היא הקונפיגורציה ההתחלתית c_0 של V על x,w.
- השורה השניה היא הקונפ' c_1 ש-V עוברת אליה בצעד מ-c_0 וכן הלאה.
- לכל הקונפיגורציות שלנו אנחנו מוסיפים # בצד שמאל.

הנחה מפשטת: נניח בה"כ כי המטריצה שמתקבלת מהטבלה היא **ריבועית** בגודל $(t+1)\times(t+1)$.

הגדרה 7.22.

$$\Delta=\Gamma\cup Q\cup\{\#\}$$

נשים לב כי הגודל Δ לא תלוי בגודל הקלט $n=|x|$. כלומר $|\Delta|=O(1)$.
משתנים:
לכל $0\leq i,j\leq t$ יהיו משתנים שיקודדו את תוכן התו ה-(i,j) בטבלה.

כיוון שישנם $|\Delta|$ משתנים אפשריים, לכל i,j ולכל $\sigma \in \Delta$ נגדיר משתנה $z_{i,j,\sigma}$.
כלומר הגדרנו $O\left(t^2 \cdot |\Delta|\right) = O\left(t^2\right)$ משתנים.
הפסוק שנבנה $f(x) = \varphi_x$ יכיל 4 חלקים:

1. φ_{cell} - בכל מקום בטבלה רשום **בדיוק** תו אחד.
2. φ_{init} - הקונפ' הראשונה היא קונפ' התחלתית של V על x,w עבור w **כלשהו**.
3. φ_{accept} - החישוב מסתיים במצב מקבל, כלומר בקונפ' האחרונה המצב הוא q_a.
4. φ_{move} - החישוב מתאר סדרה של קונפ' $c_0, c_1, \ldots, c_t$ כך ש-V עוברת כדל צעד מ-c_i ל-c_{i+1}.

הגדרה 7.23 (תיאור φ_{cell})**.** נגדיר:

$$\varphi_{\text{cell}} = \bigwedge_{0 \le i,j \le t} \varphi_{\text{cell},i,j}$$

$$\varphi_{\text{cell},i,j} = \left(\bigvee_{\sigma \in \Delta} z_{i,j,\sigma}\right) \wedge \left(\bigwedge_{\substack{\sigma_1,\sigma_2 \in \Delta \\ \sigma_1 \neq \sigma_2}} \left(\overline{z_{i,j,\sigma_1}} \vee \overline{z_{i,j,\sigma_2}}\right)\right)$$

כאשר לכל $0 \le i,j \le t$ ו-$\sigma \in \Delta$ מתקיים כי $z_{i,j,\sigma} = T$ אמ"מ σ רשום בתא ה-(i,j).
זהו פסוק CNF בגודל

$$O\left(t \cdot t \cdot |\Delta|^2\right) = O\left(t^2\right)$$

טענה 7.14. הצבה מספקת את φ_{cell} אמ"מ היא מתאימה לטבלה בה בכל מקום רשום בדיוק תו אחד.

הגדרה 7.24 (תיאור φ_{init})**.** נגדיר:

$$\varphi_{\text{init}} = \underbrace{\left(z_{0,0,\#}\right) \wedge \left(z_{0,1,q_1}\right) \wedge \left(\bigwedge_{i=1}^{n} \left(z_{0,i+1,x_i}\right)\right) \wedge \left(z_{0,n+2,','}\right)}_{\text{clauses of size } 1} \wedge \underbrace{\bigwedge_{i=1}^{\ell} \left(\bigvee_{\sigma \in \Sigma} z_{0,n+1+\ell,\sigma}\right)}_{\text{clauses of size } |\Sigma| = O(1)}$$

זהו פסוק CNF בגודל $O(t)$.

טענה 7.15. הצבה מספקת את $\varphi_{\text{cell}} \wedge \varphi_{\text{init}}$ אמ"מ היא מתאימה לטבלה בה בכל מקום רשום בדיוק תו אחד והשורה הראשונה מתאימה לקונפ' ההתחלתית של V על x ועל $w \in \Sigma^\ell$ כלשהו.

הגדרה 7.25 (תיאור φ_{accept})**.** נגדיר:

$$\varphi_{\text{accepts}} = \left(\bigvee_{1 \le j \le t} z_{t,j,q_a}\right)$$

φ_{accept} היא **פסוקית** בגודל $O(t)$.

טענה 7.16. הצבה מספקת את $\varphi_{\text{cell}} \wedge \varphi_{\text{accept}}$ אמ"מ היא מתאימה לטבלה בה בכל מקום רשום בדיוק תו אחד ובשורה האחרונה מופיע המצב q_a.

הגדרה 7.26 חמישיית תווים $(\sigma_1,\sigma_2,\sigma_3,\sigma_4,\sigma_5)$ היא **חמישייה חוקית** אם כאשר במקומות $(i,j-1),(i,j),(i,j+1),(i,j+2)$ רשומים $\sigma_1,\sigma_2,\sigma_3,\sigma_4$ בהתאמה, אז במקום $(i+1,j)$ צריכים לרשום σ_5.

הגדרה 7.27 (תיאור φ_{move}). נגדיר:

$$\varphi_{\text{move}} = \bigwedge_{0\le i\le t} \varphi_{\text{move},i}$$

כאשר $\varphi_{\text{move},i}$ יקודד את הדרישה: אם ההצבה לשורה i מתאימה לקונפ' c_i אז ההצבה לשורה $i+1$ מתאימה לקונפ' c_{i+1} כך ש-V עוברת אליה בצעד אחד מ-c_i.
נתחיל מלכתוב את φ_{move} בצורה לא תקינה (לא ב-CNF):

$$\varphi_{\text{move},i} = \bigwedge_{0\le j\le t} \varphi_{\text{move},i,j}$$
$$\varphi_{\text{move},i,j} = \bigwedge_{\substack{(\sigma_1,\sigma_2,\sigma_3,\sigma_4,\sigma_5)\\ \text{legal}\quad 5-\text{tuple}}} \left(\left(z_{i,j-1,\sigma_1}\wedge z_{i,j,\sigma_2}\wedge z_{i,j+1,\sigma_3}\wedge z_{i,j+2,\sigma_4}\right)\to z_{i+1,j,\sigma_5}\right)$$

נתרגם את הגרירה עם השקילות הלוגית המוכרת:

$$x\to y \iff \overline{x}\vee y$$

ולכן נקבל:

$$\varphi_{\text{move},i,j} = \bigwedge_{\substack{(\sigma_1,\sigma_2,\sigma_3,\sigma_4,\sigma_5)\\ \text{legal}\quad 5-\text{tuple}}} \left(\overline{z_{i,j-1,\sigma_1}}\vee \overline{z_{i,j,\sigma_2}}\vee \overline{z_{i,j+1,\sigma_3}}\vee \overline{z_{i,j+2,\sigma_4}}\vee z_{i+1,j,\sigma_5}\right)$$

הגודל של φ_{move} הוא:

$$|\varphi_{\text{move}}| = t^2\cdot|\varphi_{\text{move},i,j}| = t^2\cdot O\left(\Delta^4\right) = t^2\cdot O(1) = O\left(t^2\right)$$

טענה 7.17 תהי y הצבה למשתני φ_x המתאימה לקונפ' c_i. ההצבה הזאת מספקת את $\varphi_{\text{cell}}\wedge\varphi_{\text{move},i}$ אמ"מ היא מתאימה לקונפ' c_{i+1} ש-V עוברת אליה בצעד אחד מ-c_i.

מסקנה 7.2 הצבה מספקת את $\varphi_{\text{cell}}\wedge\varphi_{\text{init}}\wedge\varphi_{\text{accept}}\wedge\varphi_{\text{move}}$ אמ"מ היא מקיימת את 4 הדרישות:

1. היא מתאימה לטבלה בה בכל מקום רשום בדיוק תו אחד.
2. השורה הראשונה מתאימה לקונפ' ההתחלתית של V על x ועל $w\in\Sigma^\ell$ כלשהו.
3. בשורה האחרונה מופיע המצב q_a.
4. לכל $i\in[t-1]$, השורה ה-$i+1$ מתאימה לקונפ' c_{i+1} ש-V עוברת אליה בצעד אחד מ-c_i.

טענה 7.18 הצבה מספקת את φ_x אמ"מ ההצבה מתאימה לחישוב **מקבל** של V על x ועל איזשהו w, מה שאפשרי אמ"מ $x\in A$.
אורך הפסוק הוא פולינומי $|\varphi_x| = O\left(t^2\right)$, והתיאור של φ_x מראה איך לבנות אותו בזמן פולינומי. ■

מסקנה 7.3 $3SAT\in NPC$.

7.3 דוגמאות לשפות NP-שלמות

7.3.1 השפות CLIQUE, IS

טענה 7.19. $3SAT \leq_p IS$.

מסקנה 7.4. $IS, CLIQUE \in NPC$.

הוכחת טענה 7.19: תיאור הרדוקציה מ-3SAT ל-IS:

קלט: φ=פסוק 3CNF. נניח כי $\varphi = \bigwedge_{i=1}^{m} c_i$ כאשר $c_i = (\ell_{i,1} \vee \ell_{i,2} \vee \ell_{i,3})$.

נבנה גרף $G = (V, E)$ עם $3m$ צמתים:

$$V = \{\, v_{i,j} : i \in [m], j \in [3] \,\}$$

וקשתות $E = E_1 \cup E_2$ כאשר:

$$E_1 = \bigcup_{(k,j)\in\{(1,2),(1,3),(2,3)\}} \{\, \{v_{i,k}, v_{i,j}\} : i \in [m] \,\} \qquad \text{קשתות משולשים}$$

$$E_2 = \{\, \{v_{i_1,j_1}, v_{i_2,j_2}\} : \exists k \in [m] \times [3].\ \ell_{i_1,j_1} = x_k \wedge \ell_{i_2,j_2} = \overline{x_k} \,\} \qquad \text{קשתות עקביות}$$

ופלט הרדוקציה יהיה $f(\langle\varphi\rangle) = \langle G, m\rangle$.

נכונות הרדוקציה:

$\varphi \in 3SAT$: קיימת השמה מספקת ל-φ, כלומר קיימת השמה עבור בכל פסוקית c_i קיים לפחות ליטרל אחד ℓ_{i,j_i} שמסתפק.

נגדיר קבוצה:

$$I = \{\, v_{i,j_i} : i \in [m] \,\}$$

זאת קבוצה בגודל m. נראה כי היא ב"ת:

- בחרנו צומת אחד מכל משולש ולכן ואין קשתות משולש בין 2 צמתים בקבוצה.
- מכיוון שכל ליטרל ℓ_{i,j_i} מסתפק לא ייתכן ש-$\ell_{i,j_i} = x_k$ וגם $\ell_{i',j_{i'}} = \overline{x_k}$ ולכן אין בין הצמתים קשתות עקביות.

כלומר I היא קבוצה ב"ת בגודל m ב-G ולכן $f(\varphi) = (G, m) \in IS$.

$f(\varphi) \in (G, m) \in IS$: קיימת קבוצה ב"ת I בגודל m ב-G. I מכילה לכל היותר צומת אחד מכל משולש ולכן מכילה **בדיוק** צומת אחד מכל משולש (מכיוון שיש m משולשים).

נגדיר הצבה ל-φ שתספק אותה:

- לכל $v_{i,j} \in I$:
  - אם $\ell_{i,j} = x_k$ אז נגדיר $x_k = T$.
  - אם $\ell_{i,j} = \overline{x_k}$ אז נגדיר $x_k = F$.
- אם x_k לא קיבל ערך אזי בצורה שרירותית נגדיר $x_k = T$.

ההצבה הזאת מוגדרת הייטב, כלומר לא ייתכן שהצבנו $x_k = T$ וגם $x_k = F$, כי אחרת הייתה קשת בין שני הצמתים שגרמו להצבות האלה בסתירה לכך ש-I קבוצה ב"ת.

ההצבה הנ"ל מספקת כל פסוקית: לכל $i \in [m]$ קיים $j \in [3]$ כך ש- $v_{i,j} \in I$, כלומר הליטרל $\ell_{i,j}$ מופיע ב-c_i ומסתפק בהצבה.

כלומר ההצבה מספקת כל פסוקית c_i ולכן מספקת את $\varphi = \bigwedge_{i=1}^{m} c_i$ ולכן $\varphi \in 3SAT$. ■

7.3.2 השפה Subset Sum (SUSU)

הגדרה 7.28. נגדיר:

$$\text{SubsetSum}=\left\{(A,t):\ A\underset{\text{multiset}}{\subseteq}\mathbb{N},t\in\mathbb{N}\wedge\exists B\subseteq A.\ \sum_{a\in B}a=t\right\}$$

טענה 7.20. $3\text{SAT}\le_p \text{SubsetSum}$.

מסקנה 7.5. $\text{SubsetSum}\in\text{NPC}$.

הוכחת טענה 7.20. נראה רדוקציה f אשר בהינתן קלט φ שהוא פסוק 3CNF מחזירה קלט עבור SUSU כלומר מחזירה מולטיסט A ומספר t.

נניח כי ל-φ יש n משתנים $x_1,\dots,x_n$ ויש m פסוקיות $c_1,\dots,c_m$.

נבנה מולטיסט A המכילה $2n+2m$ מספרים בבסיס עשרוני (כ"א עם $n+m$ ספרות) באופן הבא:

- לכל ליטרל $z\in\{x_i,\overline{x_i}\}$ נגדיר מספר u_z כך שכל הספרות הם 0 פרט ל:
  - הספרה ה-i היא 1
  - לכל פסוקית c_j אשר הליטרל z מופיע בה, הספרה ה-$(n+j)$ היא 1
- לכל פסוקית c_j נגדיר v_j כך שהספרה ה-$(n+j)$ היא 1 ושאר הספרות 0
- נגדיר $A=\bigcup_{i=1}^{m}\{u_{x_i},\overline{u_{x_i}},v_i,v_i\}$ (זהו מולטיסט, יש חשיבות לחזרות)

נגדיר t כך ש-n הספרות הראשונות הן 1 ו-m הספרות האחרונות הן 3

פלט הרדוקציה: $f(\varphi)=(A,t)$

הוכחת נכונות:

כיוון ראשון:

נניח ש-φ ספיק, ותהא $x_1,\dots,x_n$ השמה המספקת אותו. נבנה ממנה תת קבוצה B שתפתור את SUSU:

- לכל ליטרל z, נוסיף את u_z ל-B אמ"מ z מסתפק.
- לכל פסוקית c_j, נסמן ב-$1\le s_j\le 3$ את מספר הליטרלים שמסתפקים ב-c_j. זהו מספר בין 1 ל-3 כי יש לפחות ליטרל אחד מסופק (כי ההשמה מספקת) ויש לכל היותר 3 כי יש 3 ליטרלים בפסוקית.
- נוסיף $2\ge 3-s_j\ge 0$ עותקים של v_j ל-B.

מהבנייה נובע ש-$t=\sum_{a\in B}a$.

כיוון שני:

נניח כי קיימת $A\subseteq B$ שסכומה הוא $t=1^n3^m$. נגדיר השמה המספקת את φ באופן הבא: לכל $i\in[n]$ נגדיר $x_i=T$ אמ"מ $u_{x_i}\in B$.

מדוע זאת השמה מספקת?

- לכל $i\in[n]$, מכיוון שהספרה ה-i בסכום של B היא 1, בדיוק אחד מהשניים נכון: או $u_{x_i}\in B$ או $u_{\overline{x_i}}\in B$. לכן, ההשמה שהגדרנו מקיימת:
  - אם $u_{x_i}\in B$ אז $x_i=T$

- אם $u_{\overline{x_i}} \in B$ אז $u_{x_i} \notin B$ ולכן $x_i = F$

- במילים אחרות, אם $u_z \in B$ אז הליטרל z מסתפק בהשמה שהגדרנו
- לכל $i \in [m]$ המספר v_i מופיע לכל היותר פעמיים ב-B ותורם לכל היותר 2 לסכום העמודה. לכן קיים $u_z \in B$ המקיים $u_z[n+i] = 1$. כלומר ליטרל z השייך לפסוקית c_i ומסתפק בהשמה שלנו.
- כלומר ההשמה שהגדרנו מספקת כל c_i ולכן מספקת את φ.

■

הערה 7.1. הראינו ש-SUSU היא NP-קשה כאשר המספרים מקודדים בבסיס עשרוני. זה נשאר נכון גם כאשר המספרים מקודדים בבינארי. אבל אם המספרים מקודדים באונרי אז זה כבר לא נכון ואפשר לפתור את הבעיה בזמן פולינומי.

7.3.3 השפה HAMPATH

טענה 7.21. $3SAT \le_p HAMPATH$.

מסקנה 7.6. $HAMPATH \in NPC$.

<u>הוכחת טענה 7.21.</u>

<u>הוכחת הטענה:</u>

נתאר רדוקציה f עם התכונות הבאות:

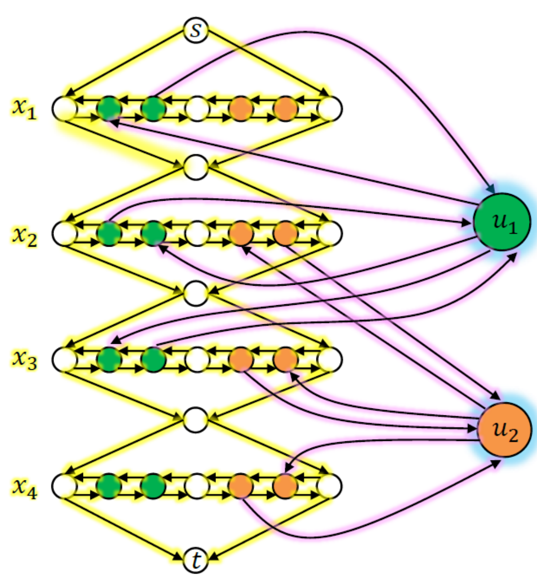
<u>קלט:</u> $\varphi =$ נוסחת 3CNF עם משתנים $x_1, \dots, x_n$ ופסוקיות $c_1, \dots, c_m$

<u>פלט:</u> $(G, s, t) =$ גרף מכוון וזוג קודקודים המוגדרים באופן הבא:

1. לכל פסוקית c_j נוסיף לגרף G צומת u_j
2. לכל משתנה x_i נוסיף לגרף G "יהלום" שניתן לעבור אותו מימין לשמאל או משמאל לימין. בשכבה האמצעית יהיו $3m+1$ צמתים, זוג לכל פסוקית עם צומת רווח בין הזוגות.
3. כל היהלומים האלה מחוברים בשרשרת בין s ל t.
4. לכל ליטרל $z \in \{x_i, \overline{x_i}\}$ ולכל פסוקית c_j שמכילה את z נוסיף "גישה" מהיהלום של x_i לצומת u_j.
<u>אם</u> $z = x_i$ הגישה היא בנתיב מימין לשמאל ואם $z = \overline{x_i}$ אז הגישה היא בנתיב משמאל לימין

דוגמה:

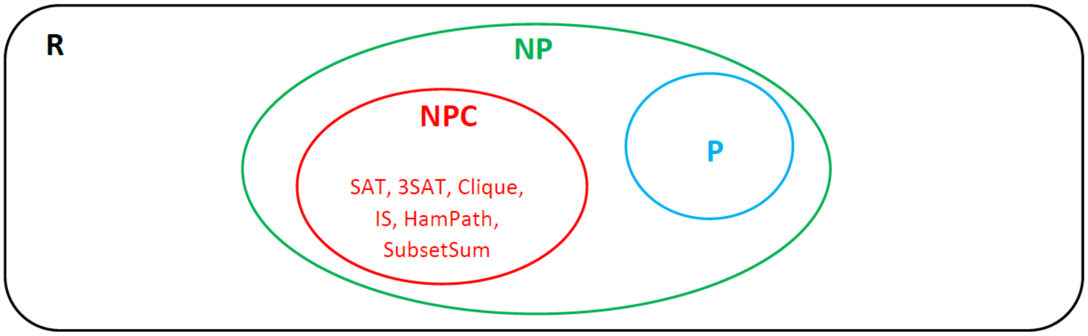
$$\varphi = (x_1 \vee \overline{x_2} \vee x_3) \wedge (x_2 \vee \overline{x_3} \vee \overline{x_4})$$



■

7.4 מה יש בין NP ל-R?

ציור חלקי של תמונת העולם שלנו:



7.4.1 המחלקה coNP

הגדרה 7.29. נגדיר

$$co\text{NP} := \left\{ \overline{L} : \ L \in \text{NP} \right\}$$

טענה 7.22. לכל זוג שפות A, B כך ש-$A \leq_p B$ מתקיים:

1. אם $B \in \text{NP}$ אז $A \in \text{NP}$
2. אם $B \in co\text{NP}$ אז $A \in co\text{NP}$

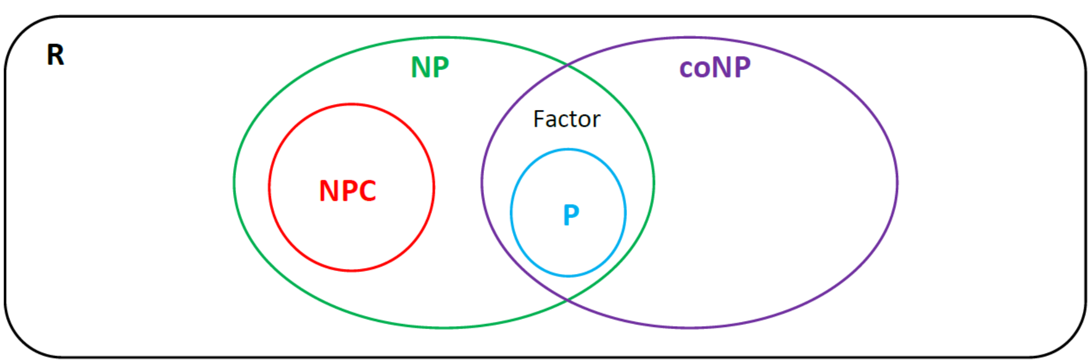
מסקנה 7.7. תהי $L \in \text{NPC}$. מתקיים:

$$L \in co\text{NP} \iff \text{NP} = co\text{NP}$$

טענה 7.23. $\text{FACTOR} \in \text{NP} \cap co\text{NP}$.

<u>רעיון ההוכחה:</u> בין אם $\langle N, k\rangle \in \text{FACTOR}$ או לא, הפירוק של N לגורמים ראשוניים הוא עד לכך. ■

תמונת עולם מעודכנת:



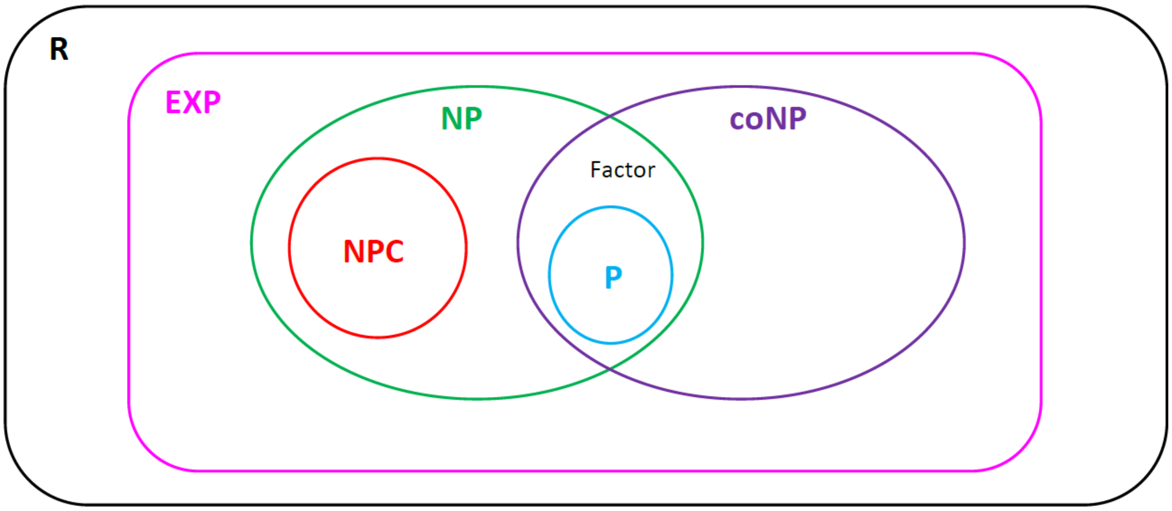
7.4.2 המחלקה EXP

הגדרה 7.30.

$$\text{EXP} := \bigcup_{c\in\mathbb{N}} \text{DTime}\left(2^{n^c}\right)$$

מסקנה 7.8. $\text{NP} \cup co\text{NP} \subseteq \text{EXP}$.

תמונת עולם מעודכנת:



מה אנחנו יודעים בוודאות לגבי התמונה הזאת?

1. $\text{P} \subseteq \text{NP} \cap co\text{NP}$
2. $\text{FACTOR} \in \text{NP} \cap co\text{NP}$
3. $\text{P} \subsetneq \text{EXP} \subsetneq \text{R}$
4. $\text{NP} \cup co\text{NP} \subseteq \text{EXP}$

כל השאר אנחנו לא יודעים בוודאות, אלא רק מאמינים. למשל:

1. $\text{P} \neq co\text{NP}, \quad \text{P} \neq \text{NP}$
2. $\text{NPC} \cap co\text{NP} = \emptyset, \quad \text{NP} \neq co\text{NP}$
3. $\text{NP} \cup co\text{NP} \subsetneq \text{EXP}$

פרק 8

חישוב אקראי

8.1 המודל הפורמלי ומחלקות סיבוכיות

הגדרה 8.1. מ"ט אקראית עם זמן ריצה $t(n)$ היא מ"ט דו-סרטית עם:

- סרט עבודה שמכיל בתחילת הריצה את הקלט x
- סרט אקראיות שמכיל בתחילת הריצה מחרוזת $r \in \{0,1\}^{t(|x|)}$

סימון 8.1.

- נסמן ב-$M(x;r)$ ריצה של מ"ט אקראית M עם קלט x ואקראיות r
- לעיתים נתייחס ל-$M(x;r)$ כאינדיקטור: 1 אם $M(x;r)$ מקבלת ו-0 אם דוחה
- נסמן ב-$M(x)$ את המשתנה המקרי $M(x;r)$ כאשר r מחרוזת אקראית באורך $t(|x|)$

הגדרה 8.2 (randomized polynomial time)**.** תהי $\alpha : \mathbb{N} \to [0,1]$. שפה L שייכת למחלקה $\mathrm{RP}(\alpha(n))$ אם קיימת מ"ט אקראית M שרצה בזמן פולינומי $t(n)$ כך שלכל n גדול מספיק ולכל קלט x באורך n מתקיים:

- אם $x \in L$ אז
$$\mathbb{P}(M(x) = 1) \geq \alpha(n)$$
- אם $x \notin L$ אז
$$\mathbb{P}(M(x) = 1) = 0$$

הערה 8.1 (אבחנות). יהיו $\alpha, \beta : \mathbb{N} \to [0,1]$. אזי:

1. אם $\alpha(n) \leq \beta(n)$ לכל n אזי $\mathrm{RP}(\beta(n)) \subseteq \mathrm{RP}(\alpha(n))$.
2. מתקיים $\mathrm{P} = \mathrm{RP}(1) \subseteq \mathrm{RP}(\alpha(n))$.
3. אם $\alpha : \mathbb{N} \to (0,1]$ מתקיים $\mathrm{RP}(\alpha(n)) \subseteq \mathrm{NP}$.

הגדרה 8.3. תהא $\alpha : \mathbb{N} \to [0,1]$. נגדיר

$$co\mathrm{RP}(\alpha(n)) := \left\{ \overline{L} : \ L \in \mathrm{RP}(\alpha(n)) \right\}$$

טענה 8.1. תהא $\alpha : \mathbb{N} \to [0,1]$. $L \in co\text{RP}(\alpha(n))$ אם ורק אם קיימת מ"ט אקראית M שרצה בזמן פולינומי $t(n)$ כך שלכל n גדול מספיק ולכל קלט x באורך n מתקיים:

- אם $x \in L$ אז
$$\mathbb{P}(M(x)=1)=1$$
- אם $x \notin L$ אז
$$\mathbb{P}(M(x)=1) \leq 1-\alpha(n)$$

8.1.1 דוגמה: כפל מטריצות

הגדרה 8.4. נגדיר את בעיית **כפל המטריצות**

$$\text{MATMULT} = \left\{ (A,B,C) \in \left(\mathbb{Z}^{n\times n}\right)^3 : \ A \cdot B = C \right\}$$

- בעזרת אלגוריתם נאיבי לכפל מטריצות ניתן להכריע את MATMULT בזמן $O\left(n^3\right)$
- האלג' הטוב ביותר לכפל מטריצות כיום רץ בזמן $O\left(n^{2.371552}\right)$

טענה 8.2. $\text{MATMULT} \in co\text{RP}\left(1-2^{-100}\right)$.

טענה 8.3. לכל $0 \neq D \in \mathbb{Z}^{n\times n}$ מתקיים $\Pr_{r \leftarrow \{0,1\}^n}[D \cdot r \neq 0] \geq 0.5$.

__הוכחת טענה 8.3:__ תהי $0 \neq D \in \mathbb{Z}^{n\times n}$, ונניח בה"כ כי $D_{1,1} \neq 0$.
נספור עבור כמה וקטורים $r \in \{0,1\}^n$ ייתכן כי $D \cdot r = 0$.
נקבע את $r_2, r_3, \ldots, r_n$. מתקיים:

$$(D \cdot r)_1 = \sum_{i=1}^{n} D_{i,1} \cdot r_i = D_{1,1} \cdot r_1 + \sum_{i=2}^{n} D_{i,1} \cdot r_i$$

אם $D \cdot r = 0$ אז בפרט הקואו' הראשונה בתוצאה שווה אפס ולכן

$$D_{1,1} \cdot r_1 + b = 0$$

כלומר

$$r_1 = -\frac{b}{D_{1,1}}$$

לכל היותר אחת מהאפשרויות $r_1 \in \{0,1\}$ תקיים את השוויון.
לכל בחירה של $r_2, r_3, \ldots, r_n$ קיימת לכל היותר בחירה אחת של r_1 כך ש-$D \cdot r = 0$.
לכן יש לכל היותר 2^{n-1} וקטורים r כך ש-$D \cdot r = 0$.
לכן,

$$\Pr_{r \leftarrow \{0,1\}^n}[D \cdot r \neq 0] = 1 - \frac{|\{r : \ D \cdot r = 0\}|}{|\{0,1\}^n|} \geq \frac{2^n - 2^{n-1}}{2^n} = \frac{1}{2}$$

■

הוכחת טענה 8.2: נתאר אלגוריתם אקראי למכונה M שרץ בזמן $O\left(n^2\right)$.

M בהינתן קלט (A,B,C):

- נחזור על הבדיקה הבאה 100 פעמים:
  - נגריל וקטור אקראי $r \in \{0,1\}^n$
  - נחשב את $x_r = A \cdot B \cdot r$ ואת $y_r = C \cdot r$
  - אם $x_r \neq y_r$ אז נדחה
- נקבל

זמן ריצה $O\left(n^2\right)$ (הכפלת מטריצה בוקטור)

נכונות:

- אם $A \cdot B = C$ אז לכל r מתקיים $x_r = y_r$ ולכן M תמיד יקבל.
- אם $A \cdot B \neq C$ אז M דוחה בהסתברות $\Pr_{r \leftarrow \{0,1\}^n}[x_r \neq y_r] = \Pr_{r \leftarrow \{0,1\}^n}[(A \cdot B - C) \cdot r \neq 0]$.
  - $A \cdot B - C \neq 0$ ולכן לפי טענה 8.3 מתקיים כי $\Pr_{r \leftarrow \{0,1\}^n}[x_r \neq y_r] \geq 0.5$.
  - לכן ההסתברות ש-M תקבל 100 פעמים מקיימת:

$$\mathbb{P}(M(A,B,C)=1) = \left(\Pr_{r \leftarrow \{0,1\}^n}[x_r = y_r]\right)^{100} \leq 2^{-100}$$

לכן המכונה עונה להגדרת $co\mathrm{RP}\left(1-2^{-100}\right)$. ■

8.1.2 דוגמה: זהות פולינומים

הגדרה 8.5. פולינום ב-n משתנים הוא סכום של מונומים, כאשר כל מונום הוא מהצורה:

$$a \cdot x_1^{e_1} \cdot x_2^{e_2} \cdots x_n^{e_n}$$

- כאשר $e_i \geq 0$ שלם עבור כל $i \in [n]$.
- דרגת המונום היא $\sum_{i \in [n]} e_i$
- דרגת הפולינום: מקסימום דרגת המונומים בפולינום.

הגדרה 8.6. נוסחה אריתמטית (AF) היא נוסחה (מעגל עם fan-out=1) עם שערי $+, \cdot, 0, 1$. כלומר אנחנו מרשים שערי כפל, חיבור ושערים קבועים $0,1$.

הגדרה 8.7. נגדיר את בעיית **זהות הפולינומים**

$$\mathrm{PIT} = \left\{\phi : \phi \text{ is an AF } \wedge \phi \equiv 0\right\}$$

משפט 8.1 (מאלגברה). יהי $0 \neq p \in \mathbb{R}_d[x]$, אז מספר השורשים של p הוא לכל היותר d.

למה 8.1 (שוורץ-זיפל). יהי $0 \neq p \in \mathbb{R}_d[x_1, \dots, x_n]$ ויהי $m \in \mathbb{N}$. תהי $S \subseteq \mathbb{R}$ בגודל $|S| = m$. אז מספר השורשים של p בקבוצה S^n הוא לכל היותר $d \cdot m^{n-1}$.

מסקנה 8.1. יהי $0 \neq p \in \mathbb{R}_d[x_1, \dots, x_n]$ ויהי $m \in \mathbb{N}$. תהי $S \subseteq \mathbb{R}$ בגודל $|S| = m$. אזי:

$$\Pr_{x \leftarrow S^n}[p(x) = 0] \leq \frac{d \cdot m^{n-1}}{m^n} = \frac{d}{m}$$

טענה 8.4. $\mathrm{PIT} \in co\mathrm{RP}(0.99)$.

הוכחה: נתאר אלגוריתם אקראי למכונה M שרץ בזמן פולינומי.

- בהינתן ϕ נבחר $S \subseteq \mathbb{R}$ כך ש-$|S| > 100 \cdot \deg(\phi)$.
- נגריל $x \leftarrow S^n$ ונקבל אמ"מ $\phi(x) = 0$.

אם $\phi \equiv 0$ אז נקבל תמיד.
אם $\phi \not\equiv 0$ אז נקבל בהסתברות לכל היותר

$$\frac{\deg(\phi)}{|S|} = \frac{\deg(\phi)}{100 \cdot \deg(\phi)} = \frac{1}{100}$$

■

8.1.3 צמצום שגיאה חד-צדדית

טענה 8.5. לכל $d, c \in \mathbb{N}$ מתקיים

$$\mathrm{RP}\left(n^{-c}\right) = \mathrm{RP}\left(1 - 2^{-n^d}\right)$$

הוכחה: הכיוון $\mathrm{RP}(n^{-c}) \supseteq \mathrm{RP}\left(1 - 2^{-n^d}\right)$ ברור.
בכיוון השני, תהי $L \in \mathrm{RP}(n^{-c})$ ותהי M מ"ט אקראית שרצה בזמן פולינומי $t(n)$ אשר מקבלת $x \in L$ בהסתברות לפחות n^{-c} ודוחה $x \notin L$ בהסתברות 1.
נגדיר מ"ט אקראית M' שרצה בזמן $O\left(t(n) \cdot n^{c+d}\right)$:
M' בהינתן קלט $x \in \Sigma^n$:

- מריצה $\ell = n^{c+d}$ פעמים את $M(x)$ ובכל הרצה משתמשת באקראיות חדשה.
- מקבלת אמ"מ לפחות אחת מהריצות קיבלה.

ניתוח:

- אם $x \notin L$ אז $M(x)$ תמיד דוחה ולכן גם $M'(x)$ תמיד דוחה.
- אם $x \in L$ אז $M'(x)$ דוחה אם ורק אם **כל** הריצות של $M(x)$ דחו. הריצות בת"ס ולכן זה קורה בהסתברות לכל היותר

$$\left(1 - n^{-c}\right)^{\ell} \leq \left(e^{-n^{-c}}\right)^{\ell} = e^{-\ell n^{-c}} = e^{-n^d} \leq 2^{-n^d}$$

■

סימון 8.2. $\mathrm{RP} = \mathrm{RP}\left(\frac{1}{2}\right), co\mathrm{RP} = co\mathrm{RP}\left(\frac{1}{2}\right)$.

8.2 שגיאה דו-צדדית

הגדרה 8.8 (bounded-error probabilitistic polynomial time). יהיו $\alpha, \beta : \mathbb{N} \to [0,1]$. שפה L שייכת למחלקה $\text{BPP}(\alpha(n), \beta(n))$ אם קיימת מ"ט אקראית M שרצה בזמן פולינומי $t(n)$ כך שלכל n מספיק גדול ולכל $x \in \Sigma^n$ מתקיים:

- אם $x \in L$ אז
$$\mathbb{P}(M(x) = 1) \geq \beta(n)$$
- אם $x \notin L$ אז
$$\mathbb{P}(M(x) = 1) \leq \alpha(n)$$

סימון 8.3. $\text{BPP} = \text{BPP}\left(\frac{1}{4}, \frac{3}{4}\right)$.

טענה 8.6. לכל $\alpha : \mathbb{N} \to [0,1]$ מתקיים:

$$\text{RP}(\alpha(n)) = \text{BPP}(0, \alpha(n)) \qquad co\text{RP}(\alpha(n)) = \text{BPP}(1-\alpha(n), 1),$$

8.2.1 צמצום שגיאה דו-צדדית

טענה 8.7. לכל $c, d \in \mathbb{N}$ ו-$\alpha : \mathbb{N} \to [0,1]$ חשיבה בזמן פולינומי כך ש-$n^{-c} \leq \alpha(n) \leq 1 - n^{-c}$ מתקיים:

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

<u>**הוכחה של מקרה פרטי:**</u> לשם פשטות נראה כי $\text{BPP} \subseteq \text{BPP}\left(2^{-0.2d}, 1 - 2^{-0.2d}\right)$.

נריץ את M (המ"ט עם השגיאה הדו-צדדית רבע) ℓ פעמים על הקלט x ונענה על פי החלטת הרוב.

נסמן ב-p את ההתסברות ש-M טועה על x (בריצה אחת). אנחנו יודעים כי $p \leq \frac{1}{4}$. נקבל:

$$\mathbb{P}(\text{majority decision is wrong}) = \sum_{t=\frac{\ell+1}{2}}^{\ell} \mathbb{P}(M \text{ is wrong } t \text{ times}) = \sum_{t=\frac{\ell+1}{2}}^{\ell} \binom{\ell}{t} p^t (1-p)^{\ell - t} \leq \sum_{t=\frac{\ell+1}{2}}^{\ell} \binom{\ell}{t} p^{\frac{\ell+1}{2}} (1-p)^{\ell - \frac{\ell+1}{2}}$$
$$= p^{\frac{\ell+1}{2}} (1-p)^{\frac{\ell-1}{2}} \sum_{t=\frac{\ell+1}{2}}^{\ell} \binom{\ell}{t} \leq p^{\frac{\ell+1}{2}} (1-p)^{\frac{\ell-1}{2}} 2^\ell = p(p(1-p))^{\frac{\ell-1}{2}} \cdot 2^\ell$$

נתבונן בפונקציה $p(1-p)$:

היא מונטונית עולה בתחום ואנחנו יודעים ש-$0 \leq p \leq \frac{1}{4}$ ולכן המקסימום של שלה מתקבל עבור $p = \frac{1}{4}$. כלומר

$$p(1-p) \leq \frac{1}{4} \cdot \frac{3}{4} = \frac{3}{16}$$

לכן:

$$\mathbb{P}(\text{majority decision is wrong}) \leq \frac{1}{4} \cdot \left(\frac{3}{16}\right)^{\frac{\ell-1}{2}} 2^\ell = \frac{1}{\sqrt{3}} \cdot 2^{-2-2\ell+2+\ell} \cdot 3^{\frac{\ell}{2}} \leq \left(\frac{3}{4}\right)^{\frac{\ell}{2}} \leq 2^{-0.2\ell}$$

■

פרק 9

סיבוכיות מקום

9.1 סיבוכיות מקום דטרמיניסטית

הגדרה 9.1. תהי $S:\mathbb{N}\to\mathbb{N}$ ו-M מ"ט עם 3 סרטים: סרט קלט לקריאה בלבד, סרט עבודה, וסרט פלט לכתיבה חד פעמית. M **רצה במקום** $S(n)$ אם לכל $n\in\mathbb{N}$ ולכל קלט x באורך n, מתקיים ש-M משתמשת בלכל היותר $S(n)$ תאים בסרט העבודה בטרם עוצרת (בפרט תמיד עוצרת).

הגדרה 9.2. תהי $S:\mathbb{N}\to\mathbb{N}$.

$$\text{DSpace}(S(n)) \coloneqq \{\, L(M) :\ M \ \text{ is turing machine running in } O(S(n)) \text{ space}\,\}$$

הגדרה 9.3 (מחלקות מקום דטרמיניסטיות)**.** נגדיר:

$$\text{PSPACE} \coloneqq \bigcup_{c\in\mathbb{N}} \text{DSpace}(n^c)$$
$$\text{L} = \text{LOGSPACE} \coloneqq \text{DSpace}(\log(n))$$

טענה 9.1. אם $\mathcal{L}\in\text{DSpace}(o(\log(n)))$ אזי $\mathcal{L}$ רגולרית.

9.1.1 סיבוכיות מקום לעומת זמן

טענה 9.2. תהי $S(n)\le\log(n)$. אזי $\text{DSpace}(S(n))\subseteq\text{DTime}\left(2^{O(S(n))}\right)$.

מסקנה 9.1.

- $\text{L}\subseteq\text{P}$
- $\text{PSPACE}\subseteq\text{EXP}$

<u>הוכחת טענה 9.2:</u> תהי $M=(Q,\Sigma,\Gamma,\delta,q_0,q_a,q_r)$ מ"ט הרצה במקום $S(n)$ ומכריעה שפה $A\subseteq\Sigma^*$.
בהינתן קלט $x\in\Sigma^n$, נחסום את מספר הקונפיגורציות $c(n)$ אליהן $M(x)$ יכולה להגיע:

$$c(n)\le \underbrace{n}_{\text{ראש קלט}}\cdot\underbrace{|\Gamma|^{S(n)}}_{\text{תוכן סרט עבודה}}\cdot\underbrace{S(n)}_{\text{ראש עבודה}}\cdot\underbrace{|Q|}_{\text{מצב}}\le 2^{O(S(n))}$$

מכיוון ש-M תמיד עוצרת, מבצעת לכל היותר $c(n)$ צעדים. ■

הגדרה 9.4. פונקציה $S:\mathbb{N}\to\mathbb{N}$ היא **חשיבה במקום** (space-constructible) אם קיימת מ"ט שבהינתן 1^n מחשבת את הקידוד הבינארי של $S(n)$ במקום $O(S(n))$.

משפט 9.1 (משפט היררכיית המקום)**.** תהי $S(n)\geq\log(n)$ חשיבה במקום. אזי

$$\mathrm{DSpace}(o(S(n)))\subsetneq\mathrm{DSpace}(S(n))$$

מסקנה 9.2. $\mathrm{L}\subsetneq\mathrm{PSPACE}$. לכן מכיוון ש-$\mathrm{L}\subseteq\mathrm{P}\subseteq\mathrm{PSPACE}$, אז **לפחות** אחד מהתנאים הבאים נכון:

1. $\mathrm{L}\subsetneq\mathrm{P}$
2. $\mathrm{P}\subsetneq\mathrm{PSPACE}$

9.1.2 קשיות מקום

הגדרה 9.5. יהיו Σ_A,Σ_B א"ב ויהיו $A\subseteq\Sigma_A^*,B\subseteq\Sigma_B^*$ שפות. **רדוקצית מיפוי במקום לוגריתמי** מ-A ל-B היא פונקציה $f:\Sigma_A^*\to\Sigma_B^*$ חשיבה במקום לוגריתמי כך שלכל $x\in\Sigma_A^*$ מתקיים

$$x\in A\iff f(x)\in B$$

סימון 9.1. $A\leq_L B$.

טענה 9.3. אם $A\leq_L B$ וגם $B\in\mathrm{L}$ אז $A\in\mathrm{L}$.

הוכחה: תהי M_B מ"ט המכירעה את B במקום לוגריתמי. תהי f רדוקצית מיפוי במקום לוגריתמי מ-A ל-B. תהי M_f המ"ט המחשבת את f במקום לוגריתמי.

נגדיר מ"ט M_f':

קלט: x ואינדקס i

פלט: הביט ה-i ב-$f(x)$

M_f' מריצה את M_f ללא כתיבת הפלט. בכל שלב ש-M_f כותבת ביט, M_f' מגדילה מונה ℓ.

כאשר $\ell=i$ היא מחזירה את הביט. אם M_f עצרה לפני שהגענו לביט ה-i בפלט אז M_f' מחזירה $\sqcup$.

תיאור M_A על קלט x (זאת המ"ט המכירעה את A בזיכרון לוגריתמי):

- נריץ את M_B על $y=f(x)$ מבלי להחזיק את y בזיכרון באופן מפורש.
- בכל שלב נזכור את מיקום הראש של M_B בסרט הקלט שלה (בעזרת מונה i) ונחשב עבורה את ערך הביט שאמור להיות שם
  - בכל שלב ש-M_B מזיזה את הראש נשנה את i בהתאם ונריץ את M_f' על x ועל i (החדש) ונקבל y_i

זיכרון M_A:

- סרטי העבודה של M_B: $\log|y|$
  $\mathrm{P}\supseteq L$ ולכן M_B רצה בזמן פולינומי ולכן $|y|\leq n^c$ ולכן $\log|y|=O(\log|x|)$
- סרטי העבודה של M_f' (שהם סרטי העבודה של M_f): $\log|x|$
- המצביע $i\in[|y|]$ ולכן דורש $\log|y|$ ביטים

סה"כ $O(\log|x|)$ מקום. ■

טענה 9.4. אם $A \leq_L B$ וגם $B \leq_L C$ אז $A \leq_L C$.

הגדרה 9.6. תהא $A_0 \subseteq \Sigma^*$.

- A_0 היא ***P*-קשה** (תחת רדוקציות מקום לוגריתמי) אם לכל $A \in \mathrm{P}$ מתקיים $A \leq_L A_0$
- A_0 היא **P-שלמה** אם היא P-קשה ובנוסף $A_0 \in \mathrm{P}$

מסקנה 9.3. אם A_0 היא P-שלמה, אזי:

$$A_0 \in \mathrm{L} \iff \mathrm{P} = \mathrm{L}$$

הגדרה 9.7.

$$\mathrm{CVAL} = \{\langle c, x\rangle : c \text{ is a boolean circuit such that } c(x) = 1\}$$

טענה 9.5. CVAL היא P-שלמה.

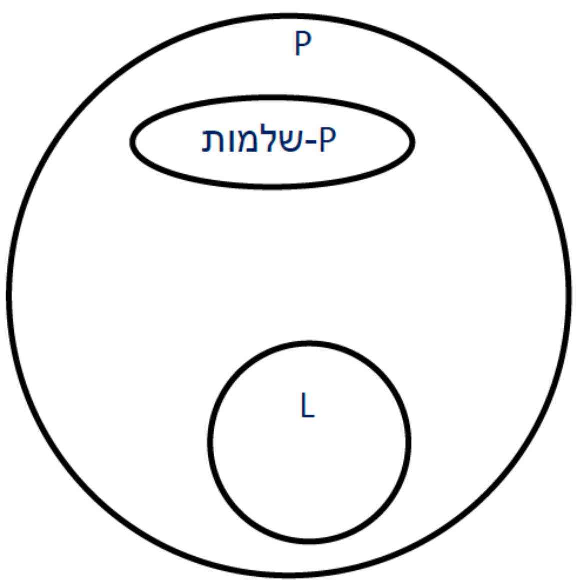
רעיון ההוכחה: דומה להוכחת משפט קוק-לוין (7.1).

רעיון הרדוקציה: לכל $A \in \mathrm{P}$ שמוכרעת ע"י מ"ט M בזמן פולינומי נראה רדוקציה לוגריתמית f אשר בהינתן קלט $x \in \Sigma^n$ מחזירה מעגל C_n מעל n משתנים ומחזירה את $\langle x\rangle$ בתורה שמה לשערי הקלט של C_n. כלומר הרדוקציה מחזירה את הזוג $\langle C_n, x\rangle$. אנחנו נבנה את C_n מתוך המ"ט M בצורה שמבטיחה שהשמה x מספקת את C_n אמ"מ M מקבלת את x. לכן נקבל ש-

$$\langle C_n, x\rangle \in \mathrm{CVAL} \iff C_n(\langle x\rangle) = 1 \iff M(x) = 1 \iff x \in A$$

בזמן חישוב הרדוקציה אנחנו לא יודעים אם $M(x)$ מקבלת ו/או אם $C_n(x) = 1$, כי יש לנו רק מקום לוגריתמי וכדי לחשב את הדברים האלה צריך (כנראה) מקום פולינומי. ■

תמונה חלקית של העולם שלנו:



9.2 סיבוכיות מקום לא-דטרמיניסטית

הגדרה 9.8. תהי $S:\mathbb{N}\to\mathbb{N}$ ו-N מטל"ד עם 3 סרטים: סרט קלט לקריאה בלבד, סרט עבודה, וסרט פלט לכתיבה חד פעמית. N **רצה במקום** $S(n)$ אם לכל $n\in\mathbb{N}$ ולכל $x\in\Sigma^n$ באורך n, בכל ענף בעץ החישוב $T_{N,x}$ מתקיים ש-N משתמשת בלכל היותר $S(n)$ תאים בסרט העבודה בטרם עוצרת (בפרט תמיד עוצרת).

הגדרה 9.9. תהי $S:\mathbb{N}\to\mathbb{N}$.

$$\text{NSpace} \coloneqq \{\, L(M) : \, M \text{ is a NTM that runs in } O(S(n)) \text{ space} \,\}$$

הגדרה 9.10.

$$\text{NL} = \text{NSpace}(\log(n))$$

הגדרה 9.11. V **מוודא במקום לוגריתמי** עבור שפה A אם V מ"ט (דטרמיניסטית) 3-סרטית:

- סרט קלט לקריאה בלבד
- סרט עד **לקריאה חד פעמית**
- סרט עבודה

כך שלכל $n\in\mathbb{N}$ וקלט $x\in\Sigma^n$, מתקיים ש-V משתמש בלכל היותר $O(\log(n))$ תאים בסרט העבודה ו-$x\in A$ אמ"מ קיים עד w כך ש-$V(x,w)$ מקבל.

טענה 9.6. $A\in\text{NL}$ אמ"מ קיים מוודא במקום לוגריתמי עבור A.

הוכחה: $\Leftarrow$: נניח כי $A\in\text{NL}$, אז קיימת מטל"ד N שמכריעה את A במקום לוגריתמי.
נגדיר מוודא במקום לוגריתמי V עבור A באופן הבא, עבור קלט $x\in\Sigma^n$ ועד $w\in\{0,1\}^*$:

- סרט הקלט יכיל את x בתחילת הריצה
- סרט העד יכיל את w בתחילת הריצה
- סרט העבודה יבצע את החישוב הבא:
  - עבור $w=w_1\cdots w_\ell$, לכל $i\in[\ell]$, N תענה לפי ענף החישוב ב-$T_{N,x}$ שמוגדר באופן הבא (בה"כ נניח כי העץ בינארי):
    - N תעבור מהקונפיגורציה ה-c_{i-1} בחישוב, לקונפיגורציה ה-w_i מבין הקונפיגורציות ש-c_{i-1} עוברת אליהן.
  - כל ענף חישוב של $T_{N,x}$ משתמש במקום $O(\log(n))$ ולכן גם הענף ש-w מכתיב

לכל x,w מתקיים ש-$V(x,w)$ משתמש במקום לוגריתמי בסרט העבודה. ולכל $x\in\Sigma^*$ קיים עד w עבורו $V(x,w)=1$ אמ"מ קיים ענף חישוב מקבל של $T_{N,x}$ אמ"מ $x\in A$.
$\Rightarrow$: נניח כי קיים ממודא במקום לוגריתמי V עבור A.
נגדיר מטל"ד N במקום לוגריתמי שמכריעה את A באופן הבא, עבור קלט $x\in\Sigma^n$. ראשית נציין עובדה, כפי שראינו בהוכחת טענה 9.2, משום ש-V משתמש במקום לוגריתמי אז בפרט הוא רץ בזמן $2^{O(\log n)}=n^{O(1)}$ ולכן בה"כ $w\in\{0,1\}^{n^k}$ עבור k קבוע.

- על סרט הקלט יהיה כתוב את x

- על סרט העבודה:
  - בתא הראשון ננחש תו $w_i \in \{0,1\}$
  - נסמלץ את $V(x, w_1 \cdots w_i)$ ואז נחזור לתא הראשון וננחש $w_{i+1} \in \{0,1\}$
  - למעשה אנחנו ניתן ל-V את w_i בכל פעם שהיא דורשת אותו לקריאה חד פעמית ובכך לא נצטרך לנחש את $|w| = O(n^k)$ ולשמור אותו במקום לא לוגריתמי
  - החישוב הכולל של $V(x,w)$ לוקח מקום לוגריתמי
- על סרט הפלט נכתוב את תוצאת $V(x,w)$ כאשר סרט העבודה הגיע למצב מקבל/דוחה

לכל $x \in \Sigma^n$ מתקיים ש-N רץ במקום לוגריתמי ו-$x \in L(N)$ אמ"מ קיים עד $w \in \{0,1\}^*$ כך ש-$V(x,w) = 1$ אמ"מ $x \in A$. ■

טענה 9.7 (מוגדר בהגדרה 7.2). $\mathrm{STCON} \in \mathrm{NL}$.

הוכחה: העד הוא רשימה סדורה של צמתים במסלול. ניתן לוודא במעבר חד-פעמי על המסלול תוך שימוש במקום לוגריתמי. ■

9.2.1 בעיות NL-שלמות

הגדרה 9.12. תהא שפה A_0.

- A_0 היא **NL-קשה** (תחת רדוקציות מקום לוגריתמי) אם לכל $A \in \mathrm{NL}$ מתקיים $A \leq_L A_0$
- A_0 היא **NL-שלמה** אם היא NL-קשה ובנוסף $A_0 \in \mathrm{NL}$

טענה 9.8. STCON היא NL-שלמה.

מסקנה 9.4. $\mathrm{NL} \subseteq \mathrm{P}$.

הוכחת מסקנה 9.4: תהי $A \in \mathrm{NL}$, אז $A \leq_L \mathrm{STCON}$ ולכן גם $A \leq_P \mathrm{STCON}$.
מכיוון ש-$\mathrm{STCON} \in \mathrm{P}$ (טענה 7.1) נקבל שגם $A \in \mathrm{P}$. ■

הוכחת טענה 9.8 (סקיצה): תהי $A \in \mathrm{NL}$ ותהי N מטל"ד עם מקום לוגריתמי $S(n) = O(\log n)$ המכריעה אותה.
תיאור הרדוקציה:
בהינתן קלט x נגדיר את גרף הקונפיגורציות $G_{N,x}$:

- הקודקודים הם הקונפיגורציות: $[n] \times \Gamma^s \times Q \times [S]$
  ניתנים לייצוג ע"י מחרוזת באורך $O(S(n)) = O(\log n)$
- קשת מכוונת מ-c ל-c' אמ"מ c δ-עוברת ל-c'
- נניח בה"כ קונפ' מקבלת יחידה

הרדוקציה בהינתן x מוציאה $\langle G_{N,x}, s = c_0, t = c_{acc} \rangle$ כאשר c_0, c_{acc} הם הקונפ' ההתחלתית/מקבלת.
ניתן לחשב במקום לוגריתמי. ■

משפט 9.2 (סאביץ'). $\text{STCON} \in \text{DSpace}\left(\log^2 n\right)$.

מסקנה 9.5. $\text{NL} \subseteq \text{DSpace}\left(\log^2 n\right)$.

טענה 9.9. לכל $S(n) \geq \log(n)$ מתקיים $\text{NSpace}(S(n)) \subseteq \text{DSpace}\left(S^2(n)\right)$.

מסקנה 9.6. $\text{PSPACE} = \text{NPSPACE}$.

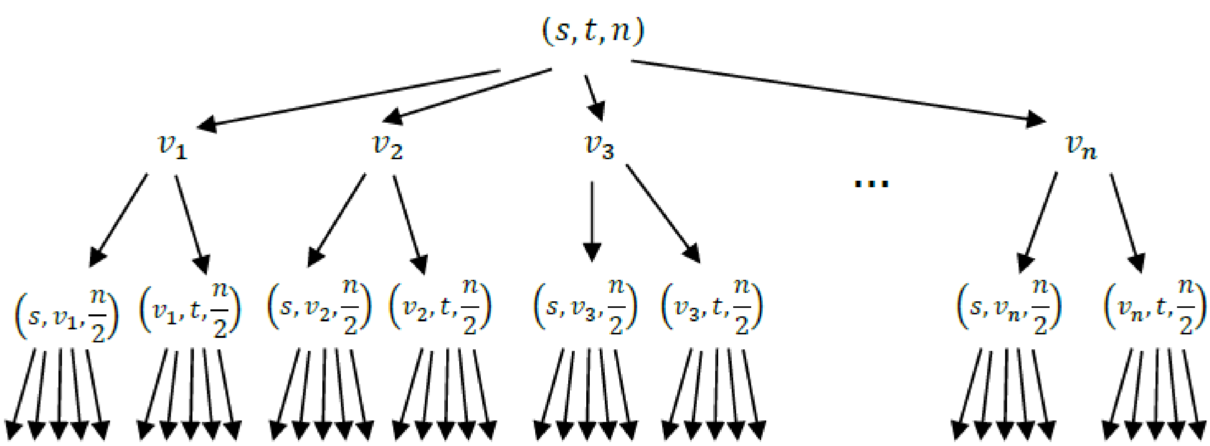
<u>רעיון הוכחת משפט סאביץ' (9.2):</u> אבחנה: אם קיים מסלול מ-s ל-t באורך $\geq T$ אזי קיים קודקוד w כך שיש מסלול מ-s ל-t באורך $\geq \frac{T}{2}$ ויש מסלול מ-w ל-t באורך $\geq \frac{T}{2}$.

על סמך האבחנה הזאת נתכנן את האלג' הרקורסיבי הבא לבדיקה האם יש מסלול באורך $\geq T$ מ-u ל-v:

- לכל $w \in V$:
  - בדוק בצורה רקורסיבית אם יש מסלול באורך $\geq \frac{T}{2}$ מ-u ל-w
  - בדוק בצורה רקורסיבית (באותו זיכרון) אם יש מסלול מ-w ל-v באורך $\geq \frac{T}{2}$
  - אם שתי הבדיקות החזירו "כן" אז החזר "כן"
- החזר "לא"

בסיס: אם $u = v$ או $(u, v) \in E$ אז החזר "כן". אחרת, אם $T \leq 1$, החזר "לא".

האלגוריתם בבירור נכון. נמצא מקום הוא צורך באמצעות עץ הרקורסיה של הריצה:



- מספר רמות הרקורסיה הוא $\log n$
- בכל שלב ברקורסיה צריך לזכור:

1. צומת w - $O(\log n)$ ביטים
2. האם בקריאה הרקורסיבית הראשונה או השנייה - $O(1)$ ביטים
3. אורך מסלול T - $O(\log n)$ ביטים

- סה"כ בכל רמה $O(\log n)$
- סה"כ $O\left(\log^2 n\right)$

■

9.2.2 סגירות למשלים

הגדרה 9.13.

$$coNL = \left\{ L : \overline{L} \in NL \right\}$$

משפט 9.3 (אימרמן). $\overline{\text{STCON}} \in \text{NL}$.

מסקנה 9.7. $\text{NL} = co\text{NL}$.

טענה 9.10. לכל $S(n) \geq \log(n)$ מתקיים $\text{NSpace}(S(n)) = co\text{NSpace}(S(n))$.

הוכחת משפט אימרמן (9.3): נתאר מוודא V במקום לוגריתמי עבור $\overline{\text{STCON}}$

סימון 9.2. עבור קלט $\langle G = (U, E), s, t \rangle$ נסמן $|U| = n$. לכל $0 \leq i \leq n$ נסמן ב-R_i את קבוצת הקודקודים שיש אליהם מסלול מ-s באורך i קשתות לכל היותר, ונסמן $r_i = |R_i|$.

מתקיים ש-$R_0 = \{s\}, r_0 = 1$.

העד לכך ש- $\langle G, s, t \rangle \notin \text{STCON}$, כלומר לכך ש-$t \notin R_n$, הוא קידוד:

$$\langle (r_1, w_1), (r_2, w_2), \ldots, (r_{n-1}, w_{n-1}), w_{t \notin R_n} \rangle$$

כאשר:

- w_i הוא עד לכך שאם r_{i-1} נכון אז גם r_i נכון.
- $w_{t \notin R_n}$ הוא עד לכך שאם r_{n-1} נכון אז $t \notin R_n$.

תיאור כללי של המוודא V:

V בהינתן קלט $\langle G, s, t \rangle$ ועד $\langle (r_1, w_1), (r_2, w_2), \ldots, (r_{n-1}, w_{n-1}), w_{t \notin R_n} \rangle$:

- כתוב $r_0 = 1$ על סרט העבודה
- לכל $i \in [n-1]$:
  - קרא את r_i מסרט העד וכתוב אותו לסרט העבודה
  - וודא את העד w_i עבור r_i בעזרת r_{i-1}. אם הווידוא נכשל אז תדחה.
  - מחק את r_{i-1} מסרט העבודה.
- וודא את העד $w_{t \notin R_n}$ בעזרת r_{n-1}. אם הווידוא נכשל אז תדחה.
- קבל.

נותר לתאר את העדים w_i ואת $w_{t \notin R_n}$ ולהראות כיצד לוודא אותם במקום לוגריתמי.

ראשית נתאר את העד $w_{t \notin R_n}$ לכך ש-$t \notin R_n$ בהנחה ש-r_{n-1} נכון:

נקבע סדר על הקודקודים ונסמן $R_{n-1} = \left\{ u_1, \ldots, u_{r_{n-1}} \right\}$ כאשר $u_1 < \cdots < u_{r_{n-1}}$.

העד $w_{t \notin R_n}$ הוא קידוד:

$$w_{t \notin R_n} = \left\langle \left(u_1, w_{u_1 \in R_{n-1}} \right), \ldots, \left(u_{r_{n-1}}, w_{u_{r_{n-1}} \in R_{n-1}} \right) \right\rangle$$

כאשר $w_{u_i \in R_{n-1}}$ הוא קידוד של מסלול מ-s ל-t באורך לכל היותר $n - 1$.

מוודא עבור העד $w_{t\notin R_n}$ לכך ש-$t \notin R_n$ בהנחה ש-r_{n-1} נכון:

בהינתן r_{n-1} והעד $w_{t\notin R_n} = \left\langle \left(u_1, w_{u_1\in R_{n-1}}\right), \ldots, \left(u_{r_{n-1}}, w_{u_{r_{n-1}}\in R_{n-1}}\right)\right\rangle$:

- לכל $i \in [r_{n-1}]$:
  - קרא את u_i לסרט העבודה.
  - בדוק ש-$w_{u_i\in R_{n-1}}$ הוא מסלול מ-s ל-u_i באורך לכל היותר $n-1$. אחרת דחה.
  - אם $1 < i$ אז בדוק ש-$u_{i-1} < u_i$. אחרת דחה.
  - בדוק **שאין** קשת מ-u_i ל-t. אחרת דחה.
  - מחק את u_{i-1} מסרט העבודה.
- קבל.

טענה 9.11. אם r_{n-1} נכון אז קיים עד $w_{t\notin R_n}$ שמתקבל אמ"מ $t \notin R_n$.

נותר לתאר את העד w_i לכך ש-r_i נכון בהנחה ש-r_{i-1} נכון:

נסמן $U = \{u_1, \ldots, u_m\}$.

העד w_i הוא קידוד:

$$w_{i,j} = \begin{cases} w_{u_j\in R_i}, & u_j \in R_i \\ w_{u_j\notin R_i}, & u_j \notin R_i \end{cases} \qquad\qquad w_i = \langle w_{i,1}, \ldots, w_{i,n}\rangle :$$

כאשר:

- $w_{u_j\in R_i}$ הוא קידוד של מסלול מ-s ל-u_j באורך לכל היותר i
- $w_{u_j\notin R_i}$ הוא עד לכך ש-$u_j \notin R_i$ בהינתן ש-r_{i-1} נכון, בדומה לעד $w_{t\notin R_n}$.

מוודא עבור העד w_i לכך ש-r_i נכון בהנחה ש-r_{i-1} נכון:

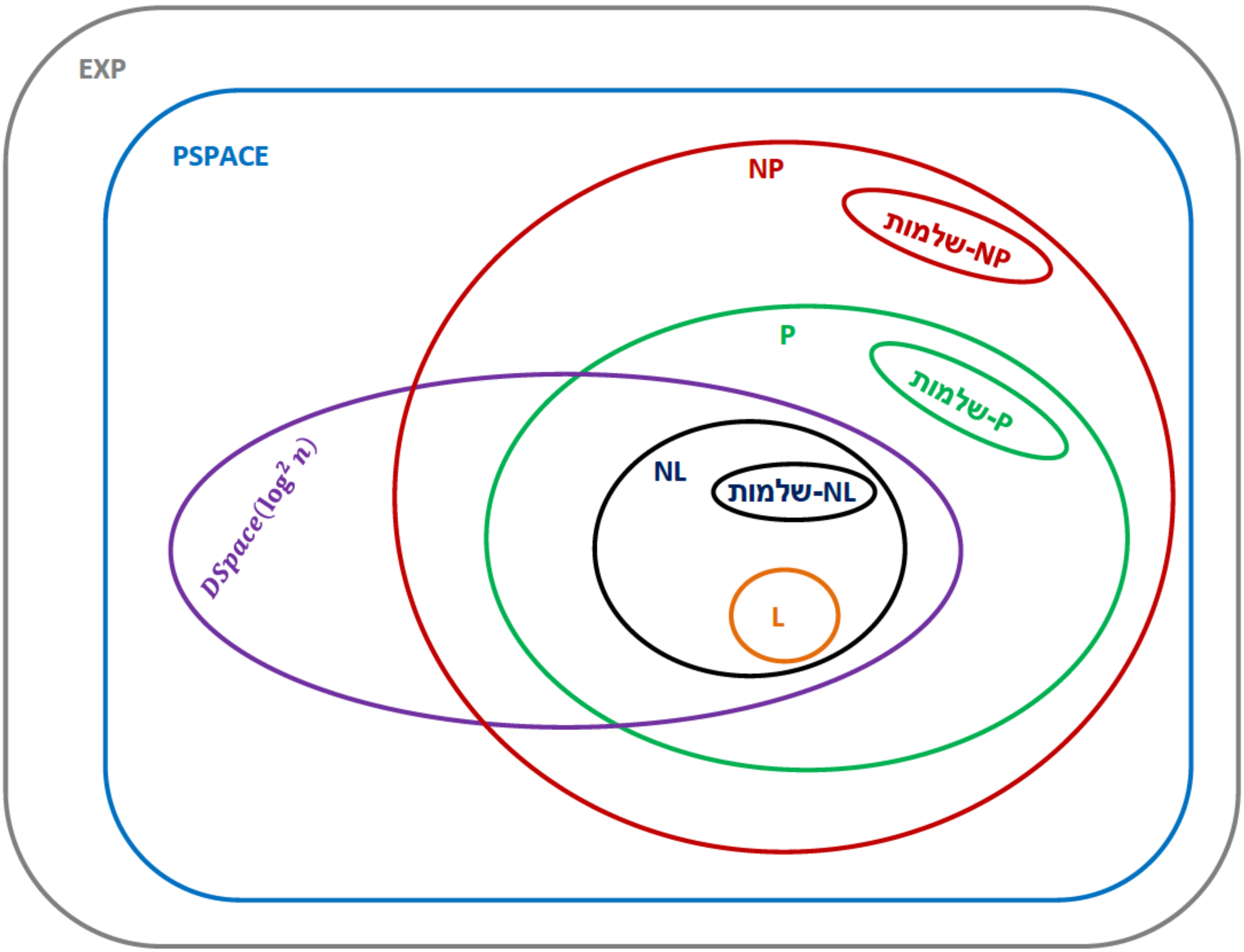
בהינתן r_{i-1} והעד $w_i = \langle w_{i,1}, \ldots, w_{i,n}\rangle$:

- אתחל משתנה $r = 0$ שסופר את מספר הקודקודים ב-R_i
- לכל $j \in [n]$:
  - וודא את העד $w_{i,j}$. אם הווידוא נכשל אז דחה.
  - אם $w_{i,j} = w_{u_j\in R_i}$ אז הגדל את המונה r ב-1.
- אם $r = r_i$ אז קבל. אחרת דחה.

טענה 9.12. אם r_{i-1} נכון אז קיים עד w_i שמתקבל אמ"מ r_i נכון.

■

תמונת עולם מעודכנת:



- לא ידוע אם $\mathrm{NL} \neq \mathrm{L}$. מאמינים שכן. בפרט מאמינים ש-$\mathrm{STCON} \in \mathrm{NL} \setminus \mathrm{L}$.
- ממשפט היררכיית המקום אנחנו יודעים שיש שפה ב- $\mathrm{DSpace}\left(\log^2 n\right) \setminus \mathrm{L}$ ושיש שפה ב- $\mathrm{PSPACE} \setminus \mathrm{DSpace}\left(\log^2 n\right)$.
- ממשפט היררכיית הזמן אנחנו יודעים שיש שפה ב-$\mathrm{EXP} \setminus \mathrm{P}$.
- לגבי NP מול $\mathrm{DSpace}\left(\log^2 n\right)$ מאמינים שאין הכלה באף כיוון.
- גם לגבי P מול $\mathrm{DSpace}\left(\log^2 n\right)$ מאמינים שאין הכלה באף כיוון.