

מודלים חישוביים, חישוביות וסיבוכיות | 67521

הרצאות | פרופ' אורנה קופרמן

כתביה | נמרוד רק

תשפ"ג סמסטר א'

תוכן העניינים

I	מבוא לאוטומטים
4	הרצאה
4	אוטומטים
5	פוקולות על שפה
9	תרגול
14	II אוטומטים אי-דטרמיניסטיים
14	הרצאה
20	תרגול
23	III שפות לא רגולריות ולמה הניפהו
23	הרצאה
26	דוגמאות לשפות לא רגולריות
27	תרגול
27	ביטויים רגולריים
30	IV משפט מיהיל-גרוז
30	הרצאה
33	מצוער אוטומטים
35	תרגול
38	V שפות חסרות הקשר
38	הרצאה
39	בעיית הריקנות ומשלים של אוטומט
40	דקוק חסר הקשר
44	תרגול
47	VI מכונות טיורינג
47	הרצאה
51	תרגול
52	מודלים שקולים למ"ט
54	VII א נמורציה ואי-כריעות
54	הרצאה
56	אי כריעות
57	תרגול
58	VIII דוקציה
58	הרצאה
62	תרגול

IX תורת הסיבוכיות	
65	הרצאה
65	תרגול
X שלמות-<i>NP</i>	
71	הרצאה
71	רذוקציות פולינומיאליות
71	תרגול
74	
XI מחלקות שלמות-<i>NP</i>	
76	הרצאה
76	תרגול
82	שפות לגרפים המילטוניים
83	
XII מחלקות סיבוכיות מקומ	
86	הרצאה
86	תרגול
89	
XIII NL ו-<i>L</i>	
92	הרצאה
92	תרגול
96	
נספח רשימת הגדרות משפטיים	
99	שפות רגולריות ואוטומטים
99	הגדרות
99	משפטים
100	שפות חסירות הקשר
101	הגדרות
101	משפטים
102	כריעות
102	הגדרות
102	משפטים
105	סיבוכיות זמן
105	הגדרות
108	משפטים
108	סיבוכיות מקום
108	הגדרות
109	משפטים
110	סיבוכיות שטח לוגריתמית
110	הגדרות
110	משפטים

שבוע ॥ | מבוא לAUTOMATIM

הרצאה

חלק א' של הרצאה

דוגמה נקבעו חלק האחרון של הקורס (סיבוכיות). בהינתן גраф לא מכוון $G = \langle V, E \rangle$, נרצה לדעת האם יש בו מעגל אוילר (כזה שעובר בכל צלע בדיקות פעם אחת).

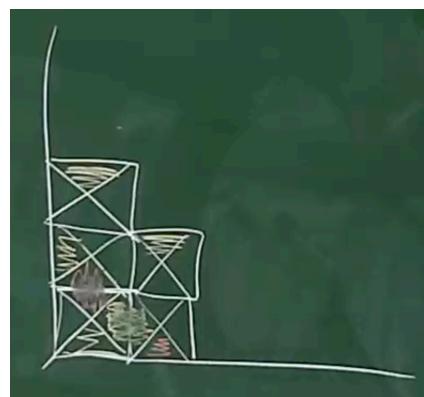
אוילר הוכח שיש מעגל כזה אם "דרגת כל הקודקודים זוגית, וכן ניתן להכריע את הבעיה בזמן לינארית כי יש לבעה אפין מתמטי. מעגל המילטון הוא מעגל שעובר בכל קודקוד בדיקות פעם אחת. לבעה זו אין אפין מתמטי, והוכחה שאין אלג' יותר טוב מאשר מעבר על כל האפשרויות, בסיבוכיות אקספוננציאלי.

דוגמה בהינתן $q \cdot p = n$, למצוא את q, p דרוש זמן חישוב אקספוננציאלי באורך הייצוג, אפ"ג שהאלג' הוא לינארי במספר עצמו. זה משומש שהפרמטר שלנו בקרה זהה הוא לא המספר אלא הייצוג (אנחנו מקבלים $n \log n$ ספרות/אחדים ואפסים, לא את המספר כולו).

דוגמה קלט: $\{t_i\}$ אריכים שלכל אחד מהם יש צלעות $\{l_i\}, \{r_i\}, \{d_i\}, \{u_i\}$ (למעלה, למטה, ימינה ושמאליה בהתאם) כאשר הצלעות הם צבעים (אדום, צהוב, ירוק).

פלט: האם ניתן לרצף באופן חוקי ריבוע $n \times n$ לכל $1 \leq n$, כאשר "חוקיות" מתחבطة בכך שצלעות סמכות מסכימות על הצבע.

דוגמה ריצה באופן אינטואיטיבי, במקרים מסוימים, נוכל להציג אחד מהאריכים בפינה, למצוא אליו אריכים מותאימים לו מבחינות הצלעות הסמכות, להציג אריכים חוקיים נוספים, וכך לחזור חלילה. לעיתים (כמו זה שבתמונה), נוצרת תבנית של אריכים חוקיים על האלבסון (כלומר אריך 'א' בפינה השמאלית התחתונה, וזו 'ב' מימינו ומעליו, וזו 'ג' מימין ומעל כל 'ב') וזה אפשר לגודם את התבנית האינסופית זו לריבוע $n \times n$ כל פעם שצורך ולהזכיר ריבוע חוקי. במקרה כזה הפלט יהיה כן.



אייר 1 : דוגמה לתבנית שנוצרת, אפשר להמשיך לצויר את האלבסון בכיוון דרום-מערב ולהזור על התבנית החוצה עוד ועוד

הבעיה היא שאין שום ערובה לכך שהתבנית באמות קיימת במקרה הכללי, או שהיא נשמרת, ואי אפשר לזרץ עד ∞ . لكن התשובה היא שאין אלג' שפותר את הבעיה.

דוגמה (בעיה העצירה) קלט : תכנית מחשב P וקלט x .

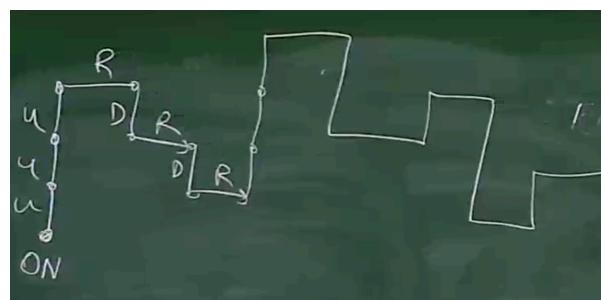
פלט : אם P עוצרת על x .

אין לבעה זו אלג' שפותר אותה בכל המקרים (תחת הנחות מסוימות, אפשר לפעמים לחתת תשובה).

אוטומטים

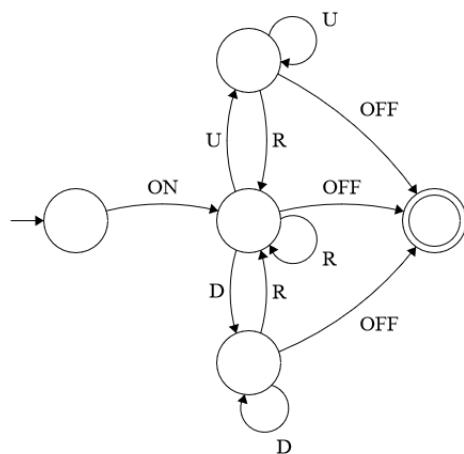
הגדרה אוטומט הוא מחשב עם זכרון מוגבל.

דוגמה נתון עט דיגיטלי שיכל לבצע את משפט פקודות, ON, OFF, U, D, L, R. סדרת פקודות היא חוקית אם היא מתחילה ב-ON, מסתיימת ב-OFF ומיצרת קו רקייע משמאלי לימין.



איור 2 : דוגמהdko רקייע חוקי, אסור לכת שמאלה ואסור לעלות מיד אחרי שיורדים (ולחפץ)

כתב אוטומט שמליט האם סדרת פקודות היא חוקית. אם נצליח לעבור בין המ מצבים (העיגולים), החל מה מצב הראשון (זה עם ח' לא מקור) ועד למצב המקביל (עם העיגול ההפוך) על קשתות קיימות, הרי שהסדרה חוקית.



איור 3 : אוטומט חוקי

אינטואיטיבית, המצב האמצעי הוא זה שמןנו אפשר לעשות מה שרצו, העליון הוא אחראי עליה והתחתון הוא אחראי ירידת. נשים לב כי מכולם אפשר לפנות ימינה.

הגדירה אוטומט (automaton, DFA) הוא חמיישיה $A = \langle Q, \Sigma, \delta, q_0, F \rangle$ שם המצביעים, הא'ב, פונקציית המעברים, המצב ההתחלתי וקבוצת המצביעים המקבלים שМОכלת ב- Q .

- δ היא $\Delta : Q \times \Sigma \mapsto Q$.
- Σ היא קבוצה סופית של אותיות, לדוגמה $\{0, 1\}^4 = \Sigma$ וכו'.
- מילה היא $w = w_1, \dots, w_n = w$ סדרה סופית של אותיות, ו- ϵ היא המילה הריקה.
- שפה היא קבוצה של מילים, $\Sigma^* = \{w : \Sigma \subseteq L\}$ כאשר w מילה סופית מעל הא'ב Σ .

דוגמא A_1 הוא האוטומט הבא. במקרה הזה $F = \{q_0\}, Q = \{q_0, q_1\}, \Sigma = \{0, 1\}$ ופ' המצביעים היא

δ	0	1
q_0	q_0	q_1
q_1	q_1	q_0

הגדירה ריצה על מילה $w = w_1 \dots w_n = r_0 \dots r_n$ מעל Σ היא סדרה של מצביעים r כך ש:

- $r_0 = q_0$ (הריצה מתחילה ב- q_0).
- לכל $i \geq 0$, $r_{i+1} = \delta(r_i, w_{i+1})$ (הריצה מכבדת את δ).

דוגמא עבור A_1 והמילה 011, הריצה היא $.q_0q_0q_1q_0$.

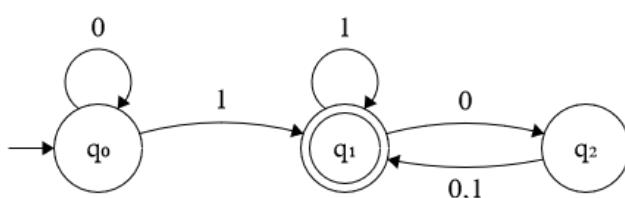
הגדירה r היא ריצה מקבלת (accepting) אם $r_n \in F$ (המצביע האחרון בריצה הוא מקבל). אחרת, r הוא דוחה (rejecting). מתקבלת ריצה r אם הריצה של A על w היא מקבלת.

השפה של האוטומט היא אוסף המילים ש- A מקבל עליהם.

דוגמא עבור A_1 , $L(A_1) = \{w : w \text{ הוא זוגי}\}$ (אפשר להוכיח באינדוקציה).

הערה אם לא קיים מעבר עבור אות ומצב, אפשר או להחיליט ש- δ לא מוגדרת על כל $\Sigma \times Q$ או להחיליט שככל קשת לא קיימת מובילה לבור דוחה, כלומר מצב לא מקבל שאינו ניתן לצאת ממנו.

דוגמא נציג אוטומט נוסף, A_2 , ונחשב את השפה שלו.



איור 4: האוטומט A_2

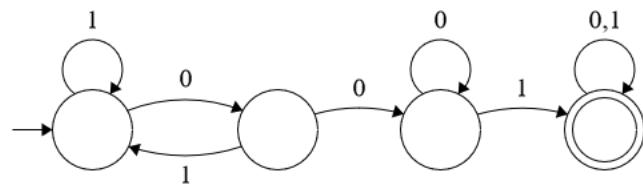
נסמן בצבוע האם כמה מיללים נבחרות הן בשפה או לא, $\textcolor{red}{.010}, \textcolor{green}{011}, \textcolor{blue}{001110}, \textcolor{green}{1}, \textcolor{red}{11}, \textcolor{red}{00000}$

אם נחשוב עוד קצת, נגלה ש-

$$L(A_2) = \{w : \text{יש } b-w \text{ לפחות } 1 \text{ אחד, ואחרי ה-1 האחרון יש מספר זוגי (או אפס) של } 0\text{-ים}\}$$

בתרגול נוכיח את זה באופן פורמלי.

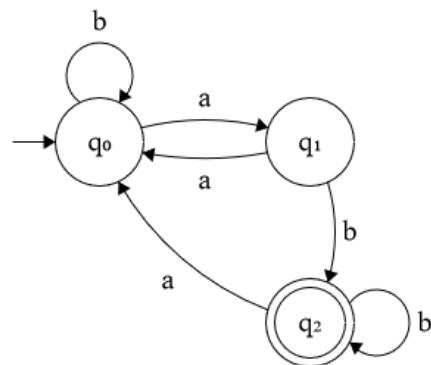
דוגמה בהינתן שפה, כניסה לחשב את האוטומט. השפה היא $\{w : w \text{ מכילה את הרצף } 001 \text{ לפחות פעם אחת}\}$



איור 5 : אוטומט שנוצר מ- L_3

חלק ב' של ההרצאה

דוגמה $L = \{w : (\text{כאשר } w \text{ הוא מספר } a\text{-ים ב-}w \text{ ו-}w_n = b) \wedge w_n \text{ האות الأخيرة במיליה}\}$.



איור 6 : אוטומט שאנו טוענים שנוצר מ- L

המצב ההתחלתי לא מקבל כי $\epsilon \notin L$. b כאות ראשונה לא מקדם אותנו כי זו לא מילה חוקית. הרעיון בהלוך-חזרה ב- q_0, q_1 הוא שרק אם המספר הוא אי זוגי של a -ים, נגיע ל- q_1 ומשם נעזר במצב מקבל רק אם אנחנו גמורים ב- b .

לכל מצב נוכל להתאים סטטוס - מה מופיע את המילה שגיעה אליו (לאחר מכון שימוש בסטטוסים האלה, נפרמל אותם ונוכיח
איitem את נכונות האוטומט):

• $w \#_a q_0$ - זוגי.

• $w \#_a q_1$ - איזוגי ו- w מסתיימת ב- a .

• $w \#_a q_2$ - איזוגי ו- w מסתיימת ב- b .

טענה $L(A) = L$

הוכחה: $\forall w \in \Sigma^*$ (אוסף המילים האפשרות) מתקיים $Q \times \Sigma^* \mapsto Q$: $(q_0, w) = q^*$, כלומר הפעלה שוב ושוב של δ על המילה החול ממצב נתון).

נוכיח את שלוש הטענות הבאות ומשם ינבע כי

$$w \in L \iff \delta^*(q_0, w) = q_2 \iff \delta^*(q_0, w) \in F$$

האם "ס" נבע ממשתי הטענות הראשונות, הטענה השלישית מספקת לנו רק כיוון אחד.

1. אם $w \#_a q_0$ - זוגי.

2. אם $w \#_a q_1$ - איזוגי ו- w מסתיימת ב- a .

3. אם $w \#_a q_2$ - איזוגי ו- w מסתיימת ב- b .

באיינדוקציה על $|w|$:

בסיס (0): נוכיח את הטענה על $w = \epsilon$: $\delta^*(q_0, \epsilon) = q_0$ וכאן $\#_a \epsilon$ זוגי.

צעד ($|w| + 1$): נוכיח את הטענה על $w \cdot a$: נוכיח רק את המקרה של $w \cdot a$ נושא לסטודנטית המשקיפה להוכיח את המקרה השני.

• אם $\#_a w \cdot a = \#_a (\delta(q_0, a))$ אז $\delta^*(q_0, w \cdot a) = q_0$ זוגי.

• ואם $\#_a w \cdot a = \#_a (\delta(q_0, a) \#_a w)$ אז $\delta^*(q_0, w \cdot a) = q_1$ –

• ואם $\#_a w \cdot a = \#_a (\delta(q_0, w) \#_a a)$ אז $\delta^*(q_0, w \cdot a) = q_2$ –

דוגמא $L = \{w : \#_a w = \#_b w\}$, $\Sigma = \{a, b\}$. אין אוטומט סופי שפותו L ! זה בגל שאחרי ה- a הראשון, נדרש "לזכור" שיש לנו 1 לטובת a , ואז אם שוב יש a נדרש לזכור עוד 1, ואם b אז אחד לטובת b וזה איינסובי בעצם.

הגדירה שפה רגולרית היא שפה שניתנית לזיהוי ע"י אוטומט, ונסמן $L \in \text{REG}$, פורמלית, L היא רגולרית אם קיים DFA כך ש-

פעולות על שפות

. $\Sigma = \Sigma_1 \cup \Sigma_2 \neq \Sigma_1$ ובקשה כזה נסמן $L_1, L_2 \in \Sigma^*$. כל הפעולות עובדות על שפות מעל Σ .

1. **איחוד** ($L_1 \cup L_2 = \{w : w \in L_1 \vee w \in L_2\}$) : (union)

2. **שרשור** ($L_1 \cdot L_2 = \{w_1 \cdot w_2 : w_1 \in L_1, w_2 \in L_2\}$) : (concatenation)

3. **כוכב** ($L^* = \{w_1 \cdot \dots \cdot w_k : k \geq 0 \wedge w_i \in L, \forall i \leq k\}$) : (star)

דוגמה $L_1 = \{1, 333\}, L_2 = \{22, 4444\}$

$$L_1 \cup L_2 = \{1, 333, 22, 4444\}$$

$$L_1 \cdot L_2 = \{122, 1444, 33322, 3334444\}$$

$$L^* = \{\epsilon, 1, 333, 11, 1333, 3331, 333333, \dots\}$$

הערה אם $\emptyset = L^* = \{\epsilon\}$ אז $L = \{a\}$ וכל שפה אחרת היא אינסופת (יש לפחות מילה אחת לא ריקה, נשרשר אותה כמה פעמים שרק נרצה).

תרגום

הגדירה נאמר כי T הוא יחס מעל $R \subseteq S \times T$ (לרוב S, T ייחס מעל R).

דוגמה $R = \{(a, b) : |a - b| \leq 1\}, A = \{1, 2, 3, 4\}$

תכונות של יחסים

- **רפלקסיביות**: $(a, a) \in R, \forall a \in A$ או בסימונו חלופי, aRa (היחס הנ"ל הוא רפלקסיבי).

- **סימטריה**: $aRb \wedge bRa \text{ אם ורק אם } a, b \in A$ (היחס הנ"ל הוא סימטרי).

- **טרנזיטיביות**: $aRc \wedge cRb \Rightarrow aRb, \forall a, b, c \in A$

• **יחס שקולות:** יחס שמקיים את שלושת הנ"ל.

$x \in [a]_R \cap [b]_R$ מחלק את A למחלקות שקולות זרות המוגדרות ע"י $[a]_R = \{b \in A : aRb\}$, כי אם קיים אבל $c \in [a]_R \setminus [b]_R$ או קיים $[a]_R \neq [b]_R$ ולכן

$$aRc \Rightarrow cRx \Rightarrow cRb \Rightarrow c \in [b]_R$$

סתירה.

דוגמה גרף לא מכון והיחס $R \subseteq V \times V$ שמשמעותו "כל זוגות הקודקודים שיש ביניהם מסלול ב- G ". קל לראות שהוא יחס רפלקטיבי, טרנזיטיבי וסימטרי ולכון זהו יחס שקולות.

הגדרה עוצמה של קבוצה היא ממד ל'גודל' הקבוצה. עבור קבוצה סופית A , העוצמה שלה היא $|A|$.

הגדרה $\aleph_0 = |\mathbb{N}|$

הערה ראיינו ש- $\aleph_0 = |\mathbb{Z}| = |\mathbb{Q}|$ (כאשר שווין עצומות ממשעו קיום פ' חח"ל בין שתי הקבוצות).

הערה נאמר כי $|A| < |B|$ אם יש העתקה חח"ע מ- A ל- B ואם אין העתקה חח"ע מ- A על B .

טענה (האלכסון של קנטור) $\aleph_0 < |[0, 1]| = 2^{\aleph_0}$

הגדרה $\Sigma^* = \bigcup_{n=0}^{\infty} \Sigma^n$ ונדיר $\Sigma \times \dots \times \underbrace{\Sigma}_{n \text{ פעמים}}$

הערה רבים מתבלבלים בכך אבל חשוב לציין ש- Σ^* סופית וכך גם Σ^n , אבל Σ^* אין סופית.

דוגמאות לשפות

$$\Sigma = \{a, b\}$$

$$L_1 = \{\epsilon, a, aa, b\} \bullet$$

$$L_2 = \{w : w_1 = a\} \bullet$$

$$L_3 = \{\epsilon\} \bullet$$

$$L_4 = \emptyset \bullet \text{זו אינה אותה קבוצה כמו } L_3!$$

$$L_5 = \{w : |w| < 24\} \bullet$$

$L_2 = \{w : w_n = b\}$ ו- $L_1 = \{w : w_1 = a\}$ • סימון לקוני למילים שמשמעותם ב- b . שפה נוספת היא

$$L_1 \cup L_2 = \{w : w_1 = a \vee w_n = b\}$$

$$L_2 \cdot L_1 = \{w : ab \text{ מכילה את הרצף } w\}$$

$$L_1 \cap L_2 = \{w : w_1 = a \wedge w_n = b\}$$

$$L_1 \cdot L_2 = L_1 \cap L_2$$

כאשר השווינו לאחריו נכוו כי המילה הראשונה בצד מתחילה ב- a והשנייה נגמרה ב- b ובאמצע לא משנה מה יש, בדומה ל- $L_2 \cap L_1$.

$$.L = \{ww : w \in \Sigma^*\} •$$

$$\bar{L} = \Sigma^* \setminus L = \{w : 2 \nmid |w|\} \cup \{w = w_1 \dots w_{2n} : w_1, \dots, w_n \neq w_{n+1} \dots w_{2n}\}$$

$$L \cdot L = \{wwxx : w, x \in \Sigma^*\}$$

הערה כל שפה מקיימת $\Sigma^* \subseteq L$, או באופן שקול $.L \in P(\Sigma^*)$

$$\text{כמה מילים יש ב-} \Sigma^* ? \aleph_0$$

$$\text{כמה שפות יש מעל } \Sigma^* ? 2^{\aleph_0}$$

כמה שפות רגולריות יש מעל Σ^* ? \aleph_0 , כי כל אוטומט מוגדר ע"י מחרוזת מעל Σ סופית (המצבים, הא"ב של האוטומט וכו') ולכן

מהן, ל'עוצמת אוסף המחרוזות שスクולות לאוטומטים היא \aleph_0 . למעשה, כל אוטומט אפשר לציר ויש מספר בן מנייה של פיקסללים

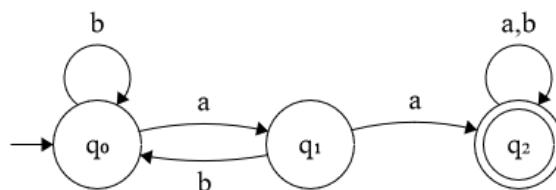
על canvas (במחשב).

מסקנה קיימות שפות לא רגולריות, ויש "יותר" לא רגולריות מאשר לא (השפות הרגולריות הן קבוצה במידה 0 מתוך כל השפות).

$$\delta^*(q, w) = \begin{cases} q & w = \epsilon \\ \delta(\delta^*(q, w'), \sigma) & w = w'\sigma, \sigma \in \Sigma \end{cases}$$

הגדרה בהינתן אוטומט A , נגיד

דוגמה נביט באוטומט הבא.



איור 7 : אוטומט לדוגמה

נחשב ערך של δ^* .

$$\delta^*(q_1, ba) = \delta(\delta^*(q, b), a) = \delta(\delta(\delta^*(q, \epsilon), b), a) = q_1$$

דוגמה עברו והשפה $\Sigma = \{0, \dots, 9, \#\}$

$$L = \{x\#a : x \in \{0, \dots, 0\}^*, a \in \{0, \dots, 9\}, a \in x\}$$

מצא את האוטומט המתאים ל- L . ראשית נשים לב לדוגמה כי L אבל $64424\#5 \notin L$.

הבעיה באוטומט זה שאין לנו זיכרון ולכן נctrck "לזכור" מספיק מידע כדי לזכור האם ראיינו # עד עכשו ואילו ספרות ראיינו עד כה.

נבחר מצב מייצג את אוסף הספרות שראינו עד כה והאם ראיינו את סולמית עד עכשו (2 אין ראיינו).

$$\Sigma = \{0, \dots, 9, \#\} \quad F = \{q_{acc}\}$$

$$\delta(\langle c, i \rangle, \sigma) = \begin{cases} \langle c \cup \{\sigma\}, 1 \rangle & \sigma \in \{0, \dots, 9\}, i = 1 \\ \langle c, 2 \rangle & \sigma = \#, i = 1 \\ q_{acc} & \sigma \in c, i = 2 \\ q_{sink} & \sigma \notin c, i = 2 \end{cases}$$

עbero על כל המצביעים והבינו את המשמעות, הרעיון בסוף הוא שם ראיינו סולמית ונטקלנו באות נוספת, קיבל או נשלול בהתאם להאם ראיינו את הספרה או לא. לשם השלמות גם נגדיר $\delta(q_{acc}, \sigma) = \delta(q_{sink}, \sigma) = q_{sink}$ כי אם הגיענו למצב המקבל והוספנו עוד تو זה כבר לא בשפה.

טענת עזר בהינתן $w \in \{0, \dots, 9\}^*$ מופיע w ב- $S(w)$ (אוסף הספרות שמופיעות ב- w). נוכחים כי $\delta^*(q_0, w) = \langle S(w), 1 \rangle$

הוכחה: בבדיקה על $|w|$.

$$\text{בסיס } \delta^*(q_0, w) = \delta(q_0, \epsilon) = \langle \emptyset, 1 \rangle : (w = \epsilon) \text{ כנדרש.}$$

$$\text{צעד } w' = w\sigma \text{ נסמן}: (|w| - 1 \rightarrow |w|)$$

$$\delta^*(q_0, w') = \delta(\delta^*(q_0, w), \sigma) \stackrel{\text{ Def }}{=} \delta(\langle S(w), 1 \rangle, \sigma) = \langle S(w'), 1 \rangle$$



$$.L = L(A) \text{ טענה}$$

הוכחה: נוכח הcola דו-כיוונית באינדוקציה על אורך המילה ; זו דרך ההוכחה המקובלת לטענות על שפות ואוטומטים.

. $a \in S(x)$ -ו $a \in \{0, \dots, 9\}$, $x \in [0, \dots, 9]$ $w = x\#a$ כאשר $w \in L$ מקבלת A על w כנדרש. נראה שريיצה של $L(A)$:

$$\begin{aligned}\delta^*(q_0, w) &= \delta(\delta^*(q_0, x\#), a) \\ &= \delta\left(\delta\left(\frac{\delta^*(q_0, x), \#}{\langle S(x), 1 \rangle}, a\right)\right)\end{aligned}$$

$$\delta = \delta(\langle S(x), 2 \rangle, a)$$

$$\delta = q_{acc}$$

. $w \notin L(A)$ או $w \notin L$ נבור על כל המילים : $L(A) \subseteq L$

. $\delta(q_0, w) = \langle S(w), 1 \rangle \neq q_{acc}$ אם $w \in \{0, \dots, 9\}^*$ •

. $w \in \{0, \dots, 9\}^* \times \{\#\}$ אם $w = x\#y$ אז $|y| > 1$ נבור •

$$\delta^*(q_0, w) = \delta\left(\frac{\delta^*(q_0, w), \#}{\langle S(x), 1 \rangle}\right) = \langle S(x), 2 \rangle \neq q_{acc}$$

אם $|y| > 1$ נבור •

$$\delta^*(q_0, w) = \delta^*(\langle S(x), 2 \rangle, y) \neq q_{acc}$$

כאשר השוויון נובע מכך שניתן לפצל את הריצעה על $x\#$ מביאה אותנו ל- $\langle S(x), 2 \rangle$ מהגדירה של δ . הא-שוויון נובע מכך ש- $1 > |y|$ ולכן גם אם אחרי הספרה הראשונה של y הגיענו ל- q_{acc} , בהכרח כל הספרות האחרות יובילו אותנו תמיד לבור דוחה.

אם $a \notin S(x)$ אבל $w = x\#a$ •

$$\delta^*(q_0, w) = \delta(\delta(\delta^*(q_0, x), \#), a)$$

$$= \delta(\langle S(x), 2 \rangle, a)$$

$$a \notin S(x) = q_{sink}$$

שבוע III | אוטומטים אי-דטרמיניסטיים

הרצאה

חלק א' של הרצאה

משפט השפות הרולגריות סגורות לאיחוד, כלומר, אם $L_1, L_2 \in \text{REG}$ אז $L_1 \cup L_2 \in \text{REG}$.

הוכחה: בהינתן DFA-ים $A = \langle Q, \Sigma, \delta, s_0, F \rangle$, $A_1 = \langle Q_1, \Sigma, \delta_1, s_1, F_1 \rangle$, $A_2 = \langle Q_2, \Sigma, \delta_2, s_2, F_2 \rangle$ שעבורו

$$L(A) = L(A_1) \cup L(A_2)$$

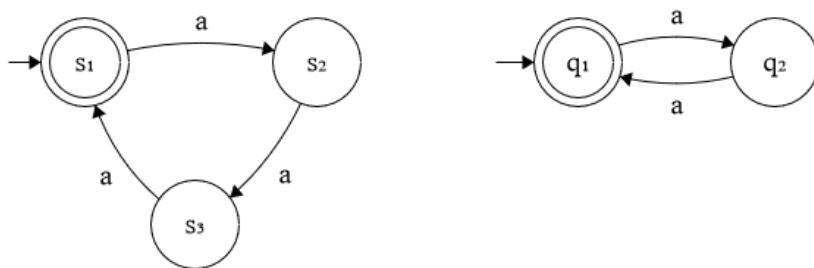
הרעיון הוא ש- A -*s* מסמלץ את A_1 ו- A_2 יחד, ואוטומט במבנה כזו נקרא אוטומט המכפלת. נבחר $s_0 = \langle s_1, s_2 \rangle$, $Q = Q_1 \times Q_2$ ופ' מעברים

$$\delta(\langle q_1, q_2 \rangle, \sigma) = \langle \delta_1(q_1, \sigma), \delta_2(q_2, \sigma) \rangle$$

כאשר אנחנו מניחים ש- A_1, A_2 לא נתקיים כי אפשר להוסיף בור דוחה במקרה הצורך.

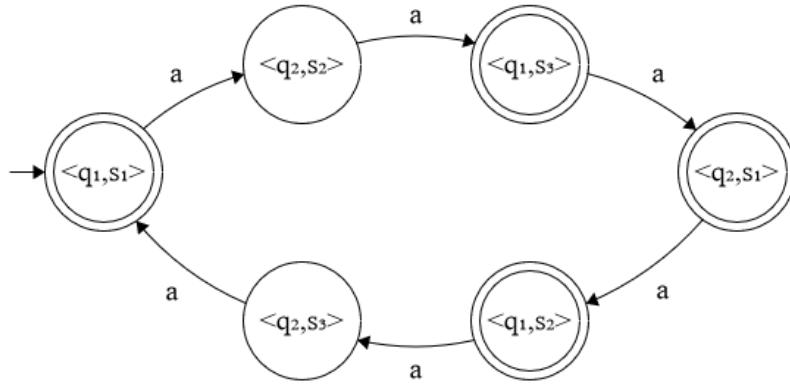
הערה אם $L \subseteq \{a\}^*$ או היא מגדירה תת קבוצה של \mathbb{N} - כל האורכים של מיללים בשפה, כלומר,

דוגמה נבחר את האוטומטים A_1, A_2 כבתמונה.



איור 8 : האוטומטים A_1 ו- A_2 (מימין) (A_1 (משמאלי)

במקרה זה, אוטומט המכפלת יראה כבאיור, כאשר בכל מעבר אנחנו "צודדים" קדימה גם במצבים של A_1 וגם בשל A_2 .



איור 9 : אוטומט המכפלה

$L(A) = \{w : |w| \bmod 2 = 0 \vee |w| \bmod 3 = 0\}$

הערה מהדוגמה הנ"ל ניתן לראות שאם הינו רוצים לבנות אוטומט שהשפה שלו היא ($A_1 \cap L(A_2)$ הינו בוחרים

$$F = \{\langle q_1, q_2 \rangle : q_1 \in F_1 \wedge q_2 \in F_2\}$$

כאשר ההבדל כאן הוא "וגם" במקום "או" על המ מצבים המקבילים.

הערה אם הינו רוצים $A = \langle Q_1, \Sigma, \delta_1, s_1, Q_1 \setminus F_1 \rangle$ כי הריצה מגיעה ל- $A = \langle Q_1, \Sigma, \delta_1, s_1, Q_1 \setminus F_1 \rangle, L(A) = \Sigma^* \setminus L(A_1)$ מספיק שהינו מגדירים A עם דוחה את w .

נווכיח כי $L(A) = L(A_1) \cup L(A_2)$. תהי $w = w_1 w_2 \dots w_n$ מילה ב- Σ^* ותהי $r = r_0 r_1 \dots r_n$ הריצה של A על w . נסמן $r_i = \langle q_1^i, q_2^i \rangle$ ותהי $r = r_0 r_1 \dots r_n$ הריצה של A על w . נסמן $s_1 = q_1^0, s_2 = q_2^0$ מהגדרת A , ותהי $r_i \geq 0$ ותהי $r_i = \langle q_1^i, q_2^i \rangle$ הריצה של A על w .

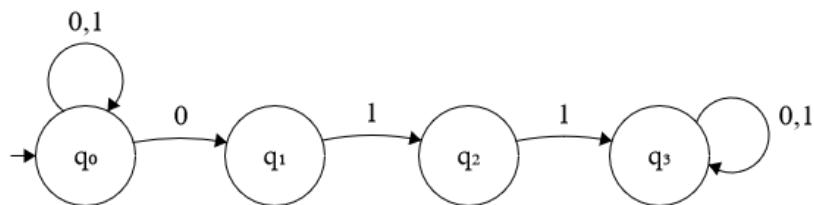
$$q_1^{i+1} = \delta_1(q_1^i, w_i), q_2^{i+1} = \delta_2(q_2^i, w_i)$$

ולכן $r^n = \langle q_1^n, q_2^n \rangle$ היא ריצה של A_1 על w ובהתאם $\rho_1 = q_1^0, q_1^1, \dots, q_1^n$ היא ריצה של A_2 על w . מכאן, r מקבלת אס"ם $r_1 \in F_1$ או $r_2 \in F_2$ או $r_1 \in F_1 \wedge r_2 \in F_2$.

הערה בדרכ להוכיח ש-REG סגור לשרשור, נתקעים בקשי הוכחתו. לכורה נפרק מילה לשני החלקים, נרץ כל חלק באוטומט המתאים לו ונסיים. הבעיה היא שלכל מילה יכולים להיות כמה פירוקים. לשם כך נוצר "לנחש" מותי לקפוץ.

אוטומטים אי-דטרמיניסטיים

דוגמה נביט באוטומט הבא,



איור 10 : אוטומט אי-דטרמיניסטי

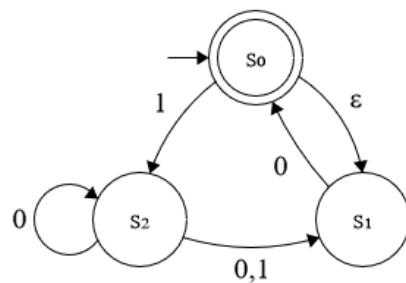
לכאורה פ' המעברים לא מוגדרת היטב עבור $0, q_0$, אבל כאן הרעיון הוא שהאוטומט יכול לבחור מתוך כמה אפשרויות בaczmo לאיזה מצב הוא עובר, כאשר מילה מתתקבלת ע"י האוטומט אם "ס" קיימת ריצה עם ניחושים כלשהם שמקבלת, ובמקרה כזה נגיד $\{q_0, 0\} = \{q_0, q_1\}$.

הגדרה אוטומט אי-דטרמיניסטי הוא אוטומט שבו פ' המעברים ממפה מצב ואות (או אפסילון) לקובוצה של מצבים אפשריים, כולל

$$\delta : Q \times (\Sigma \cup \{\epsilon\}) \rightarrow 2^Q$$

ומילה מתתקבלת אם "ס" קיימת ריצה מקבלת של A על המילה.

דוגמה נביט באוטומט הבא עם "צעד אפסילון",



איור 11 : אוטומט אי-דטרמיניסטי עם "צעד אפסילון"

המילים הבאות מתתקבלות: $0, 00, 00110, \epsilon$ (כי נוכל להשתמש קודם בצעד אפסילון במקום ליפול לבור דוחה מ- s_0) ואילו 00111 לא מתתקבלות.

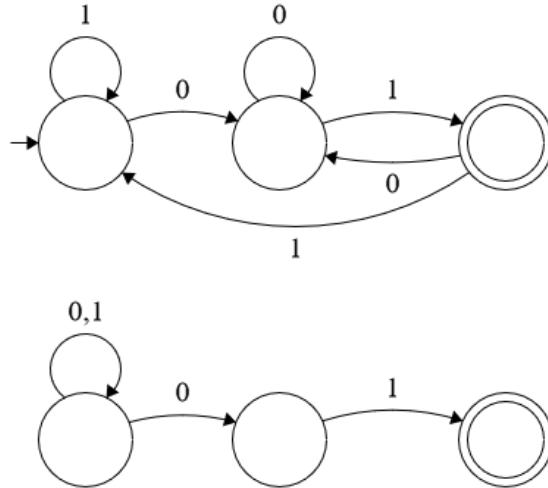
הגדרה אוטומט אי-דטרמיניסטי הוא חמשייה מהצורה $A = \langle Q, \Sigma, \delta, Q_0, F \rangle$ יכולה להיות כמה מצבים התחלתיים

$$1. \quad \delta : Q \times (\Sigma \cup \{\epsilon\}) \rightarrow 2^{Q-1}$$

ריצה של A על מילה $\sigma_n \dots \sigma_1 \sigma_2 \dots w = r_0 r_1 \dots r_m$ (כאשר $n \geq m$ בגל ריאודי אפסילון) כך שנitinן לכתוב את w כ- $x_m \dots x_2 \dots x_1$ כאשר $r_{i+1} \in \delta(r_i, x_{i+1})$ וכן $r_0 \in Q_0$ ומתקיים $x_i \in \Sigma \cup \{\epsilon\}$ בנגדוד L -ב-DFA. בנוסח, $r_m \in F$ מתקבל אם $w \in L$.

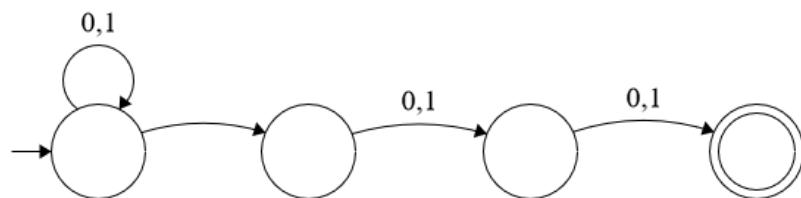
נאמר כי A מקבלת את w אם קיימת ריצה של A על w שמקבלת.

דוגמה מעל DFA $L = \{w : 0, 1\}^*$ מSTITימת ב-. $\Sigma = \{0, 1\}$. DFA שכול לו יותר פשוט,



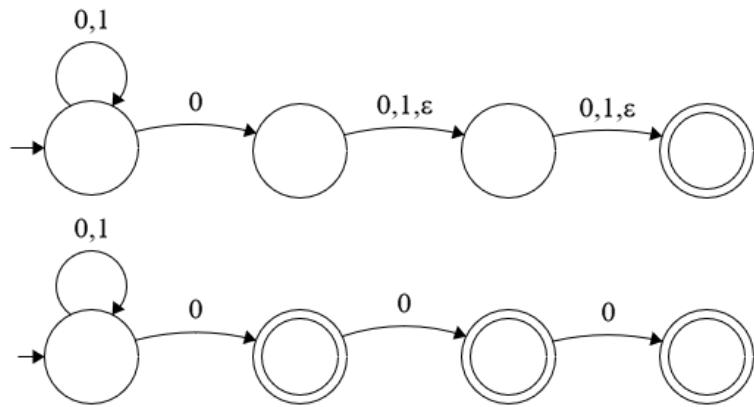
איור 12 : אוטומט דטרמיניסטי (למעלה) ואי-דטרמיניסטי (למטה) שמשרתים אותה המטרה

דוגמה עבור $\{w : 0(0+1)(0+1)\}^*$ האוטומט הבא מקבל אם מילה היא ב- L (הוכחה פורמלית פשוטהetailed בפיה),



איור 13 : אוטומט עם השפה הנ'ל

דוגמה עבור $\{0\}$ במקום הלפני לפני אחרון, הלפני אחרון או האחרון $L' = \{0, 00, 000, \dots\}$, האוטומטים הבאים הם בעלי השפה



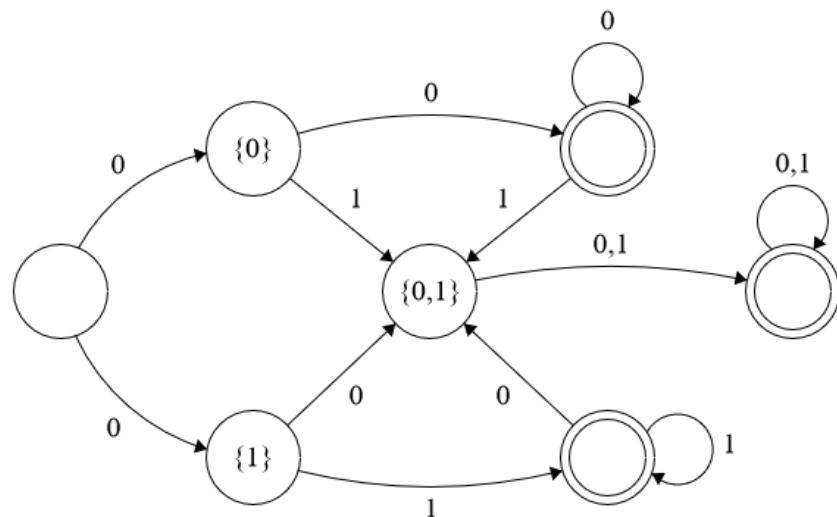
איור 14 : שני אוטומטים א-דטרמיניסטיים ששפתם L'

דוגמה מצבים התחלתיים רבים הם שימושיים לדוגמה במקרה של אוטומט המכפלת, שם אם היו יכולים להגיד כמה מצבים התחלתיים יכולים לעשות בניתה יותר פשוטה עם $Q = Q_1 \cup Q_2$.

הוכיחה לשפט בסוף הרצאה עבר לתחילת חלק ב' של הרצאה.

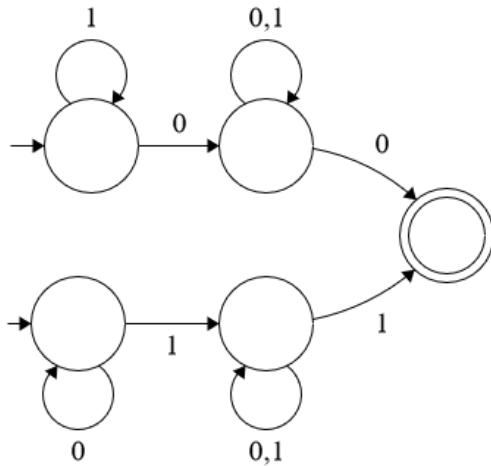
חלק ב' של הרצאה

דוגמה L היא השפה שבה כל המילים שהן האות האחורייה הופיע לפניכן במילה, מעל $\{0, 1\}^* = \Sigma$. ראו DFA שמתאים לה באירא



איור 15 : DFA שמתאים ל- L

ועתה NFA מתאים (שcoil), כאשר הרעיון כאן הוא שהחלק העליון מתאים לריצה שבה יש 0 אחד לפחות ובסוף 0 ולמטה זו כזו בהתאם שמסתיימות ב-1.



איור 16 NFA שמתאים ל- L

$$\text{משמעות לכל } A \text{ NFA קיים } A' \text{ DFA שקיים } L(A) = L(A')$$

הוכחה: בהינתן $\langle Q', \Sigma, q'_0, \rho, F' \rangle$. נבחר $A' = \langle Q', \Sigma, Q_0, \delta, F' \rangle$ וזו הרעיון הוא ש- $L(A) = L(A')$. נבנה $A = \langle Q, \Sigma, Q_0, \delta, F \rangle$ כך ש- $L(A) = L(A')$.

מגיע למצב S בדיאטה אחריו קריית w אם "ס" A יכול להגעה לביקורת כל המצביעים ב- S אחרי קריית w .

באופן אינדוקטיבי, $\delta^*(S, w \cdot \sigma) = \delta^*(\delta^*(S, w), \sigma)$ ובצעד ה- n -י $\delta^*(S, \sigma) = \bigcup_{s \in S} \delta(s, \sigma), \delta^*(s, \epsilon) = s$

נבחר $q'_0 = Q_0$ שהוא קבועה, אבל $q'_0 \in Q'$ כי Q' קבועה של קבועות ולכן זה בסדר.

$$\text{ונדר } \sigma \in \Sigma \text{ ו } s \in Q' \text{ רצוי } \delta(s, \sigma) = \bigcup_{s \in S} \delta(s, \sigma)$$

טענה לכל $w \in \Sigma^*$ מתקיים $(q'_0, w) = \delta^*(Q_0, w)$ או במילים, המצביע A' ש- w מוביל אליו קריית w (הצביע הוא קבועה בפני עצמו), שווה לקבועות המצביעים A יכול להיות בה (באחת הריצות שלו) על A .

נבחר $F' = \{S \in 2^Q : S \cap F \neq \emptyset\}$ כי אנחנו מקבלים אם הגיעו למצביע $-Q'$ אחד מ(תתי-)הצביעים שבו הם מקבלים (כי זה אומר שאנו יכולים להגיע אליו בדיאטה כלשהו של A').

נוכיח כי $(Q_0, w) \cap F' \neq \emptyset$ אם ויחי ריצה מקבלת של A על w אם ויחי ריצה מקבלת של A' על w .

הוכחה: (של הטענה המקוונת) באינדוקציה על w :

$$\text{בבסיס } \rho^*(q'_0, \epsilon) = q'_0 = Q_0 = \delta^*(Q_0, \epsilon) : (w = \epsilon)$$

$$\text{צעדים: } (|w| \rightarrow |w + 1|)$$

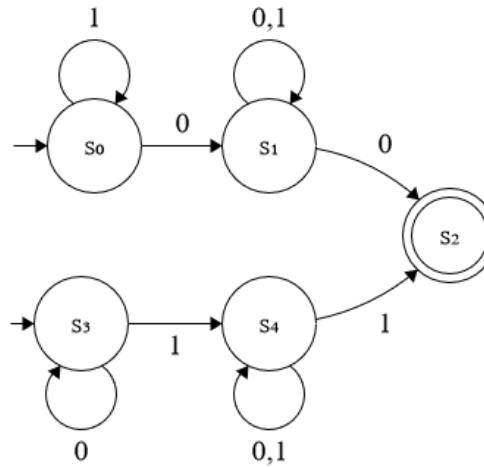
$$\rho^*(q'_0, w \cdot \sigma) = \rho(\rho^*(q'_0, w), \sigma) \stackrel{\text{הגדרת } \delta^*}{=} \delta^*(\rho^*(q'_0, w)) \stackrel{\text{עכשו}}{=} \delta^*(\delta^*(Q_0, w), \sigma) = \delta^*(Q_0, w \cdot \sigma)$$

■

■

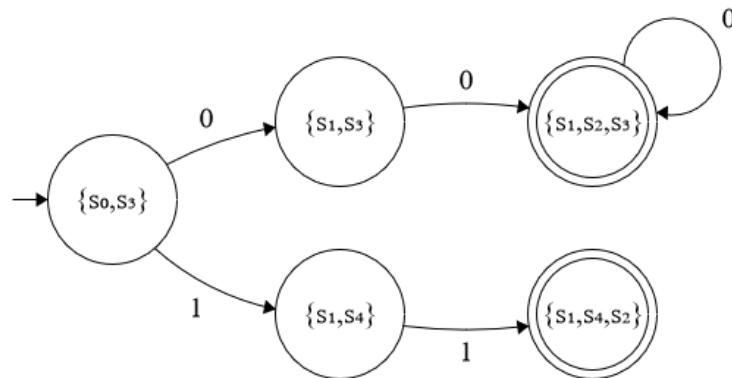
זה מסיים את ההוכחה כי השפות של האוטומטים שוות.

דוגמה בחרזה לדוגמה למעלה (מצורף איור נוסף), נמצא DFA מתאים לוזה (ນבצע דטרמיניזציה).



איור 17 : NFA שראינו למעלה

ה-DFA המתאים הוא כבאיור, כאשר הוא לא שלם כי יש 2^5 מצבים. הרעיון בכלל אופן הוא שבכל פעם אנחנו מסתכלים לאן כל אחד מהמצבים לוקח אותנו בהינתן אותן הנקודות ואוספים את-column לכדי מצב (כמו ההגדירה של ρ), ומשמעותו הוא מקבל אם הוא מכיל מצב שהוא מקבל ב-NFA.



איור 18 : חלקו שמתאים ל-NFA למעלה

תרגול

טענה לכל DFA $A = \langle Q, \Sigma, \delta, Q_0, F \rangle$ קיים DFA שקיים שפה B כך ש- B אין מעבר ϵ .

הוכחה: הרעיון הוא שנוכיח את כל הממצבים שעוברים אליו עם ϵ לאחד כל פעם ונראה שהוא שפה. נגיד

$$E(q) = \{s \in A \text{-lang} : \text{there is } \epsilon \text{ transition from } q\}$$

נשים לב כי תמיד $(q \in E) \neq \emptyset$ ובפרט $\emptyset \neq E(q)$ (לא לצוד מ- q זה כמו לצוד אפסילון מ- q כי לא קראנו כלום).

נגידר $B = \left\langle Q, \Sigma, \delta', \bigcup_{q \in Q_0} E(q), F \right\rangle$ כאשר הרעיון במצבים ההתחלתיים הוא כל המצבים שאפשר להגיע אליהם מ对照检查 התחלתי כלשהו רק בצעד אפסילון.

נגידר $E(s) = \bigcup_{s \in \delta(q, \sigma)} E(q, \sigma)$ כלומר כל מצב שאפשר להגיע אליו עם האות ומיברי אפסילון מ- q (בפרט זה כולל גם את מצבי (q, σ) המוקוריים).

לא נוכח נוכנות אבל כן נסביר למה הבניה הזו היא פולינומיאלית: אפשר לחשב כל $E(q)$ בזמן יעיל באמצעות DFS כאשר קשת קיימת בגרף
■ שלנו אם "ס היא מעבר אפסילון בין שני מצבים באוטומט.

טענה REG סגורה לאיחוד, כלומר אם $L_1, L_2 \in \text{REG}$ אז $L_1 \cup L_2 \in \text{REG}$

הוכחה: יהיו $Q_1 \cap Q_2 = \emptyset$ בהתאם. בה"כ אפשר לשנות DFA $A_1 = \langle Q_1, \Sigma, \delta_1, q_1, F_1 \rangle, A_2 = \langle Q_2, \Sigma, \delta_2, q_2, F_2 \rangle$ בזמנן ייעיל באמצעות DFS כאשר קשת קיימת בגרף את השמות, זה לא מעניין). נבנה B NFA לשפה $L_1 \cup L_2$ כך ש-

$$B = \langle Q_1 \cup Q_2, \Sigma, \delta, \{q_1, q_2\}, F_1 \cup F_2 \rangle$$

ו' המעברים מוגדרת ע"י

$$\delta(q, \sigma) = \begin{cases} \delta(q, \sigma) & q \in Q_1 \\ \delta_2(q, \sigma) & q \in Q_2 \end{cases}$$

כך, מילים מ- L_1 יוכלו להתקבל מריצות שמתחליות ב- q_1 ומילים מ- L_2 מתקבלות על ריצות החל מ- q_2 (למעשה יש לנו שני אוטומטים זרים שכל ריצה יכולה לבחר אויפה היא מתחילה).

נראה ש- $L(B) = L_1 \cup L_2$ באמצעות הכללה דו כיוונית.

תהי $w \in L_1 \cup L_2$ ובה"כ $w \in L_1$. הריצה של A_1 על w מקבלת ונסמנה $r_0, \dots, r_{|w|} \cdot w$. הריצה של A_1 על w מקבלת ונסמנה $r_0, \dots, r_{|w|} \cdot w$ ובה"כ $r_0 \in F_1$ ו- $r_{|w|} \in F_1$ ולכן $r_0 = q_1$ ו- $r_{|w|} \in F_1 \subseteq F_1 \cup F_2$ ולכן הריצה גם מקבלת, כלומר $w \in L(B)$ במקורה ש- $q \in Q_1$ וזה מתקיים לכל אורך המסלול ובנוסף $r_0 \in F_1 \cup F_2$.

תהי $w \in L(B)$, כלומר ריצה מקבלת של B על w שנסמנה $r_0, \dots, r_{|w|} \cdot w$. מהגדotta $r_0 \in \{q_1, q_2\}$ ונני בה"כ $r_0 = q_1$. היות ש- $r_0 \in Q_1$, כלומר r_0 מתקבל מ- i -ל- r_{i+1} נעשה דרך ה' δ_1 (δ_1 מוגדרת רק על מצבים $r_0, \dots, r_{|w|} \in F_1 \cup F_2$). בנוסח, $r_0 \in Q_1 \cap Q_2 = \emptyset$ ולכן $r_0 \in F_1 \cup F_2$. כלומר $r_0 \in F_1$ (לכן $r_0 \in F_1 \cup F_2$) ולכן $r_0 \in F_1$. ■

טענה REG סגורה לשרשור, כלומר אם $L_1, L_2 \in \text{REG}$ אז $L_1 \cdot L_2 \in \text{REG}$

הוכחה: הרעיון הוא שאפשר קפיצה (בניחס) מכל מצב מקבל ב- A_1 להתחלה של A_2 ואז כך ניתן לשרשור של מילים.

יהיו B NFA לשפה L_1, L_2 -ים ל- Σ -DFA $A_1 = \langle Q_1, \Sigma, \delta_1, q_1, F_1 \rangle, A_2 = \langle Q_2, \Sigma, \delta_2, q_2, F_2 \rangle$. נגידר $Q_1 \cap Q_2 = \emptyset$ בהתאמה. בה"כ $A_1 \cup A_2 = \langle Q_1 \cup Q_2, \Sigma, \delta, \{q_1\} \cup \{q_2\}, F_1 \cup F_2 \rangle$ יי"ע $L_1 \cdot L_2$ כאשר

$$\delta(q, \sigma) = \begin{cases} \delta_1(q, \sigma) & q \in Q_1, \sigma \in \Sigma \\ \delta_2(q, \sigma) & q \in Q_2, \sigma \in \Sigma \\ \{q_0\} & q \in F_1, \sigma = \epsilon \end{cases}$$

נוכיח הכלה דו כיוונית. הוכחה: $L_1 \cdot L_2 \subseteq L(B)$: תהי $w \in L_1 \cdot L_2$ כולם $y \in L_2 \cdot x = w$ כאשר ישן ריצות מקובלות של A_1 על x ושל A_2 על y , בהתאם נסמן $r_{|x|}, r'_0, \dots, r'_{|x|}, r_0, \dots, r_{|y|}, r'_0, \dots, r'_{|y|}$. נשים לב כי הריצה $r'_0, \dots, r'_{|y|}$ היא ריצה של B על y .

■ $w = x \cdot y$

$r_{|x|} = q_0$ הוא אכן מצב התחלתי- B ועד $r_{|x|}$ הריצה של B על x ממשיכה כמו זו של A_1 ומסתויימת ב- F_1 . מכאן יש מעבר $\delta(r_m, \epsilon) = \{q_2\}$ ומשם הריצה של B על החמש w שהוא בדיק y היא כמו זו של A_2 על y .

וזו מסתויימת ב- F_2 .

$L(B) \subseteq L_1 \cup L_2$: תהי $w \in L(B)$ ותהי $r_{|w|}, r_0, \dots, r_k$ ריצה מקבלת (כלשהי) של B על w . מתקיים $\{q_1\} \subseteq F_2$ ו- $r_{|w|} \in F_2$ ו- $r_0 = \{q_1\}$. מהגדרת B , כדי להגיע ל- F_2 חייב להיות קיים $k \in [|w|]$ השתמש במעבר ϵ ממצב ב- F_1 ל- F_2 . מהגדרת B , הריצה $r_k \rightarrow r_{k+1}$ על x שמסתויימת ב- F_1 ולכן זו נבייט במילים, הריצה r_k, r_{k+1}, \dots, r_0 היא ריצה של A_1 על x שמסתויימת ב- F_1 ולכן זו ריצה מקבלת של A_1 על x ולכן $x \in L(A_1)$.

באופן דומה, הריצה של B על y החל מ- r_{k+1} היא ריצה של A_2 על y שמסתויימת במצב מקבל ב- F_2 ולכן $y \in L(A_2)$.

טענה REG סגורה לפועלה Kleene-Star כלומר אם $L \in \text{REG}$ אז $L^* \in \text{REG}$

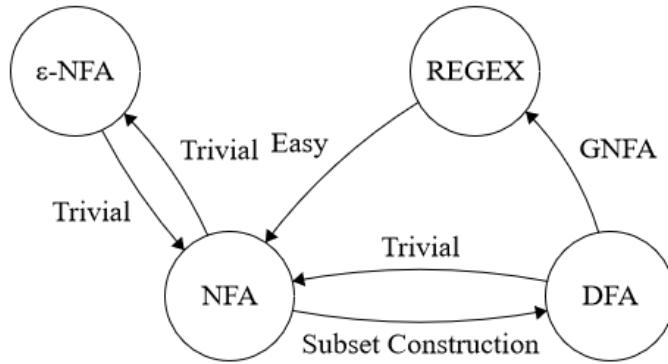
הוכחה: יהיו L DFA $A = \langle Q, \Sigma, \delta, q_0, F \rangle$. לכארה הינו יכולים לבנות NFA A' שהוא פשטוט עם חיבור מהמצבים הסופיים למצב התחלתי שובי עם צעד אפסילון. הבעה היא שם A לא מקבל את המילה הריקה, גם הבניה לא אבל $L^* \in \epsilon$. לכן נוסף מצב נוסף q_{start} שהוא יהיה המצב התחלתי היחיד שיש ממנו צעד אפסילון למצב התחלתי של A .

בנייה B NFA לשפה L^* “ $\exists \delta . q_{start} \notin Q \text{ כאשר בה } \delta \text{ מוגדרת ע”י}$

$$\delta'(q, \sigma) = \begin{cases} \{\delta(q, \sigma)\} & q \in Q \\ \emptyset & q = q_{start} \\ \emptyset & q = q_{start} \wedge \sigma = \epsilon \\ \{q_{start}\} & q \in F \wedge \sigma = \epsilon \\ \{q_0\} & q = q_{start} \wedge \sigma = \epsilon \end{cases}$$

■

הערה ראו איור של מבנים מבינים שקיים של אוטומטים, כאשר בקרוב נלמד על REGEX-ים.



איור 19 : מפת שקיים בין אוטומטים

שבוע III | שפות לא רגולריות ולמה הניפוח

הרצאה

חלק A' של הרצאה

הערה בהרצאה הקודמת הראנו איך לעשות דטרמיניטיזציה ל-NFA A' עם n מצבים, ל-DFA השקלול לו יש לכל היוטר

2^n מצבים (חסם עליון).

היום נראה שאין פולינום p שביחסו (כל) NFA עם n מצבים, יש לו DFA שקיים לכל היוטר (n) p מצבים (חסם תחתון).

מקרים פרטיים כמו כן יכולים להיות חסומים ע”י פולינום בגודלה שלהם כשם DFA, אבל שום בנייה לא תעבור לכל NFA אפשרי.

הערה לא מספיק שנראה, לדוגמה, שפה L כך שיש ל-NFA L עם 10 מצבים, אבל כל DFA עבור L צריך 2^{10} מצבים.

זה לא מוכיח שום דבר כי זה לא סותר את הפולינום $p, n > 2^{10}$ (10) שבעורו $= n^3 + 500$ וכאן הוא מצליח לחסום ε-NFA-ים כליהם (כמו כן שלא את colums).

משפט לכל פולינום p , קיימת שפה L כך של- L -NFA עם n מצבים וה-DFA הקטן ביותר עבור L צריך יותר (n) p מצבים.

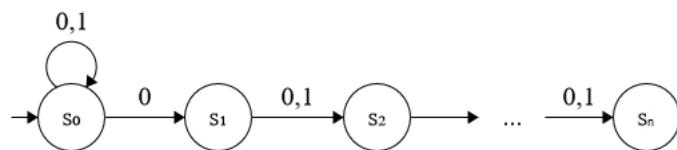
הוכחה: מספיק שנראה שלכל $1 \leq n$ קיימת L_n כך של- L_n -DFA עם $n+1$ מצבים אבל ה-DFA הקטן ביותר עבור L_n צריך לפחות 2^n מצבים.

כי אם בשלילה קיים פולינום כאמור, נתבונן ב- n_0 שモבטה שעבורו $(n_0 + 1) > p(2^{n_0})$ ונתבונן ב- L_{n_0} . שם ה-DFA הקטן ביותר עבור L_{n_0} מכיל $(n_0 + 1) > p(2^{n_0})$ מצבים כפי שנוכיח עכשו בסתרה לקיום פולינום שמייקם את התנאים.

$$\text{ນບחר } \Sigma = \{0, 1\}$$

$$L_n = (0+1)^* 0 (0+1)^{n-1} = \{w : 0 \text{ הוא } n\text{-ית מהסוף}\}$$

כאשר הביטוי משמאלו נקרא ביוטי רגולרי - 1, 0 כמה פעמים שנרצה (רישא), 0, ואז 1 או $n-1$ או 0. ראו איור של DFA מתאים לשפה,



איור 20: L_n -NFA

נניח בשלילה שיש DFA ש- L_n מ- 2^n מצבים. ישנו 2^n וקטורים באורך n מעל $\{0, 1\}$ ולכן 2^n מיללים שונים באורך n מעל הא"ב $\{0, 1\}$.

אם ב- D_n יש פחות מ- 2^n מצבים, אז מעקרון שובך היונים יש שתי מיללים $w_1 \neq w_2 \in (0+1)^n$ שעבורו D_n מגיע לאותו המצב בסוף קרייאתן. ופורמלית, עבור $D_n = \langle \{0, 1\}, Q, q_0, \delta, F \rangle$ כך ש-

$$q = \delta^*(q_0, w_1) = \delta^*(q_0, w_2)$$

מהיות $w_2 \neq w_1$, הרי שקיים $i \in [n]$ כך ש- $w_1[i] = 0, w_2[i] = 1$ ובה"כ $w_1[i] \neq w_2[i]$. נוכיח שהבקרה האוטומט טועה כי נשרש סיפה למילים כך ש- i יהיה האינדקס ה- n מהסוף ואז האוטומט מסוו את שתי המיללים באותה הדרך בניגוד לכך שאחת הווה אמרה לקבל והאחרת לדוחות (מהגדרת השפה). נתבונן ב- $s = \delta^*(q, 1^{i-1})$.

• אם D_n מקבל את $w_2 \cdot 1^{i-1}$ בסתרה לנכונות, שכן $w_2 \cdot 1^{i-1} \notin L$ (האות ה- n מהסוף היא 1).

• אם D_n לא מקבל את $w_1 \cdot 1^{i-1}$ בסתרה לנכונות, שכן $w_1 \cdot 1^{i-1} \in L$ והוא היחידה מגיעה ל- s .

כלומר הגיעו לסתירה בכל המקרים.

טענה אין DFA עבור $.L = \{0^n 1^n : n \geq 0\}$

הוכחה: נניח בשלילה כי $w = 0^p 1^p$ הוא DFA $A = \langle Q, \Sigma, q_0, \delta, F \rangle$ נtabون במילה $L(A) = L$. כלומר $|Q| = p$. מכאן הריצה של A על w , $w = q_0 q_1 \dots q_{2p}$, מתקבלת, כלומר $q_{2p} \in F$.

ברישא q_0, \dots, q_p יש מעגל, כלומר קיימים $l < j \leq p$ כך ש- $q_j = q_l$ (מעקרון שובך היוניים). לכן יש ל- A ריצה מקובל גם על $q_0 \dots q_l q_{j+1} \dots q_{2p}$ (כי אפשר לגזור את המעגל מ- l - j ולהסתכל על הריצה $q_0 \dots q_l q_{j+1} \dots q_{2p} \notin L$). ■

משפט (למה הניפוח לשפות רגולריות, pumping lemma) אם L רגולרית אז קיים $1 \geq p$ (קבוע הנפוח) כך שלכל מילה $w \in L$, אם $|w| \geq p$ אז קיימות חלוקה $w = x \cdot y \cdot z$ כך ש:

$$|x \cdot y| \leq p .1$$

$$(y \neq \epsilon) |y| > 0 .2$$

$$.xy^i z \in L, \forall i \geq 0 .3$$

הערה אם L סופית אז אפשר לקחת $1 = l + 1$ עבור l אורך המילה הארוכה ביותר ב- L ואז הלמה מתקינה באופן ריק.

דוגמה עברו $(0+1)^*$ ו- $0(0+1)$ נtabון במילה $w \in L$ (כל המילים שהאות הלא-אחרונה שלהם היא 0). ניקח $3 = p$ ונtabון במילה $w = x \cdot y \cdot z$ כאשר $x = \epsilon, |y| = 1, |z| = |w| - 1$ נבחר $z = w$ ומכובן $3 \neq y$ וכן $|x \cdot y| = 1 \leq i \geq 2$ כי $xy^i z \in L$, אבל $0 \leq |y| < 1$ ולכן $xy^i z \in L$ לשארת האות הלא-אחרונה ב- z , הלא היא 0.

הוכחה: תהי L שפה רגולרית. יהיו DFA A שモזה את L ובחר p להיות מספר המגבאים ב- A . נtabון במילה $w \in L$ עם $|w| \geq p$. בሪצה של A על w , יש מצב ש חוזר בקריאה p האותיות הראשונות, כלומר קיימים $l < j \leq p$ כך ש- $q_j = q_l$ (מעקרון שובך היוניים). נבחר x, y, z עיי' ו-

$$w = \frac{w_1 \dots w_j}{x} \frac{w_{j+1} \dots w_l}{y} \frac{w_{l+1} \dots w_n}{z}$$

ונראה שהתנאים של הלמה מתקינים. $l < j \leq p, |y| > 0$ כי $xy^i z \in L$ ו- $|x \cdot y| \leq p$ כי הריצה היא

$$q_0, \dots, q_j, (q_{j+1} \dots, q_l)^i, q_{l+1}, \dots, q_n$$

■ כאשר זו ריצה חוקית כי יש מעבר מ- q_l ל- $q_{l+1} = q_{j+1}$.

חלק ב' של הרצאה

הערה נוכל להשתמש בשילוט למת הניפוח כדי להוכיח ששפות חן לא רגולריות. אם למת הניפוח מספרת לנו ש- $\alpha \Rightarrow \alpha$ הוא שלכל $p \geq 1$, קיימת מילה $w \in L$ עם $|w| \geq p$ כך שלכל חלוקה $w = x \cdot y \cdot z$, אם $|x \cdot y| \leq p$ וגם $|y| > 0$, קיימים $i \geq 0$ כך $xy^i z \notin L$.

או בambilים, לכל קבוע ניוף קיימת מילה אורך מהקבוע כך שלא משנה איזו חלוקה נבחר עם $\epsilon \neq y$ ו- $p \leq |xy| \leq n$, אחד הניפורים של y לא בשפה.

את הבחירה על השיליה של שלושת התנאים עשינו כי זה נכון אבל אפשר היה גם לעשות שאם 3, מתקיימים אז 2 לא מתקיים.

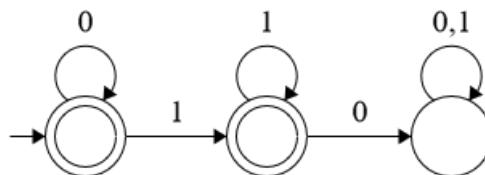
דוגמאות לשפות לא רגולריות

1. תהי $\{0^n 1^n : n \geq 0\} = L_1$. זו שפה לא רגולרית (ראינו כבר אבל גם) כי לכל p , נוכל להתבונן במילה $1^p 0^p$. לכל חלוקה $xyz = 0^p 1^p$ כז ש- $y = 0^{p+j} 1^j$ עבור $j \leq 1$ (אחרת xy זולג ל-1-ים ויצא שהוא ארוך מ- p). לכן, $|xy|^2 z = 0^{p+2j} 1^j \notin L_1$.

2. תהי $L_2 = \{w : \#_0 w = \#_1 w\}$ היא גם לא רגולרית. ההוכחה הנ'ל עובדת גם כן כי גם שם L יש דרכי אחרות בהינתן שידועו ש- L_1 לא רגולרית להוכיח ש- L_2 לא רגולרית.

• ניסיון 1: $L_2 \subseteq L_1$ לא רגולרית ולכן L_2 לא רגולרית - לא עובד: $(0+1)^*$ אבל האחורונה כן רגולרית (טריוויאלי).

• ניסיון 2: עבור $L_3 = 0^* 1^*$ קיים DFA שמצויה אותה (ראו אior). מתקיימים $L_1 = L_2 \cap L_3$ ומסגרות שפות רגולריות לחיתוך, ובע-ש- L_2 לא רגולרית (אחרת החיתוך שלו עם L_3 היה רגולרי בסתיו לכך ש- L_1 לא רגולרי).



איור 21: DFA ל- L_3

3. $L_4 = \{0^n 1^m : n > m\}$ לא רגולרית לפחות אינטואיטיבית. נוכיח זאת עם למת הניפור. בהינתן p , נתבונן במילה $0^{p+1} 1^p$ ובחלוקת xyz כז ש- $y = 0^j$ עבור $1 \leq j \leq p$. הניפור עם $i = 0$ מוציאה מהשפה (ניוף מטה), כי $0^{p+1-j} 1^p = xy^0 z = xz$

$$0^{p+1-j} 1^p = xy^0 z = xz$$

אבל $p+1-j \leq p$ וזה לא בשפה.

4. $L_5 = \{w \cdot w : w \in (0+1)^*\}$ היא לא רגולרית (אינטואיטיבית) ונראה זאת עם למת הניפור. בהינתן $1 \geq p$, נתבונן במילה $w = 0^p 1^p$ וכאן $|w| \geq p$. לכל חלוקה $xyz = w$ כז ש- $y = 0^j$ עבור $1 \leq j \leq p$ מתקיימים $|xy| \leq p$ ו- $|y| > 0$. נסמן $x = 0^p 1^0$ (כרגיל) ונתבונן $xy^2 z = 0^{p+j} 1^p$ שמדובר במילה לא בשפה (הצדדים שלו לא שווים).

5. $L_6 = \{a^p : p \text{ ראשוני}\}$ היא לא רגולרית (כלומר גם אין אפיון עם מספר מצבים סופי של המספרים הראשוניים). בהינתן p , יהיו q ראשוניים עם $p > q$. נתבונן במילה $a^q = w$ ותחי חלוקה $xyz = w$ כז ש- $y = 0^r$ ו- $0 < r < q$. נסמן $|x| = n$, $|y| = m$ ולכן $|z| = q - (n + m)$.

$$|xy^i z| = n + mi + q - (n + m) = m(i - 1) + q$$

עבור i מתקיים $|xy^iz| = m((q+1)-1) + q = (m+1)q = q+1$ כי זה פריק (0 $< m$ ולכן $(m+1) > 1$).

6. $\{w \in L_7 : w = xy^2z \text{ ו } |y| > 0 \text{ ו } |xy| \leq p\}$ נתבונן ב- $\Sigma = \{0, 1\}$ אז אם כי ה-1 לא באמצע.

תרגול

ביטויים רגולריים

הגדרה ביטוי רגולרי מעל א"ב Σ הוא אחד מה הבאים:

\emptyset •

ϵ •

$a \in \Sigma$ •

• t^* , t כאשר $s, t \in \text{ביטויים רגולריים קצרים יותר}$.

הערה דרך נוספת ליצוג ביטוי רגולרי מעל $\{a, b\}$ היא $.r := \emptyset | \epsilon | a | b | r \cup s | r \cdot s | r^*$

דוגמה נביט בביטויי מעל $\Sigma = \{a, b\}$. השפה שלו היא כל המילים שמכילות את הרצף $bb(a \cup b)^*$.

דוגמה הביטויי $(2^* \cup 1^*)^*$ מייצג את כל המילים שמתחלות באחד או יותר אפסים ונגמרות ברצף כלשהו של 1-ים או של 2-ים.

הגדרה בהינתן ביטויים רגולריים s, t, r , נגדיר את השפה שלהם כך:

$L(r) = \emptyset \text{ אם } r = \emptyset$ •

$L(r) = \{\epsilon\} \text{ אם } r = \epsilon$ •

$L(r) = \{a\} \text{ אם } r = a \in \Sigma$ •

$L(r) = L(s) \cdot L(t) \text{ אם } r = s \cdot t$ •

$L(r) = L(s) \cup L(t) \text{ אם } r = s \cup t$ •

טענה אם $L \in \text{REG}$ אז $L = L(r)$

הוכחה: \Rightarrow : יהיו r ביטוי רגולרי ונראה שקיים NFA A_r כך ש-סדרת היצורה של r (מספר התווים בכתיבת השפה של הביטוי הרגולרי, $\epsilon \in \Sigma$ באורך 1 לדוגמה).

• אם $r = \emptyset$ אז נבחר A_r להיות ריקה (ששפטו ריקה).

• אם $r = \epsilon$ אז ניקח את A_r להיות NFA ששפטו היא $\{\epsilon\}$ (לדוגמא אוטומט שהמצב ההתחלתי שלו הוא מקבל וכל אות מובילה לבור

דוחה).

- אם Σ או נבחר A_r להיות NFA שشرطו היא $\{a\}$ (מצב התחלתי לא מקבל, מעבר ממנו למצב מקבל רק על a וכל השאר לבור דוחה).

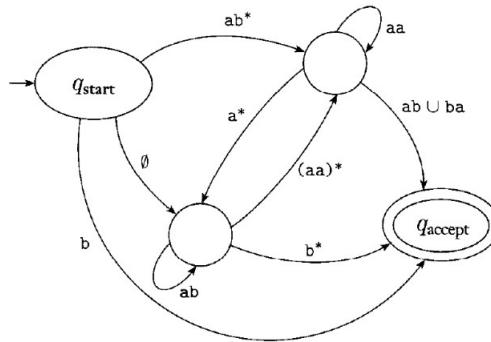
• אם $\cup t = s$ אז קיימים A_s, A_t מה"א וمسגורות לאיחוד קיים אוטומט $l(A_s \cup A_t)$.

• אם $s \cdot t = r$ אז קיימים A_s, A_t מה"א ומסגורות לשרשור, קיים אוטומט $l(A_s \cdot A_t)$.

• אם $t^* = r$ אז מה"א יש A_t שشرطו שווה לשל t ולכן מסגורות לפועלות הכוכב, קיים אוטומט $l(A_t)^*$.

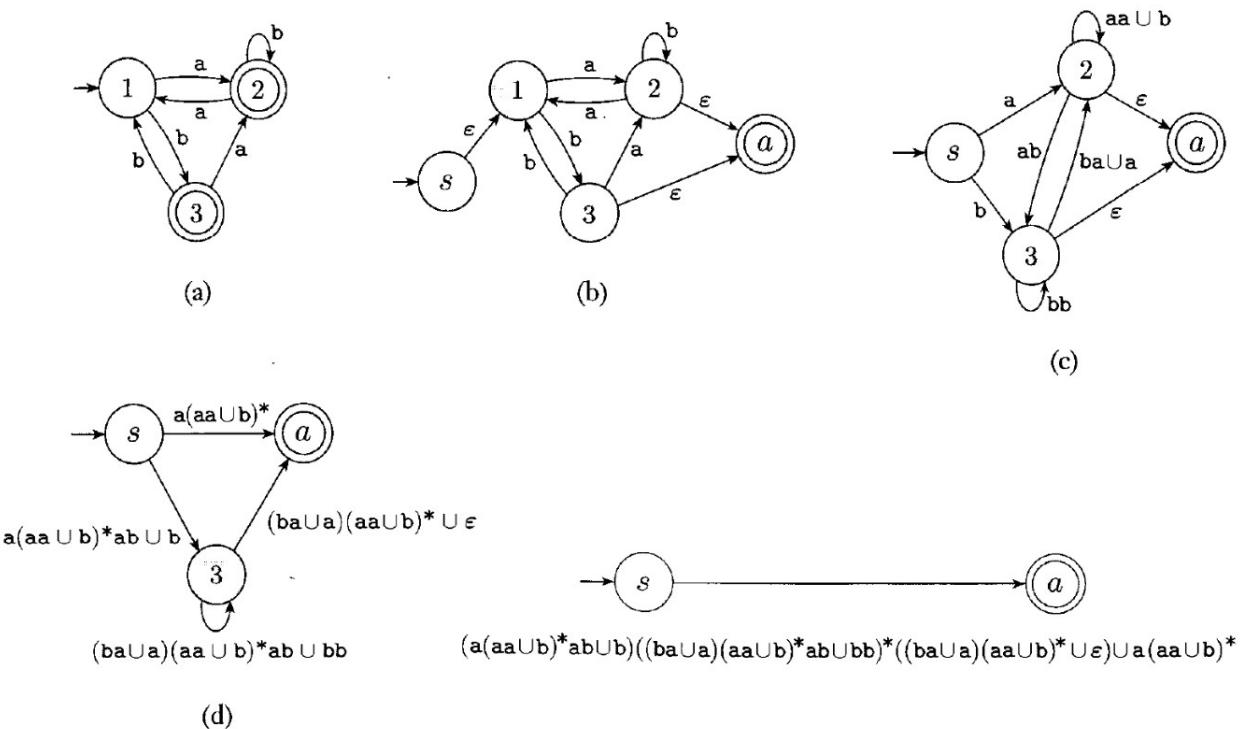
\Leftarrow : יהיו DFA ונוסח שקיים לו ביטוי רגולרי r עם שפה שcolaה. נוכיח בדוגמה של הרצת אלג' שמדובר DFA לביטוי רגולרי.

נניח שモתר לנו להשתמש ב-GNFA, שהוא NFA בעל קשרות עם ביטויים רגולריים במקום אוטיות. בנוספ', נניח של- A (או של- NFA המקביל לו) יש מצב התחלתי ומתקבל יחיד (כל באמצעות צעדי אפסילון), וכן שהמצב התחלתי והמקבל זרים (גם כל עם צעדי אפסילון). ראו דוגמה $,GNFA$ -ל.



איור 22 : דוגמה, אפשר לעبور בין קשרות ורק באמצעות מילה שעונה על הביטוי בקשת

עתה נעקוב אחר הדוגמה שלקומה מהתרגול כי אני לא מזוכיסט, ראו איור ואחריו הנחיה בנוגע למה אנחנו רואים.



איור 23 : LDוגמה, אפשר לעבור בין קשיות רק באמצעות מילה שעונה על הביטוי בקשתי

במעבר הראשון אנחנו מוסיפים את המצב ההתחלתי והמקבל החדש כדי לקיים את ההנחות שלנו.

במעברים הבאים אנחנו מוחקים מצבים (במקרה שלנו אחד כל פעם) ומחלאים מהם ביטויים רגולריים מתאימים עד שנישאר רק עם המצב ההתחלתי והמקבל החדש. נציג נימוקים כמה מהמצטומים האלה.

במעבר השני אנחנו מוחקים את :

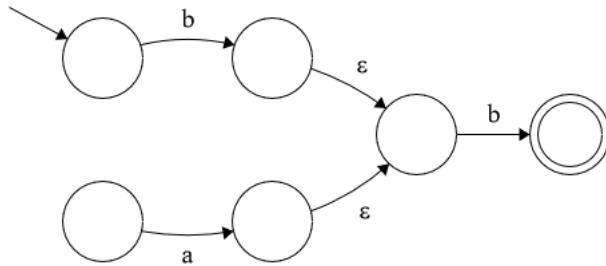
- ל-2 אפשר להגיע דרך 1 מ-s ולכן צמצמנו את צעד האפסילון ;
- מ-s ל-3 צריך b ואז רצף כלשהו של bb, لكن יש לנו קשת b וחוג של 3 עם קשת bb ;
- כדי להגיע מ-3 ל-2 אפשר או לлечת ישר באמצעות a, או לעبور דרך 1 באמצעות b ואז a, כולם a ∪ ba ∪ ab ∪ bb ∪ bb*
- בנוסף, אפשר להגיע מ-2 ל-3 באמצעות סיבוב דרך 3 ו-1 ולכן יש לו חוג סיבוב עצמו עם ערך b ∪ aa ∪ aabb ∪ abbb ∪ ...ל'

במעבר השלישי אנחנו מוחקים את :

- מ-s ל-a אפשר להגיע או דרך 2 באמצעות a ואיזושהי כמות של סיבובי סיבוב 2 באמצעות aa ∪ ab ∪ ... ∪ aabb ∪ abbb ∪ ...ל'
- מ-3 ל-a אפשר להגיע עם מספר כלשהו של bb זהה, או דרך 2 עם a ∪ ab ∪ ... ∪ aabb ∪ abbb ∪ ...ל' או ישר עם אפסילון .

הרידור האחרון לא מורכב מדי, הוא די ישיר מבחינת האינודים כי אין יותר מדי אפשרויות, רק לכתוב את זה זה נראה.

דוגמה $(a \cup b) \cdot b = b \cdot a \cup b \cdot b$, נוכל להרכיב אוטומט ל- $a, b, a \cup b$ ואז $b \cdot a \cup b \cdot b$, זהו כל אחת מהבנייה באיור השלם (שים לב שב- $b \cup a$ שני הזוגים משמאלי היו מקבלים אבל זה הוסר לטובת המצב הסופי).



איור 24 : מבטו הרגולרי הנ"

דוגמה תהי $L = \{1^{n^2} : n \in \mathbb{N}\}$. נראה ש- L לא רגולרית. לכן קיים קבוע ניוף p כך שלכל מילה $w \in L$ עם $|w| \geq p$ ניתן כתוב $w = xyz$ כך ש- y נקי $|y| > 0$, $|xy| \leq p$ ונבחר אותו כך ש- $x = 1^j, y = 1^k, z = 1^l$ כאשר $j + k < p$ ו- $w = 1^{p^2} \in L$. נכתוב $w = xyz$ כך ש- y נקי $|y| > 0$ ו- $w = 1^{p^2}$ נביט במילה $w = 1^j 1^{2k} 1^l$. נשים לב כי $xy^2z = 1^j 1^{2k} 1^l$.

$$p^2 < p^2 + k \leq p^2 + p < p^2 + 2p + 1 = (p+1)^2$$

כלומר $|xy^2z| < p^2$ ולכן $|xy^2z| < |xy^2z| < (p+1)^2$

דוגמה $L = \{w \in \{0,1\}^* : \#_0 w = \#_1 w\}$. נראה כי L לא רגולרית. בהינתן p קבוע ניוף, נבחר $w = 0^p 1^p$ ונכתוב $w = xyz$ כך ש- y נקי $|y| > 0$, $j + k < p$ כאשר $x = 0^j, y = 0^k, z = 0^l 1^p$. עבור $i = 2$, נקבל את הניוף $xy^2z = 0^{j+2k} 0^l 1^p$

$$xy^2z = 0^{j+2k} 0^l 1^p$$

וברוור שיש יותר אפסים מאחדים ולכן הניוף לא בשפה סטירה.

שבוע VII | משפט מייהיל-נורד

הרצאה

חלק א' של הרצאה

הזרה $\forall L \subseteq \Sigma^*$, נגיד יחס \sim_L על Σ^* ב- L שכל $x, y \in \Sigma^*$ מתקיים $x \sim_L y$ אם ויחד $x \sim_L y$.

הערה מילולית, $y \sim_L x$ אם לא משנה איזו מילה נבדיק לסוף של שתיהן, הן או שתיהן יהיו בשפה או שתיהן לא.

דוגמה $L = (0+1)^* 0 (0+1)^*$. במקרה כזה $1 \sim_L 0$ כי 0 זנב מפריד ($L \notin \text{ABEL}(00)$).

הזרה מילולית, $z \sim_L x \cdot y$ אם $z = 11 \cdot z \in L$, $1 \sim_L 11$ כי $z \in \Sigma^*$ מילולית אם והותם לפני אחורונה היא 0 .

$01 \sim_L \epsilon$ כי ϵ זנב מפריד (המילילים עצמן מופרדות כבר).

טענה לכל שפה $L \sim$ היה יחס שקולות.

הוכחה: רפלקסיביות: $\forall x . x \sim_L x$

סימטרי: $\forall x_1, x_2 \in \Sigma^* x_1 \sim_L x_2 \iff x_2 \sim_L x_1$ כי התנאי עצמו סימטרי.

טרנזיטיביות: $\forall x_1, x_2, x_3 \in \Sigma^* x_1 \sim_L x_2 \wedge x_2 \sim_L x_3 \implies x_1 \sim_L x_3$ כי אם בשליליה $x_1 \sim_L x_2 \wedge x_2 \sim_L x_3 \implies x_1 \sim_L x_3$ מתקיים גם $x_1 \sim_L x_2 \wedge x_2 \sim_L x_3 \implies x_1 \sim_L x_3$ כי אם בשליליה $x_1 \sim_L x_2 \wedge x_2 \sim_L x_3 \implies x_1 \sim_L x_3$ קיימים z כך $x_1 \cdot z \in L \iff x_2 \cdot z \in L \iff x_3 \cdot z \in L$ אבל $x_1 \cdot z \in L \iff x_2 \cdot z \in L \iff x_3 \cdot z \notin L$

$$x_3 \cdot z \notin L \iff x_1 \cdot z \in L \iff x_2 \cdot z \in L \iff x_3 \cdot z \in L$$

סתירה. ■

הערה נסמן $[w]$ מחלקת השקולות של המילה w .

דוגמה עבור L הנ"ל, נמצא את מחלקות השקולות של היחס \sim_L .

ϵ לא מקיימים את היחס, והמילה 1 מפרידה ביןיהם. מתקיים $[\epsilon] = [\epsilon \cdot 0] = [0 \cdot \epsilon] = [00]$ מחלוקת חדשה, ושה"כ המחלקות הן 01 גם מחלוקת חדשה, ושה"כ המחלקות הן 10 גם מחלוקת חדשה, ושה"כ המחלקות הן 01.

$$[0] = 0, \Sigma^* 10 \quad [\epsilon] = \epsilon, 1, \Sigma^* 11 \quad [00] = \Sigma^* 00 \quad [01] = \Sigma^* 01$$

הערה נשים לב כי אם $x_1 \sim_L x_2$ וגם $x_2 \sim_L x_3$, אז x_3 מפריד בין x_1 ו- x_4 , אך מתקיים $x_1 \sim_L x_4$.

ניתן לראות זאת בדוגמה הנ"ל עבור $10 \sim_L 01 \sim_L 101 = \epsilon \cdot 101 \sim_L 101 \cdot \epsilon = 101 \sim_L 01$ בין היתר בוכות ϵ .

משפט (מייהיל-נווד) $\Sigma^* \subseteq L \in \text{REG} \iff \exists L \sim \text{מספר סופי של מחלקות שקולות}$.

הוכחה: \Rightarrow : נניח של \sim_L יש מספר סופי של מחלקות שקולות. נגיד $A = \langle \Sigma, Q, q_0, \delta, F \rangle$ DFA שעבורו נבחר

• מחלקות השקולות של \sim_L .

$$\bullet .q_0 = [\epsilon]$$

$$\bullet .\delta([w], \sigma) = [w \cdot \sigma]$$

$$\bullet .F = \{[w] : w \in L\}$$

נשים לב שהגדרה של F , δ , לא תלולה בבחירה הנציג (w) כי הרבה מאוד מצבים הם בעלי אותו נציג (אם $w \sim_L y$ אז $\forall z$ כי אחרת z מפheid של w , y).

טכnic שלכל $w \in L$, $\delta^*(q_0, w) = [w]$, $w \in \Sigma^*$ וכאן מהגדרת δ^* (q_0, w) = $[w]$, $w \in \Sigma^*$ ונסיים. באינדוקציה על $|w|$.

בסיס ($q_0, \epsilon) = q_0 = [\epsilon]$ $w = \epsilon : (w = \epsilon)$

צעד ($|w| \rightarrow |w| + 1$)

$$\delta^*(q_0, u \cdot \sigma) = \delta(\delta^*(q_0, u), \sigma)$$

$$\stackrel{\text{חגורה}}{=} \delta([u], \sigma)$$

$$\stackrel{\text{חגורה}}{=} [u\sigma]$$

נניח ש- A DFA הוא L שמזז את L ונראה ש- $L \sim_A$ מספר סופי של מחלקות שיקילות. נ חסום את המספר הזה עם מספר המצביעים ונסיים.

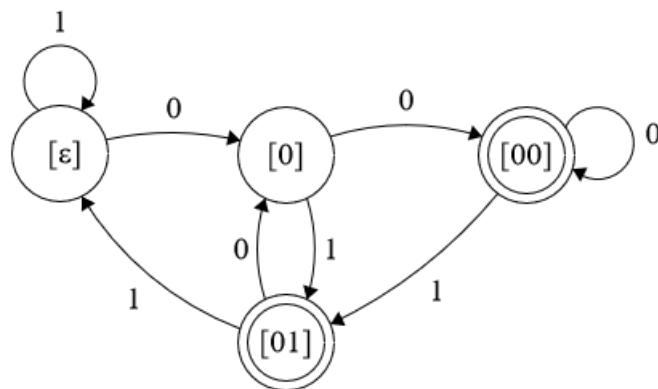
וגדר יחס \sim_A ונאמר כי $x, y \in \Sigma^*$ אם $x \sim_A y$ אם $\exists z \in \Sigma^*$ xz, yz נגשות אחרי x, y ומשם ממשיכות יחד בריצעה על z וכן תמיד יגיעו באותו מקום, וכן אם $x \sim_A y$ אז אין להן זנב מפheid כי xz, yz נגשות אחרי x, y ופומלית, אם $x \sim_A y$ אז $\forall z \in \Sigma^*$ $x \sim_A y$

$$\delta^*(q_0, xz) = \delta^*(\delta^*(q_0, x), z) = \delta^*(\delta^*(q_0, y), z) = \delta^*(q_0, yz)$$

ולכן $x \sim_L y$ ולכן $xz \in L \iff yz \in L$

מכאן שמספר מחלקות השיקילות של $L \sim_A$ חוסם את מספר מחלקות השיקילות של L , והראשון חסום ע"י $|Q|$ וכן גם האחרון ולכן הוא סופי. ■

דוגמה נפעיל את המשפט על הדוגמה הנ"ל ($L = (0+1)^* 0 (0+1)^*$)



איור 25 : אוטומט שמתאים לשפה L

כאשר בינו כל קשת ע"י בדיקה של היקן נמצא הנציג יחד עם האות על הקשת, לדוגמה [01] עם 0 חולך ל-0 כי 010 הוא בחלוקת השקלות של 0, ושאר הקשיות בהתאם.

שימושים של משפט MN

1. סיווג REG או לא REG.

דוגמה $L = \{0^n 1^n : n \geq 0\}$ אינה רגולרית כי $0^i 1^i \in L$ כי $i \geq 0$ ו- 0^j זנב מפ прид ($0^j 1^j$ לא) ולכן יש אינסוף מחלקות שקלות ל- \sim_L וסימנו.

דוגמה $L = \{0^i 1^j : \gcd(i, j) \neq 1\}$. נראה שעבור שני ראשוניים, $p_1 \neq p_2$ (כאן $0 = j$). נשים לב כי 1^{p_1} הוא זנב מפ прид (כי $1^{p_1} \in L$ אבל $0^{p_2} \notin L$ לא). لكن ל- \sim_L מ"ש.

2. מצוצים/מזרע DFA-ים.

הרעיון הוא שאם לאוטומט יש יותר מצבים ממחלקות שקלות ל- \sim_L , אפשר למצוץ את ה-DFA עוד. נראה אלג' שבנהנו DFA $A = \langle \Sigma, Q, q_0, \delta, F \rangle$ נחיזיר A' DFA שקול ל- A כך שלכל DFA A'' $|A'| \leq |A''| \leq |A|$ אם $A'' = L(A)$ או $A'' \neq L(A)$. מעבר לכך, נראה שאוטומט זה הוא ייחד עד כדי שמות.

מזרע אוטומטיים

נדיר סדרה של יחסים $Q \times Q$ נ�זרו הוא ש- $s_i \sim s_j$ אם $\exists z \in \Sigma^*$ $\forall i \geq 0, \sim_i Q \times Q$ $\delta^*(s_i, z) = \delta^*(s_j, z)$. הרעיון הוא ש- $s_i \sim s_j$ אם מילים עד אורך i מתקבלות (כשהריצה מתחלפת מהה').

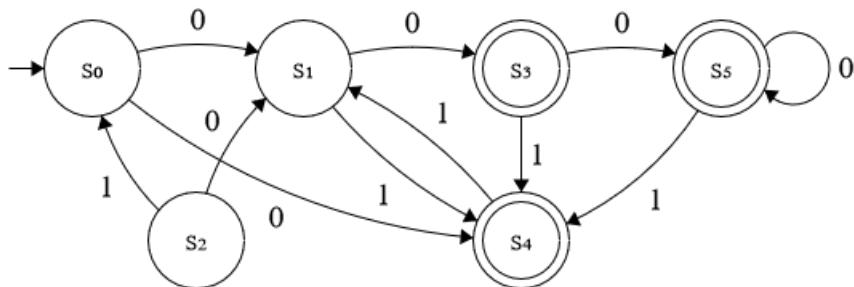
כלומר אינטואיטיבית $s_i \sim s_j$ אם מילים עד אורך i מתקיימים על אילו מילים עד אורך j מתקבלות (כשהריצה מתחלפת מהה'). מתיישהו נPsiק לעין את מחלקות השקלות ומחלקות השקלות שנקבעו לנו את המצבים ל-DFA המינימלי.

הגדרה נגידר את הסדרה \sim באופן אינדוקטיבי.

בבסיס ($i = 0$) $s_0 \sim s_0$ אם $\delta(s_0, z) = \delta(s_0, z)$ לוייש לו שתי מחלקות שקלות, כל המקבילים וכל הלא מקבילים).

צעד ($i \rightarrow i + 1$): נגידר $s_0 \sim s_1 \sim \dots \sim s_i$ אם $\delta(s_0, z) = \delta(s_1, z) = \dots = \delta(s_i, z)$ ($\forall z \in \Sigma^*$ כלומר אם מילים באורך i גם על כל הארכה באורך $i + 1$).

דוגמה נביט באוטומט הבא שモזהה את השפה $L = (0 + 1)^* 0 (0 + 1)^*$



איור 26: אוטומט שמתאים לשפה L

$$\{\{s_0, s_1, s_2\}, \{s_3, s_4, s_5\}\}$$

עבור מילים באורך 1, נעדן את מחלקות השקלות. האם $s_1 \sim_0 s_0 \sim_0 s_3 = \delta(s_0, 0) \sim_0 \delta(s_1, 0)$ ולכן $s_1 = \delta(s_0, 0)$? מתקיים $s_1 \sim_0 s_0$? מתקיים $s_0 \sim_0 s_1$? אבל $s_3 = \delta(s_1, 0) \sim_0 s_0$? התשובה היא לא. עם זאת $s_2 \sim_1 s_0$ כן מתקיים כי הפעלה של 0 ו-1 מובילות אותנו לeltsים שהם באותה מחלוקת שקלות בהתאם.

אחרי חישוב מקבלים שמחלקות השקלות \sim_{-1} הן

$$\{\{s_0, s_1\}, \{s_2\}, \{s_3, s_5\}, \{s_4\}\}$$

ואז עבור \sim_2 מקבלים את אותה מחלוקת שקלות ושם נעזרו (הגענו לנקודת שבת) ואכן ארבעת המחלוקות הללו נותרות לנו אוטומטית. מזערנו.

חלק ב' של הרצאה

نبיאו בסדרת היחסים שהגדנו \sim_i (שכל אחד מהם אוסף זוגות שלeltsים). בהכרח שעבור i גדול מסביר, נקבל $\sim_{i+1} = \sim_i$ (שווין בין קבוצות המוכילות ב- $Q \times Q$) כי אם $s_2 \sim_2 s_1 \sim_{i+1} s_1$ אז $s_2 \sim_{i+1} s_1$ ולכן $\sim_i \subseteq \sim_{i+1}$. מכאן שאנו הגיענו לנקודת שבת וنعוזר, או שהורדנו לפחות זוג אחד מ- \sim_i , ולכן תוקן לכל היותר $|Q|^2$ איטרציות נעוזר. בנוסף, המעבר מ- \sim_i ל- \sim_{i+1} מתבצע בזמן פולינומייאלי, שכן יש מספר פולינומייאלי של זוגות (לכל היותר $|Q|^2$) וחישוב האם זוג עבור ליחס הבא או לא דורש זמן קבוע.

טענה לכל $0 \leq i \leq Q-1$ $s_1, s_2 \in Q$ אם $\delta^*(s_1, w) \in F \iff \delta^*(s_2, w) \in F$, w באורך i .

הערה בתרגיל נוכיח שזה מספיק כדי להראות שמחלקות השקלות מהוות מצלבים לאוטומט המזערוי.

הוכחה: נראה באינדוקציה על i :

בסיס ($i = 0$): $w = \epsilon$. מההגדרה $\delta^*(s_1, \epsilon) = s_1 \in F \iff \delta^*(s_2, \epsilon) = s_2 \in F$.

צעד ($i \rightarrow i + 1$):

\Leftarrow : נניח ש- \sim_{i+1} נוכיח לכל מילה w , אם $\delta^*(s_1, w) \in F$ אז $\delta^*(s_2, w) \in F$.

• אם $w = \epsilon$ ו- $s_1 \sim_{i+1} s_2$ ולכן $\delta^*(s_1, \epsilon) = s_1 \in F \sim_{i+1} \delta^*(s_2, \epsilon) = s_2 \in F$.

• אם $w = \sigma y$ ו- $\delta^*(s_1, \sigma) \sim_i \delta^*(s_2, \sigma)$ ו- $\delta^*(s_1, y) \sim_{i+1} \delta^*(s_2, y)$.

$$s'_1 = \delta(s_1, \sigma) \sim_i \delta(s_2, \sigma) = s'_2$$

ולכן מה"א (עבור y שהיא באורך i)

$$\delta^*(s'_1, y) \in F \iff \delta^*(s'_2, y) \in F$$

ולכן

$$\delta^*(s_1, \sigma y) = \delta^*(\delta(s_1, \sigma), y) \in F \stackrel{\text{חכימתי}}{\iff} \delta^*(\delta(s_2, \sigma), y) \in F = \delta^*(s_2, \sigma y)$$

כלומר w מקיימת את התנאי.

\Rightarrow : נניח s_2, s_1 מסכימים מילים עד לאורך $i+1$ ונווכח $s_2 \sim_{i+1} s_1$.

נניח בשלילה $s_2 \sim_{i+1} s_1$. לכן או $s_2 \sim_i s_1$ או קיימת $\Sigma \in \sigma$ כך $\sigma \sim_i \delta(s_2, \sigma)$ (מההגדירה).

אם $s_2 \sim s_1$, קיימת מילה y באורך i כך $\sigma \sim_i \delta(s_1, y) \sim_i \delta(s_2, y)$ לא מסכימים על מילה באורך i סתירה.

אם קיימת σ כך $\sigma \sim_i \delta(s_1, \sigma), \delta(s_2, \sigma)$ אז $\delta(s_1, \sigma), \delta(s_2, \sigma) \sim_i \delta(s_2, \sigma)$ הם מצבים לא ביחס \sim ולכן מה"א הם לא מסכימים על השפה עד אורך i .

כלומר, קיימת y עם $|y| \geq i$ כך $\sigma \sim_i \delta(s_1, y), \delta(s_2, y) \in F$ אבל $\delta(s_2, y) \notin F$ בסתירה לכך s_2 מסכימים על מילים באורך $i+1$.

■

תרגול

טענה תהי $f : \mathbb{N} \rightarrow \mathbb{N}$ מונוטונית עולה ממש כך $\forall n \in \mathbb{N}, f(n)$ היא אזי השפה $L_f = \{a^{f(n)} : n \in \mathbb{N}\}$ לא רגולרית.

הוכחה: נשטמש בלמת הניפוח ע"י מציאה לכל n , מילה באורך בין $f(n+1) - f(n)$ ונסיים.

טענת העזר תהי $f : \mathbb{N} \rightarrow \mathbb{N}$ אזי $\forall K, N \in \mathbb{N}$ קיים $n > N$ כך $f(n+1) - f(n) > K$. כלומר נצליח לחסום ממתחת את ההפרשיות בין האיברים, עבור מספרים מסויק גדולים).

הוכחה: (של טענת העזר) נניח בשלילה שלא קיימים, لكن קיימים $K, N \in \mathbb{N}$ שעבורם $M \in \mathbb{N}$ כך $f(n+1) - f(n) \leq M$ $\forall n > N$. (מקסימום ההפרשיות עד N).

לכן מתקיים $f(n) \leq (n-1)M + f(1)$ ובצעד ה- $n-1$, $f(3) \leq f(2) + M \leq f(1) + 2M$, ועוד $f(2) - f(1) \leq M$ ולכן

$$\frac{f(n)}{n} \leq \frac{n-1}{n}M + \frac{f(1)}{n} \xrightarrow{n \rightarrow \infty} M + 0$$

ולכן ממונותוניות הגבול, $\lim_{n \rightarrow \infty} \frac{f(n)}{n} \leq M$ בסתירה לכך הגבול הזה הוא ∞ מהגדרת ω .

נחוור לטענה. נניח בשליליה שלמת הניפויה מתקיימת ויהי $0 < p < n$ שמתענתה
 $N = K = p$ קבוע הניפויה. נבחר $m > 0$ ו- $l + m \leq p$, $l + m + s = f(n)$. נבחר $w = xyz = a^l a^m a^s$ כאשר $f(n+1) - f(n) > k$
 $\text{נביט ב-} z \mid xy^2z = f(n) + m \cdot xy^2z$ ומתקיים

$$f(n) < f(n) + m \leq f(n) + p < f(n+1)$$

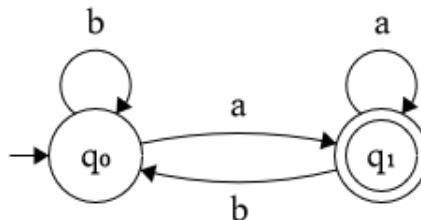
כאשר המעבר הראשון והשני נובעים מהתנאים של למת הניפויה על l, m והמעבר השלישי נובע ממתענתה העוזר ($K = p$). לכן $L \notin L$ בסתיויה למת הניפויה.

למעשה המעבר המהותי הוא שנייפחנו ב- m את המילה, אבל m קטן מאשר החסם התיכון שמצאנו להפרש ולכן הוא לא במילה.

הערה בכתיבה מתמטית נטו, יחס השקילות שמודדר במייהיל-נרווד מוגדר באופן הבא,

$$\forall x, y \in \Sigma^* (x \sim_L y \iff (\forall z \in \Sigma^*, xz \in L \iff yz \in L))$$

דוגמה נביט בשפה $\{w \in \Sigma^* \mid w \text{ מסתויימת ב-} a\} = L = \{w \in \Sigma^* \mid \{a, b\}^* : a\}$. היא רגולרית כי האוטומט הבא מזזה אותה.



איור 27 : אוטומט שמתאים לשפה L

nocich zat um MN. Nastcel ul milimim shpah avon shiyiti.

- אם $x, y \in \Sigma^*$ מסתויימות ב- a : $xz \in L$ אם z או $sh-z$ עצמה מסתויימת ב- a (זהו אותו התנאי על y) ולכן $y \sim_L x$ וזו מחלוקת שקיילות אחת.
- אם $x, y \in \Sigma^*$ לא מסתויימות ב- a : $xz \in L$ אם z מסתויימת ב- a (באותו האופן על y) ולכן $y \sim_L x$ וזה עוד קבוצה במחלקה שקיילות, עדין לא ידוע אם שונה מהקבוצה.
- אם x לא מסתויימת ב- a ו- y מסתויימת ב- a : $y \sim_L x$ כי $y = z$ זנב מפheid, ולכן שתי מחלוקות השקיילות הנ"ל שונות ומיפינו את כל המרכיב לשתי מחלוקות שקיילות.

דוגמה נביט בשפה $\{w \in \Sigma^* \mid w \text{ מאורך שאינו חזקה של } 2\} = L$. מעל $\{\}$ = Σ . ראיינו שהמשמעות של השפה זו היא לא רגולרית ולכן נצפה גם זו תהיה (אחרת נוכל לבנות אוטומט עם מצבים מקבלים הופכים).

נראה ש- L לא רגולרית ע"י מציאת אינסוף מחרט L ו- Σ^* (ולא ב- L אבל זה לא מעניין). נשים לב שעבור $x = a^{2^n}, y = a^{2^m}, z = a^{2^{n-m+1}}$ נקבל $xyz \in L$ אבל $yz = a^{2^{n-m}} \notin L$ ולכן $xyz \not\sim_L$. לעומת זאת, לכל $n > m, x, y, z$ כנ"ל מוצאות במח"ש שונות ויש אינסוף זוגות מספרים כאלה ולפניהם יש ∞ מחרט L .

תרגיל יהי $\langle Q, \{0, 1\}, q_0, \delta, F \rangle$ DFA. מה מבאים נכוון בהכרח?

$$0^*1^* \subseteq L(A) \quad .1$$

$$L(A) \subseteq 0^*1^* \quad .2$$

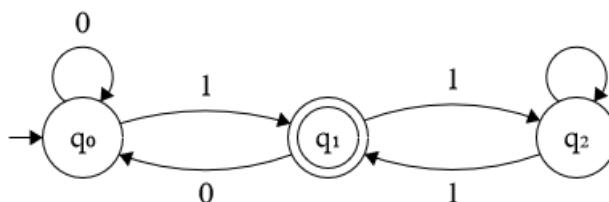
$$0^{ir}1^{ir} \in L(A) \quad .3$$

$$0^{r+ik}1^{r+k} \in L(A) \quad .4$$

פתרון (1) לא נכוון כי אוטומט עם שני מצבים לשפה שמקילה את כל המיללים עם מספר זוגי של אפסים. אוטומט כזה קיבל את 0011 אבל לא את 00111.

(2) לא נכוון כי עברור האוטומט הנ"ל, $L \in \{010\}$ (מספר זוגי של אפסים) אבל $0^*1^* \notin L$.

(3) לא נכוון כי עברור האוטומט באյור, שעבורו $0^31^3 \in L(A)$, מתקיים 0^61^6 . זה מושם*ן* 0^31^3 הגיע עד q_2 ויחזר ל- q_1 , ואילו 0^61^6 הגיע עד q_2 וילך הלוך ושוב וייסים ב- q_2 ולא יוכל.

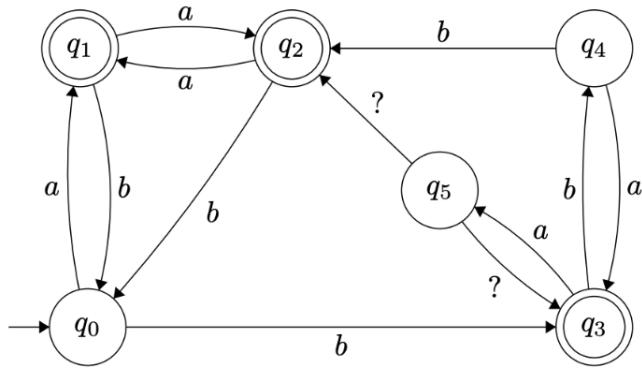


איור 28 : אוטומט שיפוריך את (3)

(4) כן נכוון, נוכחות עם למת הניפוי. בריצות על המיללים 0^r ו- 1^r , יש מצב ש חוזר על עצמו (לפחות אחד) ולפניהם בריצה על 0^r יש מעגל באורך k_1 ובבריצה על 1^r יש מעגל באורך k_2 .

את המעגלים האלה נוכל לשכפל עוד ועוד ולהגיע לאותו המצב. נביט בריצת A הדומה לו על 0^r1^r אבל ריצה על המעגל של ik_20^r פעמים ועל המעגל של ik_11^r פעמים. נסמן $k = k_1k_2 = ik$ וזו הטענה מתקבלת (הוספנו ל- ik אפסים וגם ל- ik אחדות ונשארנו בשפה).

תרגיל נתון ה-DFA כבאיור, A ,



איור 29 : האוטומט A לתרגיל

נתון כי $L(A)$ יש 4 מילים MN. מה אמור להיות במקומות סימני השאלה באיור?

$$1. \delta(q_5, a) = q_2, \delta(q_5, b) = q_3$$

$$2. \delta(q_5, a) = q_5, \delta(q_5, b) = q_2$$

3. (1) ו-(2) נכונות.

4. כל התשובות לא נכונות.

פתרון נשים לב שמקבץ של- A מילים MN, האלג' המצויץ אמור לאחד מצבים עד שנגיע ל-4.

- הצעד הראשון באלג' יגיע למילים $(F \setminus \{q_1, q_2, q_3\})$, $\{q_0, q_4, q_5\}$.

- השלב השני יפריד עם זנב a לפחות q_0, q_4, q_5 ו- $\{q_1, q_2\}$, $\{q_3\}$ עברו תשובה ל-

- בשלב השלישי, ab לא יפריד לנו שום דבר. עברו זנב aa , q_4 קיבל $\{q_1, q_2\}$, q_5 קיבל $\{q_3\}$, q_0 קיבל $\{q_0, q_4\}$. q_4 הגיע למינימלי.

כאן נעבור כי הגענו ל-4 מחלקות שקולות ובגלל שתשובות (2), (1) מקיימות את המילוי q_0, q_4, q_5 הלא, אלה התשובות הנכונות ולכן (3) היא התשובה הנכונה.

הערה נשים לב שאם היינו בוחרים זנבות אחרים, היינו יכולים להציג מחלקות שקולות שונות.

שבוע VII | שפות חסרות הקשר

הרצאה

חלק א' של הרצאה

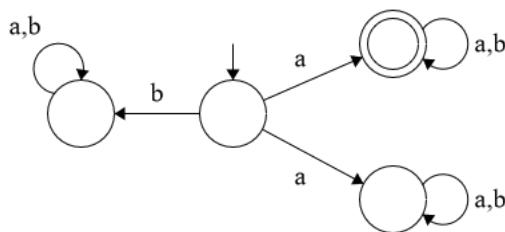
הערה בהרצאה הקודמת ראיינו איך למצער אוטומט דטרמיניסטי. כיצד נוכל למצער NFA? אם אנחנו יודעים להכריע האם קיים NFA שקיים k מצבים, נוכל לעבור על כל $N \in \mathbb{N}$ עד שנענה כן וזה יהיה NFA מינימלי.

בעיית הריקנות

- בעיית הריקנות שואלת, בהינתן אוטומט A , האם $\emptyset \in L(A)$?
- אפשר להזכיר ע"י חיפוש בגרף (DFS/BFS) החל מ- Q_0 , ואם מגיעים לקודקוד כלשהו והוא מקבל נציג "שקר" ואחרת אם כל הקודקודים היישגים לא מקבלים, נציג "אמת".
- הבעיה הדואלית לעביעת הריקנות, בעיית האוניברסליות, שואלת, בהינתן אוטומט A , האם $\Sigma^* \in L(A)$?
- מתקיים $\Sigma^* \in L(\bar{A}) = \emptyset$ אם $\bar{L}(\bar{A}) = \emptyset$ (כשה \bar{A} הוא המשלים של A , נגידו אותו עוד רגע). לכן מספיק שנייצר את \bar{A} ונבדוק האם $\emptyset \in L(\bar{A})$.

בנייה המשלים של A

- עבור DFA $A : Q \setminus F \rightarrow \bar{A}$ הוא אוטומט עם מצבים מקבלים הכל חזק מהמצבים המקבלים של A .
- עבור NFA A : החלפת המצבים מקבלים לא מספיק, לדוגמה באירור הבא, קיבל גם במקורו וגם בבנייה החדש שמיילים שמתחלות ב- a מתתקבלות. הבעיה היא שכאן הבנייה מקבלת את כל המילאים שקיים להן ריצה לא מקבלת, ולא כזו שכל ריצה שלhn היא לא מקבלת.



איור 30 : אוטומט שסותר את הבניה המקורית למשלים

מה שכן יעבוד, הוא לעשות דטרמיניזציה ל-DFA A' שקול \bar{A} , דואליותה למשלים \bar{L}' ובדיקת ריקנות ל- \bar{A}' .
הסיבוכיות של אלג' זה היא אקספוננציאלית כי A' במקרה הגורע הוא בעל מספר מצבים אקספוננציאלי ב- a גודל ה-NFA.

משפט אין פולינום p כך שבhinתן (כל) NFA A , ניתן לייצר \bar{A} עם $(|A|)^p$.

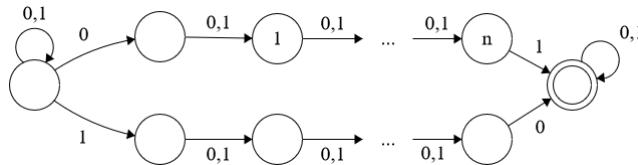
מסקנה האלג' שהראנו לעיל הוא אכן טוב שאפשר ואין אחד עם סיבוכיות קטנה יותר, כי זה במקרה אקספוננציאלי.

הוכחה: נראה משפחה של שפות $\{L_n\}_{n=1}^{\infty}$ עבור \bar{A}_n NFA עם $O(n^2)$ מצבים ולכל \bar{L}_n דרוש לפחות 2^n מצבים.

נבחר $\{0+1\}^n$. כך שדוגמה $L_2 = \{0000, 0101, 1010, 1111\}$ ו- $\bar{L}_2 = \{ww : w \in \{0+1\}^n\}$ כל השאר המילאים).

נראה שקיימים NFA עם $O(n^2)$ מצבים ל-

נשים לב כי $w \in L_n$ אם $2n \neq |w|$ או שקיים אינדקס $i \in [n]$ כך ש- $w_{n+i} \neq w_i$. לכן האוטומט הבא יזהה נכון את $\overline{L_n}$, כי הוא יכול לנחש כל אינדקס לא נכון (נניח שניחס שזה 0 בתחילת ו-1 בסוף או אחריו n צעדים במסלול העליון הוא יקבל).



איור 31 : אוטומט שמצווה את L_n

זהו אוטומט עם $\mathcal{O}(n)$ מצבים.

נראה שככל NFA ל- $\overline{L_n}$ נדרש 2^n מצבים. נניח בשילוב שקיים DFA המזווהה את $\overline{L_n}$ עם פחות מ- 2^n מצבים.

לכל מילה $u \in (0+1)^n$, נתבונן בקבוצת המצבים

$$good(u) = \{s \mid s \text{ מקבלת של } \overline{A_n} \text{ על } u \text{ שמקורת } -s \text{ אחרי קריית } u\} \subseteq Q$$

כלומר אוסף המצבים שבהם בדיקו באמצעות ריצה מקבלת על u הגענו אליהם.

מהיות מספר המצבים של $\overline{A_n}$ פחות מ- 2^n מצבים, ולכן מעקרנו שובך היונים קיימים $u_1 \neq u_2 \in (0+1)^n$ כך ש- $good(u_1) \cap good(u_2) = \emptyset$ וכאן אם s בחיתוך הזה, מתקיים

$$s \in \delta^*(Q_0, u_1), \quad \delta^*(s, u_2) \cap F \neq \emptyset \quad \Rightarrow \quad \delta^*(Q_0, u_1 u_2) \cap F \neq \emptyset$$

■ כלומר $\overline{A_n}$ קיבל את u_2 בסתירה לכך שברור-ש- L_n ($u_1 u_2 \in \overline{L_n}$ היא השפה עם כל המילים שאינם חוזרת על מילה).

שפות חסר הקשר

שפות חסרות הקשר מוגדרות ע"י דקדוק חסר הקשר.

דוגמה נביט בדקדוק הבא,

$$A \rightarrow 0A1$$

$$A \rightarrow B$$

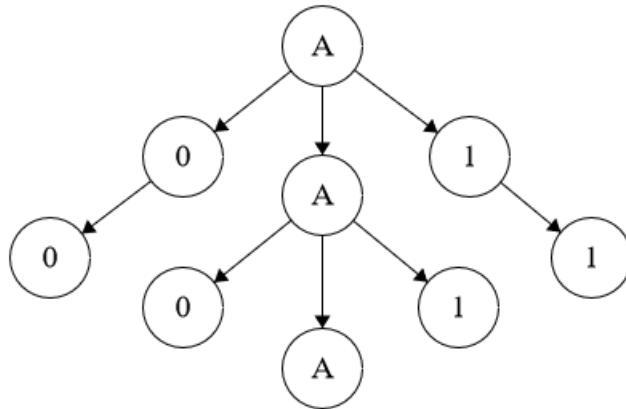
$$B \rightarrow \#$$

נשים לב שיש לנו משתנים A, B , טרמינלים ('א', 'ב', '#, 0, 1,), ומשתנה התחלתי.

במקרה כזה שרשות פעולות הגזירה הבאה מייצרת לנו מילה, $A \rightarrow 0A1 \rightarrow 00A11 \rightarrow 00B11 \rightarrow 00\#11$, כאשר נשים לב שהשפה

שחדקוק מגדיר אינה רגולרית, ובפרט היא $.L(G) = \{0^n\#1^n\}$

ונכל בנוספּ לצייר את עץ הגזירה של הריצחה הנ"ל, כאשר העלים של העץ משמאלי לימין מייצרים לנו את המילה הסופית שקיבלו בשרשרת הגזירה



איור 32 : עץ הגזירה של שרשרת הגזירות הנ"ל

הערה דקדוק חסר הקשר הינה תחילה מעיבוד שפות טבעיות, שם נוכל לאפיין תארים ושמות עצם על ידי גזירה, לדוגמה $N \rightarrow AN$ מאפשר הוספת שם תואר לשם עצם באנגלית.

הגדרה דקדוק חסר הקשר הוא $G = \langle V, \Sigma, R, S \rangle$ כאשר :

- קבוצה סופית של משתנים.
- קבוצה סופית של אותיות.
- $V \rightarrow (V \cup \Sigma)^*$ קבוצה של חוקי גזירה מהצורה $vAu \Rightarrow vwu$ היא הטענה והוא ייחד.
- $S \in V$ משתנה התחלתי.

הערה דקדוק נקרא חסר הקשר כי יש הצד שמאל ריק משתנה והוא ייחיד.

. $vAu \Rightarrow vwu$ הוא חוק בדקדוק, אז יצירה/גזירה היא המעבר $v \Rightarrow^* w$ אם $v, w \in (V \cup \Sigma)^*$ ו- $w \Rightarrow^* u$ אם קיימים $u_1, \dots, u_k \in (V \cup \Sigma)^*$ כך ש- $v \Rightarrow^* u_1 \Rightarrow^* \dots \Rightarrow^* u_k \Rightarrow^* w$ או $w \Rightarrow^* u$ אם $u = u_1$ ו- $u = u_k$.

הגדרה עברו G דקדוק ח"ה, נגדיר את השפה שלו להיות $L(G) = \{w : w \in \Sigma^* \wedge S \Rightarrow^* w\}$ (ונסמן $L(G) = L$ אם יש CFG כ- G).

דוגמאות

1. כאשר החוקים הם $G = \langle \{S, A\}, \{0, 1\}, R, S \rangle$

$$S \rightarrow A1A$$

$$A \rightarrow \epsilon | 0A|1A$$

כל תחлик נזירה יתחיל ב- A . כלומר $\epsilon \in L(G)$ אבל $\epsilon \notin L(G)$. לכן $S \rightarrow A1A$.

.2

$$S \rightarrow 0S1|SS|\epsilon$$

מגדיר את שפה הסוגריים המקבנים חוקית כאשר 0 הוא). נctrיך שbullet רישא לא יהיה יותר 1-ים מ-0-ים, ובסוף יהיה לנו מספר שווה של 0-ים ו-1-ים.

נשים לב כי $L(G) \cap \{0^*1^*\} = \{0^n1^n : n \geq 0\}$ לא רגולרית.

משפט $\text{REG} \subseteq \text{CFL}$

הוכחה: בהינתן DFA $A = \langle Q, \Sigma, q_0, \delta, F \rangle$ ונבחר $G = \langle V, \Sigma, R, S \rangle$, נסמן $L(A) = L(G)$.

$$V = \{V_q : q \in Q\}$$

$$S = V_{q_0}$$

לכל מצב $q \in Q$ ו- Σ נסמן $V_q \rightarrow \epsilon$, אם $\delta(q, \sigma) = s$, נוסיף (מעבר לנ'ם) $V_q \rightarrow \sigma V_s$.

הרעيون כאן הוא שגירה של מילה מ- V_q הסתומים בדיק על כל המילים שמתקבלות מ- q .

נראה שלכל מצב $q \in Q$ ומילה $w = \sigma_1, \dots, \sigma_k$ נסמן $V_q \Rightarrow^* w \iff \delta^*(q, w) \in F$. נסמן $r_i = \delta(r_i, \sigma_{i+1}), 0 \leq i \leq k$ על w של A על w כך ש- $r_0 = q$ ולכל $r_{i+1} = \delta(r_i, \sigma_{i+1})$.

$$V_{r_0} \Rightarrow \sigma_1 V_{r_1} \Rightarrow \dots \Rightarrow \sigma_1 \dots \sigma_k V_{r_k} \Rightarrow \sigma_1 \dots \sigma_k \epsilon = w$$

■

חלק ב' של הרצאה

דוגמה הדקוק $\epsilon \rightarrow aSa|bSb$ מיציר פולינדרומים באורך זוגי (באינדוקציה הוא מוסיף בכל צד אותו). אם נרצה כל אורך, נוסיף ריצה לחוק היחיד שלנו.

משפט (למה הניטוח ל-CFL) תהי $L \in \text{CFL}$ אז קיימים $p \geq 0$ קבוע הניטוח כך לכל מילה $w \in L$ עם $|w| \geq p$, ניתן לכתוב $w = uvxyz$ כך ש- $uv^ixy^iz \in L$ לכל $i \in \mathbb{N}_0$, מתקיים

$$|vxy| \leq p .1$$

$$|vy| > 0 .2$$

$$\text{לכל } i \in \mathbb{N}_0, uv^i xy^i z \in L .3$$

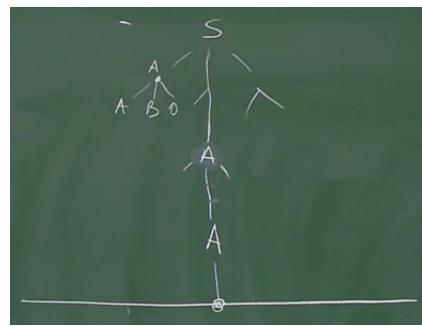
דוגמה שפת הפלינדרומים מקיימת את למת הניפוח. נבחר $3 = p$, ואז אם $w \in L$ ו- $w \geq 3$ -ו, אז $|w| \geq 3$.

- אם $|w| \geq 3$ זוגי, נבחר x להיות האות האמצעית, y, z שכנותיה ו- u הרישא והסיפא בהתאם.
- אם $|w| \geq 3$ זוגי נבחר x להיות ϵ וכל השאר כנ"ל (y, z שמאל לאמצע וימין לאמצע בהתאם).

רק כך המילה המnopחת תהיה מספיק גודלה גם $b=0$, בחלוקת אחרות לא היו לנו מספיק אותיות בניפוח $i=0$.

הוכחה: במלת הניפוח ל-REG מצאנו מעגל במצבים (כאשר $|Q| > p$) וחזרנו עליו i פעמים. יהיו $b \geq 2$ האורך של צד ימין ארוך ביותר בדקודוק של L (כלומר ב-(2) \rightarrow (1) מדובר במספר המשתנים/טרמינלים ב-(2)).

עתה נבחר p שיבטיח שבע הגזירה של מילים באורך גדול מ- p , יש מסלול עם משתנה שחזור לפחות פעמיים (כబיאור, A יכול לחזור אין ספור פעמיים, לא תמיד מיד אחורי עצמו).



איור 33 : עץ הגזירה עם חזרה של משתנה

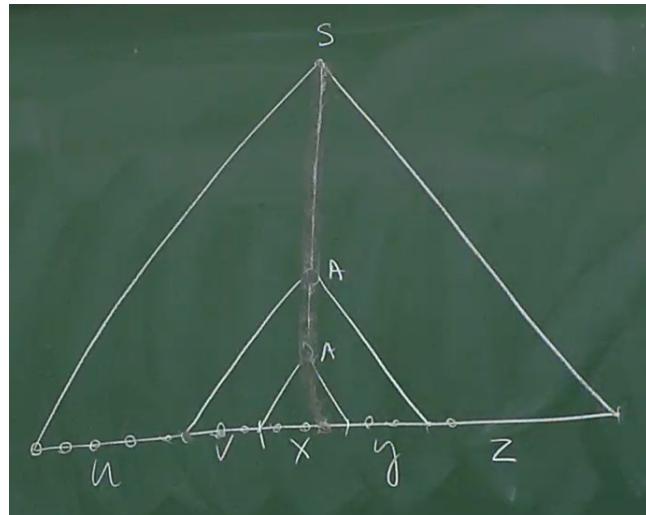
מתקיים שדרגת הפיצול של העץ (מספר הבנים של קודקוד כלשהו) $\geq b$ כי כל פיצול מותאים לחוק. נטען שהמילה מספיק אורך כדי שימושה יחזיר לפחות p פעמיים ועליו יוכל לחזור שוב ושוב.

נזכור כי אם מספר העלים $\leq b^{|V|+1}$ אז הגובה $\leq |V| + 1$ (מבנה נתונים).

נבחר $p = b^{|V|+1}$ ותהי $w \in L$ עם $|w| \geq b^{|V|+1}$. נתבונן בעץ הגזירה הקטן ביותר של w (יש כמה דרכים אולי לגוזר ולהגיע ל- w). בהכרח מתקיים שגובה העץ $\leq |V| + 1$ מההבחנה הנ"ל.

יש $|V|$ משתנים ויש עלה עם עומק $\leq |V| + 1$ (מהגדרת הגובה) שמקיל רק p משתנים (כי אם היה טרמינל היינו עוצרים ולא ממשיכים הלאה).

לכן יש משתנה (שנופיע כ- A באյור הבא) שחזור על עצמו באחת מ- $|V| + 1$ הרכות הקרובות לעלים מעוקרונו שובך היונים.



אייר 34 : חלוקה של המילה על פני עץ הגזירה, משולש מוגדר תת-עץ גזירה

ນבחר חלוקה כבאירור הנ"ל (מספריק פורמללי). נראה שמתקיים התנאים.

1. $|vxy| \leq b^{|V|+1}$ כי בחרנו את החזורה הכי נמוכה של A בעץ, שהיא בגובה (ביחס לעליים) לכל היותר $1 + |V|$ ומהיות דרגת הפיצול לכל היותר b הרי שהמילה שנוצרת מהעלים היא באורך לכל היותר $b^{|V|+1}$.

2. $0 > |uy|$ כי בחרנו את עץ הגזירה המינימלי ואם גם u וגם y ריקים, זה לא עץ גזירה מינימלי (היתה לנו תת-גזירה $A \Rightarrow^* A$ כשיםכלנו לדלג עליה, הבינו באירור לאינטואיציה).

3. $A \Rightarrow^* v^iAy^i z \in L$ לכל $i \in \mathbb{N}_0$ כי אנחנו יודעים שנייתן לגוזר $S \Rightarrow^* uAz$ וגם x -ו $A \Rightarrow^* vAy$ ולכן נוכל גם לבצע $uv^i xy^i z$ וכך $S \Rightarrow^* uv^i xy^i z$

■

תרגול

דוגמאות

1. נביט בדקדוק הבא

$$A \rightarrow 0A1|B$$

$$B \rightarrow \#$$

במקרה זה נוכל לנזר

$$A \rightarrow 0A1 \rightarrow 00A11 \rightarrow 00B11 \rightarrow 00\#11$$

וכמו שראינו בהרצאה, השפה היא כל המילים מהצורה $.0^n\#1^n$.

2. נמצא דקזוק לשפה $L = \{a^n b^{2n} : n \geq 0\}$ נגזר מספיק החוק $S \rightarrow aSbb|\epsilon$, כאשר כדי להציג $aabb$ -ים נגזר $S \rightarrow aSbb \rightarrow aaSbbb \rightarrow aabb$

$L = \{a^i b^j : j \geq i\}$.3. כאן נגידיר $S \rightarrow aSb|Sb|\epsilon$ וזו נוכל להוסיף כמה b -ים שנרצה מעבר ל- a -ים.

$L = \{a^i b^j c^j d^i : i, j \in \mathbb{N}_0\}$.4. כאן נגידיר $S \rightarrow aSd|T|\epsilon$

$T \rightarrow bTc|\epsilon$

זה יספק כידר להציג לנו (המשתנה הנוסף כאן אינו הכרחי למעשה).

טענה CFL סגורה לאיחוד.

הוכחה: תהיינה $V_1 \cap V_2 = \emptyset$ (שינוי CFG G_1, G_2 ו- $L_1, L_2 \in \text{CFL}$ המתאימים להן. נניח בה"כ כי $\emptyset \neq$ שמות).

נדיר

$$G = \langle V_1 \cup V_2 \cup \{S\}, \Sigma, R_1 \cup R_2 \{S \rightarrow S_1|S_2\}, S \rangle$$

כאשר $S \notin V_1 \cup V_2$. קל לראות מכאן שמילה מתקבלת ע"י $S \rightarrow S_1 \rightarrow \dots \rightarrow S_n$ כאשר היא יכולה להשתמש מ- S_1 בזירה המקורית שלה (ומ- S_2 -ה). ■

טענה CFL סגורה לשרשור.

הוכחה: תהיינה $V_1 \cap V_2 = \emptyset$ (שינוי שמות). CFG G_1, G_2 ו- $L_1, L_2 \in \text{CFL}$ המתאימים להן. נניח בה"כ כי $\emptyset \neq$ שמות).

נדיר

$$G = \langle V_1 \cup V_2 \cup \{S\}, \Sigma, R_1 \cup R_2 \{S \rightarrow S_1 \cdot S_2\}, S \rangle$$

כאשר $S \notin V_1 \cup V_2$. קל לראות שכל השרשורים מתקיים כאן, וכל מה שאינו שרשור לא מתקיים. ■

משפט (למה הניפוי ל-CFL) תהי $L \in \text{CFL}$ אז קיים $0 \leq p$ קבוע הניפוי כך שלכל מילה $w \in L$ עם $|w| \geq p$, ניתן לכתוב $w = uvxyz$ כאשר מתקאים

$$1. |vxy| \leq p$$

$$2. |vy| > 0$$

$$3. \text{ לכל } i \in \mathbb{N}_0, \text{ מתקיים } uv^i xy^i z \in L$$

הערה למה זו דומה מאוד לлемת הניפוי המקורי רק שעכשו יש לנו שני סגמנטים שונים לנפח (ורק אחד מהם יכול להיות ריק), והחלוקת הוא לכל היותר p לא חייב להיות רישא של המילה.

דוגמה $w = a^p b^p a^p \in \text{CFL}$. נראה ש- $L \notin \text{CFL}$. נניח בשלילה ש- $L = \{a^n b^n a^n : n \in \mathbb{N}\}$ ותהי $w = uvxyz$ חלוקה של w שמקיימת את התנאים.

$$\text{או עבור } 0 \leq i < p \text{ מכיל פחות } a\text{-ים } vxy \text{ כ } |vxy| > 0 \text{ ולכן } L \notin \text{CFL} \text{ סתירה.}$$

$$\text{או } vxy \subseteq b^p \text{ .}$$

$$\text{או } vxy \subseteq a^p \text{ .}$$

כאשר אנחנו מכילים לפחות a אחד או לפחות b אחד, או בהכרח שבניפוי עם $i = 0$ נקטין את מספר ה- a -ים או ה- b -ים וכן נצא מהשפה סתירה.

$$\text{או } vxy \subseteq b^p a^p \text{ .}$$

דוגמה ננסה להבין האם CFL סגורה לחיתוך. $L_1 = \{a^n b^n a^m : n, m \geq 0\}$ היא כן ב- CFL עם הדזוק

$$S \rightarrow XA$$

$$X \rightarrow aXb|\epsilon$$

$$A \rightarrow Aa|\epsilon$$

וגם $L_2 = \{a^n b^m a^m : n, m \geq 0\}$ היא גם ב- CFL עם הדזוק

$$S \rightarrow Ax$$

$$X \rightarrow bXa|\epsilon$$

$$A \rightarrow Aa|\epsilon$$

אבל L כאשר L היא מהדוגמה הנ"ל וראינו שהיא לא ב- CFL אך $L_1 \cap L_2 = L$ סגורה לחיתוך.

הערה בנוסף אינה סגורה להשלמה כי אחרות מזה-מורגן $L_1 \cap L_2 = \overline{L_1} \cup \overline{L_2}$ ואילו CFL הייתה סגורה לחיתוך ויהיא לא.

דוגמה אם $L \in \text{CFL}$, לא! נשתמש בلمת הניפוח ל-CFL. $L = \{ww : w \in \{a,b\}^*\}$

תהי $w = a^p b^p a^p b^p \in L$, ותה חלוקה $w = uvxyz$ כך $|v| = |y| > 0$, ניפוח ב- i נקבל

- אם $vxy \subseteq a^p$ או $vxy \subseteq b^p$ במופע הראשון או b^p במופע השני, אז מהיות $uv^i y^i$ ניפוח ב- i .
- שב- a -ים $uv^i y^i$ יש פחות a -ים (או b -ים) מאשר בצד השני ולכן יצאו מלהשפה סתירה.

- אם $vxy \subseteq a^p b^p$ במופע הראשון או uv מכיל לפחות a אם v לא ריק ולפחות b אחד אם v ריק. אז כנונפה $uv^i y^i$ ניפוח ב- i מאשר בצד השני.

- אם $vxy \subseteq b^p a^p$ או $vxy \subseteq a^p$ לא ריק והוא מכיל b או a ננפח $uv^i y^i$ ניפוח ב- i ונקבל שאחד הצדדים

نبיט ב- \bar{L} , וזה השפה $\{uv : |u| = |v|, u \neq v\} \cup \{w : |w| \equiv 1 \pmod{2}\}$ (כל המילים האיזוגניות או זוגיות עם חזאים שונים). נוכיה כי $L_1 \in \text{CFL}$ וגולרית (אוטומט שבודק זוגיות של אורך המילה) ולכן $\bar{L} \in \text{CFL}$. נותר להוכיח כי $L_2 \in \text{CFL}$ (למרות שהראנו כבר בהרצתה שהיא גולרית) ונסיים מסגרות לאיחוד.

תהי $w \in L_1$, כלומר $w = xaybz$ כאשר $x, y, z \in \{a, b\}^*$, $|x| = i - 1$, $|y| = n - 1$, $|z| = n - i$. נגידיר את L_1 מחדש כ- $L_1' = \{w : |w| = 2n, \exists i \in [n] \text{ כך } w_i = b \text{ ו } w_{n+i} = a\}$. נסמן $w = w_1 \dots w_n$.

$$\{xaybz, xbyaz : x, y, z \in \{a, b\}^*, |y| = |x| + |z|\}$$

נמצא דקדוק ל- L_1' .

$$\begin{aligned} S &\rightarrow AB|BA \\ A &\rightarrow aAa|aAb|bAa|bAb|a \\ B &\rightarrow aBa|aBb|bBa|bBb|b \end{aligned}$$

מזהה את L_1 כאשר הרעיון כאן הוא שהגזרה $M-S$ מחלקת אותן להאם יש לנו a קודם ואו b קודם ואו a , וכך לשמר על דרישת האורך, בכל פעם שנוסף טרמינל $-x$ או $-z$ נוסיף גם אותן $-y$ כדי לשמר על שוויון בין האגפים.

שבוע VII | מכוונות טיורינג

הרצאה

חלק א' של הרצאה

דוגמה עברו $L = \{w\#w : w \in (0+1)^*\}$, קל מאוד לכתוב תכנית שמכריעה את השפה (האם קלט הוא בשפה או לא), אבל CFL ו-REG לא עוזרו לנו למגדל את הפתרון. מכוונות טיורינג כן יכולות למגדל אלג' כללה.

איןטואיטיבית, מכונת טיורינג (מ"ט) היא סרט אינסופי שאליו אפשר לכתוב ולקראן ובהתחלה כתובות עליו אותן מילת הקלט (וכל השאר רוחים). הראש (הקורא/כותב) יכול לנוע שמאלה וימינה, כל עוד לא הגיעו למצב סיום (קבלה/דוחה).

דוגמה נתאר מ"ט לא פורמלית עבור L הנ"ל.

1. סרווק את הקלט ונוזדא שיש לפחות # אחת, אם אין, דחה. אם יש #, חזר לתא הראשון.
2. זוג בין מיקומים מתאימים משאל ומימין ל-# וודא שמסומנים באותו הזוג. אם לא, דחה. אם הסטיימה הבדיקה ואין אותן נוספות מימין ל-#, קבל.

הגדרה מכונת טיורינג היא שבייעיה $M = \langle Q, \Sigma, \Gamma, \delta, q_0, q_{acc}, q_{rej} \rangle$ כאשר :

- Q היא קבוצה סופית של מצבים.
- Σ היא א"ב הקלט ($\Sigma \neq \{\}$).
- Γ היא א"ב העבודה, $\Gamma \subseteq \Sigma^*$ (אותיות שאפשר לכתב על הסרט).
- $q_0 \in Q$ מצב התחלתי.
- $q_{acc} \in Q$ מצב מקבל.
- $q_{rej} \in Q$ מצב דוחה.
- δ היא פ' המעברים המוגדרת לפי $\{L, R\}$ כאשר אם לדוגמה $(q, a) = (q', b, R)$ אז δ או כאשר נהייה במצב q ונקראת האות a , נعبر למצב q' , נכתב b בתא הנוכחי ונוזז ימינה.

הגרסה האי-דטרמיניסטיבית שבה משתמש היא עם הגדרה זהה לנו'ל רק שעתה הפ' δ מעתיקה $\Gamma \times Q \times \{L, R\} \rightarrow Q \times \Gamma \times \{L, R\}$.

הערה DFA הוא מ"ט כאשר $\delta(q, a) = \langle \delta'(q, a), a, R \rangle$ δ' עברים המקבילים וכיו'.

הגדרה פעילות מ"ט כלשיי מוגדרת באופן הבא :

1. מילת הקלט כתובה על סרט העבודה, מרווחת ב-_. אם $\sigma_n \dots \sigma_1 = w$, הקוניגורציה ההתחלתייה תראה כבסרט הבא

σ_1	σ_2	\dots	σ_n	$-$	$-$	\dots
------------	------------	---------	------------	-----	-----	---------

2. המכונה מתקדמת לפני פונקציית המעברים.

• קונפ' שנייתן לעבור בינהון באמצעות פ' המעברים נקראות קוֹפְּנִי מעברים.

• ריצה היא סדרה של קוניגורציות עוקבות, החל מהקונפ' ההתחלתייה.

• שלושה גורלות לריצה :

1. מגיעה למצב מקבל \rightarrow עצרת ומקבל.

2. מגיעה למצב דוחה \rightarrow עצרת ודוחה.

3. לא עצרת ודוחה את מילת הקלט.

הגדירה קוֹנֶפְּן של מ"ט מדיריה ע"י המצב הנוכחי, תוכן הסרט ומיוקם הראש. קוֹנֶפְּן מתוארת ע"י מילה ב- $\Gamma^* \cdot Q \cdot \Gamma$. כאשר הקונפ' uqv אומרת לנו שאנו במצב q , שהראש מצביע לאות הראשון של v ושתוכן הסרט הוא uv ולאחר מכן (הReLUION) הוא q הוא על הסרט, בין u ל- v .

הקוֹנֶפְּן ההתחלתי היא wq_0 כאשר w מילת הקלט.

הגדירה יהיו Γ ו- Q $u, v \in \Gamma^*, a, b, c \in \Gamma$. איזי הקונפ' העוקבת של uqv היא (ראו הדגמה, הכו כאן והדוגמאות הבאות הוא תקלת טכנית בלתי פתירה):

				q
u	a	b	v	

$$\delta(q, b) = (q', c, L) \text{ אם } uq'acv \bullet$$

				q'
u	a	c	v	

$$\delta(q, b) = (q', c, R) \text{ אם } uacq'v \bullet$$

				q'
u	a	c	v	

- אם $u = \epsilon$ (אנחנו בקצה השמאלי) ו- $\delta(q, b) = (q', c, L)$ העוקבת תהיה cvq' (מנועים מעבר שמאלה).

הגדירה ריצה של M על מילה w היא סדרה c_0, c_1, \dots של קוֹנֶפְּן כך ש:

1. c_0 היא קוֹנֶפְּן ההתחלתי של M על w .

2. עוקבת c_i לכל i לעוקבת c_{i+1} .

3. הסדרה סופית ומסתiyaota בקונפ' עצרת (קוֹנֶפְּן מקבל את המצב שלה הוא q_{rej} וודוחה את המצב שלה הוא q_{acc}), או שאינה סופית.

M מקבלת את w אם יש ריצה של M על w שמגיעה לקונפ' מקבלת. אחרת (כל הריצות מגיעה לקונפ' דוחה או לא עצורות).

נדיר את השפה של M להיות { יש ריצה מקבלת של M על $w : w \in L(M) }$

הגדירה נאמר כי מ"ט מזוהה שפה L אם $L = L(M)$ (recursively enumerable RE). מחלוקת השפות ליזיהו ע"י מ"ט.

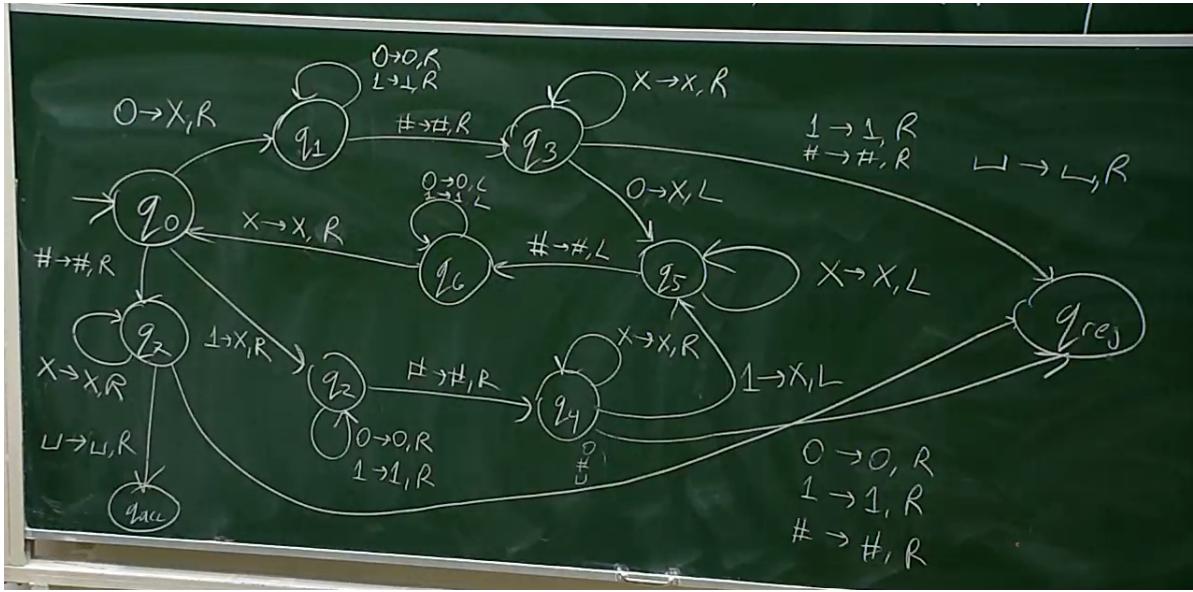
נאמר כי M מכירעה שפה L אם M מזזה את L ובנוסף M עצרת על כל קלט. מחלוקת השפות R (recursive) היא כל שפות הנitinoot ליזיהו להכרעה ע"י מ"ט.

הערה מההגדרה $R \subseteq RE$, אבל האם $R \not\subseteq RE$? כן! נוכיה בהמשך ש-RE.

דוגמא נסתכל על $L = \{w\#w : w \in (0+1)^*\}$ ונבנה מכונה שמזזה אותה.

nbחר $\Gamma = \{0, 1, \#, \times, _\}$, $\Sigma = \{0, 1, \#\}$

נקבל את גרף המצב הבא $a \rightarrow b, \Delta$ אם קראנו a , נכתוב b ונוזז Δ .



איור 35 : מ"ט שמצוה את L

איןתוואציה :

1. אם הטענה הנוכחית מסומן ב-#, בדוק האם יש תאים לא מחוקים מימיינו.

אם מ- q_0 מצאנו #, נלך ימינה על \times וnochzer כל פעם ל- q_2 עד שנקרה לטענה אחרת. אם קראנו רווח הצלחנו (q_{acc} , אחרת יש יותר תווים מימיין מאשר ממשאל ונדחה (q_{acc}).

(א) אם הטענה הנוכחית מסומן ב-#, מחק אותו, אך ימינה עד ל-# ואז ימינה עד לתא הלא מחוק הראשון. אם מסומן ב-#, 1, 1,#, עבור ל-2. דחלה. אחרת, עבור ל-4.

אם מ- q_0 מצאנו 0, מחק אותו ועבור ל- q_1 . קרא דברים וחזור כל פעם ל- q_1 עד לסולਮית. קרא X-ים וחזור כל פעם ל- q_3 עד שנגיעה לשזהו שהוא לא \times . אם קראנו אחד מהתווים האסורים, דוחים,

(ב) אם הטענה הנוכחית מסומן ב-1, בצע את המקירה הדואלי ל-2. המצביעים שמשים את ההתנהגות הדואלים הם q_2, q_4 .

(ג) נלך שמאלה (על מחוקים) עד ל-# ואז נלך שמאלה עד למחוק המני ביוטר, ועוד אחד, ואז חזור ל-1. אנחנו ב- q_5 , זרים שמאלה כל עוד מחוק, ואז ב-# עוברים ל- q_6 שעליו זרים כל עוד אנחנו ב-1, 0 ואז כשמגיעים למחוק זרים עוד פעם אחת ל- q_0 .

חלק ב' של הרצאה

נתונה M מ"ט ומחליפים בין q_{acc} ו- q_{rej} . האם מקבלים מכונה עם $\Sigma^* \setminus L(M)$? לא! אם M לא עצרה על מילה w או $w \notin L(M)$ וגם

$$w \notin L(\overline{M})$$

אם M מכירעה את L אז ההחלפה כן הייתה משלימה את השפה.

מסקנה R סגורה למשלים.

הגדירה אס"ם $\overline{L} \in \text{RE}$ co- RE היא מחלוקת כל השפות שקיימת מ"ט שמצויה את המשלים שלן.

משפט $\text{RE} \cap \text{co-RE} = R$ כלומר ניתן להכריע שפה אס"ם ניתן לזיהות אותה ואת המשלים שלה.

הוכחה: נוכח חכלה דו-כיוונית.

הגדירה מתקיים $R \subseteq \text{RE} \cap \text{co-RE}$ ($L \in \text{RE}$, $\overline{L} \in \text{co-RE}$) אם מכיריעים גם מזוהים). $L \in R$. מיהו $R \in \text{RE}$, הרי $\overline{R} \in \text{co-RE}$.

כלומר $\overline{L} \in \text{RE} \subseteq \text{co-RE}$, ולכן $L \in \text{co-RE}$.

הוכחה: מהגדירה $L \in \text{RE} \cap \text{co-RE}$ ($M \in \text{RE}$, $\overline{M} \in \text{co-RE}$) שמצויה את L .

בננה מכונה שמרייצה את שתי המכונות בו זמנית, ואז בוטח אחת מהן תעוצר מתישחו ולכן תמייד נעצור בעצמנו (ונחזיר תשובה בהתאם לתוכאה שהתקבלה משתי המכונות). באופן מעט יותר פורמלי, עבור $\dots, i=1,2$:

1. הרץ את M על w i פעמים. אם M קיבלת w , עוצר וקובל.

2. הרץ את \overline{M} על w i פעמים. אם \overline{M} קיבלת w , עוצר ודחה.

טענה M' עוצרת על כל קלט w .

הוכחה: זאת ממש שאם $w \in L$ או לריצה המתקבלת r של M על w יש מספר $j < \infty$ של פעמים ואו M' תעוצר באיטרציה ה- j .

אחרת, לריצה M' על w יש מספר $k < \infty$ שעוברה M' תעוצר ותדחה באיטרציה ה- k .

טענה $L(M') = L(M)$

הוכחה: אם $w \in L(M)$ או w התקבלה בעקבות ריצה מקבלת של M על w כלומר $w \in L(M')$ או M' תעוצר בגלל זה ותקבל.

הערה: כיצד נרץ דברים במקביל? בכל איטרציה נשכפל את המילה על הסרט וນפרד אותה עם איזשהו סימן מפריד וערך של מונה שעולה בכל פעם. לא כל כך חשוב להבין איך זה עובד, ונראה בקרוב שאפשר להניח שיש לנו כמה סרטים שאנו חנו רצים עליהם במקביל וזו שקול.

תרגול

הערה: בהגדירה של מכונת טיורינג אין לנו זיכרון, אבל הוא מגולם בתוך פ' המעברים וה מצבים שמאפשרים לנו לכתוב דברים שנשмарים על הסרט.

הערה אינטואטיבית, קופן מוגדרת כמידע המיניימי שנוצר כדי שם נכבה את המחשב, נוכל לשחזר את המצב שהיינו בו לפני שביבנו את המחשב.

הגדרה תהינה מילה w ומ"ט M . נאמר כי c_1, \dots, c_k גוררת את $c_i, i \in [k-1]$ הינה ריצה חיליקת של M על w אם $c_1 = q_0 w$ ולכל δ לפ"ג.

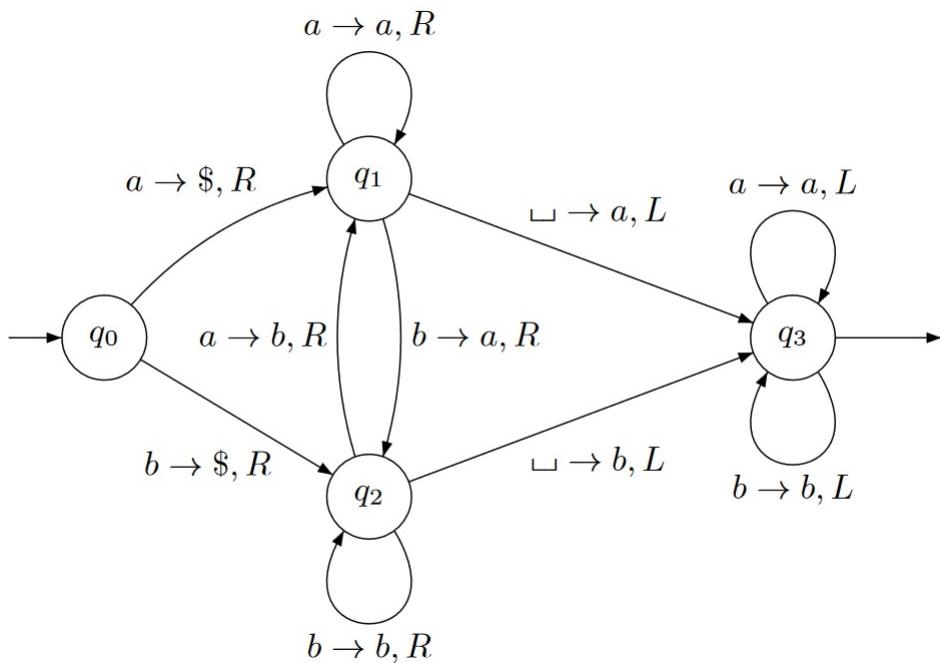
הגדרה תהינה $\mathbb{N} \rightarrow \mathbb{N}$: f ו- M מ"ט. נאמר כי מ"ט מחשבת את f אם בתחילת הריצה של M כתוב את w על הסרט ובסיום הריצה (המוכנה $f(w)$) אכן עוצרת) הסרט מכיל רק את $f(w)$.

דוגמה נתאר מ"ט שמחשבת את הפ' $(n) = n+1$ ביצוג הבינארי. המוכנה שלנו תתחיל בסימון התו הראשוני בסרט - \$ ותזיז את הקלטתו אחד ימינה. מכאן, אינטואטיבית נחליף את רצף ה-1ים הראשון מימין (LSB) ב-1 עם הרבה אפסים (111...1000...). ממשם, במצב q_0 ותסורך את הסרט ימינה עד שתגיעו ל- _ וזו תעבור ל- q_1 . ב- q_1 , אם M קוראת 1 היא משנה אותו ל- 0 וממשיכה שמאליה. אם היא רואה 0, היא משנה אותו ל- 1 ועוצרת.

אם M קוראת \$, הקלט יהיה 1...1 (כי הינו עוצרים אם ראיינו 0) ובמקרה כזה היא תנסה את התו הראשון ל-1 ותזיז את כל הסרט אחד ימינה ותכתב \$ בהתחלה (ככה יש לנו 1 ורבה אפסים).

התיאור הזה מספיק, חוץ מהעובדת שלא הסבכנו איך להזיז את כל הסרט ימינה. באior ניתן לראות מ"ט שהרעיון שלו הוא ש- q_1 הוא המצב שזכור שהתו הקודם שקרהנו הוא a ו- q_2 זוכר שעכשיו קראונו b .

כך, מ- q_1 לא משנה מה קוראים, נכתב a ומ- q_2 נכתב b . אם נקרא רוח נדע שישיםנו



ש

איור 36 : מ"ט שמצויה ימינה את הסרט

מודלים שקולים למ"ט

• מ"ט שסרצה לא חסום משמאלי.

• מ"ט עם k סרטים.

• מ"ט שיכולה להישאר במקומם בנוסף לבחירה ימינה/שמאלה (Stay-TM).

• מ"ט שבמקום סרט יש לה גריד דו ממדי אינסופי.

• מ"ט אי-דטרמיניסטיבית.

הגדירה נאמר כי שתי מכונות חישוב N , M הן שקולות אם לכל $w \in \Sigma^*$:

• M מקבלת את w אם "ס" N מקבלת את w .

• דוחה את w אם "ס" N דוחה את w .

• M לא עוצרת על w אם "ס" N לא עוצרת על w .

הגדירה שני מודלים חישוביים \mathcal{X} , \mathcal{A} הם שקולים אם לכל מכונה מסווג \mathcal{U} יש מכונה שköלה מסווג \mathcal{A} ולהפוך.

הגדירה מ"ט עם שני סרטים היא מכונה רגילה, עם שני סרטים אינסופיים מימין, שני ראשים קוראים ו' מעברים המוגדרת ע"י $\delta : Q \times \Gamma^2 \rightarrow \{L, R\}^2$.

הערה משמעות פ' המעברים כאן היא שאנחנו קוראים בכל פעם את התווים משנה הראשים הקוראי, ויחד עם המצב החדש קבועים לאייה צד הולכים בכל סרט בנפרד.

משפט מ"ט עם שני סרטים היא מודל חישובי שקול למ"ט קלاسي.

הוכחה: ברור של מ"ט קלاسي יש מכונה עם שני סרטים שköלה (פישוט מנוגנים את הסרט השני). נוכיח את הכיוון השני.

תהי מ"ט עם שני סרטים $M = \langle Q, \Sigma, \Gamma, \delta, q_0, q_{acc}, q_{rej} \rangle$ הרעיון הוא שנסביר את שני הסרטים לסרט אחד שבו א"ב הסרט (העובדת) הוא מתוק $\{0, 1\}^2 \times \Gamma^2$ שייצג את האות בכל סרט והאם כל ראש קורא נמצא כרגע על התו ההוא.

נגדיר $M' = \langle Q', \Sigma', \Gamma', \delta', q'_0, q'_{acc}, q'_{rej} \rangle$ פועלת כך:

1. מתחילה עם סרט שעליו כתובה $\sigma_1 \dots \sigma_n = w$ ומחליפה לפי הסדר את σ_i ב- $(\sigma_i, 0)$, לכל i , עד שמנגיעה לסוף המילה ואז חוזרת לתחלת הסרט ומחליפה את התו הראשון ב- $(\sigma_1, 1)$.

2. מסרווק את הסרט שלו עד שתמצא את המיקום של הראש הקורא הראשון בሪיצה של M על w (תזהה $(*)$).

משם תעביר למצב שמקודד את זה שנמצא הראש הראשון ונקרה אותן כלשיי σ במקומות הזה בסרט הראשוני של M .

משם היא תחזיר לראש הסרט ותתחל ללחפש באופן דומה את הראש השני ותזכיר במצביםஇயே איזו אותן נקרה.

משם, M' תביט בפ' המעברים של M ותתחל לעדכן את הסרט שלו בהתאם - מסרווק שוב את הסרט כשנחפש את הראש הקורא הראשוני, תעדכן את האות במיקום הזה וגם את סמני הקוראים המודומים, תחזיר לתחלת הסרט, ותעשה את אותו הדבר עבור הראש הקורא השני.

טענה R סגורה לאיחוד.

הוכחה: נרץ את המוכונה שמכריעה שפה אחת, אם היא תקבל נקלט ואם לא נרץ את המוכונה השניה (נפס את הסרט וכו') ונקלט/נדחה בהתאם לה. המזל כאן הוא ששתי המוכנות תמיד עוצרות ולכן זה עובד.

הערה גם RE סגורה לאיחוד, אבל שם צריך להריץ את שתי המוכנות במקביל וזה קצת יותר מורכב.

שבוע VII | אונמורציה ואי-כריעות

הרצאה

חלק A' של הרצאה

הגדרה ספרן E (*Enumerator*) הוא מ"ט שלא מקבלת קלט ומדפיס מילים (עם "אנטוריים" ביןיהם), ופתחה היא

$$L(E) = \{w : w \text{ בסופו של דבר מדפסת את } w\}$$

$$\text{משפט } \Sigma^* \text{ יש ספרן } E \text{ כך } \forall L \in \text{RE}, L = L(E)$$

הוכחה: \Rightarrow : נניח שיש ספרן E כך $L = L(E)$. נזכיר M שמצויה את L .

בhinintn מילה, M תריץ את E ובכל פעם שידפיס מילה y , M בודקת האם $w = y$. אם כן, עוזרת ומקבלת. אם לא, ממשיכה להריץ את E Again מזהה את L כי אם $w \in L$ אז E ידפיס את w בסוף של דבר ולכן נעצור ואז M תעוצר ותקבל. אם לא אז E לא ידפיס את w ואז M תרוץ לנצח ולא תקבל את w (או שתעצור ותדחה אם E עוצר).

\Leftarrow : נתונה M מ"ט שמצויה את L ונזכיר ספרן E כך $L = L(E)$. נזכיר Σ^* בת מניה, ולכן יש סידור \dots, w_1, w_2, \dots של Σ (עבור $\Sigma = \{0, 1\}$ הסידור $\dots, 0, 1, 00, 01, \dots, \epsilon$ עובד).

לא נוכל להריץ את M על המילים אחד אחרי השני כי M מזהה ולא מכיריה ולא יתכן שלא נעצור ולא נגיע למילים אחרות. נרץ את כל המילים במקביל ע"י הרצה למשק i צעדים של w_i, \dots, w_1 באופן איטרטיבי. אם M מקבלת את w_j עברו j במחלך הריצה, ידפיס את w_j .

אם $L \in \text{RE}$ אז w תודפס בסופו של דבר כי קיים i כך $w_i = w$ ואז קיים t כך w תוק t צעדים. לכן w תדפיס בכל איטרציה $.k \geq \max\{i, t\}$.

אם $L \notin \text{RE}$ אז w לא תדפיס את w מהגדotta.

הבעיה העשירה של הילברט היא הבעיה הבאה: תאך אלג', שהינתן פולינום במספר משתנים, יカリ האם יש לו שורש שלם.

ב-1970 הוכח שאין אלג' שיכריע את הבעיה במספר צעדים קבוע (כלומר לא- P). עם זאת, $\{\langle p \rangle : \text{יש ל-}p \text{ שורש שלם}\} \in \text{RE}$ כי אפשר לסדר את \mathbb{Z}^n כאשר n מספר המשתנים ולבודק האם כל אחד מה- n -יות היא שורש של האלג'.

שלוש רמות לתיאור אלג'

1. ע"י מ"ט, כאשר ניוכח שכל עצם קלט A ניתן לקודד כמילה $\langle A \rangle$.

דוגמה $G = \langle V, E \rangle$ אפשר לקודד כרשימה של קודקודים (עם מפ прид #) ואז רשימה של קשרות בין קודקודים (עם מפ прид §).

2. תיאור פעולות של מ"ט (בسانגו "זו" עם הראש הקורס שמאללה").

3. שפה עילית (pseudo-code).

התזה של צ'ץ' וטיירינג קובעת שהכרעה ע"י מ"ט שקופה לאלג', כלומר כל תיאור ברמה 3 שקול לתיאור ברמה 1.

הערה לא נוכח שהזהה נכונה, אבל נעשה כמה דוגמאות שישכנעו אותנו.

דוגמה מ"ט שמכריעה את $\{G\}$ גראף לא מכון קשייר: $.CG = \{\langle G \rangle$

1. כיצד נתון גראף: נניח ש- G -ו רשימה של קודקודים (מספרים בסיס 2) מופרדים ב-# ורשימת קשרות מופרדות ב-§.

2. אלג': $C = \emptyset, T = \{v_0\}$ ואז:

כל עוד $\emptyset \neq T$, נוציא u מ- T , נוסיף אותו ל- V , ולכל $(u, v) \in E$, אם $v \in T$, נוסיף את u ל- T .

אם $C = V$ קיבל אחרת נדחה.

3. תיאור האלג' ע"י מ"ט: נבחר $\Gamma = \Sigma \cup \{_\} \cup \{0, 1\} \times \{C, T, A\}, \Sigma = \{0, 1, \#, \$\}$

המכונה יכולה T -لسמן קודקודים ע"י הפיכת התו הראשון בקידוד שלהם לתו ב- 0_T או 1_T (וכך גם C -תסמן).

(א) T -סמן את הקודקוד הראשון.

(ב) חוזר כל עוד יש קודקודים T מסומנים:

i. A -סמן קודקוד T -מסומן (הוצא מ- T קודקוד כלשהו).

ii. עבר על רשימות הקודקודים, אם יש קודקוד לא מסומן (בשם דבר), בדוק האם יש קשר בין ובין הקודקוד ה- A .

מסומן.

אם יש, T -סמן את הקודקוד הנבדק.

iii. C -נסמן את הקודקוד ה- A -מסומן.

(ג) אם כל הקודקודים C -מסומנים נקבל, אחרת נדחה.

דוגמה A הוא DFA $.A_{DFA} = \{\langle A, w \rangle : w \in L(A)\}$ נקודד את הקלט כרצף אותיות, #, רצף מצבים, דולר, מצב התחלתי,

מצבים מקבילים וכו' מופרדים.

המ"ט תסמלץ ריצה של A על w . נשמר את המצב הנוכחי ואיינדקס במיליה, ובכל איטרציה נעדק מצב ונגדיל איינדקס. נבדוק בכל פעם מה δ אומרת ואם קיבל בסוף נקלט ואחרות נדחה.

אם היה מדובר ב- A_{NFA} , פשוט נריץ את ה-NFA כאשר נשמר את קבוצת המצבים שאלייהם אפשר להגיע בריצה כלשהי (כלומר subset construction פונקציונלי).

אי בריאות

משמעות יש שפה C ש- R אם $L \notin R$.

הוכחה: משיקולי ספירה: עבור A ב- C יש \aleph_0^2 שפות ב- Σ^* . עם זאת, יש רק \aleph_0 מ"ט, כי כל מ"ט ניתן לקודד באמצעות מספר סופי של תווים.

לחולפים, כל תכנית בפייתון מגדרה מ"ט, ויש \aleph_0 תכניות פייתון סופיות שמנדרירות מ"ט.

■ ממשפט קנטור, $\aleph_0 < \aleph^2$ ולכן יש שפה L כך שאין מ"ט שמכריעה אותה.

חלק ב' של הרצאה

הוכחה: נבנה קונסטרוקטיבית: נקבע על שפה R $A_{TM} = \{\langle M, w \rangle : w \in L(M) \text{ ו- } M \in R\}$. נוכיח כי R מתקבלת את w הראשית $A_{TM} \in RE$ כי מ"ט אוניברסלי מזהה את A_{TM} - בהינתן M ו- w היא מרכיבת את M על w ווענה כמותה. אם M מקבלת את w אז מקבל גם. יתכן שהיא מתקע זהה בסדר כי זה יקרה רק אם אס M לא עוצרת.

נניח בשיליה כי קיימת מ"ט H מכירעה כך ש- $A_{TM} = H(\langle M \rangle, w)$, כלומר H מקבלת את M על w ודוחה אם M דוחה על w או לא עוצרת על w .

نبנה מ"ט D מכירעה כך $D(\langle M \rangle) = H(\langle M \rangle, \langle M \rangle)$ (המילה שמקודדת את M) ודוחה אחרת.

■ נבנה מ"ט \tilde{D} שמחליפה בין q_{acc} ו- q_{rej} של D , כלומר \tilde{D} מקבלת את M דוחה או לא עוצרת על $\langle M \rangle$ ודווחה אם היא מקבלת על $\langle M \rangle$. ותקבל את \tilde{D} דוחה את \tilde{D} על $\langle \tilde{D} \rangle$ ותזחזה אחרת, סטירה!

הערה: נשים לב שהנ"ל היא סוג של הוכחה בלכסון! $\aleph_0 < \aleph^2$ הוכיחו ע"י הנחה בשיליה האם יש סידור בן מנייה של \mathbb{N}^2 לקבוצות נסדר אותן בטבלה ואז נסתכל על קבוצה שמודדרת הפוך מהאלכסון, כלומר $i \in S$ אם $s_i \notin i$. ואז S לא בטבלה.

עתה נוכל לכל מ"ט לסדר את $\langle M_i \rangle$ לפי האם היא מקבלת או לא, ואז D היא האלכסון ו- \tilde{D} היא הדואלי לאלכסון.

דוגמה: M עצרת על w אם $\langle M, w \rangle \in A_{TM}$. לו הייתה מכונה M_2 שמכריעת את $HALT_{TM}$, היינו יכולים לבנות מכונה M_1 שמכריעת את A_{TM} סטירה.

נעשה זאת ע"י הרצת M_2 על M_1 . מ"ט עצרת ולכון אם היא עצרה ודוחתה, נעצור, אם היא עצרה וקיבלה, נריץ את M_1 על w ללא חשש שנתקע, ונחזיר מה- M מחזירה.

. $A_{TM} \subseteq HALT_{TM}$

$$. REG_{TM} = \{ \langle M \rangle : L(M \in \text{REG}) \}$$

טענה $.REG_{TM} \notin R$

תרגול

טענה אם $L_1 \cdot L_2 \in \text{RE}$ אז $,L_1, L_2 \in \text{RE}$

הוכחה: ראשית נתאר מ"ט M_3 שמצויה את השפה $\{u\#v : u \in L, v \in L_2\}$. אם M_1 מקבלת את u , תסמלץ את M_2 על v . אם M_2 מקבלת אז M_3 תקבל.

ובה"כ חלוקה היא באינדקס i או M_3 קיבל את המילה $s^{\#}$ אחרי מספר סופי k של צעדים.

אחרת תמשיך הלאה עד מיצויו כל החלוקה במס' j צעדים. לאחר מכן נגדיל את j ב-1 ונאפס את מונה החלוקות ל- $-l$ וכן $k = 0$.

אם קיימת חלוקה של w ל- u ו- v כך ש- M_1 לא תעצור או תדחה או ש- M_2 לא תעצור או תדחה ולכן אנחנו לא נעצור או נדחה.

הגדרה מכוֹן טיווּרִינְג אָנוֹבִירֶסְלִיטִית היא מ"ט שמקבלת כקלט מ"ט M ומילה w ומתנהגת בבדיקה כמו M על w , כלומר הינה מסמלצת את M על w כאשר היא מקבלת/דוחה/א עוצרת בהתאם ומסמלצת את תוכן הסרט.

הגדירה קידוד של מ"ט הוא $w_M \in \{0, 1, \#\}^*$

- נקודד את המיצבים ב- Q באמצעות מס' בינאריים בסדר עולה, מופרדים ע"י #(...#0#1#00#...). לבסוף נסיף ####.
 - נקודד את Γ (וכך גם את $\Gamma \subseteq \Sigma$). נעשה זאת באמצעות קידוד ביןארי, שהוא אורך $|\Gamma| \log_2 |\Gamma|$, ולבסוף ####.
 - נקודד את פ' המעברים δ ע"י $\langle \cdot \rangle \langle q \rangle \# \langle \sigma \rangle \# \langle q' \rangle \# \langle \sigma' \rangle \# \langle L/R \rangle$ #### זה הקידוד של אובייקט כלשהו), כאשר R הוא אובייקט כלשהו. לבסוף נסיף #### $\langle L \rangle = 0, \langle L \rangle = 1$.
 - נקודד את המיצבים המיוחדים ע"י $. \langle q_0 \rangle \# \langle q_{acc} \rangle \# \langle q_{rej} \rangle$.

נבנה מ"ט אוניברסילית U שמקבלת כקלט $\langle w, M \rangle$. U תהיה מכונה עם 3 סרטים. בסרט הראשון יהיה שמור תיאור של M , הסרט השני תבצע סימולציה של הסרט השלישי M , והסרט השלישי ישמר את המצב הנוכחי שבו M נמצא וישמש לחישובים.

תפעל בד:

1. תסורך את סרט 1 ותמצא את w .

2. תעתק את w לסרט 2 ותחזיר את הראש הקורא השני לתחילת סרט 2 ואת הראש הראשון לתחילת הסרט הראשון.

3. תסורך את סרט 1, תמצא את q_0 ותעתק לסרט 3 ושוב תחזיר את ראש 1 להתחלה.

4. בכל איטרציה :

- תשווה את המצב בסרט 3 ל- q_{acc}, q_{rej} ותקבל/תדחה לפי הצורך.

- תסורך את סרט 1 ותמצא את תחילת התיאור של δ .

- תשווה את המצב בסרט 3 והאות מתחת הראש הסרט 2 לכל המעברים עד שתמצא את המעבר המתאים.

- תחליף את האות מתחת הראש הסרט 2 בהתאם למעבר שנמצא ותעביר את ראש 2 ימינה/שמאליה בהתאם.

- תחליף את המצב בסרט 3 לפי המעבר שנמצא.

הגדירה מכונת טיורינג א"ד (NTM) היא מ"ט עם $w \in L(N)$ אם וקצת קיימת ריצה מקבלת של N על w .

בහינתן מילה $L^* \in w$, עץ הריצה של מ"ט א"ד N על w הוא $T_{N,w} = \langle V, E \rangle$ המוגדר כך : תהי C קבוצה כל הקונפ' האפשריות בריצה כלשיי של N על w .

- כלומר כל קודקוד מגדר קונפ' ומיקום בריצה.

- שורש העץ הוא $\langle q_0 w, 0 \rangle$.

- $E \subseteq \bigcup_{i \geq 0} (C \times \{i\}) \times (C \times \{i+1\})$ כאשר $E(\langle c, i \rangle, \langle d, i+1 \rangle)$ היא קונפ' עוקבת של c .

טענה לכל מ"ט א"ד N קיימת מ"ט דטרמיניסטית M שסקולה לה.

הוכחה : M תפעל כך : בהינתן Σ^* w , M תבנה במהלך הריצה את עץ הריצה של N על w שלב אחר שלב, תוך שהיא מבצעת חיפוש BFS על הקודקודים ומחפשת מצב מקבל.

אם נמצא מצב מקבל, M מקבלת את w . אם כל הענפים עצרו במצב דוחה, M דוחה את w . אחרת, M ממשיך לזרץ ולא תעוצר על w .

■ כל לראות ש- M מקבלת/דוחה/לא עוצרת אם w מקבלת/דוחה/לא עוצרת.

הערה הבנייה הנ"ל מתרגמת ב- $\mathcal{O}(|Q|^{|w|})$. לא ידוע האם אפשר לעשות זאת בזמן קצר יותר.

שבוע VII | רזוקציה

הרצאה

חלק א' של החרצאה

הגדירה $\Sigma^* \rightarrow \Sigma^*$ היא פונקציה ניתנת לחישוב אם קיימת מ"ט M_f שבгинתו קלט x , עוצרת עם $f(x)$ על הشرط.

דוגמה $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ המוגדרת ע"י $f(x, y) = x + y$. נניח ש- y, x מקודדים באונריית, אז נניח שקיבלו את y, x בהפרדה של #, כל שנctrיך לעשות הוא להסיר את ה-# ולהזיז את y אחד שמאלה.

דוגמה מ"ט \rightarrow מ"ט f , המוגדרת ע"י $\langle\langle M' \rangle\rangle f = L(M) \cap \langle\langle M' \rangle\rangle$ לא עוצרת על קלטים שאינם ב- $L(M)$. נctrיך לקבל קידוד של מכונה, אז לקודד מצב q_{loop} עם חוג עצמי ולשנות את המעברים שהולכים ל- q_{loop} .

הגדירה עבור שתי שפות Σ^* , נאמר כי $A, B \subseteq \Sigma^*$ ניתנת לרדוקציה מיפוי ל- B ונסמן $A \leq_m B$ אם קיימת פ'נית לחישוב $\Sigma^* \rightarrow \Sigma^*$ כך שלכל $w \in A$ מתקיים $w \in B \iff f(w) \in B$

הערה אם $A \leq_m B$ אז נוכל במקומות לשאול שאלות שיכוות ל- A נוכל לשאול לשיכוות ב- B .

דוגמה $f(y) = \{x : |x| \leq 5\}, B = \{x : |x| \leq 10\}$. נניח שקשה לנו לחשב האם $w \in A$, נוכל להגיד $y = 2w$ ועם הפ' הזו יתקיים $A \leq_m B$ וכן נוכל להיעזר בשיכוות ל- B כדי להגיד דברים על A .

משפט (הרדווקציה) לכל $A, B \leq_m B, A \leq_m B$

הוכחה: יהיו מ"ט M_B שמכריעה את B ומ"ט M_A שמחשבת את הרדווקציה מ- A ל- B . נבנה M_A שמכריעה את A .

בгинון $w \in \Sigma^*$ מರיצה את M_f על w ואז מריצה את M_B על $f(w)$ ועונה כמוה.

נשים לב ש- w עוצרת על כל קלט והיא נכונה כי $w \in A \iff f(w) \in B \iff f(w) \in L(M_B)$

מסקנה אם $A \leq_m B$ אז A "M-קלה".

הערה נשתמש הרבה במשפט הרדווקציה כי אם $A \leq_m B$ ו- $B \notin R$ אז $A \notin R$.

דוגמה נראה ש- w שעובד ש- R אם $w \in A_{TM} \leq_m HALT_{TM}$ אך $w \notin HALT_{TM}$. נראה ש- w לא שעובד. נctrיך גדייר פ' $\{A_{TM} \mid f(\langle\langle M \rangle\rangle, w) = \langle\langle M' \rangle\rangle, w' \in \{A_{TM}\}$ קלטים ל- M מתקבלת את w אם עוצרת על w' .

בгинון w הפ' f תחזיר $w' = w$ מכונה שעובד רק כשהיא מקבלת ואחרות מתבדרת (כמו שראינו בדוגמה לעיל) עם $(q_{loop}$.

אכן ניתן לחישוב. וכן מתקיים כי $(\langle\langle M \rangle\rangle, w) \in A_{TM} \iff (\langle\langle M' \rangle\rangle, w') \in HALT_{TM}$

• אם $w \in A_{TM}$ אז $w' \in HALT_{TM}$ עוצרת על w .

• ואם $w \notin A_{TM}$ אז $w' \notin HALT_{TM}$ לא עוצרת על w .

כלומר אם M דחפה את w , אז M' תגיע ל- q_{loop} ותתקע על w' .

דוגמה M עוצרת על ϵ . $HALT_{TM}^\epsilon = \{\langle M \rangle : L(M) \in \text{REG}\}$. זו שפה ב-RE כי אפשר פשוט להריץ ולקבל אם עוצרים (ואם נתקעים אז זה בסדר). נוכח

$$. HALT_{TM}^\epsilon \leq_m HALT_{TM}^\epsilon \notin R$$

נגיד $\{ \text{קלטים ל-} f \mid \langle M' \rangle \text{ כasher } M' \text{ היא מכונה שМОוחקת את}\}$ מילת הקלט ומריצה את M על w (לא משנה מה הקלט, בפרט אם הוא ϵ).
אכן f ניתן לחישוב כי כל מה שצריך לעשות זה למחוק כמה אוטיות, להוסיף מילה קבועה וללכט למכב החתולי של M .

עוצרת על w אם M' מסמלצת ריצה של M על w בהינתן כל קלט.

דוגמה $\text{REG}_{TM} = \{\langle M \rangle : L(M) \in \text{REG}\}$. נוכח כי $\text{REG}_{TM} \notin \text{co-RE}$ וגם לא $\text{REG}_{TM} \notin \text{RE}$. ראשית נראה כי $\text{REG}_{TM} \leq_m \text{REG}_{TM}$.

נראה כי $A_{TM} \leq_m \text{REG}_{TM}$, כלומר, נראה שיש פ' f שבהינתן w , $\langle M \rangle$ (קלט למ"ט ב- A_{TM}), מזירה $\langle M' \rangle$ (קלט למ"ט ב- REG_{TM}) כך ש- M מקבלת את w אם M' רגולרית (w לא משנה ממש כמובן).

בהינתן w , נגיד M' שמקבלת $x \in (0+1)^*$ כך:

1. אם $x \in \{0^n 1^n : n \geq 0\}$ אז M' מקבלת את x .

2. אחרת M' מריצה את M על w ועונה כמוות.

הזרוקציה נcona, ככלומר, אם $\langle M' \rangle \in \text{REG}_{TM}$ אז $\langle M, w \rangle \in A_{TM}$ כי:

1. אם M מקבלת את w אז נזיר M' שמקבלת כל $(0+1)^*$ (או שנתקבל בשלב הראשון או שבוטח מקבלת בשלב השני) ככלומר

$$\text{שזה אכן רגולרי. } L(M') = (0+1)^*$$

2. אם M לא מקבלת את w אז נזיר M' שמקבלת את $(0+1)^*$ אם $x \in (0+1)^*$ אז $x \in \{0^n 1^n : n \geq 0\}$ (שזה אכן לא רגולרי).

נשים לב שלא בנינו כאן מבחין לשפות רגולריות, אלא רק התאמה בין השאלה ("קלה") האם M מקבלת את w לשאלה ("קשה") האם שפה של מ"ט היא רגולרית.

M היא אחת מבין שתי אפשרויות: $(0+1)^*$ שהוא רגולרי ומיצג קבלה של M על w ו- $\{0^n 1^n : n \geq 0\}$ שמייצג אי קבלה של M על w (שפות הדמה הן proxy לשאלה הקבלה של M).

לכן $\text{REG}_{TM} \notin R$ ויזע כי $A_{TM} \notin R$ וכן $A_{TM} \leq_m \text{REG}_{TM}$

משפט (הזרוקציה, גרסה (RE)) אם $A \in \text{RE}$ אז $B \in \text{RE}$ ו- $A \leq_m B$ $\iff A \leq_m \overline{B}$ (באמצעות אותה פ' ניתנת לחישוב).

הערה אם $A \leq_m B$ אז $\overline{A} \leq_m \overline{B}$.

דוגמה נMISS' עם REG. ידוע כי $A_{TM} \in \text{RE} \setminus \text{REG}_{TM}$ (אחרת $A_{TM} \in \text{REG}_{TM}$ ו- $A_{TM} \in \text{RE} \cap \text{co-RE} = R$).

לכן מיהיות $A_{TM} \leq_m \text{REG}_{TM}$ (הוכחנו לעיל) הרו ש- $\text{REG}_{TM} \notin \text{co-RE}$.

במיש' לנימוק חנ'ל, $\text{REG}_{TM} \notin \text{RE}$ ומשמעותו $\overline{A_{TM}} \leq_m \text{REG}_{TM}$ נקבל $\text{RE} \subseteq \overline{A_{TM}}$ ו- $\overline{A_{TM}} \neq \text{RE}$.

לשם כך מספיק שונוכיח כי $A_{TM} \leq_m \overline{\text{REG}_{TM}}$ ואז מההערה חנ'ל נקבל את הנדרש.

נמצא פ' ניתנת לחישוב שעבור M מתקיים ש- M מקבלת את w אם ו惩 $L(M)$ לא רגולרית.

על קלט $x \in (0+1)^*$ המכוון' M' תפעל כך:

1. אם $x \in \{0^n 1^n : n \geq 0\}$ אז M' מרכיב את M על w ועונה כמוותה.

2. אחרת תדחה את x .

הרדוקציה נכונה, כולם M מקבלת על w אם ו惩 $L(M) \notin \text{REG}$ כי:

• אם M מקבלת את w אז $L(M') = \{0^n 1^n : n \geq 0\} \notin \text{REG}$

• אם M לא מקבלת את w אז נדחה ב-1 תמיד וגם ב-2 ולכן $L(M') = \emptyset \in \text{REG}$

חלק ב' של הרצאה

דוגמה מתקיים $(00)^* \leq_m A_{TM}$. $A = (00)^*$, $B = A_{TM}$ (איינטואיטיבית * (00) מאד קלה). נוכיח זאת.

$$f(x) = \begin{cases} \langle M_1 \rangle, \epsilon & x \in (00)^* \\ \langle M_2 \rangle, \epsilon & x \notin (00)^* \end{cases}$$

ונדר

לא מתקיים כמובן $(00)^* \in R$ כי $A_{TM} \leq_m (00)^*$ אבל כמובן ש- R

דוגמה בבעיית הריצוף יש לנו אריכים עם ארבעה צבעים בכל כיוון ואנו נורווגים לרצף "יפה". פורמלית,

$TILE = \{\langle T, H, V, t_0 \rangle : 1 \leq n \text{ לכל } n \times n \text{ יש ריצוף חוקי}\}$

כאשר:

• $T = \{t_0, \dots, t_k\}$ קבוצה סופית של אריכים.

• H תנאי שכנות במאוזן $(t, t') \in H$ אם ו惩 t, t' יכולים לשמש את t משמאלי ל- t' .

• V תנאי שכנות במאונך.

• אריך התחלתי t_0 .

וრיצוף חוקי הוא $\forall i \in [n-1], j \in [n] \exists f : [n] \times [n] \rightarrow T$ כך $f(i, j), f(i+1, j) \in H$ ו- $f(1, 1) = t_0$ ומתקיים $f(1, 1) = t_0$ ו- $f(i, j) = t$ אם $i \in [n], j \in [n-1]$ ו- $f(i, j) = t'$ אם $i \in [n], j \in [n-1]$.

ונכיה כי $TILE \in \text{co-RE}$, כלומר שקיימת מכונה שモזהה האם קיים $t \in T$ כך שאין ריצוף חוקי $n \times n$ כי $TILE \in \overline{\text{RE}}$, כלומר שקיימת מכונה שモזהה האם קיים $t \in T$ כך שאין ריצוף חוקי $n \times n$.

המכונה פשוט תבדוק את כל $|T|^{n^2}$ הריצופים $n \times n$ ואם אין עבור n כלשהו, מקבלת, אחרת תמשיך ל- $n+1$ הבא.

ונכיה ש- $TILE \notin R$ (ומכוון לכך גם $TILE \notin \text{RE}$). נשים לב שהגדרה שקולת של $TILE$ היא

$TILE = \{\langle T, H, V, t_0 \rangle : \text{יש ריצוף חוקי של ריבע מיشور}\}$

כasher ריצוף חוקי על רבע מישור משמעו שקיימת $T \rightarrow \mathbb{N} \times \mathbb{N}$ כך שמתקיים יחס שכנות חוקיים לכל \mathbb{N} .
נראה את שיקילות ההגדרות באמצעות הלמה של קניג, לפיה בעז מכון אינסופי עם דרגת פיצול סופית, יש מסלול אינסופי. נגדיר עץ באופן הבא:

השורש יהיה ריצוף 1×1 והילדים שלו יהיו כל הריצופים החוקיים 2×2 שמכילים את הריצוף, והילדים שלהם יהיו כל הריצופים 3×3 שמכילים את ההורדים שלהם וכו'. מהלמה של קניג, יש כאן מסלול אינסופי ולכן יש שייכות ל-TILE (נדר בעז כמה שצדך עד שנגיאו לריצוף שמכיל את j , i , כדי לראות שהשכנות חוקיות).

נחוור להוכיח ש-R-TILE $\notin \overline{\text{HALT}_{TM}^e}$. נראה ש- Γ (כל המ"ט שלא עוצרות על ϵ) ניתנת לדודקציית מיפוי ל-TILE.
קונפ' של M היא מילה ב- Γ^* . גרים לכל קונפ' להיות שורה של ארכיטים ברבע מישור ונגידר שכנות חוקיות רק אם קונפ' הנו עוקבות בדרכו של M על ϵ . לבסוף יהיה ריצוף חוקי אינסופי אם M לא עוצרת אף פעם על ϵ כלומר $\langle M \rangle \in \overline{\text{HALT}_{TM}^e}$.
נגדיר את הארכיטים שימשו את הרעיון:

1. מרכפות השורה הראשונה: $t_0 \xrightarrow{*} \dots$ והוא $\xrightarrow{*} \dots$
2. מרכפות שמתאימות לתזוזה של הראש.
3. ריפוד: לכל $\Gamma \in c$, נוסיף את המרכפת \xrightarrow{c} .

תרגול

משפט (חרדוקציה ל-RE) יהו L_1, L_2 שפות כך ש- $L_1 \leq_m L_2$ אם גם $L_2 \in \text{RE}$.

1. אם $L_1 \in \text{RE}$ אז גם $L_2 \in \text{RE}$.
2. אם $L_2 \in \text{co-RE}$ אז גם $L_1 \in \text{co-RE}$.

הוכחה: קיימת מ"ט M שמצויה את L_2 ופ' ניתנת לחישוב $\Sigma^* \rightarrow f : \Sigma^* \rightarrow L_2$ כך ש- $f(x) \in L_1$ אם ורק אם $x \in L_1$ $\iff f(x) \in L_2$.
শUCHASHBAT AT f. נגידר N שמצויה את L_1 : N תחשב את $f(X)$ ותסמלץ את ריצת M על $f(x)$.
נשים לב כי N מקבלת את x אם $f(x) \in L_2$ אם $f(x) \in L_1$ מקבלת את x . לכן N מזזה את L_1 כלומר RE

הערה כדי להוכיח רדוקציה מיפוי נבצע שלושה שלבים:

1. נזזה את הצורה של הרדוקציה ונבחר פ' מיפוי.
2. נוכיח שהפ' ניתן לחישוב.
3. נוכיח נכונות של הרדוקציה.

סיכום שפות

$A_{TM} \leq_m ALL_{TM}$ (ויאו). $ALL_{TM} \in \overline{\text{RE} \cup \text{co-RE}}$. נוכיח כי $ALL_{TM} = \{\langle M \rangle : L(M) = \Sigma^*\}$.¹

$$\overline{A_{TM}} \leq_m ALL_{TM}$$

(א) נראה ש- $x \in A_{TM} \iff f(x) \in ALL_{TM}$. נמצא פ' ניתנת לחישוב f שמקיימת על w ומקבלת

$$\langle M, w \rangle \in A_{TM} \iff f(\langle M, w \rangle) = \langle M' \rangle \in ALL_{TM}$$

נגידיר את f כך: $\langle M, w \rangle \mapsto M'$ שפועלת כך: בהינתן $M', x \in \Sigma^*$ מתעלמת מ- x ומסמלצת את M על w ומקבלת את (כל) x אם "ס" M מקבלת את w .

נשים לב כי f ניתן לחישוב כי ניתן בזמן סופי ליצר את M' שמסמלצת את M על w .

אם $L(M') = \Sigma^*$ אז M מקבלת את w (מההגדירה) ולכנ"ט M קיבל את x ואז $L(M') \neq \Sigma^*$ ובפרט $L(M') = \emptyset$ לא מקבל את w ואז M לא קיבל אף מילה כלומר \emptyset ונדרש

לכן סה"כ קיבלנו $\langle M, w \rangle \in A_{TM}$ אם "ס" M' $\in ALL_{TM}$ נסמלץ של הרדיקוציה.

(ב) נראה ש- $ALL_{TM} \notin \text{RE}$ ע"י רדוקציה מ- $\overline{A_{TM}}$. נגידיר f שהינתן $\langle M, w \rangle$, מפנה למ"ט M' שפועלת כך: בהינתן x , נסמלץ

את M על w לשאך $|x|$ צעדים ונדרה אם "ס" M קיבלה.

ניתן לחישוב כי חישוב מילה אפשר לעשות בזמן סופי, ולהזכיר מ"ט שמסמלצת את ה"ג" גם קורה בזמן סופי.

אם $L(M) \neq \Sigma^*$ לא מקבלת על w ולכנ"ט M תמיד מקבל (כי M אף פעם לא מקבל את w לא משנה כמה צעדים נרץ

אותה) כלומר $L(M') = \Sigma^*$

אם $L(M) = \Sigma^*$ אז M מקבלת את w ולכנ"ט M' תזדהה מותישחו כי עבור קלט מסוים אורך נסמלץ את M על w מספיק

צעדים כך שתתקבל ואז נדרה. לכן $L(M') \neq \Sigma^*$

לכן סה"כ קיבלנו $\langle M, w \rangle \in \overline{A_{TM}}$ אם "ס" M' נסמלץ של הרדיקוציה.

.2

$$U = USELESS = \{\langle M \rangle : \text{יש מצד ב-} M \text{ שאין } q_{acc} \text{ ו-} q_{rej} \text{ שלא מבקרים בו לעולם}\}$$

נשים לב שגם אם יש בפ' המעברים מעבר למצב לא בהכרח שנגיעה אליו. נראה ש-

(א) ראשית נראה כי $U \in \text{co-RE}$. נבנה מ"ט T שמצויה את \overline{U} , כלומר אוסף המ"ט שהבאים כל המ מצבים משומשים, שתפעל כך:

T תבודוק אם הקלט הוא קידוד תקין של מ"ט, אם לא, תקבל. אחרת נסמן $\langle M \rangle = x$ ואז T תסמלץ את ריצת $\langle M \rangle$ במקביל באופן אינקרמנטלי (בסדר minlex) ותשמר על סרט נפרד את כל המ מצבים שבוקרו עד כה. אם כל המ מצבים חוץ מ- M בוקרו, T תקבל את $\langle M \rangle$ (אחרת נתקע).

מכונה כי אם $x \in \overline{L}$ אז או x לא קידוד תקין של מ"ט ואז T מקבלת או ש- $\langle M \rangle = x$ ו- M -ת בקורסוט בכל המ מצבים של T

מתישחו כלומר T תקבל. אם $\overline{L} \neq x$ אז M יש מצב לא ישיג ולכנ"ט T אף פעם לא תקבל כלומר תרצו לנצח. לכן

$$L(T) = \overline{U}$$

(ב) נוכח כי $\text{RE} \notin \overline{A_{TM}}$. נראה רדוקציית מיפוי מ- L - U .

$$\langle M, w \rangle \in \overline{A_{TM}} \iff \langle M' \rangle = f(\langle M, w \rangle) \in U$$

כלומר, M לא מקבלת את w אם ו惩 M' מקבל לא ישג.

נגידיר f : תmphה את $\langle M, w \rangle$ ל- M' שפועלת כך: בהינתן x , M' תסמלץ את M על w . אם M מקבלת את w , M' תיכנס

למצב חדש שמננו תברך בכל מצבה (של M') לא כולל q_{acc} , q_{rej} , אחרות M' דוחה (ולא עוברת במצב החדש).

אם $\langle M, w \rangle \in \overline{A_{TM}}$ אז M לא מקבלת על w ולכן M' לעולם לא תברך במצב החדש כלומר $U \langle M' \rangle$

אם $\langle M, w \rangle \notin \overline{A_{TM}}$ אז M מקבלת על w لكن M' עוברת על כל המצבים שלה כלומר $U \langle M' \rangle \notin \overline{A_{TM}}$

f ניתן לחישוב כי סמלץ היא פעולה חשיבה, לכן יותר להראות שנייתן ממש את מצב הטויל. נסיף @ לא"ב של M' .

מעבר במצב טיול ל-@ במצב הראשו של M' ובכל מצב נסיף מעבר עם @ למעבר הבא בקידוד כשאנו לא מזיזים את הראש

(ראיינו שקל לעשوت). להסביר את הקידוד הזה אפשר לעשות בזמן לינארי במספר המצבים, שזה כמובן סופי.

.3

$$REP = REPEAT = \{\langle M, w \rangle : \text{מ"ט שלא עוצרת על } w \text{ ויש קונפ' בריצת } M \text{ על } w \text{ שחזרה פעמיים}\}$$

נשים לב שם יש קונפ' כזו, אף פעם לא נעצור (נחזיר עליה שוב ושוב). בנוסף, קל לבנות מכונה שלא עוצרת אבל שאין לה קונפ' חוזרת (לדוגמה הולך ימינה כל הזמן). נראה ש- $R \in \text{RE} \setminus \text{R}$.

(א) נגידיר T מ"ט שמזזה את REP . T תפעל כך: בהינתן $\langle M, w \rangle$ היא תסמלץ את M על w תוך שמירת כל הקונפ' שבוקרו עד

כה בסרטט נפרד. בכל שלב היא תסרוק את הקונפ' הקודמות ותשווה לנוכחית. אם נמצאה חזרה, T תקבל את $\langle M, w \rangle$. אם

עוצרת אז T תיכנס ללולאה אינסופית.

T ניתן למימוש כי סמלץ ראיינו אכן ייך לעשות ומעקב קונפ' זו פעולה חשיבה.

אם $\langle M, w \rangle \in REP$ אז M לא עוצרת על w ויש חזרה על קונפ' בריצת M על w . לכן T ברגע השני של הקונפ' תזזה את

החזרה ותקבל את $\langle M, w \rangle$.

אם $\langle M, w \rangle \notin REP$ אז M לא חוזרת על w כלומר T לא עוצרת על $\langle M, w \rangle$.

(ב) נראה ש- $HALT_{TM} \leq_m REP$ רדוקצייה. צריך להתקיים $HALT_{TM} \leq_m REP \notin \text{co-RE}$.

$$\langle M, w \rangle \in HALT_{TM} \iff \langle N, w' \rangle \in REP$$

כלומר M עוצרת על w אם ו惩 N שחזרת בריצת N על w' .

נגידיר f שהינתן $\langle N, w' \rangle$, מחזירה $\langle M, w \rangle$ שמסמלצת את M על w , ואם היא עוצרת, N תחזיר על קונפ' שלה (תיכנס ללולאה שלא משנה את הסרטט), ואחרת נתקע וכמובן לא חוזר על קונפ'.

f ניתן לחישוב כי צריך רק להוציא עוד מצב ללולאה של הקונפ' החזרת לקידוד המ"ט. נכוונות נובעת ישירות.

שבוע XII | תורת הסיבוכיות

הרצאה

חלק א' של הרצאה

נסים את ההוכחה שבעיית הריצוף אינה כריעה. ראיינו ש- $TILE$ קולה לרכיב חוקי של רבע מישור באמצעות הלמה של קניג. נעשה

$$TILE \notin R - \overline{HALT}_{TM}^{\epsilon}$$

מסוף הרצאה הקודמת:

נוצרים לכל קונפ' להיות שורה של אריחים בربע מישור ונגידר שכנות חוקית רק אם קונפ' הן עוקבות בריצה של M על ϵ . לבסוף

$$\langle M \rangle \in \overline{HALT}_{TM}^{\epsilon} \text{ לא עוצרת אף פעם על } \epsilon \text{ כלומר}$$

האריחים בהם השתמש הם כדלקמן:

$$1. \text{ מרצפות השורה הראשונה: } t_0 \text{ הוא } \boxed{- \quad - \quad *} \text{ והשאר הם } \boxed{* \quad \overset{(q_0, -)}{-} \quad *}$$

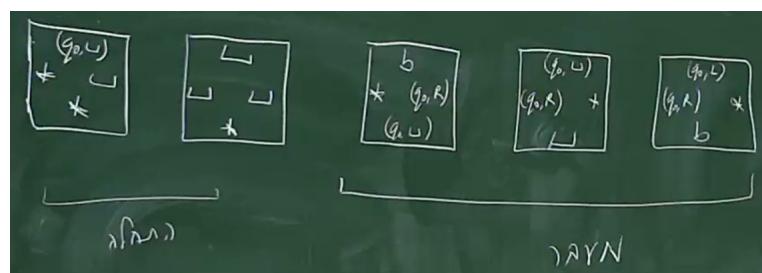
2. מרצפות עבור מעברים:

$$\begin{aligned} & \boxed{\begin{matrix} (q', c) \\ (q', R) \\ c \end{matrix}} * \text{ גם } c \in \Gamma \text{ וכל אות } \Gamma \text{ ולבסוף } \boxed{* \quad \overset{b}{(q', R)} \quad (q, a)} \text{ המרצפת } q, q \notin \{q_{acc}, q_{rej}\} \text{ עבור } \delta(q, a) = (q', b, R) \\ & * \quad \boxed{\begin{matrix} (q', c) \\ (q', L) \\ c \end{matrix}} \text{ גם } c \in \Gamma \text{ וכל אות } \Gamma \text{ ולבסוף } \boxed{(q', L) \quad \overset{b}{*} \quad (q, a)} \text{ המרצפת } q, q \notin \{q_{acc}, q_{rej}\} \text{ עבור } \delta(q, a) = (q', b, L) \end{aligned}$$

$$3. \text{ ריפוד: לכל } \Gamma \in \Gamma, c \in \Gamma \text{ נוסיף את המרצפת } \boxed{* \quad \overset{c}{*} \quad c}$$

נשים לב כי ב- T יש 2 מרצפות התחלתיות, $|\Gamma| + 1$ לכל מעבר $-|\Gamma|$ ריפוד כלומר מספר סופי פרופורציוני $-|\Gamma|$.

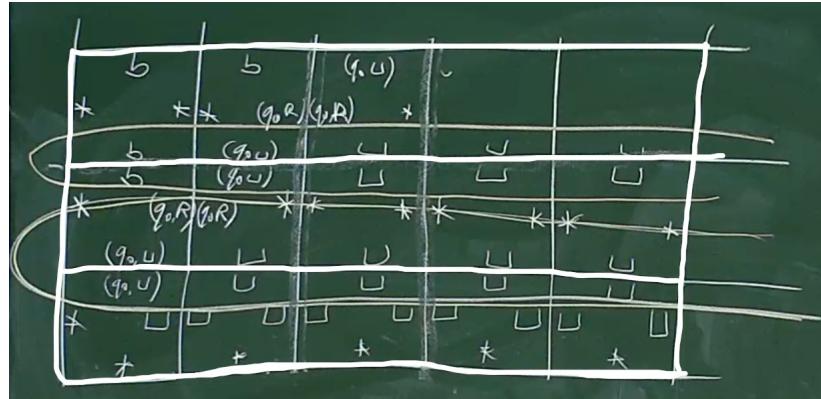
דוגמה נגדיר מ"ט עם $\{ _, b \} = \Gamma$ ופ' מעברים $\{ _, \delta \}$. $\delta(q_0, _) = (q_0, b, R)$ זו מכונה שלא עוצרת אף פעם (כל הזמן הולכת ימינה). נראה שאכן הרזקציה מניבה ריצוף חוקי.



איור 37 : המרצפות ב- T המתאימים למ"ט שהגדכנו, בלי מרצפות הריפוד

בහינתן הקונפ' התחלтиית (השורה הראשונה, המוגדרת עם t_0), ננסה לבנות ריצוף חוקי. באירור נין לראות את הריצוף, כאשר השרוולים על הצלעות הצמודות כיצד הקונפ' מटבطة בחיבור זהה. נשים לב כי לאחר הקונפ' התחלתי, הדבר היחיד

שאפשר לעשות זה להוסיף מעלה שורה שגדירה את הקונפ' bq_0 , ואז בשורה הבאה העיקרי אפשר לבחור משהו אחר עבור האות השמאלי ביותר אבל נתעלם לעת מהמקרה הזה - אחד הריצופים החוקיים שנייתן לשים הוא באמצעות הקונפ' השלישי בירצ'ת המ"ט על ϵ וכן הלאה.



איור 38 : דוגמת ריצוף לקונפ' המגדירות את ריצ'ת המ"ט על ϵ

טענה M לא עוצרת על ϵ אם יש ריצוף חוקי של רביע מישור עם T המושרה מ- M .

הוכחה: \Leftarrow : זה עתה הרנו את הקונפ' שמאפשרות ריצוף שיכולה להמשיך עד אין סוף לדוגמה הספציפית הזו, אבל זה מותקיים גם במקרה הכללי (פשוט לא נראה פורמלית).

\Rightarrow : אם היינו עוצרים אז היה לנו q_{acc}/q_{rej} ואז לא היו לנו מרצפות חוקיות להמשיך איתן למעלה (המרצפות מוגדרות לכל $q \notin \{q_{acc}, q_{rej}\}$).
בrama העקרונית: אם היינו מושגים עוד ראש קורא באրיך השמאלי באיזשהו שלב (אפשרי מהגדרת הארכיהם), היינו רק מקשים על עצמונו כי ככל הפחות יהיו לנו יותר מרצפות לא חוקיות (כלו עם (q_{acc}, q_{rej}) ■

עד כה ראיינו את RE, RE, co-REG, R. עתה נסתכל מה קורה בתוך R. ראיינו אפיון אחד והוא סיוג לפי REG, CFL וכו'. האפיון הנוסף שנייתן להביט בו על R הוא כמות המשאים שדרושים להכרעה (זמן, זכרון, אكريואות וכו').

דוגמה $\{0^k 1^k : k \geq 0\} = L$. כדי להכרייע את השפה, ניתן להגדיר מ"ט שמכרייע את השפה ע"י מכילה של ה-0 וה-1 הראשו וה-0 וה-1 השני וכו' עד שאין עוד אותיות. הסיבוכיות של האלג' היא $O(k^2)$ כי אנחנו עושים k איטרציות בכל אחת מהן דורשת O צעדים.

הגדירה לכל $\mathbb{N} \rightarrow \mathbb{N}$, גדרת מחלוקת

$$TIME(t(n)) = \{L : \text{זמן } O(t(|w|)) \text{ ועצרת על כל קלט } w \text{ תוך } \text{ צעדים}\}$$

דוגמה השפה הנ"ל היא ב- (n^2) TIME($n \log n$) ולמעשה גם ב- $(n \log n)$ מייקיה של חצי מהאותיות (וציפוי המילה) בכל פעם.

משמעות אם ניתן להכרייע את L ב- $(n \log n)$ (פחות ממש מ- $O(n \log n)$) אז L רגולרית.

מסקנה השפה הנ"ל לא ניתנת להכרעה בפחות מ- $\mathcal{O}(n \log n)$ צעדים.

הערה החד-סטריות חשובה כי אפשר לעשות כל מיני דברים במקביל שmagical בתוכם סיבוכיות יותר מורכבת עם כמה סרטים.

טענה (שראיינו בתרגול) לכל מ"ט רב סרטית דטר' שרצה בזמן $(t(n))$ יש מ"ט דטר' שcolaה שרצה בזמן $(t^2(n))$.

הגדרה נגדיר את המחלקה $NPTIME = \bigcup_{i \geq 0} TIME(n^i)$, כלומר כל השפות שניתן להכריע בזמן פולינומיAli, ונסמן $NP = NPTIME$.

הערה בגל שנסתכל על סיבוכיות פולינומיאלית לעומת פולינומיאלית, לא يعنيו אותנו עוד ריבוע על פולינום ולבן נוכל להניח שהמ"ט שלנו יכולה להיות גם רב סרטית.

הערה עבור מ"ט א"ד, נגדיר את זמן הריצה להיות המסלול הכי ארוך בעז הריצה (וכמובן נאמר שהיא מכניתה שפה אם כל הריצות שלה סופיות).

טענה (שראיינו בתרגול) לכל מ"ט א"ד שרצה בזמן $(t(n))$ ישנו מ"ט דטר' שcolaה שרצה בזמן $2^{\mathcal{O}(t(n))}$ (באמצעות סימולץ כל הריצות יחד).

הגדרה לכל $\mathbb{N} \rightarrow \mathbb{N}$ נגדיר

$$NTIME(t(n)) = \{L : \text{קיים מ"ט א"ד חד סרטית שמכניתה את } L \text{ ועוצרת על כל קלט } w \text{ תוך } \mathcal{O}(t(|w|)) \text{ צעדים}\}$$

הגדרה נגדיר את המחלקה $NPTIME = \bigcup_{i \geq 0} NTIME(n^i)$, כלומר כל השפות שניתן להכריע בזמן פולינומיאלי באמצעות ניחושים, ונסמן $NP = NPTIME$.

הגדרה $EXPTIME = \bigcup_{i \geq 0} TIME(2^{n^i})$ כלומר שניון בסיבוכיות אקס' להכריע אותן עם מ"ט דטר'.

הערה מתקיים $NP \subseteq EXPTIME$ אבל לא ידוע אילו מההכלות הן ממש ואייפה יש שוויון (לא ניתן שני שוויונים כי ידועות שפות ב- $P \setminus NP$).

דוגמה בהינתן גרף $G = \langle V, E \rangle$, מסלול אוילר- G הוא מסלול שעובר בכל הקשתות- G בבדיקה פעם אחת ומסלול אוילר- G הוא מסלול שעובר בכל הקודקודים- G בבדיקה פעם אחת.

נגדיר את המחלקות

$$D - ST - HAMPATH = \{\langle G, s, t \rangle : t \text{ גראן מכוון ויש מסלול המילטון מ-} s \text{ ל-} t \text{ פעם אחת}\}$$

-1

$$U - HAMPATH = \{\langle G \rangle : \text{לא מכון ומכל מסלול המילتون}\}$$

לא ידוע האם $P \in NP$ – ST – HAMPATH $\subseteq EXPTIME$ – D – ST – HAMPATH הוא מ"ט דטרמיניסטי שמכריע את זה בזמן אקס' שפועלת באופן הבא: בحينו t , G, s, t , עוברת על כל המיללים ב- V^n ולכל מילה, בודקת האם מתחילה ב- s מסתיימת ב- t ומכליה את כל הקודקודים בבדיקה פעם אחת ומהווה מסלול, ואם כן, מקבלת.

עתה נוכח כי $NP \in NP$ – ST – HAMPATH – D. מ"ט א"ד שמכריע את השפה בזמן פולינומיAli תפעל כך: בحينו t, G, s , מוחשת מילה π ב- V^n ומקבלת אם "ס" היא מסלול המיליטון מ- s ל- t .

הבדיקה על π דורשת זמן פולינומיAli ולכן השפה דורשת זמן פולינומיAli.

דוגמה $\text{COMPOSITE} = \{x \in \mathbb{N} : 1 \neq \exists p, q \in \mathbb{N}, n = pq\}$

COMPOSITE $\in EXPTIME$ כי אפשר לעבור על כל המיללים מ-1 ועד $2^{|x|}$ (מספר הספרות הבינאריות בהן הוא נתון) וראות אם הם מחלקים. בוסף COMPOSITE $\in NP$ כי אפשר להגדיר מ"ט א"ד שמכריע את COMPOSITE בזמן פולי' ע"י כך שהحينו x , היא תנחש \mathbb{N} עבورو $1 < p < x - 1$ ותקבל אם "ס" מחלק את x ללא שארית.

פ' המעברים לחלק של הגרלת p תקיים $\{\text{לסיים את הכתיבה}, \langle \text{לכתוב } 1 \rangle, \langle \text{לכתוב } 0 \rangle, \langle _ \rangle\}$. נשים לב כי אין לנו בדיקה ש- $1 < p < x - 1$ אבל פשוט נדחה אם זה המצב.

חלק ב' של הרצאה

הערה בעיות ב-NP מתאפיינות ע"י התכונות הבאות (מודגמות על ST – D – HAMPATH – D – NP אבל נכוונות לכלו):

- קשה להכריע האם יש מסלול המיליטוני בגרף.

- קל לבדוק האם מועמד למסלול המיליטוני אכן ממשכנע.

הערה לא ברור (אלא אם יש אפיון מתמטי) שאפשר לשכנע בנסיבות שאין מסלול המיליטוני (או כל בעיה אחרת).

דוגמה לבדוק שמספר הוא פריק זה קל, לבדוק האם הוא ראשוני גם אפשר לשכנע בנסיבות שאין מסלול המיליטוני (או כל בעיה אחרת).

דוגמה קריית x והדפסת * לכל $i = 1 \dots n$ עד x היא בעלת סיבוכיות ליניארית באורך הקלט אם x נתון בסיסיס אונארי, ואילו בסיבוכיות אקס' אם x נתון בסיסיס $b > 1$. זאת משום שבמקרה כזה אורך הקלט הוא $\log_b x$.

הגדרה מודא V עבר שפה L הוא מ"ט דטר' כך ש-{קיים c כך ש-} מקבלת את (w, c)

דוגמה נוכל להגיד מודא-HAMPATH כך שפטו G גраф מכובן ו- π -מ-המיליטון מסלול s ל- t : $\left(\frac{\langle G, s, t \rangle}{w}, \frac{\pi}{c} \right)$

הגדרה שפה L היא NP-שלמה אם $L \in NP$ ואם $P \in NP$ אז $P \subseteq L$, כלומר שנייה להכריעים בזמן פולי' עם מ"ט א"ד, ואם נמצא אלג' בזמן פולי' דטר' להכרעת L נפתר בעיה פתוחה במדמ"ח $?P \equiv NP$.

הערה אם L היא NP-שלמה אפשר להפסיק לחפש אלג' פולי' ל- L כי חיפוש אלג' כזו פותר בעיה פתוחה ולא סביר שסטם נפתר עכשו את $P = NP$.

הגדרה משתנה בוליאני הוא משתנה שמקבל ערכים מ- $\{T, F\}$.

נוסחה בוליאנית היא משתנה בוליאני, או $\varphi_1, \varphi_2 \wedge \varphi_3$ כאשר φ_1, φ_2 נוסחות בוליאניות.

בהתנן השמה $f : X \rightarrow \{T, F\}$ למשתני הנוסחה, ניתן לחשב את ערך האמת של הנוסחה (באינדוקציה).

$\ell_i^j \in \{x_1, \dots, x_n, \bar{x}_1, \dots, \bar{x}_n\}$ כאשר $(\ell_1^1 \vee \dots \vee \ell_1^{k_1}) \wedge \dots \wedge (\ell_m^1 \vee \dots \vee \ell_m^{k_m})$ נסחה θ היא ב-CNF אם θ מ machora.

דוגמא שפת הנוסחאות הспיקות היא NP-שלמה. ϕ נוסחה פסיפה $\text{SAT} = \{\langle \phi \rangle : \text{CNF } \phi\}$. משפט קוק-לוין הוכיח ש-SAT אס"

$$\text{P} = \text{NP}$$

טענה $\text{SAT} \in \text{NP}$

הוכחה: מ"ט א"ד עבור SAT פשוט תוחש השמה f עבור המשתנים ומשערכת את הנוסחה לפי f ואם השטערכה ל- T , מקבלת. בדומה, ניתן לוודא מועמד להשמה בזמן פוליאי ולכן מהאפיון השקול עם מודדים, SAT גם כו- NP עם המודד ששפטו

$$L(V) = \{\langle \theta, f \rangle : \theta \text{ נסחה ב-} f\text{-CNF ו-} \text{השמה מספקת עבור } \theta\}$$

■

תרגול

תרגיל L הוא L -MSCIMOT: $L = \{\langle M_1, M_2 \rangle : L(M_1), L(M_2)\}$ כאשר L_1, L_2 שפות 10 -MSCIMOT אם קיימות לפחות 10 מילים ב- Σ^* .

$$L \notin \overline{\text{RE}} \cup \overline{\text{co-RE}} \quad i \in [10] \quad w_i \in L_1 \iff w_i \in L_2 \quad \{w_i\}_{i=1}^{10}$$

1. נראה ש- $\text{HALT}_{TM}^\epsilon \leq L$ ע"י רזוקציה.

נדיר f באפנ הבא: בהינתן M , נזכיר שני מ"ט M_1, M_2 כך ש- M_1 מסמלצת את M על ϵ ועונה כמוות (אם היא עצרת), ו-

מקבלת כל קלט. ברור ש- f -חסיבה, נראה נכוונות.

אם $M \in \text{HALT}_{TM}^\epsilon$ אז M_1 מקבל כל קלט וגם M_2 וברור שהן 10 -MSCIMOT כלומר $L \in L$.

אם $\langle M_1, M_2 \rangle \notin L$ אז M_1 לא מקבל אף קלט ו- M_2 מקבל כל קלט ולכן לא מסכימות על שום דבר כלומר

2. נראה ש- $\text{RE} \leq L$ ע"י רזוקציה.

נדיר f באפנ הבא: בהינתן M , נזכיר שני מ"ט M_1, M_2 כך ש- M_1 מסמלצת את M על ϵ ועונה כמוות (אם היא עצרת), ו-

זוכה כל קלט (אותה בנייה רק ש- M_2 הפוכה). ברור ש- f -חסיבה, נראה נכוונות (הוכחה משלימה לנ"ל).

אם $\langle M_1, M_2 \rangle \in L$ אז M_1 לא מקבל אף קלט ו- M_2 גם לא מקבל אף קלט ולכן לא מסכימות על הכל ולבן L .

אם $\langle M_1, M_2 \rangle \notin L$ אז M_1 מקבל כל קלט ו- M_2 לא מקבל אף קלט כלומר $L \notin L$.

הגדרה תכונה סמנטית של מ"ט היא קבוצה P של מ"ט, כך שלכל זוג מ"ט M_1, M_2 אם $M_1 \in P$ ו- $M_2 \in P$ אז $L(M_1) = L(M_2)$.

משפט (רייס) נגדיר $L_P = \{\langle M \rangle : M \in P\}$ עבור P תכונה סמנטית לא טריוויאלית, אווי $R \notin$

דוגמא $L = \{\langle M \rangle : \forall w \in \Sigma^*, w \in L(M) \iff ww^Rww^R \in L(M)\}$. כאן התכונה הסמנטית P מכילה את כל המ"ט שעונთ. אותו הדבר על w ו- L $L_P = L, ww^Rww^R$ (מכילה קידודים).

טענה תהי P תכונה סמנטית לא טריוויאלית של מ"ט כך ש- $P \notin \text{co-RE}$ (כלומר $A_{TM} \leq L_P$ ו- $T_\emptyset \notin P$ (המכונה עם השפה הריקה), או $I_P \in A_{TM}$).

הוכחה: מהות P לא טריוויאלית, קיימות $\langle M, w \rangle \in A_{TM}$ -ן ו- $f \in P$ כך ש- $L(f) \neq \emptyset$ (רצתה f ב- P כי $\langle H \rangle \in P$ (כך ש- $\emptyset \neq L(H) \in P$)). נניח $x \in T_\emptyset \notin P$. נאמר $f(x) \in L_P$ כי $\langle M, w \rangle = \langle T \rangle \in L_P$.

נגיד f באופן הבא: בהינתן $\langle M, w \rangle$, תחזיר $\langle T \rangle$ מ"ט שפועלת כך - בהינתן x :

1. T תסמלץ את ריצת M על w . אם M דוחה T , אז x דוחה את w . אחרת אם מקבלת, ניבור לשלב הבא.

2. T תסמלץ את ריצת H על x והתענה כמוות.

חישיבה כי קל להניח מילה על הסרטן ולסמלץ מ"ט אחרית שנตอน הקידוד שלה מראש, נראה נכונות. אם $L(T) = L(H) \in A_{TM}$ או $\langle M, w \rangle \in A_{TM}$ ו- $L \in P$ ו- $H \in P$ ולכן מההגדרה $T \in P$ כלומר $\langle T \rangle \in L_P$

■ $T \notin P$ כי נדחה תמיד בשלב הראשון אבל $\emptyset \neq L(T) \neq \emptyset$ (כלומר מההגדרה $\langle M, w \rangle \notin A_{TM}$).

הוכחה: (משפט ריס) אם $L(H) \neq L(T) \neq \emptyset$ ו- $L(H) \notin \text{co-RE}$ ו- $L(T) \notin \text{co-RE}$ ו- $L_P \notin \text{co-RE}$ ו- $T_\emptyset \in P$ ולכן $L_P \notin \text{co-RE}$ ו- $L_P \notin P$ ו- $L_P \notin R$.

דוגמה ניתן להשתמש במשפט ריס (בלמה בתוכו) כדי להוכיח שפותה לא ב- R (לא בדוגמה הנ"ל כי היא הכללה זוגות של מ"ט ואנחנו יכולים להסתכל על שפה של קידודים של מ"ט ייחידה).

נסתכל על שפה של קידודים של מ"ט ייחידה. $\text{ALL}_{TM} = \{\langle M \rangle : L(M) = \Sigma^*\}$ ו- $\overline{\text{RE}} \cup \overline{\text{co-RE}}$ (מתוייחס לשפות בלבד) וגם $A_{TM} \leq \text{ALL}_{TM}$ ו- $L_P = \text{ALL}_{TM}$ (כלומר $\text{co-RE} \leq \text{ALL}_{TM}$).

דוגמה { w } מספר בייצוג בינארי שאינו ראשוןי: $\text{COMPOSITE} \in \text{NP}$. נוכיח כי $\text{COMPOSITE} = \{w : \text{נבנה } NTM \text{ שמכריעה את השפה } T \text{ תנחש גורם בין } 1 \text{ ל-} w \text{ וتبזוק בכל ענף בנפרד אם } a \text{ מחלק את } w\}$. כל בדיקה נעשית בזמן פולינומיائي.

דרך אחרת להסתכל על השפה (או המ"ט), היא שזה אוסף המספרים שאפשר לבדוק בזמן פולינומיائي האם הם בשפה באמצעות גורם שיתנתנו לנו.

הגדרה תהי V מ"ט דטר'. נאמר כי V מודא לשפה L אם

$$L = \{w : (\exists c : \langle w, c \rangle \in L(V))\}$$

ונאמר ש- V מודא פולי' אם

$$L = \{w : (\exists c : |w| \geq |c| \text{ בגודל פולינומי ב-} w \text{ ו-} \langle w, c \rangle \in L(V))\}$$

ו- V רצתה בזמן פולי' ב- w על $\langle w, c \rangle$.

משפט (שקלות הגדרת NP) $L \in NP$ אם ו רק אם קיימים לה מודא פוליאור.

הוכחה: \Rightarrow : אם קיימים ל- L מודא פוליאור V אז מהיות V פוליאור, קיימים $N \in k$ כך שלכל w ולכל c, V רץ על $\langle w, c \rangle$ בזמן פוליאור $-|w|$.

מ"ט א"ד N שמכריעה את L הפעלת c : עבור קלט w , תנחש c בגודל פוליאור $-|w|$ ותסמלץ את V על הניחוש.

V רצתה בזמן פוליאור ולכנן כל ענף בענף הריצות של N על w הוא באורך פוליאור.

\Leftarrow : יש מ"ט א"ד N שמכריעת את L . נבנה מודא V פולינומי ל- L : V מקבל $\langle c, w \rangle$ כאשר c הוא תיאור של ענף בענף הריצת N על w . בדוק ש- c היא אכן ריצה חוקית לפי פ' המעברים של N והאם היא מסתויימת במצב מקבל/דוחה, ותקבל/תדחה בהתאם.

מהיות N מ"ט א"ד שמכריעת את L בזמן פוליאור, ענף הריצת c הוא באורך פוליאור ($\geq |w|^k$ עבור איזשהו k) ולכן V רץ בזמן פוליאור על w (ולכן פוליאור $-|w|$). ■

שבוע 2 | שלמות ב- NP

הרצאה

חלק א' של הרצאה

רדווקציות פולינומיאליות

הגדרה $f : \Sigma^* \rightarrow \Sigma^*$ היא פ' ניתנת לחישוב בזמן פוליאור אם קיימת מ"ט M_f שעלה קלט x , עוצרת תוך מספר פוליאור $-x$ של צעדים עם $(f(x))$ על הסרט.

הגדרה $f : \Sigma^* \rightarrow \Sigma^*$ היא פ' ניתנת לרדווקציה פוליאור- B אם קיימת $A \leq_p B$ ונסמן $w \in A \iff f(w) \in B$, כלומר $w \in A \iff f(w) \in B$.

משפט (הרדווקציה עברו P) אם $A \in P$ אז $B \in P$ ו- $A \leq_p B$.

הוכחה: בהינתן M_f שמחשבת את הרדווקציה ו- M_B שמכריעת את B בזמן פוליאור, נבנה M_A שמכריעת את A בזמן פוליאור: בהינתן $w \in \Sigma^*$ המוכונה M_A תרץ את M_f , תחשב (בזמן פוליאור) את $f(w)$, תרץ את M_B על $f(w)$ (בזמן פוליאור $-|f(w)|$).

■ $w \in A \iff f(w) \in B \iff M_A \text{ פוליאור ו-} M_B \text{ פוליאור}$ ולכן $w \in A \iff f(w) \in B$.

מסקנה אם $B \notin P$ או $A \notin P$ ו- $A \leq_p B$ (קונטרה-פוזיטיב על משפט הרדווקציה).

הגדרה נאמר ששפה $L \subseteq \Sigma^*$ היא NP -שלמה אם :

1. $L \in NP$ (חסם עליון).

2. $L' \leq_p L, L' \in NP$ -קשה, כלומר שלכל שפה L' הקיים $L' \subseteq L$ (חסם תחתון).

הערה אינטואיטיבית, החסם התיכון אומר שכל דבר רע שאפשר להגיד ב- NP , אפשר להגיד גם על L .

הערה נאמר שבעה היא פתרה אם החסם התיכון והעליון שלנו הם שווים, כאמור שלמה בחלוקת כלשיי (ולא שהוא P -קשה ושיכת-ל- EXPTIME לדוגמה, שזה לא מכריע לנו את סיבוכיות הבעיה).

טענה אם $L \in \text{P}$ -קשה אז $L \in \text{NP}$ -קשה.

■ $L' \in P$ גם $L \in P$ וגם $L' \leq_p L$ ולכן $L' \in \text{NP}$ -קשה, הרו ש- P -קשה ($L' \in \text{NP}$).

טענה תהי L'' שפה NP -קשה, ו- Σ^* או $L'' \leq_p L$ או $L \subseteq \Sigma^*$ הינו NP -קשה (מטרזיטיביות של רדוקציות).

הערה זו הגדרה שקולה הרבה יותר נוחה להוכחת קושי-ב- NP .

טענה אם $B \neq \emptyset$, Σ^* לכל $A \leq_p B$ אז $A \in \text{P}$

הוכחה: נגדיר M_f שתפעל כך: בהינתן w , תבודק (בזמן P) האם $w \in A$ או $w \in B$, $w \notin B$ או $w \in A$. יהי $w \in A$.

■ $w \in A$ ניתנת לחישוב ונכונה ולכן $A \leq_p B$.

דוגמאות

1. { θ } נוסחה ספיקת-ב- 3CNF : $3\text{SAT} = \{\langle \theta \rangle : \text{3CNF}(\theta) \text{ true}\}$.

היא NP -שלמה.

2. גраф לא מקוון שיש בו קליקה בגודל k : $\text{CLIQUE} = \{\langle G, k \rangle : \text{CLIQUE}(G, k) \text{ true}\}$.

כל $E \subseteq V$ ניתן לנחש את הקבוצה ולעשות לה ולידציה בזמן פולי (יש $|V|^{|V|}$ צלעות לכל היותר לבדיקה).

טענה $3\text{SAT} \leq_p \text{CLIQUE}$

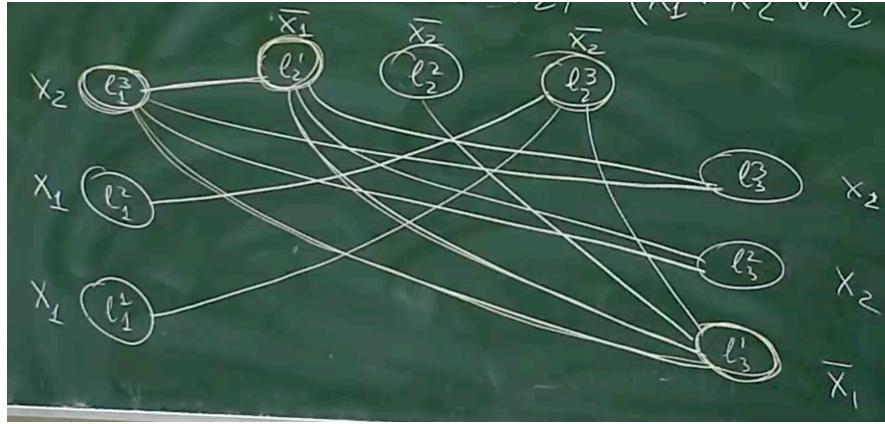
הוכחה: נסמן $c_i = \ell_i^1 \vee \ell_i^2 \vee \ell_i^3$, $\theta = c_1 \wedge \dots \wedge c_m$ ונזכיר f באופן הבא: בהינתן θ , נחזיר $\ell_i^j \in \{x_1, \dots, x_n, \bar{x}_1, \dots, \bar{x}_n\}$ כasher $c_i = \ell_i^1 \vee \ell_i^2 \vee \ell_i^3$, $\theta = c_1 \wedge \dots \wedge c_m$ ו- Σ^* כי אפשר לנחש את הקבוצה ולעשות לה ולידציה בזמן פולי (יש $|V|^{|V|}$ צלעות לכל $E \subseteq V$).

את E נגדיר כך ש-3-קליקה תשרה השמה מספקת של θ , מילולית מדובר בכל זוג קודקודים שאינם מאותו הפסוקית או משתנה והשילילה שלו, מתמטית,

$E = V \setminus (\{(v_1, v_2) : (v_1, v_2) \in \{v_1, v_2\} \cup \{(v_1, v_2) : v_1 \text{ מזוהה עם משתנה ושלילתו : } v_2\}\})$

דוגמה ($\theta = (x_1 \vee x_1 \vee x_2) \wedge (\bar{x}_1 \vee \bar{x}_2 \vee \bar{x}_2) \wedge (\bar{x}_1 \vee x_2 \vee x_2)$) הגרף המושרחה מ- θ הוא

כמפורט



איור 39 : גраф המושרחה מהנוסחה

נשים לב שעתה θ היא m -קיליקה ב- G . הדוגמה כאן היא מקרה פרטי שבו $m = 3$, אבל נשים לב שהוא עבר הכללה (או יהיו לנו יותר צדדים של שלשות בgraf).

ההוכחה פולינומיאלית כי יש $3m$ קודקודים, ועבורם על $(3m)^2$ קשיות אפשרות בהגדירה של E . נכון נוכנות.

נניח $\theta \in 3\text{SAT}$, או קיימת $X \rightarrow \{T, F\}$ כך $\neg g$ מספקת את θ . בכל פסוקית c_i יש לפחות ליטרל אחד $\ell_i^{j_i}$ ש- $\neg g$ מספקת. נטען $V \supseteq S = \{\ell_1^{j_1}, \dots, \ell_m^{j_m}\}$.

לכל $S, u_1, u_2 \in S$ מתקיים $(u_1, u_2) \in E$ כי הם מזוהים עם ליטרלים מסוימות שונות (מהגדירת $\ell_i^{j_i}$) שלא מזוהים עם משתנה ושלילתו, כי $\neg g$ לא שרעק ליטרלים עם x_i מופיעים ב- S או רק כאשר x_i אינו מזוהה עם $\neg T$, T מסופקים שניהם זהה לא אפשרי).

נניח שיש ב- G - m -קיליק S . בהכרח לכל פסוקית c_i יש ב- S רק נציג אחד ℓ_i^1 או ℓ_i^2 (קודקודים מזוהים עם ליטרלים מאותה הפסוקית לא מוחברים בקשתי). מכיון $|S| = m$, לכל פסוקית נציג אחד. הקיליק משווה השמה שכן לכל משתנה לא יתכן שיש לו מופע חיובי וגם מופע שלילי (אין קשút בין ליטרלים מזוהים לא כולם עם x_i או כולם עם $\neg x_i$). המשתנים שלא מופיעים בקיליק אפשר להשיבו T/F באופן שירוט כי יש לנו השמה מספקת באופן ב"ת בהם (יש לנו ליטרל אחד חיובי בכל פסוקית, סה"כ כל הפסוקיות מסוימות).

לכן $3\text{SAT} \leq_p \text{CLIQUE} \iff \langle G, k \rangle \in \text{CLIQUE}$

חלק ב' של ההרצאה

משפט 3SAT היא NP-קשה, כלומר $L \leq_p 3\text{SAT}$ לכל $L \in \text{NP}$

הוכחה: תהי L שפה ב-NP, לכן קיימת מ"ט $t : \mathbb{N} \rightarrow \mathbb{N}$ מכירעה את L , ולכל מילה w , כל הריצות של M על w עוצרות תוקן $t(|w|)$ צעדים.

בහינתן w , נזכיר נוסחה φ ב-CNF כך $w \models \varphi$ ספיקה. הרעיון הוא ש- φ תגיד האם יש ריצה מקבלת של M על w . קלומר שיש סדרה c_0, \dots, c_m של קונפ' כך c_0 הנקונפ' ההתחלתית של M על w , לכל $1 \leq i \leq m - 1$ c_i עוקבת ל- c_{i+1} ו- c_m קונפ' מקבלת.

נשים לב שלכל $(|w| \leq t)$ הם כולם _ כי הראש לא מגע אליהם. לכן ניתן ליצג ריצה של M על w ע"י מטריצה שבסכום קומה תהיה קונפ' (בזומה ליצוף), ושבכל כתובות יש לה אוטם-# $\cup Q \cup \Gamma = S$. נוצר קונפ' ע"י מילה ב-# $\Gamma^* Q \Gamma^*$. המטריצה אם כן תהיה במדים $(n+3) \times t(n)$ כאשר $|w| = n$ (אורץ הייצוג של קונפ' עם ריפוד על מספר הקונפ' לכל היותר). תגיד האם אפשר למלא מטריצה $(n+3) \times t(n)$ באותוות מ- S באופן שמתאר ריצה מקבלת חוקית.

המשתנים שלנו יהיו $x_{i,j,s}$ כאשר $i \in [t(n)+3], j \in [t(n)], s \in S$ כאשר $g(i,j) = S$ ורכם יהיה T אם "ס" מושך $g(i,j) = s$ $\iff f(x_{ijs}) = T$ (משרה הכוונה לכך נגידיר את g , לאחר שנראה שהיא מגדירה היטב מטריצה).

נדיר φ שארת מטריצה f משורה מטריצה g מוגדרת היטב, שמנדרת ריצה מקבלת של M על w כאשר:

1. φ תודא שההשמה אכן מתארת את המטריצה חוקית, כלומר שבסכום תא יש אותן אחת ו ורק אותן אחת, ופורמלית φ_{cell} .

$$\varphi_{cell} = \bigwedge_{i \in [t(n+3)], j \in [t(n)]} \left(\left(\bigvee_{s \in S} x_{ijs} \right) \wedge \left(\bigwedge_{s_1 \neq s_2 \in S} \overline{x_{ijs_1}} \wedge \overline{x_{ijs_2}} \right) \right)$$

או מילולית, יש לפחות אותן אחת ב- (i,j) (שימוש מההשמה f), ולאין יותר משתי אותן מושמות באותו התא.

2. φ תודא שהשורה הראשונית במטריצה מקודדת את c_0 , כלומר שהשורה הראשונית היא $w_n \# q_0 w_1 \dots w_{n+3}$, ופורמלית φ_{init} .

$$\varphi_{init} = x_{11\#} \wedge x_{12q_0} \wedge \bigwedge_{i \in [|w|]} x_{1(i+2)w_i} \wedge \bigwedge_{i=n+3}^{t(n)+2} x_{1i_} \wedge x_{1t(n+3)\#}$$

■

תרגול

הגדעה יהי G גראף. נאמר כי $C \subseteq V$ כיסוי קודקי ב- G אם לכל צלע $e = \{u,v\} \in E$, לפחות אחד הקודקודיים של e נמצא ב- C .

הגדעה $\{G\}$ גראף לא מכובן ויש ב- G כיסוי קודקי גדול לכל היותר k .

הערה באלו וריאנו אלג'ר-2 מקרוב לעניית הכיסוי הקודקי.

טענה VC היא NP-שלמה.

הוכחה: נראה ראשית ש- VC -ב-NP ע"י מציאת מודא פוליאי לה. V קיבל $\langle G, k \rangle$ כאשר c היא תת-קובוצה של קודקי G . יספרור את $|c|$ ויודא שכן $k \leq |c|$ וכן ש- c מוכלת בקודקי G , אם לא, ידחה. אם שתי הבדיקות עובرت, V יעבור על כל הצלעות ב- G ויודא שיש לכל צלע לפחות קודקודה אחד ב- c , ויקבל אס"ם זה מתקיים.

רץ בזמן פוליאי כי שתי הבדיקות הראשונות הן בזמן פוליאי ב- c (שהוא פוליאי לכל היתר ב- k כי אחרת נדחה, כאשר k פוליאי ב- $|G|$ אם הוא תקין), ובדיקה השלישייה לוקחת $(|E| \cdot |V|) \cdot \mathcal{O}$. בנוסף V מודא נכון (ברור). לכן $\text{VC} \in \text{NP}$.

נראה ש- VC היא NPH (NP-קשה) ע"י הרדוקציה $\text{CLIQUE} \leq_p \text{VC}$. כלומר נחפש f פוליאי כך ש- CLIQUE אם "מ יש ב- G' $\langle G, k \rangle \in \text{CLIQUE}$ ו- $\text{VC} \in \text{NP}$.

טענת עזר יש ב- G -קליקה אם "מ יש ב- \bar{G} כיסוי קודודי בגודל $n - k$ והוא G עם הצלעות ההפוכות $e \in E(\bar{G})$ אם $e \notin E(G)$.

הוכחה: \Leftarrow : נניח שיש ב- G -קליקה ונסמנה ב- C . נביט ב- $\bar{C} = V(G) \setminus C$, שכן $\bar{C} = n - k$ כיסוי קודודי ב- \bar{G} ונסיים. נניח בשליליה ש- \bar{C} , איןו כיסוי קודודי, ותהי $x, y \in \bar{C}$ אבל C קליקה ב- G ולכן $\{x, y\} \in E$ כלומר $\{x, y\} \notin E$.

\Rightarrow : נניח שיש ב- \bar{G} כיסוי קודודי בגודל k ונסמן בו S . יהיו $x, y \in S$ ונניח בשליליה ש- $\{x, y\} \notin E$. ■ נראה ש- S היא k -קליקה ב- \bar{G} . יהיו $x, y \in S$ סטירה להיות \bar{S} כיסוי קודודי (מצאו צלע שפיטפס).

נסים את הוכחת הטענה. הרדוקציה של f תפעל כך. בהינתן $\langle G, k \rangle$ כאשר \bar{G} מתקיים $n - k$ ע"י הפיכת כל הצלעות $.n = |V(G)|$ ו-

פולינומית כי הפיכת הצלעות לוקחת $\mathcal{O}(|G|)$ וחותיר $\langle \bar{G}, n - k \rangle$ כולם סה"כ $\mathcal{O}(|V(G)|)$ ו- VC נcona מהלמה שכוון.

הגדירה יי- $G = \langle V, E \rangle$ גראף. נאמר כי Dominating Set $D \subseteq V$ או ש- $v \in D$ אם לכל $v \in V$ או ש- v חלק מצלע שהקצה השני שלה ב- D , כלומר D קבוצה של קודודים כך שכל קודוד במרקם לכל היתר 1 מקודוד כלשהו ב- D .

נדיר את השפה

$$\text{DS} = \{\langle G, k \rangle : k \geq \text{DS } G \text{ בגודל } DS\}$$

טענה DS היא NPC .

הוכחה: נוכחים כי $\text{DS} \in \text{NP}$ ע"י מציאת מודא פוליאי V שיפעל כך: V מקבל $\langle G, k \rangle$ ו- $D \subseteq V$ לאחר מכון יעבור על כל קודוד ב- G ויבדק לכל קודוד v האם הוא ב- D , ואם לא יעבור על הצלעות ב- G ש- v חלק מהן ויבדק אם הקצה השני של הצלע ב- D . אם לו אף צלע צו, ידחה. אחרת לאחר מעבר מוצלח על כל הקודודים, יקבל הסיבוכיות של V היא

$$\mathcal{O}(|V(G)| |V(G)| |E(G)| |V(G)|)$$

שזה פולינומי באורך הקלט ו- V נכון.

עתה נראה כי DS היא NPH ע"י כך שנראה רדוקציה $\text{DS} \leq_p \text{VC}$. כלומר רוצחים g פולינומית כך ש- DS ביחס ל- G , הרדוקציה g תחזיר $\langle G', k' \rangle$ כך ש- G' מתקבל מ- G באופן הבא: לכל צלע $e \in E[G]$ תוסף קודקוד חדש $v_e = \{x, y\}$ (כל צלע הופכת למשולש (x, v_e, y)). פורמלית ושתי צלעות חדשות $\{x, v_e\}, \{y, v_e\}$ (כל צלע $\{x, y\} \in E(G)$)

$$V(G') = V(G) \cup \bigcup_{e \in E(G)} v_e$$

$$E(G) = E(G) \cup \{\{x, v_e\}, \{y, v_e\} : \{x, y\} \in E(G)\}$$

לבסוף, g תסיר את מס' הקודקודיים המבודדים ב- G ותחזיר $\langle G', k' \rangle$ כאשר $k' = f + k$

g רצה בזמן פולי' כי ספירת קודקודיים מבודדים לוקח ($|V(G)|$) $\mathcal{O}(E(G))$ והוספה צלעות חדשות גם $\langle G', k' \rangle \in \text{VC}$ נראתה כוננות, כלומר $\langle G, k \rangle \in \text{VC}$.

\Leftarrow : נניח שיש ב- G כיסוי קודקודי C בגודל k . נראה שיש ב- G' קבוצה דומיננטית D מגודל לכל היותר $f + k$ (גודל אוסף הקודקודיים המבודדים, F). נביט ב- D ונראה שהוא D הינו $D = C \cup F$. מתקיים $|D| \leq |C| + |F| = k'$ (אולי יש חpięה בין C, F). נוכיח כי G' - D D

$v \in V(G')$ יחי.

• אם $v \in D$ ו- $v \in F$ (מהגדות D).

• אם $v \in F$ אז v חלק מצלע מקורית ב- G ולכן הוא במרקח 1 לכל היותר מ- C ולכן גם מ- D .

• אם $v \in V(G') \setminus V(G)$, בהכרח v הוא מהצורה xy והוא כיסוי קודקודי ב- G , או x או y ב- D ובפרט ב- D . בנו סך v_{xy} מחובר בצלע גם $-x$ וגם $-y$, ולכן במרקח 1 לכל היותר מ- D (אולי אפילו פעמיים!).

\Rightarrow : נניח שיש ב- G' קבוצה דומיננטית D' מגודל $f + k$. נגדיר $D = D' \setminus F$ והוא כיסוי קודקודי בגודל $\geq b$. נוכיח כי $|D| = |D'| - |F| \leq k' - f = k$. אין קשת שתקרב את הקודקודיים המבודדים ל- D אם הם לא כבר שם (ולכן D מ- G).

נוכיח כי בה"כ $v \in D$. נניח שקיים קודקood ב- D שאינו ב- G . הקודקודיים היחידים שאינם ב- G הם מהצורה v_e . לכן אם $v_{xy} \in D$ אז הוא נוגע רק ב- x וב- y ולכן אם נחליף את v_{xy} ב- x או y נוכל רק להגדיל את מספר הצלעות בהן D נוגעת.

נסים בכך שnocich ש- D כיסוי קודקודי ב- G . תהיו $x, y \in E(G)$. מהיות D' קבוצה דומיננטית ב- G' , כל קודקood ב- G' הוא במרקח לכל היותר 1 מ- D' ומהיות $D \subseteq V(G)$ כיסוי קודקודי ב- G , כי D כולל קודקood מכל צלע ב- G מהיותו נזורה של קבוצה דומיננטית (של גראן), שמכיל את G , להוציא מוקודודיים שרלוונטיים רק להגדרת קבוצה הדומיננטית ולא להגדרת הכיסוי הקודקודי.

שבוע II | מחלקות NP-שלמות

הרצאה

חלק א' של הרצאה

הוכחה: נמשיך את הוכחת משפט קוק-לוין. נסיים את הגדרת 3SAT- φ , נסחfat $\varphi_{cell} \wedge \varphi_{init} \wedge \varphi_{acc} \wedge \varphi_{move}$ אליה העתיק את Σ^* בראזרקציה ה поляי'. את φ_{cell} הגדרנו כך שנוכל לאכוף ש- f -מידירה היטב את המטריצה g , ואת φ_{init} הגדרנו כך שהונכל לאכוף שהשורה הראשונה היא הקונפ' ההתחלתית של ריצת M (מ"ט שמכריעה את L) על $w \in \Sigma^*$.

$$\varphi_{acc} = \bigvee_{i \in [t(n)+3], j \in [t(n)]} x_{ijq_{acc}} \text{ כלומר } \varphi_{acc} \text{ 1.}$$

2. φ_{move} תודא שהקונפ' באמת עוקבות אחת אחר השניה. מספיק שנבדוק שכל חלון 2×3 במטריצה הוא תקין (מושם שהקשן קורה רק על פנוי לצל היותר שלוש משבצות הצמודות לאיפה שהמצב נמצא וכל השאר נשאר זהה).

$$\varphi_{move} = \bigvee_{i \in [t(n)-1], j \in [t(n)]-1} legal(i, j)$$

כאשר הנסחה שמוגדרת שהחלון מ- (i, j) עד ל- $(i+2, j+1)$ (כולל) חוקי, כלומר בודקת האם החלון הוא אחד מבין החלונות החוקיים האפשריים

$$legal(i, j) = \bigvee_{(s_1, \dots, s_6) \in W} (x_{ijs_1} \wedge x_{(i+1)js_2} \wedge \dots \wedge x_{(i+2)(j+1)s_6})$$

כאשר W קבוצת החלונות החוקיים. W מוגדרת באופן הבא:

- לכל מעבר $(\Gamma, \delta, \delta, \delta)$, נוסיף את החלונות (כל האותיות ב-

c_2	c_3	b
c_2	c_3	q

c_3	b	q'
c_3	q	a

b	q'	c_4
q	a	c_4

q'	c_4	c_5
a	c_4	c_5

כיאנו משתמשים על החלון הכללי הבא שבו קורה האקסן:

c_2	c_3	b	q'	c_4	c_5
c_2	c_3	q	a	c_4	c_5

- לכל מעבר δ נוסיף בדומה את החלונות

c_1	c_2	q'
c_1	c_2	c_3

c_2	q'	c_3
c_2	c_3	q

q'	c_3	b
c_3	q	a

c_3	b	c_4
q	a	c_4

b	c_4	c_5
a	c_4	c_5

כיאנו משתמשים על החלון הבא שבו קורה האקסן

c_1	c_2	q'	c_3	b	c_4	c_5
c_1	c_2	c_3	q	a	c_4	c_5

- לכל Γ $c_1, c_2, c_3 \in \Gamma$ נוסיף את החלון

c_1	c_2	c_3
c_1	c_2	c_3

הראנו כבר בהרצאה הקודמת שהרדזוקציה פולוי', עתה נוכחים כי M מקבלת את w_A , ס' ספיקה, כלומר שהרדזוקציה נכונה.

\Leftarrow : יש ריצה מקבלת של M על w ולכן המטריצה שמתארת אותה מושה השמה שמספקת את φ .

$\Rightarrow \varphi$ ספיקה ולכון יונה f השמה מספקת.

- מהיות φ_{cell} מסופקת, f מתארת מטריצה מוגדרת היטב.

- מיהו φ מסופקת, השורה הראשונה במטריצה מתארת את הקונפ' התחלתי של M על w .

- לפי φ_{move} ידוע לנו שמעבר בין שורות במטריצה מתאים למעבר בין קונפ' עוקבות.

- מ- φ_{acc} הריצה, שהיא חוקית, מקבלת מתישחו.

כולם M מקבלת את w .

$\text{CNF} \leq_p 3\text{SAT}$

לכל פסוקית θ $\exists k \leq 3$ $\ell_k = \ell_1 \vee \dots \vee \ell_k$ מעתנים חדשים y_1, \dots, y_{k-3} , $k > 3$ נסיף y_k ונוחריר

את הנוסחה

$$\theta' = (\ell_1 \vee \ell_2 \vee \ell_1) \wedge (\overline{y_1} \vee \ell_3 \vee y_2) \wedge \dots \wedge (\overline{y_{k-3}} \vee \ell_{k-1} \vee \ell_k)$$

נפנ' ידים למה θ ספיקה אם θ' ספיקה: בכוון הלא, הראו הוא שאם $\ell_i = T$ בהשמה מספקת $\ell - \theta$ אז כך יהיה גם בהשמה מספקת $\ell - \theta'$ אז עברו $2 - \theta' y_j$, $j \leq i$ והוא משוחררים להיות מה שהם רוצים (יהיו T לדוגמה) ואילו לכל $j \leq i + 1$ יהיה F . משחו. ראו בתרגול.

הגדירה בעיית sum subset מקבלת קלט קבוצה (יתכן עם חזרות) של טבעים \mathbb{N} ומספר יעד s , וצריכה לענות

$$\text{קלט האם יש } \sum_{a_i \in B} a_i = s. \text{ פורמלית נגידיר את השפה}$$

$$\text{SS} = \left\{ \langle A, s \rangle \in 2^{\mathbb{N}} \times \mathbb{N} : \left(\exists B \subseteq A : \sum_{a_i \in B} a_i = s \right) \right\}$$

טענה SS היא NP-שלמה.

הוכחה: ראשית $\text{SS} \in \text{NP}$ כי מ"ט יכולה לנחש את B ולבזוק האם היא נסכמת ל- s , או לחלופין מודא פוליאי מקבל את B ובזוק אותו. נשים לב שהבעיה עדין ב-NP גם עבור ייצוג אונארי כמו עבור בסיס $b > 1$.

נוכחה כי היא NPH ע"י רדוקצייה פוליאי מ-3SAT. נגידיר f שבהינתן נוסחה ב-3CNF, נחזיר קלט $\text{L-SS}(A, s)$, כך שלכל $\theta, \theta \in 3\text{CNF}$ אם $\theta \in \text{MSB}(f)$ אז $\langle A, s \rangle \in \text{SS}$.

תהי θ מעל $2(n+m)$ ותייצר A עם $s = \frac{1}{n} \dots \frac{1}{n} \frac{3}{m} \dots \frac{3}{m}$ ותחזיר f $.c_1, \dots, c_m$ מספרים בבסיס 10 (לכל בסיס של ייצוג של הקלט), כשבכל אחד $m+n$ ספרות:

- לכל משתנה x_i נגידיר מספרים t_i ו- f_{i-1} , כך שהгадירה שלהם תאכוף ספיקות של θ אם $\langle A, s \rangle \in \text{SS}$. הספרה ה- i -ית (הבית הראשון) הוא של f_i, t_i ועבור $m+1 \leq j \leq m+n$ הינה:

– ב- t_i : 1 אם x_i מופיע חיובי ב- c_j .

– ב- f_{i-1} : 1 אם x_i מופיע שלילי ב- c_j .

- לכל פסוקית c_j נגידיר בנוסף שני מספרים p_j, q_j , שיהיו ריפוד: הספרה ה- j -ית של p_j, q_j היא 1 והשאר אפס.

דוגמא

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

כאו $n = 4$, ולכן אנחנו מגדירים מספרים עם 7 ספרות, המספרים שיוגדרו הם (כל מקום שלא כתוב מספר הכוונה היא ל-0)

	1	2	3	1 (4)	2 (5)	3 (6)	4 (7)
t_1	1			1			1
f_1	1				1	1	
t_2		1		1		1	
f_2		1			1		1
t_3			1	1	1		
f_3			1			1	
p_1				1			
q_1				1			
p_2					1		
q_2					1		
p_3						1	
q_3						1	
p_4							1
q_4							1
s	1	1	1	3	3	3	3

כאשר חשוב לציין שמדובר במספרים עשרוניים (מיליון...). אינטואטיבית כדי להגיע לסכום למיטה, יהיה חיבים לבחור או את t_i או את f_i אבל לא את שניהם (אחרת לא יסכם) כך שההשמה מוגדרת היטב.

הזרוקציה פוליאו. וכך נותר להוכיח נכונות, כלומר שניינו הגיעו ל-3...3...3...3. אם $s = \frac{1\dots1}{n} \cdot \frac{3\dots3}{m}$ ספיקת θ .

\Rightarrow תהי f השמה מספקת. נכניס B -את המספרים הבאים: לכל $i \in [n]$ או t_i או f_i . לכל $j \in [m]$ $f(x_i) = T$, אם $j \in [m]$ נכניס רק את t_j , אם $j \notin [m]$ נכניס רק את f_j . קל לראות שאכן מגיעים לסכום הנדרש (מהדוגמא הנ"ל).

\Leftarrow אם $\langle A, s \rangle$ גדייר $f : X \rightarrow \{T, F\}$ באוף הבא: יהי B כך $s = \sum_{i \in [n]} B_i$. מובטח שלכל $i \in [n]$, בדוק אחד מתוך t_i, f_i ב- B ולכן נוכל להציג את $f(x_i)$ היבר בהתאם למה שנבחר. ■

חלק ב' של הרצאה

הגדרה תהי M מ"ט דטר', חד סרטית שעוצרת על כל קלט. סיבוכיות הזיכרון של M היא $F(N) = s$ כען קלט באורך n , M משתמש בכל היותר ב- $(n-s)$ תנאים, ונאמר ש- M רצה בשטח ($n-s$)

$\text{SPACE}(s(n)) = \{L : L \text{ שמכריע את } \mathcal{O}(s(n))\}$

ואז NSPACE המקבילה הא"ד להגדירה הנ"ל.

הערה נניח שנוכל לקנות שריצה בזמן לינארי או מקום לינארי, מה נגיד? מקום לינארי כי עBOR $\mathbb{N} \rightarrow \mathbb{N}$, מתקיים

$$\text{TIME}(f(n)) \subseteq \text{SPACE}(f(n))$$

כי אם M עוצרת תוך $f(n)$ צעדים, היא לא יכולה להגיע מעבר לתא ה- $f(n)$ -י.

טענה עBOR \mathbb{N} הוכח $f : \mathbb{N} \rightarrow \mathbb{N}$

הוכחה: ראשית מכונה דטר' שעוצרת לא מבקרת באוטה קונפ' פעמיים (אחרת הייתה כניסה לולאה אינסופית). לכן אם עסקנו ב-(n) תאים, לכל היותר עברנו בכל הקונפ' שלולונטיות לתאים האלה פעמי אחד בדיק כל אחד, ויש מספר אקספ' ב-(n) f של קונפ' כלשה. כמו כן, שנות יש למcona עם סיבוכיות זיכרון (n ? קונפ' מתוארת ע"י s ? $\Gamma^{s(n)} \times [s(n)] \times Q$ (מצב, מיקומו בסרט, תוכן הסרט), ואם נסמן $|Q| = c_1$, $|s| = c_2$, $|c_1 s(n) c_2^{s(n)}| = c_3$, אז מספר הקונפ' הוא c_3 מאיינפי.

$$\text{הגדירה} \cdot \text{NPSPACE} = \bigcup_k \text{NSPACE}(n^k) \text{ ו-} \text{PSPACE} = \bigcup_k \text{SPACE}(n^k)$$

מסקנה מההערה הנ"ל,

טענה $\text{P} \subseteq \text{NP} \subseteq \text{PSPACE}$

דוגמה נוכחים כי $\text{SAT} \in \text{PSPACE}$. זה נכון כי SAT ניתנת להכרעה ע"י מ"ט דtag' שריצה בשטח לינארי. הרעיון הוא ש- M תעBOR על כל השימוש האפשריות, ותקבלו אם אחת מהן מספקת את הנוסחה. אחרת, תדחה.

נשתמש $\{\perp\} \cup 2^X \rightarrow 2^X$ פ' שטעה השמות עוקבות באופן שמקסם את כל 2^X , כלומר שקיים סידור $f_{2^{|X|}}$ של 2^X (לקסיקוגרפי נגיד) כך שלכל $2^n < i$ $f_i = f_{i+1}$ ו- $g(f_i) = \perp$.

אכן קיימת g כזו שניתנת לחישוב בשטח לינארי (למשל סידור לקסיקוגרפי, שעוברים לפי סדר הביטים וכל פעם הופכים בהתאם את הערכיהם למספר הבא בתור).

לסיום, פורמלית, M בהינתן נוסחה φ מעל X :

1. כותבת על הסרט את f_1 .

2. משערכת את φ לפי הคำשה שכזובה על הסרט.

(א) אם השתערכה ל- T מקבלת.

(ב) אם השתערכה ל- F , מחשבת (f_i) . אם \perp דוחה (לא מצאו השמה מספקת), אחרת עוברת ל-2.

הוכחה: תהי $P \in L$. לכן יש מודא דטר' ל- L שרצ בסיבוכיות (n) פוליאי כך ש- $(|w|)$. לכן $|c| \leq (|w|)^t$.

$$L = \{w : (w, c) \in \Sigma^* \text{ מקבלת את } V \text{ כיוון } c \in \Sigma\}$$

נראה מכונה שמכריעה את L ב-PSPACE. יהיו c_1, \dots, c_k סידור המילים ב- $\Sigma^{(|w|)^t}$. המכונה עוברת על כל העדים ומריצה את V על כל עד c_i . אם יש עד כך ש- V מקבלת את (w, c_i) , המכונה תעצור ומתקיים, אחרת תעוצר ותודה לאחר כל החרצאות. סיבוכיות הזיכרון היא כמוגן פוליאי כי אנחנו עוברים על כל העדים (עם g אפשרי במקום לינארי), והריצה של V (שרצ בזמן פוליאי בקלט שהוא פוליאי בקלט, לכן גם עם שטח פוליאי).

דוגמה: A הוא $\{ \langle A \rangle : L(A) = \emptyset, \text{NFA} \}$ הינה שפה ב-P-empty. כדי שפה $\text{ALL}_{\text{NFA}} = \{ \langle A \rangle : L(A) = \Sigma^*, \text{NFA} \}$ תהיה שפה PSPACE-שלמה. למקבל. לעומת זאת A הוא $\{ \langle A \rangle : L(A) = \Sigma^*, \text{NFA} \}$ למקבל. לעומת זאת A הוא $\{ \langle A \rangle : L(A) = \emptyset, \text{NFA} \}$ לא-שלמה.

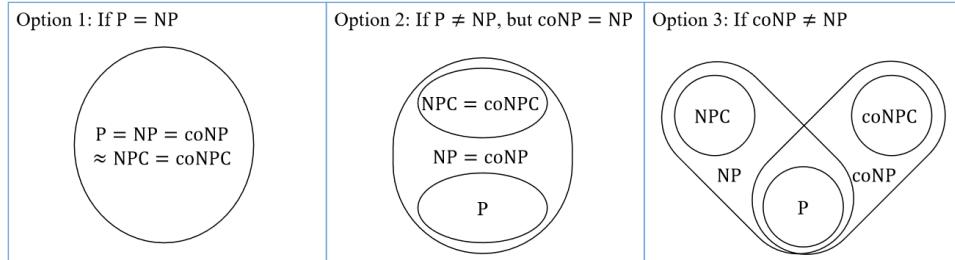
תרגול

הגדירה נאמר כי L היא NP-קשה אם $L \leq_p \bar{L}$ והוא coNP-קשה אם $\bar{L} \leq_p L$. ו- L היא NP-שלמה אם $L \in \text{NP}$ ו- $\bar{L} \in \text{coNP}$.

טענה: L היא NP-שלמה אם \bar{L} היא coNP-שלמה.

הוכחה: \Leftarrow : נניח כי L היא NP-שלמה. לכן לכל $K \in \text{NP}$ מתקיים $K \leq_p \bar{L}$ (ראינו בעבר), כלומר לכל coNP-קשה \bar{L} ולכל $K \in \text{coNP}$ $K \leq_p \bar{L}$ הינה coNP-קשה ומזהות $L \leq_p \bar{L}$ נובע $L \in \text{NP}$.

הערה: נוכיח בתרגיל כי אם $P \neq NP$ או $NP \neq coNP$, ולכן העולם יכול להיות בשלושה מצבים שונים



איור 40 : שלושת האפשרויות למציאות

הגדירה שפת הנוסחאות שלא ניתן לסייע היא

$$\overline{\text{SAT}} = \text{CONTRADICTION} = \{ \langle \varphi \rangle : \varphi \text{ נוסחת CNF לא ספיקה} \}$$

ושפת הטאולוגיות היא $\{\langle\varphi\rangle : \text{CNF TAUTOLOGY} = \{\langle\varphi\rangle : \text{CNF}\}$ טאולוגיה בצורת TAUTOLOGY

טענה TAUTOLOGY היא coNP-hard.

הוכחה: TAUTOLOGY היא NP-hard כי אפשר פשוט לנחש השמה ולבזק אותה, ולאחר מכן לקבל אם היא לא מספקת. נראה רדוקציה פוליאריה מ-CONTRADICTION ל-TAUTOLOGY ואז בעזרת הטענה הנ"ל נקבע ש-TAUTOLOGY היא NP-hard. f תפעל כך: לכל φ נוסחת CNF, $\neg\varphi = \neg(\varphi)$. בזר שהרדווקציה נכונה ופוליאריה (אם φ היא סתירה אז $\neg\varphi$ טאולוגיה אחרת לא).

שפות לגרפים המילטוניים

הגדרה השפות המרכזיות לגרפים המילטוניים הן

$D - ST - HAMPATH = \{\langle G, s, t \rangle : t \in V(G) \text{ גראף מכון ויש מסלול המילטון מ-} s \text{ ל-} t\}$

$D - HAMPATH = \{\langle G \rangle : G \text{ מכון ויש ב-} G \text{ מסלול מכון המילטוני}\}$

$D - HAMCYCLE = \{\langle G \rangle : G \text{ מעגל מכון המילטוני}\}$

לשלאש אלה יש מקבילות לא מכוונות.

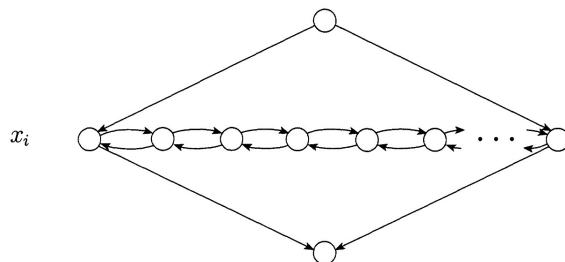
טענה D – ST – HAMPATH היא NPC.

הוכחה: ראשית D – ST – HAMPATH היא NP-complete במאזעות מודא V שיפעל כך: בהינתן $\langle G, s, t \rangle$ וקובצי קודקודים c , יבדוק האם $c \subseteq V(G)$. אם אחת הבדיקות נכשלות נדחה. אחרת V עברור על כל זוגות עוקבים ב- c ויודא שקייםת ביןיהם צלע ב- G . כמו כן נודא שהקדוקדו הראשון ב- c הוא s והאחרון t . אם כל הבדיקות מצליחות נקבל, אחרת נדחה.

נראה רדוקציה HAMPATH \leq_p 3SAT ונסיק ש-HAMPATH היא NP-hard. נחש רדוקציה שבහינתן נוסחה ב-3CNF, נחזר גראף ושני קודקודים, כך שהנוסחה ספיקה אם גראף יש מסלול המילטוני בין שני הקודקודים הללו.

f תפעל כך: בהינתן θ נוסחה ב-3CNF עם משתנים $x_1, \dots, x_l, \bar{x}_1, \dots, \bar{x}_l$ וליטרלים c_1, \dots, c_k , פסוקיות x_1, \dots, x_l תחזיר גראף ושני קודקודים, כך שהנוסחה ספיקה אם גראף יש מסלול המילטוני בין שני הקודקודים הללו. באופן הבא.

לכל משתנה x_i ב- θ נתאים "מבנה יהלום" ב- G שנראה כבאיור, כאשר שורת הקודקודים מכילה $3k + 1$ קודקודים פנימיים ועוד שניים בקצוות

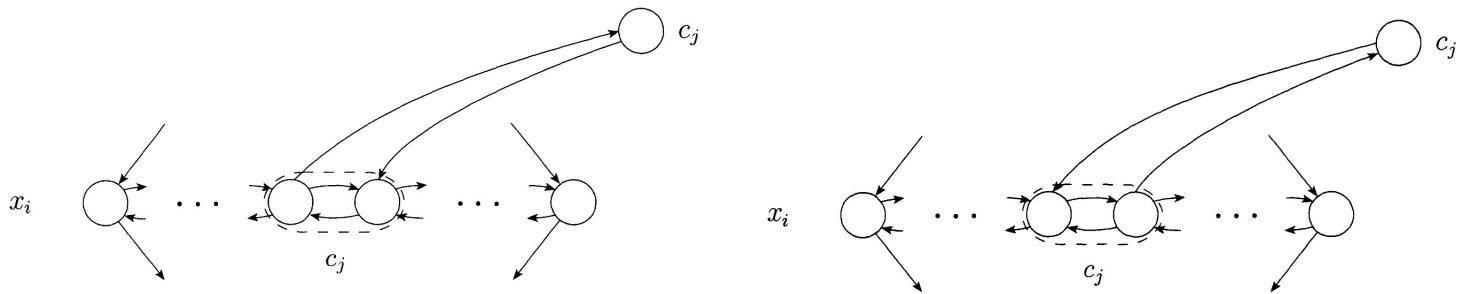


איור 41 : מבנה היהלום

את מבני היהלום נחבר באופן הבא : הקודקוד העליון ביהלום 1 יהיה s , ולכל $1 < i$ הקודקוד העליון ביהלום i יהיה הקודקוד התחתיו של $1 - i$, והקודקוד התחתיו של k הוא t . מעבר לכך נוסיף עוד k קודקודות לכל פסוקית c_j .

ນחווב על כל שורה ביהלום כך : לכל פסוקית c_j יתאימו זוג קודקודות בשורה וקודקוד נוסף מפרד (כלומר השורה מחולקת לשלוות - זוג פסוקיות c_j ומفرد בין הזוג של j ושל $1 + j$).

עת, נחבר בין קודקודי פסוקיות ויהלומים של משתנים כך : אם הליטרל x_i מופיע ב- c_j , נחבר את היהלום של x ל- c_j כבאיור משמאלי, ואם הליטרל \bar{x}_i מופיע ב- c_j , נחבר את היהלום כבאיור מימין (ההבדל הוא האם החז יוצאה מהראשון ונכנס אל השני או הפוך).



איור 42 : חיויות בטוחות ליטרל למשתנה x_i למיניהם c_j : משמאלי x_i ומימין \bar{x}_i

ראשית הבניה הזו פולי' כי אנחנו בונים גראף עם לכל היוטר פי $4k$ קודקודות מהפסוקית, שזה כMOVEDן פולי' בגודל הקלט. נראה נכוןות, ככלומר שיש ב- G_φ מסלול המילוטוני אם "יש ב- φ השמה מספקת".

\Rightarrow קיימת השמה מספקת ל- φ , ככלומר לכל פסוקית c_j יש ליטרל אחד לפחות שמקבל T . מסלול המילוטוני מ- s ל- t יראה כך : נתחיל ב- s ולכל x_i , אם x_i מקבל T בהשמה המספקת של φ , נטיל על היהלום x מלמעלה למטה כך שנכנסים מצד השמאלי ויוצאים מצד הימני (זיג-זאג).

אם \bar{x}_i מקבל T בהשמה $(F x_i)$, נטיל על היהלום x_i מימין לשמאלי (זאג-זאג).

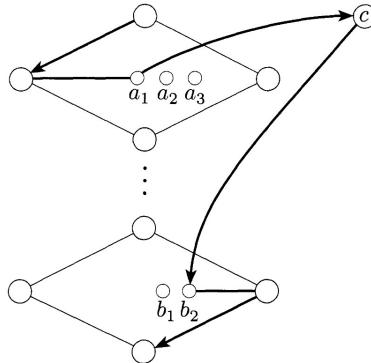
היוטר ולכל c_j קיים לפחות ליטרל אחד שמקבל T , נוכל לחתוך מעקפים לכל c_j כך שאם x_i מופיע ב- c_j והוא T , נעשה זיגזאג עם הקפיצה ל- c_j וחזרה לשרשראת, ואם \bar{x}_i מופיע ב- c_j והוא T , נעשה זאג-זאג עם הקפיצה ל- c_j וחזרה לשרשראת.

נשים לב שמאופן ההגדרה של הקפיצה, נוכל לעשות את המעקב הזה באופן חוקי כי הוא מסודר באופן שמתאים להאם הליטרל מופיע בחיבור או בשילחה. ככלומר, אם הליטרל מופיע בחיבור אז הקפיצה היא משמאלי ויורדת לקודקוד הימני, בהתאם לעובדה שאנו חנו מטילים משמאלי מימין, ואם מופיע בשילחה אז אנחנו מטילים מימין לשמאלי וקפוצים מימין ונוחתים שמאלה יותר, כמובן.

נשים לב כי המסלול הזה לא מוגדר ביחידות (בכל פסוקית אשפר לבחור אחד משולש קודקודים שיקפצו עליו במסלול) אבל בטוח קיים יותר אחד כזה בין s ל- t .

\Leftarrow : נניח שיש ב- G_φ מסלול המילטוני בין s ל- t . אם יש מסלול המילטוני מ- s ל- t והוא נורמלי, כמובן מティיל על היחסים לפי הסדר ויוצא לעקף דרך קודקוד בזוג שמותאים l_{-x} ו- a_j חזר לקודקוד הבא באותו הזוג, אז נדע שיש השמה מספקת ל- φ , בדיק על פי כיוון הטויל (שמאל לימין - נבחר T , ימין לשמאל - $(F$ -).

מסלול לא נורמלי הוא מסלול שבו המסלול יוצא לעקף אבל חוזר לקודקוד מחוץ לזוג שדרכו נכנס לעקף, כבאיור



איור 43 : עקף במסלול המילטוני לא נורמלי

נשים לב כי או a_2 או a_3 הם קודקודים מפרידים :

- אם a_2 מפריד, אפשר להגיע אליו דרך a_3 או a_1 .

- אם a_2 לא מפריד, אפשר להגיע אליו דרך a_3 או a_1 או c .

אבל זה אומר שהמסלול ההימלטוני חייב להיכנס ל- a_2 דרך a_3 (כי כבר בירורנו ב- c , a_1) אבל אז הוא נתקע ולעולם לא מגיע ל- t ולכן זה לא מסלול המילטוני בסתירה להנחה. לכן כל מסלול המילטוני ב- G_φ הוא נורמלי ולכן משרה השמה מספקת של φ .

■

טענה $\text{HAMPATH} \leq_p \text{U} - \text{ST} - \text{HAMPATH}$.

הוכחה: ברור שהוא NP-hard. נראה רדוקציה $HAMPATH \leq_p U - ST - HAMPATH$. הרדוקציה f תפעל כך: בהינתן $\langle G, s, t \rangle$ מכובן, נזכיר $\langle G', s', t' \rangle$ כאשר לכל קודקוד v ב- G יהיו שלושה קודקודים v_{in}, v_{mid}, v_{out} ב- G' , ולכל צלע (u, v) נגדיר את הצלע $\{u_{out}, v_{in}\}$. ובנוסף נחבר את v_{mid} ל- v_{in} ו- v_{out} לכל v . פורמלית יש לנו

$$V(G') = \{v_{in}, v_{mid}, v_{out} : v \in V(G)\}, E(G') = \{\{v_{in}, v_{mid}\}, \{v_{mid}, v_{out}\} : v \in V\} \cup \{\{u_{out}, v_{in}\} : (u, v) \in E\}$$

ברור שהבנייה פולית. נראה נכוןות.

\Rightarrow : אם יש מסלול המילוטוני $s_{in}, s_{mid}, s_{out}, v_{in}^1, v_{mid}^1, v_{out}^1, \dots, v_{in}^k, v_{mid}^k, v_{out}^k, t_{in}, t_{mid}, t_{out}$ ב- G אז המסלול s, v_1, \dots, v_k, t ב- G' הוא המילוטוני בין s_{in} ל- t_{out} .

\Leftarrow : נניח שיש מסלול המילוטוני בין s_{in} ל- t_{out} ב- G' . נניח בשיילה שיש במסלול ב- G' (הגרף לא מכון אבל המסלול כן) צלע (v_{in}, u_{out}) (כלומר נקדים הופיעו) ונניח שזו הצלע הראשונה מהצורה הזו במסלול. אם כבר המסלול ביקר קודם ב- v_{mid} , אז המסלול חייב היה להגיע אליו דרך v_{out} , אבל זאת אומרת שהמסלול הגיע אליו דרך x_{in} (x_{in} מחובר רק ל- v_{out} * אחרים בהגדרת E'), סתייה לכך שזו הפעם הראשונה ל去过 "הופיע" שכזה. לכן מבקרים ב- v_{mid} , ככלומר שהיבטים להיכנס אליו מ- v_{out} , אבל אז נתקיים ולא מגיעים ל- t_{out} . לכן זה לא מסלול המילוטוני.

שבוע XIII | מחלקות סיבוכיות מקום

הרצאה

חלק א' של הרצאה

הגדירה המחלקות המתאימות לביעית הריקנות והאוניברסליות חן

$$\text{EMPTY}_{\text{NFA}} = \{\langle A \rangle : L(A) = \emptyset \text{ NFA ו-} A\}$$

$$\text{ALL}_{\text{NFA}} = \{\langle A \rangle : L(A) = \Sigma^* \text{ NFA ו-} A\}$$

הערה כזכור, עברו אוטומט דטר', הפיכת המכבים המקבלים תניב את האוטומט המשלים. הטריך הזה לא יעבוד עברו אוטומט א"ד ובונים את המשלים באמצעות ה-subset construction.

הערה מתקיים $\text{EMPTY}_{\text{NFA}} \in \text{P}$ $\text{EMPTY}_{\text{NFA}} \in \text{P}$ בנסיבות BFS (בודקים אם יש מסלול למצב מקבל) ו- P סגורה להשלמה.

בנוסף $\text{ALL}_{\text{DFA}} \in \text{P}$ כי בניה המשלים נעשת בזמן פוליאי (ועליו בודקים האם $L(\overline{D}) \in \text{EMPTY}_{\text{DFA}}$ בזמן פוליאי).

נראה איך לבדוק $w \in L(A)$ עברו A בזמן פוליאי: ניתן להציג A_w DFA עם $L(A_w) = \{w\}$ (שרוך של המילה בזמן פוליאי, ובנוסף לחשב אוטומט מכפלה של A_w ו- A לוקח זמן פוליאי ואז נזכיר ש- $L(A) \cap L(A_w) \neq \emptyset$ אם ו- $w \in L(A)$ (בנסיבות השפה של אוטומט המכפלה)).

הערה לכואורה אפשר להכניס את המחלקה NP בנסיבות עד שהוא מילה שלא בשפה ואז לבדוק שהוא לא בשפה באמצעות השיטה הנ"ל. הביעה היא שהעד המינימלי יכול להיות באורך אקספ' ואז האלג' כבר לא פוליאי.

טענה $\text{ALL}_{\text{NFA}} \in \text{NPSPACE}$ (אוטומטים הא"ד עם שפה לא אוניברסלית).

הוכחה: אם $L(A) \neq \Sigma^*$ אז יש מילה w כך ש- $w \notin L(A)$ (מסלול פשוט ב- A) ($|w| \leq 2^{|Q|}$ (SS-construction)). כלומר w כזו היא עד לחוסר הריקנות של \overline{A} .

בנה מ"ט א"ד שמכריעה את $\overline{\text{ALL}_{\text{NFA}}}$ בשטח פוליאי', שמסמלץ את ה- $\text{on-the-fly SS-construction}$, כלומר לא בונה את כולם אבל לוגית הוא יהיה האלג':

1. נאותחל $S = Q_0, c = 0$

2. כל עוד $c \leq 2^{|Q|}$

(א) אם $S \cap F = \emptyset$ נעוצר ונקבל (כל הריצות לא מקבלות).

(ב) אחרת, נחש אותן $\Sigma \in S$ וnochשב $\delta(S, \sigma) = \delta(S, \sigma) + +$.

נכונות: אם $\Sigma^* \neq L(A)$ אז יש w והוא באורך $\geq 2^{|Q|}$, ולכן יש ריצה של האלג' שתנחש את w (ותקבל ב-(a) כאשר $c = |w| - 1$).

■ פוליאי' זיכרו: בכל רגע המכונה שומרת על הרטט את $S \subseteq Q$ (פוליאי') ומונה c שסופר על $2^{|Q|}$ ולכן באורך $\log_2 2^{|Q|}$ (שזה פוליאי').

הערה ההוכחה הנ"ל רצה בזמן אקס' ($|Q|^2$) ולאחר הכנסנו את השפה ל- NP .

הערה בתרגול נוכיח ש- $\text{NPSPACE} = \text{PSPACE}$ ומשם נסיק $\text{NSPACE}(s(n)) \subseteq \text{SPACE}(s^2(n))$.

הערה עד כה יש לנו

$$\begin{array}{ccccccc} \text{coP} & & \text{coPSPACE} & \stackrel{\text{סביר}}{=} & \text{coNPSPACE} & & \text{coEXPTIME} \\ \parallel & \subseteq & \parallel & = & \parallel & \subseteq & \parallel \\ \text{P} & \subseteq & \text{PSPACE} & & \text{NPSPACE} & \subseteq & \text{EXPTIME} \\ & \subseteq & \text{coNP} & \subseteq & & & \end{array}$$

הגדירה נאמר כי שפה שלמה ב- PSPACE אם:

1. $L \in \text{PSPACE}$

2. $L' \leq_p L, L' \in \text{PSPACE}$ (רדווקציה בזמן פוליאי').

טענה $\overline{\text{ALL}_{\text{NFA}}}$ היא PSPACE -קשה.

הוכחה: נראה לכל שפה $w \in \Sigma^*$ ($L \leq_p \overline{\text{ALL}_{\text{NFA}}}$ (ומשם $\overline{L} \leq_p \text{ALL}_{\text{NFA}}$). כלומר בונה פ' שבהינתן $L \in \text{PSPACE}$ כך ש- $w \notin L$ ($L(N) = \Sigma^* \text{ אם } w \notin L$).

תהי M מ"ט דטר' שמכריע את L בשטח (s פוליאי' באורך הקלט. A שנזיר יקבל x אם "מ

• x לא קידוד חוקי של ריצה של M על w .

- או x קידוד של ריצה דוחה של M על w .

כך אם $L \notin w$, אין אף ריצה מקבלת ולכון אין אף קידוד חוקי של ריצה מקבלת, לכן תמיד נקבל.

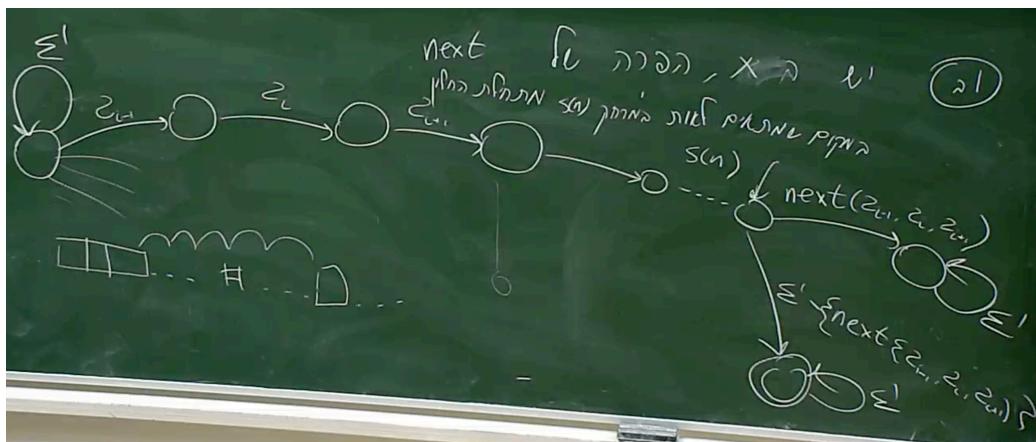
הא' ב של A הוא $\# \cup \{ \# \cup (Q \times \Gamma) = \Gamma \cup (Q \times \Gamma)$. קידוד חוקי של ריצה של M הוא מילה מעל ' Σ' , שהיא רצף קונפ' עוקבות כאשר קונפ' מקודדת ע"י $\# \gamma_1 \dots (q, r_i) \dots \gamma_{s(n)}$.

איך נבדוק שקובע' σ עוקבות? נסמן $\sigma'_I = (\sigma_{i-1}, \sigma_i, \sigma_{i+1})$ מה אנחנו מוצאים לראותה במקום ה- i ? בקובע' עוקבת לקובע' שמקומות $i-1, i, i+1$ שלה יש את σ'_I . אפשר לחשב את הערך הזה בזמן ושטח פולי' בהינתן δ (לראות איך הראש הקורא צריך להיות והאם משתמשות אוטוות).

- בדיקת הקידוד הלא חוקי, A קיבל את x אם :

1. x לא מתחילה ב-_#. ואפשר לבנות לזה שרווק-ב- NFA (דורשים # אחרית בור דוחה, ואז (q_0, a_1) $a_2 \dots a_n \dots$ בור דוחה וכו').

הkonopf לא עוקבת, תהיה ריצה שתנסה את ההפרה הזו שתגיע לבור המקביל.



איור 44: שרוֹץ המיצג היפה של *next*

- לבדוק אם הריצה מקבלת, A קיבל מילה שמכילה את מהצורה $\{q_{acc}\}$.

השרוד הראשון הוא באורך $l_{\text{inner}} = (n-1) \times 3s$ ויחס $(n-1)$ שוכנים באורך $l_{\text{outer}} = n \times 3s$. כלומר סה"כ במבנה בזמן פולי' $-(n)$. נוכנות ■
ברורה.

חלק ב' של הרצאה

דוגמאות

$$\text{.CONT}_{\text{NFA}} = \{\langle A_1, A_2 \rangle : L(A_1) \subseteq L(A_2) \text{ and } \text{-NFA } A_2 \text{ -} \text{CONT } A_1\}$$

מתקיים אם $A \subseteq B$ ו $A \cap \overline{B} = \emptyset$, ולכן אפשר לעשות SS-construction ואז אוטומט המכפלה, כך שהשפה ב-EXPTIME (גודל אוטומט המכפלה) היא $|Q_1 \times 2^{Q_2}|$.

. $\text{ALL}_{\text{NFA}} \leq_p \text{CONT}_{\text{NFA}}$ אבל לא נראה את זה. כן נראה שהשפה היא PSPACE-קשה. נוכיח NFA מוחזירה זוג NFA-ים כך שהקלט אוני' אם השפה של האוטומט הראשון מוכלת בשל השני.

כלומר נמצא f שבحينו NFA מוחזירה זוג NFA-ים כך שהקלט אוני' אם השפה של האוטומט הראשון מוכלת בשל השני.

f מקבל NFA A ויזיר $\langle A_{\Sigma^*}, A \rangle$ כאשר A_{Σ^*} אוטומט טריוויאלי שמקבל כל מילה. מבון שהרדווקציה פוליאי, וגם שהיא נכונה.

. $\text{CONT}_{\text{DFA,NFA}} = \{\langle A_1, A_2 \rangle : L(D_1) \subseteq L(A_2) \text{ ו- DFA } D_1 \text{ ו- NFA } A_2\}$.2

זו שפה קלה יותר מאשר CONT_{NFA} ולכן מ- PSPACE. נשים לב שהרדווקציה הינה' עובדת לבדוק אותו הדבר ולכן זו שפה PSPACE-קשה.

. $\text{CONT}_{\text{NFA,DFA}} = \{\langle A_1, A_2 \rangle : L(A_1) \subseteq L(D_2) \text{ ו- DFA } D_2 \text{ ו- NFA } A_1\}$.3

עדין ב- PSPACE. הפעם הרדווקציה לא עובדת כי אין אפשרות להעתיק את ה-NFA אל תוך הסלוט השני כי מצופה לו DFA.

למקרה השפה לא PSPACE-קשה כי השפה ב- P : ניתן להכريع $\emptyset = L(A_1) \cap \overline{L(D_2)}$ בזמן פוליאי בגודל הקלט (משלים לדfas ניתן לחישוב פוליאי).

. $\text{MIN}_{\text{DFA}} = \{\langle D, k \rangle : \text{DFA } D \text{ יש שקול עם לכל היותר } k \text{ מצבים}\}$.4

נשים לב שלא משנה אם k מוצג באונארית או ביןארית כי קלט מעניין רק אם $k > |D|$ ואז הקלט בכל מקרה גדול מהייצוג האונארית של k .

השפה היא ב- P כי ראיינו אלג' צמצום עם מחלקות השקילות של מייהיל-נווד.

. $\text{MIN}_{\text{NFA}} = \{\langle D, k \rangle : \text{NFA } D \text{ יש ש竽ול עם לכל היותר } k \text{ מצבים}\}$.5

בתרגיל נוכיח כי השפה ב- PSPACE (כי ב- NPSPACE באמצעות עד שהוא NFA שאמור להיות ש竽ול וקטן מספיק).

$L(A)$ נוכיח כי MIN_{NFA} היא PSPACE-קשה. נוכיח $\text{ALL}_{\text{NFA}} \leq_p \text{MIN}_{\text{NFA}}$. הרעיון יהיה שם ל- DFA יש מצב אחד אם $s = k = 1$ אז נבחר תמיד $\Sigma^* \vee L(A) = \emptyset$

$L(A) = \emptyset$ תחזיר את B כך שיש ל- DFA B ש竽ול עם מצב אחד אם A אוניברסלי, לעומת נחזר, נוכון. ואחרת $\langle A_{\Sigma^*}, 1 \rangle$.

את בעיית הריקנות אפשר להכريع עם BFS כאמור ולכן זה חשוב, וגם נכון.

תרגול

משפט (סביצ') לכל n $\text{NSPACE}(s(n)) \subseteq \text{SPACE}(s^2(n))$, $s(n) \geq \log n$

הערה במקרה של סיבוכיות בזמן, שlimnu בניפוי אקספ' ולא רק פוליאי.

הערה נוכיח עכשו ל- $n \geq s(n)$ ובהמשך נראה למה ההוכחה זהה במקרה הכללי.

הוכחה: תהי M מכונה א'ד שמכריעה שפה L בסיבוכיות זכרו (n) s ונניח ש :

1. לכל מילה w , יש ל- M רק קונפ' התחלתי אחת על w ונסמן אותה c_{init}^w .

2. ל- M יש רק קונפ' מקבלת אחת c_{acc} (כשתבויה לקבל המכונה תמחוק את הסטר ותליך שמאללה עד הסוף ורק אז תקבל).

יהי $1 \geq d$ כך של- M יש לכל היותר $2^{d \cdot s(n)}$ קונפ' שונות על מילה באורך n . d כזה קיים כי יש ל- M $|Q|$ קונפ' שונות,

כלומר

$$\begin{aligned} c_1 \cdot c_2^{s(n)} \cdot s(n) &= c_1 \cdot 2^{s(n) \log c_2} \cdot 2^{\log s(n)} \\ &= c_1 2^{\log c_2 s(n) + \log s(n)} \end{aligned}$$

המכונה M' שניצר תרי' פ' דטרמיניסטיבית שמחזירה אם "ס ניתן להגעה ב- M מהקונפ' c_1 ל- c_2 ב- t לכל היותר.

מכיון ש- M מקבלת את w רק אם קונפ' c_{init}^w מתקבלת מ- c_{acc} ותקבל אם היא מחזירה true ואחרת תדחה. המכונה נוכна כי M' מקבלת את w אם "ס תרי' את M' ריצה מקבלת על w שלא חוזר על אף קונפ' פעמיים (אחרת נהיה במעגל אינסופי).

נוכח כי סיבוכיות הזיכרון של can_yeild היא $\mathcal{O}(s(n) + \log t) \log t$ וזו' מזדקק לזיכרון M'

$$\mathcal{O}(s(n) + \log 2^{d \cdot s(n)}) \log 2^{d \cdot s(n)} = \mathcal{O}(s(n) + d \cdot s(n)) s(n) = \mathcal{O}(s^2(n))$$

נגידר את הפ' : $c_1, c_2 \in \Gamma^* Q \Gamma^*$, כאשר can_yeild(c_1, c_2, t)

1. (תנאי עצירה) אם $t = 1$ או החזר true ואם $c_1 = c_2$ או עיקבת ל- c_1 .

2. אם $t > 1$ או עבר על כל הקונפ' $c \in \bigcup_i \Gamma^i Q \Gamma^{s(n)-i}$ ובזוק האם c הינה באורך t לכל היותר. האם c הינה באמצע ריצה מקבלת מ- c_1 ל- c_2 באורך t לכל היותר.

אם כן, החזרה true. אם לא, עברו ל- c -הבא.

M' דטר' כי לא מוחשים שום דבר אלא עוברים על כל האפשרויות.

M' כניסה עמוקה ריקורסית מקסימלי של $\log t$. בכל קראיה, שומרים שתי קונפ' וחס מספר צעדים שערכו לכל היותר t , כלומר $2s(n) + \dots + 1$. סה"כ יש לנו $\mathcal{O}(s(n) + \log t) \log t$.

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

הגדירה נוסחה ב-QBF היא נוסחה (לא בהכרח CNF) שכל המשתנים שלה מכומתיים (יש להם או \exists או \forall , בסדר מסוים) ונגידר את השפה

$$\text{TQBF} = \text{QSAT} = \{\langle \varphi \rangle : \text{True} \text{ הוא } \varphi \in \text{QBF}\}$$

דוגמה נביט בנוסחה $(x_1 \vee x_2) \wedge (\overline{x_1} \vee \overline{x_2})$. האם $\exists x_1 : \forall x_2 : \exists x_1$ הנוסחה true ? לא! האם $\exists x_2 : \forall x_1$ הנוסחה true ? כן!

משמעות TQBF היא PSPACE-שלמה.

הוכחה: נוכיח כי $\text{TQBF} \in \text{PSPACE}$. בהינתן $Q_i \in \{\forall, \exists\}$ כאשר $Q_1 x_2 Q_2 x_2 \dots Q_k x_k \varphi(x_1, \dots, x_k)$

1. (תנאי עזרה) אם אין כמותים ($k = 0$) אז אין משתנים ולכן נשערך את הנוסחה בשטח פוליאו וnochzir את ערך האמת שלה (T או F).

2. אחרת:

(א) אם הנוסחה מהצורה $\psi \exists x \psi$ נשערך ריקורסיבית את $\psi_{x \leftarrow T}$ ו- $\psi_{x \leftarrow F}$ ונחזיר אמת אם "ס אחד מהשעரוכים לפחות הוא אמת.

(ב) אם הנוסחה מהצורה $\psi \forall x \psi$ נשערך ריקורסיבית את $\psi_{x \leftarrow F}$ ו- $\psi_{x \leftarrow T}$ ונחזיר אמת אם "שני השעரוכים הם אמת".

עומק הריקורסיה הוא k (כל פעם מורידים משתנה אחד), ובכל קראיה שומרים את הנוסחה עם השמה חלקית שלה, כך שהה"כ נדרש זכרון פוליאו.

עתה נוכיח כי לכל מוגדרים משותנה אחד, ובכל קראיה שומרים את הנוסחה עם השמה חלקית שלה, כך שהה"כ נדרש זכרון לבנות נוסחה כך ש- M מקבלת את w אם "ס φ היא true".

נניח ש- s -חסם על מספר התאים ש- c -מתASHMATOT בהם. נקודד קונפ' c על ידי המשתנים הבאים:

1. לכל אות $\Gamma \in [s]$ ו- $i \in [s]$ משתנה $X_{i,a} \in \Gamma$ שערךו T אם "ס בתא ה- i כתוב a .

2. לכל $i \in [s]$ משתנה y_i שערךו T אם "ס ראש קורא מצביע על התא ה- i .

3. לכל מצב $q \in Q$ משתנה z_q שערךו T אם "ס המכוונה במצב q .

לכן קידוד קונפ' יכול את המשתנים

$$c = \langle x_{1a_1}, \dots, x_{1a_m}, \dots, x_{sa_1}, \dots, x_{sa_m}, y_1, \dots, y_s, z_{q_1}, \dots, z_{q_l} \rangle$$

כאשר $Q = \{q_1, \dots, q_l\}$ ו- $\Gamma = \{a_1, \dots, a_m\}$ נשתמש בנוסחות הבאות להגדרת φ הסופית:

1. הנוסחה

$$\varphi_{valid} = \bigvee_{i \in [s]} (y_i \wedge \neg(y_1 \vee \dots \vee y_{i-1} \vee y_{i+1} \vee \dots \vee y_s))$$

תקבע שבדיוק y_j הוא T וכל השאר F , ובדומה נظرף לה נוסחת שמודעת שיש מצב אחד לכל הקונפ' ואות אחת בדיק לכל תא כמו שכבר עשינו בעבר.

2. הנוסחה $\varphi_{move}(c_1, c_2)$ בודקת שהקונפ' c_2 עוקבת ל- c_1 (וגם שתיהן חוקיות).

מציג שני ניסיונות לא מוצלחים להגדרת φ הכללית לכל w :

1. אם נגדיר

$$\exists c_1 \dots \exists c_t (c_1 = c_{init}^w) \wedge (c_t = c_{acc}) \bigwedge_{i \in [t-1]} \varphi_{move}(c_i, c_{i+1})$$

זה לא יספק (ברמה העקרונית כי לא השתמשנו ב- \forall ואז זה מוכל-ב-SAT והמסקנה היא ש- $NP = PSPACE$) כי M מקבלת את w לא בהכרח תוך מספר פוליא(t) של צעדים כי היא ב- $PSPACE$ ולא P ! זה יבוד אם $2^{\ell \cdot s(n)}$ אבל אז הרדוקציה לא פוליא.

2. נסמן $\varphi(c, c', k)$ האם יש ריצה מ- c ל- c' שאורכה k ונחשב

$$\varphi(c, c', k) = \exists c'' \varphi\left(c, c'', \lfloor \frac{k}{2} \rfloor\right) \wedge \varphi\left(c'', c', \lceil \frac{k}{2} \rceil\right)$$

אם נציב c_{acc} ו- $c_{init}^w, k = 2^{d \cdot s(n)}$ נקבל נכונות, אבל לא פולינומיאלית כי אורך הנוסחה הוא $s(n) \cdot k$ שהוא שוב אקספ'.

הניסיון המוצלח הוא הגדרת

$$\varphi(c, c', k) = \exists c'', \forall c_1, \forall c_2 \left(((c_1 = c) \wedge (c_2 = c'')) \vee ((c_1 = c'') \wedge (c_2 = c')) \rightarrow \varphi\left(c_1, c_2, \lceil \frac{k}{2} \rceil\right) \right)$$

כלומר אפשר להגיע מ- c ל- c' ב- k -צעדים אם קיימת קונפ' ביניהם c'' , כך שלכל $c_1 \rightarrow c_2$ ו- $c_2 \rightarrow c_3$ הוא $c'' \rightarrow c_3$ או אפשר להגיע מ- c_1 ל- c_2 ב- $\frac{k}{2}$ צעדים.

עתה מתקיים

$$\ell(k) = \mathcal{O}(s(n)) + \ell\left(\frac{k}{2}\right) = \mathcal{O}(s(n)) \log k$$

שהזיהוי ב- $(k = 2^{d \cdot s(n)})$ נכון.

■ לכן הרדוקציה פוליא, ונכונה, כלומר TQBF היה PSPACE-קשה.

שבוע 11 ו-12 | סבבון

הרצאה

חלק א' של החרצתה

הערה מחלוקת תת-lienאריות לא מעניינת בהקשר של סיבוכיות זמן כי לא נוכל לקרוא את כל הקלט בכלל, וגם בחיפוש ביןاري הסיבוכיות האמיטית היא לפחות ריבועית בגלל הדרוש שבנה אנחנו נגשים לערבים שרירותיים בזיכרון.

נשנה את המודל של מ"ט לסרט קלט שהוא קרייה- בלבד, וסדרט העבודה שמאפשר קרייה וכתיבה.

הגדרה סיבוכיות הזיכרון של M היא (n) אם סרט העבודה של M מכיל (n) s תאים בעיבוד של קלט באורך n .

הגדרה $\text{NL} = \text{NSPACE}(\log n)$ ו- $\text{L} = \text{SPACE}(\log n)$

דוגמה $\{0^n 1^n : n \geq 0\}$ EQ. מ"ט שמכריע את השפה יכולה למחוק אוטיות מכל צד עד שיש שווין (או לא) - זה דרוש זיכרוןlienארי. עתה לא נוכל לבקש על סרט הקלט, אבל עדיין $L \in \text{EQ}$: מ"ט שמכריע את EQ בשטח לוג:

1. סופרת בסיס 2 את מספר ה-0-ים, c_0 .

2. סופרת בסיס באותו הבסיס את מספר ה-1-ים, c_1 .

3. משווה את c_1 ו- c_0 .

אכן זכרון לוג'י כה המונה $c_0 \log(|w|)$ ביטים, $c_1 \log(\#_1 w)$ ביטים וההשוואה . $\log(\mathcal{O}(|w|))$ דורש

דוגמה $\{G, s, t : t \in \text{PATH}\}$

מכריע את PATH בזמןlienארי (זיכרוןlienארי). קל לראות ש- $\text{PATH} \in \text{NL}$ - המכונה תנחש מסלול באורך $|V|$ מ- s ל- t :

1. תאתחל $s := v$ ו- $c := 0$.

2. בכל צעד: תנחש קודקוד v' כך ש- $E(v, v')$. אם $v' = t$ העצור ותקבל אחרת, $v = v'$ ו- $c + 1$, ואם $v' = c$ ו- $c = |V|$ עוצרת וzdocha.

המכונה המכונה כי יש מסלול מ- s ל- t אם קיימים חישוב מקובל של המכונה. המכונה סיבוכיות זיכרון לוג'י כה המכונה שומרת קודקוד $V \in V$ ומונה עד $|V|$, כל אחד דורש $\log|V|$ זיכרון.

הערה בהוכחת משפט סביצ', המכנו ש- $n \geq s(n)$. ההוכחה עובדת גם עבור $n \geq \log s(n)$. זאת משום שהשתמשו בהנחה כדי לטעון של המכונה יש $2^{\mathcal{O}(s(n))}$ קומפ' שונות לכל היותר. זה נכון גם למכונה עם $n = \log s(n)$

קונפ' של המכונה עם $n = \log s(n)$ ניתנת לקידוד כ밀יה מהצורה $Q \times n \times \log n \times \Gamma^{c_1 \log n}$ - המצב, מקום הראש הקורא, מקום הראש הקורא-כותב ותוכן סרט העבודה. אותה הטרנס' תיתן לנו שמספר הקונפ' עדין חסום ע"י $2^{\mathcal{O}(s(n))}$.

מסקנה $\text{NL} \neq \text{SPACE}(\log^2 n)$. כלומר סרט $\text{NL} = \text{NSPACE}(\log n) \subseteq \text{SPACE}(\log^2 n)$.

הגדרה נאמר כי A היא שלמה ב- NL אם:

1. $A \in \text{NL}$.

2. לכל שפה $B \leq_{\text{logspace}} A, B \in \text{NL}$ (קשה).

הגדרה log-space transducer (משרן) הוא מ"ט שמחשב בת' בשטח לוג'י (של סרט העבודה) וכותבת את התוצאה על סרט שלישי לכתייה- בלבד. נאמר כי $f : \Sigma^* \rightarrow \Sigma^*$ שניתנית לחישוב בשטח לוג'י אם קיימים מרן M שעלה קלט w (בסרט הקלט) עוצר עם $f(w)$ על סרט הפלט ומשתמש ב- $\mathcal{O}(\log|w|)$ תאים בסרט העבודה.

הערה רוב הפ' הילו הופ' שמעתיקות את הקלט לפלט עם שינויים קטנים שאפשר לעשות בזמן לוג'.

דוגמה F' שמעבירה גרפ' ממושקל $G = \langle V, E, w \rangle$ כך ש- $E' = \langle V, E', w' \rangle$ לא ממושקל כך ש- $G' = \langle V, E', w' \rangle \geq 8\gamma E(v, v')$.

הגדעה נאמר כי $A \leq_{\text{logspace}} B$ אם יש פ' f ניתנת לחישוב בשטח לוג', כך שלכל $w \in \Sigma^*$

$$B \in L \iff f(w) \in A$$

הערה חיקוי של ההוכחה של משפט הרדוקציה ל-P ו-NP לא יצליח: אם M_A מ"ט שמכריעה את A בשטח לוג' ו- M_f מ"ט שמחשבת פ' לרדוקציה $A \leq_{\text{logspace}} B$. נבנה M_B שמכריעה את B בשטח לוג' ע"י הרצת M_f על w ואז הרצת M_A על הפלט שלה.

זה לא יעבוד כי הפלט של f הואلينארי לכל היותר $-|w|$, ואת זה אי אפשר לשים על סרט העבודה של M_B כי הוא צריך לוג', שכן סיבוכיות הזיכרון לינארית ולא לוג' ולא השגנו כלום.

הוכחה: נניח שיש לנו את M_f כנ"ל, M_B שתכרייע את B בשטח לוג' תרוץ תחת העיקרון הבא: בכל פעם לקרוא את האות

ה-i-ית ב- $f(w)$, היא מחשבת את (w) מחדש, ובודקת מה האות ה-i-ית. פורמלית:

1. מחזיקה מונה i שמאתחל ל-1, שהוא האינדקס של האות המעניינת ב-(w).

2. מריצה את M_f , עד ש- M_f כותבת את האות ה-i-ית σ - נסמלץ את סרט העבודה של M_f וונעשה "hijacking" ("כתיבות שלה לסרט הפלט, כאשר נתעלם מכל הערכים אלא אם היא עכשו כתבה לו ה-i-ית" בסרט הפלט).

3. בהינתן מעבר M_A של $\delta_A(q_0, \sigma, \gamma) = (q', *, R/L)$ לפי התזוזה של ראש הקורא (את הקלט) של M_A .

4. חוזרת לשלב 1 עד ש- M_A עצרת.

טענה PATH היא NL-קשה.

הוכחה: תהי $f(w) = \langle G, s, t \rangle$, ונכיה $B \in L \leq_{\text{logspace}} \text{PATH}$, כלומר נמצא $w \in L$ כך ש- s ו- t ב- G יש מסלול מ- s ל- t .

יהיה גרפ' הקונפ' של M_B (המכונה שמכריעה את B בשטח לוג'), s הקונפ' ההתחלתית של M_B על w ו- t הקונפ' המתקבלת היחידה (בה"כ הראננו איך להמיר) של M_B . תהיה קשת בין שני קודקודים אם אלו קונפ' עוקבות.

קונפ' של M_B תקיים אם הא"ב $\Sigma = \Gamma \cup (Q \times \Gamma) \cup \{0, 1, \$\}$ כאשר קונפ' היא

$$\frac{\gamma_1 \dots (q, \gamma_i) \dots \gamma_{s(n)}}{\text{מיקום הראש הקורא}} \text{ סרט העבודה ומצב הראשיים}^{\$(0+1)^{\log_2 n}}$$

הרדוקציה תעבור על כל המילים מעל Σ מהצורה

$$\Gamma^{i-1} \cdot (Q \times \Gamma) \cdot \Gamma^{\log n - (i+1)} \$ (0+1)^{\log n}$$

(שהן באורך i לכל $[\log n + 2n \log n + 1]$) ותעתיק לסרט הפלט את המילים שמקודדות את הקונפ'.

עתה היא תייצר את רשימת הקשיות, באמצעות מעבר על מילים מעל Σ באורך $(1 + 2 \log n) 2$ ותעתיק לרשימה הקשיות מילים שמקודדות קונפ' עוקבות (בדיקה שנעשית בשטח לוג').

■ בנוסף את $t = c_{acc}$ -ו $s = c_{init}^w$ אפשר לכתוב בשטח לוג'. لكن לסיום הרדוקציה נcona ובשטח לוג'.

הערה ידוע $\text{PATH} \in \text{P}$ -PATH.

מסקנה $\text{NL} \subseteq \text{P}$.

הוכחה: בהינתן $B \in \text{NL}$, נוריד אותה ב- logspace -PATH. נשים לב שככל רדוקציה שעובדת ב- logspace , עוצרת בזמן פוליאי (מספר הקונפ' שלו הוא פוליאי) ולכן יש פתרון ב- P ל- B .

■ הערה עד כה יש לנו

$$\text{L} \subseteq \text{NL} \subseteq \text{P} \subseteq \text{NP} \subseteq \text{PSPACE} = \text{NPSPACE} \subseteq \text{EXPTIME}$$

ובתרגול נראה ש $\text{NPSPACE} \subsetneq \text{PSPACE}$ ולכן איזושי הכללה בדרך היא הכללה ממש.

דוגמה $\overline{\text{EMPTY}_{\text{NFA}}} = \{ \langle A \rangle : L(A) \neq \emptyset, \text{NFA } A \} \in \text{P}$

מתקיים $\text{NL} \in \text{CIMTAA}'$ שמעירכה את $\overline{\text{EMPTY}_{\text{NFA}}}$ בשטח לוג' מנהשת ריצה מקבלת ושומרת בכל רגע מצב בריצתה ומונה עד $|Q|$ (אורך מקסימלי לרכיב/מילה מגולמת מורצת).

נוכיח כי $\overline{\text{EMPTY}_{\text{NFA}}}$ היא NL-קשה. בהינתן $\langle G, s, t \rangle$, נתאים NFA כך שיש מסלול בין s ל- t אם ומן NFA מכיל שפה לא ריקה.

בහינתו $E(q, q') \sqsubseteq \delta(q, a)$ כאשר $q' \in \delta(q, a)$ נזכיר $\langle \Sigma, Q, Q_0, \delta, F \rangle = \langle \{a\}, V, \{s\}, \delta, \{t\} \rangle$, $\langle \langle V, E \rangle, s, t \rangle$ הרדוקציה לוקחת שטח לוג' ונcona, לכן השפה NL-שלמה.

חלק ב' של ההרצאה

דוגמה נגידר

$$\text{BBPATH} = \{ \langle G, s, t, b \rangle : b \in \mathbb{N}, t-s \leq b \leq \min(Q, |V|) \}$$

אכן $\text{NL} \in \text{BBPATH}$ כי אפשר להשתמש באlg' שלו ל-PATH רק שהמכונה תשמר במקום מונה של מספר הצעדים, את משקל המסלול המוצטבר. בנוסף במקום לעצור אחר $|V|$ צעדים, נעצר אחרי שמונה שנזהיק גיע למספר אחר (לא נרחב כי אין זמן אבל זה אפשרי).

BBPATH היא בנוס NL -קשה בגל הרודקציה $\text{PATH} \leq_{\text{logspace}} \text{BBPATH}$: בהינתן $G' = \langle V, E, w \rangle$, נגיד $G = \langle V, E \rangle$ PATH עם $b = |V| - 1$ ו- $w(e) = 1$. אם נדרש $b \in \mathbb{N}^+$ אפשר לחסיף קודקוד לפני s וכו'. אכן הרודקציה היא ב-logspace כי רק מעティקים את הגרא.

דוגמא האם נוכל לסwoג את BBSPTH , כלומר $\langle G, s, t, b \rangle$ כנ"ל רק שהמסלול צריך להיות פשוט? זו בעיה NP קשה, כי אפשר בקלהות לעשות רודקציה מה-HAMPATH ($D - ST -$) HAMPATH .

משפט (*איירמן*). $\text{NL} = \text{coNL}$

הערה אימרמן הוכיח ש- $\text{NL} \neq \overline{\text{PATH}}$ וסיים כי PATH בעיה קשה ב-NL. נציג את רעיון ההוכחה:
אימרמן הסתכל על שפת כל $\langle G, s, t, c \rangle$ כך ש- G מכובן כך שיש לכל היתר \mathbb{N} קודקודים ישיגים מ- s ואין מסלול מ- s ל- t . מספיק שנצבע על c קודקודים שונים מ- t ישיגים מ- s (ואז t לא יכול להיות ישיג מ- s כי הגענו למכסה) ואת זה אפשר לעשות ב-NL.

תרגול

הגדרה נאמר שפ' $\mathbb{N} \rightarrow \mathbb{N}$ שעבורה $t = \Omega(n \log n)$ היא ניתנת לבניה בזמן אם הפ' שמנפה את n^t לייצוג הבינארי של (n) t ניתנת לחישוב בזמן $\mathcal{O}(t(n))$.

הערה רוב הפ' הלא-פטולוגיות מקיימות את ההגדרה הנ"ל.

משפט (ההיררכיה בזמן) תהיו $\mathbb{N} \rightarrow \mathbb{N}$: t ניתנת לבניה בזמן. אז קיימת שפה L שמכריעה בזמן $(n) \mathcal{O}(t(n))$ אבל לא כריעה בזמן $\mathcal{O}\left(\frac{t(n)}{\log t(n)}\right)$.

מסקנה לכל $1 < \epsilon_1, \epsilon_2$, מתקיים $\text{TIME}(n^{\epsilon_1}) \subsetneq \text{TIME}(n^{\epsilon_2})$ ($n^{\epsilon_2} / n^{\epsilon_1} > 1$).

הוכחה: מאינפי מתקיים $n^{\epsilon_1} = o\left(\frac{n^{\epsilon_2}}{\log n^{\epsilon_2}}\right)$ ולכן ממש פטור יותר ממש בעיות בזמן $\mathcal{O}(n^{\epsilon_2})$ מאשר ב- $\mathcal{O}(n^{\epsilon_1})$. ■

מסקנה $\text{P} \subsetneq \text{EXPTIME}$

הוכחה: מתקיים $\text{P} \subseteq \text{TIME}(2^n) \subsetneq \text{TIME}(2^{n^2}) \subseteq \text{EXPTIME}$, ולכו' $n^k \subseteq \mathcal{O}(2^n)$ לכל k .

טענה קיימת מ"ט S כך שבгинן $\langle S, \langle M, t, w \rangle \rangle$ מחשבת את הקונפ' בריצת של M על w במשך t צעדים תוק זמן ($|M|$).

פולינום כלשהו.

הוכחה: אם היו לנו שלושה סרטים אפשרי לשמור את הקידוד בסרט 1, לחשב בזמן פוליאי קונפ' עוקבת הסרט 2, ולעשות את זה t פעמים עם מונה בגודל $t \log t$ הסרט 3. הבעיה היא שצמצום שלושה סרטים לאחד לוקח זמן פוליאי לא ניתן.

בסרט אחד, נוכל להכפיל פי 3 את הא"ב וכי להימנע מסיריקות מיותרות בחיפוש אחר $\langle M \rangle$, "נסחוב אותו" עם הראש הקורא בכל צעד (טכנית אפשרי).

הוכחה: (של משפט ההיררכיה בזמן) נגדיר

$$L = \left\{ \langle M \rangle \# 0^k : t'(n, m) = \frac{t(n)}{p(m) \log t(n)} \text{ ו } m = |\langle M \rangle|, n = |\langle M \rangle \# 0^k| \text{ תזק } t'(n, m) \text{ צעדים כאשר } \langle M \rangle \# 0^k \text{ לא מקבלת את } M \right\}$$

נראה שניתן להכרייע את L בזמן (n) $\mathcal{O}(t(n))$ שמכריעת את L תפעל כך, בהינתן x :

1. תבדוק אם $x = \langle M \rangle \# 0^k$ כלשהם -

. $\mathcal{O}(n \log n) - m = |\langle M \rangle| - n = |x|$

3. תחשב $\mathcal{O}(t(n)) - t = t(n)$

4. תחשב $\text{polylog } t(n) - t' = t'(n, m) = \frac{t}{p(m) \log t}$

5. תסמלץ את M על x במשק' צעדים. אם M מקבלת את x , תדחה, אחרת תקבל -

$k \geq 0$. $r(n) \leq \frac{1}{p(m)} \cdot \frac{t(n)}{\log t(n)}$ ותהי M מ"ט שעושה זאת. יהיו $n > m + 1$ ו n ופ'. נניח בשילילה שניתן להכרייע את L בזמן $\mathcal{O}\left(\frac{t(n)}{\log t(n)}\right)$ ונקבע $\langle M \rangle \# 0^k$ על M ונביט בריצעה של M על $-n$.

• אם M מקבלת את $\langle M \rangle \# 0^k$ תזק $\langle M \rangle \# 0^k \in L$ צעדים, אז M דוחה את $\langle M \rangle \# 0^k$ (מהגדרת L), סתיירה.

• אם M דוחה את $\langle M \rangle \# 0^k$ אז $\langle M \rangle \# 0^k \notin L$ צעדים (מהגדרת L), סתיירה.

הגדירה { G } גראף מכובן קשור חזק : $\text{SCC} = \{\langle G \rangle$ כאשר גראף קשור חזק הוא גראף שבו לכל $V \in u, v$, יש מסלול $m-u$ ל- v וגם $m-v$ ל- u ב- G .

טענה SCC היא NL-שלמה.

הוכחה: כדי להראות $\text{SCC} \in \text{NL}$, ממשפט אימרמן מספיק שוכיח $\overline{\text{PATH}} \in \text{NL}$. מ"ט א"ד T שמכריעת את $\overline{\text{SCC}}$ בשטח לוג' תפעל כך : נחשב באופן א"ד שני קוד' $V \in u, v$. אם אין ביניהם מסלול נקי, אחרת נדחה (נחשב באמצעות הרצת מ"ט $\overline{\text{PATH}}$ שמכריעת את $\overline{\text{PATH}}$).

נראה כי SCC היא NL-קשה עם הרדוקציה $\text{SCC} \leq_{\text{logspace}} \text{PATH}$. נגדיר f באופן הבא : בהינתן $\langle G, s, t \rangle$, נחזיר $\langle G' \rangle$ כך ש- G' מתקבל מ- G ע"י הוספת הצלעות הבאות : נסיף לכל $V \in v$ צלעות (v, s) ו- (t, v) .

הרידוקציה לוג' בשטח כי בכל שלב בסדרת העבודה אנחנו שומרים מונה ואת הרכיב הנוכחי מעティקים לשרטט הפלט, מוחקקים את הרכיב הנוכחי, מגדילים את המונה וחזור חלילה. הרידוקציה נcona כי:

- אם $\langle G' \rangle \in \text{SCC}$ אז יש מסלול מ- s ל- t : $s \rightarrow s \rightarrow \dots \rightarrow t \rightarrow v, u \in V$, יש מסלול u ב- G' , כלומר $\langle G', s, t \rangle \in \text{PATH}$.
- אם $\langle G' \rangle \notin \text{SCC}$ אז גם ב- G' אין מסלול מ- s ל- t ולכן $\langle G, s, t \rangle \notin \text{PATH}$.

■

הגדירה {יש ב- G בדיק 2 רכיבי קשריות חזקה : $.2\text{SCC} = \{\langle G \rangle :$

טענה 2SCC שלמה ב- NL .

הוכחה: $\text{NL} \in 2\text{SCC}$ באמצעות מ"ט שבודקת שאין רכיב קשריות חזקה אחד (ראינו לעיל), ובודקת שאין לפחות 3.

השפה קשה ב- NL באמצעות רידוקציה $2\text{SCC} \leq_{\text{logspace}} \text{NL}$ עם הפ' הבאה: בהינתן $\langle G \rangle$, תחזיר G' הבנויה מ- G -ו ועוד קודקוד מבודד.

■ כך ל- G יש רכיב קשריות חזקה אחד (כolio קשר חזק) אם ו רק יש בדיק 2 רכיבי קשריות שניים. הרידוקציה כמובן בשטח לוג' ונcona.

סוף.

נספח | רשיימת הגדרות ומשפטים

יש לקחת רשיימה זו בערבון מוגבל - הרשיימה מוצתת בעוררת סקריפט אוטומטי שרצ' על הסיכום, וכן יכול להיות שפיספס הגדרות ומשפטים חשובים (שנמצאו בדוגמאות לצורך העניין). בפרט, אין לראות ברשיימה זו או בכל חלק אחר של הסיכום מקור רשמי לחומר הקורס ו/או חומר המבחן!

משפט רגולריות ואוטומטיים

הגדרות

1. אוטומט הוא מחשב עם זכרון מוגבל.
2. אוטומט (automaton, DFA) הוא חמייה (automaton, DFA) שהם המצבים, הא"ב, פונקציית המעברים, המצב ההתחלתי וקבוצת המצבים המקבלים שモכלת ב- Q .
3. ריצה על מילה $w_n \dots w_1 = w$ מעל Σ היא סדרה של מצבים $r_n \dots r_0 \dots r$ כך ש :
4. r היא ריצה מקבלת (accepting) אם $r_n \in F$ (המצב האחרון בריצה הוא מקבל). אחרת, r היא דוחה (rejecting).
5. שפה רגולרית היא שפה שנינתה לזיהוי ע"י אוטומט, פורמלית, $L \in \text{REG}$, היא רגולרית אם קיים DFA כך ש- $L(A) = L$.
6. נאמר כי $R \subseteq S \times T$ הוא יחס מעלה ($S = T$ (לרוב)).
7. עוצמה של קבוצה היא ממד ל"גודל" הקבוצה. עבור קבוצה סופית A , העוצמה שללה היא $|A|$.
8. $|\mathbb{N}| = \aleph_0$.
9. $\Sigma^* = \bigcup_{n=0}^{\infty} \Sigma^n$ ונגיד $\Sigma^n = \underbrace{\Sigma \times \dots \times \Sigma}_n$ פעמים.
10. בהינתן אוטומט A , נגדיר $\delta^*(q, w) = \begin{cases} q & w = \epsilon \\ \delta(\delta^*(q, w'), \sigma) & w = w'\sigma, \sigma \in \Sigma \end{cases}$
11. אוטומט אי-דטרמיניסטי הוא אוטומט שבו פ' המעברים ממפה מצב ואות (או אפסילון) לקבוצה של מצבים עוקבים אפשריים, כוללם

$$\delta : Q \times (\Sigma \cup \{\epsilon\}) \rightarrow 2^Q$$

ומילה מותקבלת אם "ס" קיימת ריצה מקבלת של A על המילה.

12. אוטומט אי-דטרמיניסטי הוא חמייה מהצורה $A = \langle Q, \Sigma, \delta, Q_0, F \rangle$ שעבורו $Q_0 \subseteq Q$ ויכולים להיות כמה מצבים ההתחלתיים) ו- $\delta : Q \times (\Sigma \cup \{\epsilon\}) \rightarrow 2^Q$.
13. ביטוי רגולרי מעל א"ב Σ הוא אחד מה הבאים :

\emptyset •

ϵ •

$a \in \Sigma$ •

• כאשר $t^*, t \cup s, t \cdot s$ ביטויים רגולריים קצרים יותר.

14. בהינתן ביטויים רגולריים t, s, r , נגידר את השפה שליהם כך:

$L(r) = \emptyset \text{ או } r = \emptyset$ •

$L(r) = \{\epsilon\} \text{ או } r = \epsilon$ •

$L(r) = \{a\} \text{ או } r = a \in \Sigma$ •

$L(r) = L(s) \cdot L(t) \text{ או } r = s \cdot t$ •

$L(r) = L(s) \cup L(t) \text{ או } r = s \cup t$ •

$y \cdot z \in L \iff x \cdot z \in L, \forall z \in \Sigma^* \text{ אם } x \sim_L y, x, y \in \Sigma^*$ כך שלכל $\sim_L \subseteq \Sigma^* \times \Sigma^*$ מתקיים $x \sim_L y \iff \exists z \in \Sigma^* x \cdot z \sim_L y \cdot z$. 15

16. נגידר את הסדרה i ~ באופן אינדוקטיבי.

בבסיס ($i = 0$) $s_1 \sim_0 s_2 \iff s_1 \in F$ • ויש לו שתי מחלקות שקליות, כל המקבלים וכל הלא מקבלים).

צעדי ($i \rightarrow i + 1$): נגידר $s_2 \sim_{i+1} s_1 \iff \forall \sigma \in \Sigma^* \delta(s_1, \sigma) \sim_i \delta(s_2, \sigma)$ וגם (s_1, s_2 מסכימים על מילים באורך i וגם על כל הארכה באורך $i + 1$).

משפטים

1. קיימות שפות לא רגולריות, ויש "יותר" לא רגולריות מאשר לא (השפות הרגולריות הן קבוצה במידה 0 מותוך כל השפות).

2. השפות הרולגריות סגורות ליחוד, כלומר, אם $L_1, L_2 \in \text{REG}$ אז $L_1 \cup L_2 \in \text{REG}$.

3. לכל DFA A' קיים DFA A שקול כך ש- $A = A'$.

4. לכל $w \in \Sigma^*$ מתקיים $(q'_0, w) = \delta^*(Q_0, w)$ או במלים, המצב ב- A' ש- A' מגיע אליו אחרי קריאת w (ה מצב הוא קבוע מפני עצמו), שווה לקבוצת המצבים ש- A יכול להיות בה (באחת

5. הריצות של A על w .

6. לכל NFA $A = \langle Q, \Sigma, \delta, Q_0, F \rangle$ קיים NFA B שקול B כז שב- B אין מעבר ϵ .

7. REG סגורה ליחוד, כלומר, אם $L_1, L_2 \in \text{REG}$ אז $L_1 \cup L_2 \in \text{REG}$.

8. REG סגורה לשורש, כלומר, אם $L_1, L_2 \in \text{REG}$ אז $L_1 \cdot L_2 \in \text{REG}$.

9. REG סגורה לפועלה Kleene-Star כולם אם $L \in \text{REG}$.

10. לכל פולינום p , קיימת שפה L כך של- L -קיום DFA עם n מצבים והוא הקטן ביותר עבור L צריך יותר (n) p מצבים.

. $L = \{0^n 1^n : n \geq 0\}$ DFA אין עבור .11

12. (лемת הניפוח לשפות רגולריות, pumping lemma) אם $|w| \geq p$, $w \in L$ ו- L רגולרי אז קיימ $1 \geq p$ (קבוע הנפוח) כך שלכל מילה w קיימים x, y, z כך ש:

$$|x \cdot y| \leq p \quad \bullet$$

$$(y \neq \epsilon) |y| > 0 \quad \bullet$$

$$xy^i z \in L, \forall i \geq 0 \quad \bullet$$

. $L = L(r)$ REG אם "ס קיימים ביטוי רגולרי r כך ש .13

14. לכל שפה L , $L \sim$ היא יחס שקילות.

15. (מייהיל-נרווד) $\Sigma^* \subseteq L \in \text{REG}$ אזי L יש \sim_L מספר סופי של מחלקות שקילות.

16. לכל $0 \leq i \leq Q$ ו- $s_1, s_2 \in Q$, מתקיים $s_1 \sim_i s_2 \iff \delta^*(s_1, w) \in F \iff \delta^*(s_2, w) \in F$ לא רגולרית.

17. תהי $f : \mathbb{N} \rightarrow \mathbb{N}$ מונוטונית עולה ממש כך ש- (n) היא איזי השפה $\{a^{f(n)} : n \in \mathbb{N}\}$.

. A DFA ניתן לייצר \overline{A} עם $|A| \leq p$ אין פולינום p כך שבහינתן (כל).

18. האלג' שהראנו לעיל הוא הכי טוב שאפשר ואין אחד עם סיבוכיות קטנה יותר, כי זה במקרה אקספוננציאלי.

שפות חסרות הקשר

הגדרות

1. דקדוק חסר הקשר הוא $G = \langle V, \Sigma, R, S \rangle$ כאשר:

V קבוצה סופית של משתנים. •

Σ קבוצה סופית של אותיות. •

R קבוצה של חוקי גזירה מהצורה $.V \rightarrow (V \cup \Sigma)^*$ •

$S \in V$ משתנה התחלתי. •

2. אם $vAu \Rightarrow A \rightarrow w$ ו- $w, u, v \in (V \cup \Sigma)^*$ הוא חוק בדקדוק, אז יצירה/גזירה היא המעבר $vawu$.

3. עבור G דקדוק ח'ה, נגדיר את השפה שלו להיות $L(G) = \{w : w \in \Sigma^* \wedge S \Rightarrow^* w\}$ (ונסמן $L(G) = L$).

אם יש שפה L כך $L = L(G)$ CFG.

.REG ⊆ CFL .1

2. למלת הניפוי $L \in \text{CFL}$ תהי $w = uvxyz$ איזי קיים $p \geq 0$ קבוע הניתן לכך שכליל מילה w^p גם $|w| \geq p$.

כasher matkayim :

- $uv^i xy^i z \in L$, מתקיימים $i \in \mathbb{N}_0$, $u, v, x, y, z \in \Sigma^*$
 - לכל $p \in \mathbb{N}$, $|vxy| \leq p \Rightarrow |vy| > 0$

סגורה לאיחוד .3 CFL

.4 CFL לשrhoה סgorה.

כריעות

הגדרות

1. מוכנות טיריניג היא שבייעיה $M = \langle Q, \Sigma, \Gamma, \delta, q_0, q_{acc}, q_{rej} \rangle$ כאשר :

הגרסה האי-דיארמיינית שבה משתמש היא עם הגדולה זהה לכך שעתה הפ' δ מועטיהה $\Gamma \times Q \times \Gamma \times \{L, R\}$.

2. פטיות מ"ט כלשי מוגדרת באופן הבא:

א) מילת הפלט בתובה על סרטן העוברה, מרופדת ב-*ז'ים*, אט $\sigma_1, \sigma_2, \dots, \sigma_n$ = *הונגיגוראים* הפתוחתנית תראה בסרטן הבא

$$\sigma_1 \quad \sigma_2 \quad \dots \quad \sigma_n \quad - \quad - \quad \dots$$

יב) המכונה מתקדמת לפי פונקציית המ鞠רים.

- קונפ' שנייה לעבור בינהו באמצעות פ' המעברים נקראות קונפ' מעברים.
- ריצה היא סדרה של קונפיגורציות עוקבות, החל מהקונפ' התחלה.
- שלושה גורלוֹת לריצה :

 - מגיעה ל McCabe ← עצרת ומקבל.
 - מגיעה ל McCabe דוחה ← עצרת ודוחה.
 - לא עצרת ודוחה את מילת הקלט.

3. קונפ' של מ"ט מגדירה ע"י המצב הנוכחי, תוכן הסרט ומקום הראש. קונפ' מתוארת ע"י מילה $b^* \cdot Q \cdot \Gamma^*$. כאשר הקונפ' uqv אומرت לנו שנחנו במצב q , שהראש מצביע לאות הראשון של v ושתוכן הסרט הוא uv ולאחר מכן $_q$ הוא על הסרט, בין u ל- v .

4. יהיו $q \in Q$ -ו $u, v \in \Gamma^*$, $a, b, c \in \Gamma$. אזי הקונפ' העוקבת של uqv היא (ראו הדוגמה,eko) וכן הדוגמות הבאות הוא תקלת טכנית בלחתי פתרה :

		q	
u	a	b	v

$$\delta(q, b) = (q', c, L) \text{ אם } uqvacv \cdot$$

		q'	
u	a	c	v

$$\delta(q, b) = (q', c, R) \text{ אם } uacqv \cdot$$

		q'	
u	a	c	v

- אם $u = \epsilon$ (אנחנו בקצת השמאלי) ו- $\delta(q, b) = (q', c, L)$ העוקבת תהיה $q'cv$ (מוניים מעבר שמאליה).

5. ריצה של M על מילה $w \in \Sigma^*$ היא סדרה c_0, c_1, \dots של קונפ' כך ש :

- c_0 היא הקונפ' התחלה של M על w .
- עוקבת ל- c_{i+1} לכל i .
- הסדרה סופית ומסתiya מ-קונפ' עצרת (קונפ' מקבלת אם המצב שלה הוא q_{acc} ודווחה אם המצב שלה הוא q_{rej}), או שאינה סופית.

- M מקבלת את w אם יש ריצה של M על w שמניעה לקונפ' מקבלת. אחרת (כל הריצות מגיעות לקונפ' דוחה או לא עצרות). נגידר את השפה של M להיות {יש ריצה מקבלת של M על w } . $L(M) = \{w : \text{יש ריצה מקבלת של } M \text{ על } w\}$
6. נאמר כי מ"ט M מזזה שפה L אם $L = L(M)$. מחלקת השפות מזזה (recursively enumerable) RE היא כל השפות הנינטות לזיהוי ע"י מ"ט.

. $\bar{L} \in \text{RE}$ אם “ $\exists L \in \text{co-RE}$.7

8. תהא $w \in M$. נאמר כי c_1, \dots, c_k גוררת את $c_i, i \in [k-1]$ היא ריצה חלקית של M על w אם $c_1 = q_0 w$ ולכל $[k-1]$ הינה ריצה חלקית של M על w אם $c_i = q_i c_{i+1}, i \in [k-1]$ גוררת את c_i , ו “ δ ” לפיה.

9. תהא $f : N \rightarrow M$. נאמר כי M מcomputable אם בתחילת הריצה של M כתוב את w על הסרט ובסוף הריצה (המכונה $f(w)$) הشرط מכיל רק את w .

10. נאמר כי שתי מכונות חישוב M, N הן שקולות אם לכל $w \in \Sigma^*$:

- M מקבלת את w אם “ $\exists s \in N$ מקבלת את w .
- N דוחה את w אם “ $\exists s \in M$ דוחה את w .
- M לא עצרת על w אם “ $\exists s \in N$ לא עצרת על w .

11. שני מודלים חישוביים \mathcal{U}, \mathcal{X} הם שקולים אם לכל מכונה מסווג \mathcal{U} יש מכונה שkööhה מסווג \mathcal{X} ולהפך.

12. מ “ $\delta : Q \times \Gamma^2 \rightarrow \Gamma^2$ ” עם שני סרטים היא מכונה רגילה, עם שני סרטים אינטואיטיביים מימיין, שני ראשים קוראים ופ' מעברים המוגדרת ע “ δ ” $.Q \times \Gamma^2 \times \{L, R\}^2$

13. ספרן (E) הוא מ “ δ ” שלא מקבלת קלט ומדפסה מילים (עם “אנטרים” ביןיהם), ושפה היא

$$L(E) = \{w : E \text{ בסופו של דבר מדפסה את } w\}$$

$$. REG_{TM} = \{\langle M \rangle : L(M \in \text{REG})\} .14$$

15. מכונת טירינג אוניברסלית היא מ “ δ ” שמקבלת כקלט מ “ δ ” M ומיליה w ומתחגה בדיקון כמו M על w , כלומר היא מסמלצת את M על w כאשר היא מקבלת/דוחה/לא עצרת בהתאם ומסמלצת את תוכן הסרט.

16. קידוד של מ “ δ ” הוא $.w_M \in \{0, 1, \#\}^*$

- נקודד את המ מצבים ב- Q באמצעות מס’ ביןaries בסדר עולה, מופרדים ע “ $\#$ ” (…#00#1#0#), לבסוף נסיף $\#\#\#$.
- נקודד את Γ (וכך גם את Σ). נעשה זאת באמצעות קידוד ביןاري, שהוא באורך $\lceil \log_2 |\Gamma| \rceil$, לבסוף $\#\#\#$.
- נקודד את פ’ המעברים δ ע “ $\#$ ” לכל מעבר $(q, \sigma) \# (q', \sigma') \# \langle L/R \rangle \#\#\#$ זה הקידוד של אובייקט כלשהו, כאשר $\langle L \rangle = 0, \langle R \rangle = R$.
- נקודד את המ מצבים המיוחדים ע “ $\#$ ” לבסוף נסיף $\#\#\#$.

17. מכונת טירינג א “ δ ” (NTM) היא מ “ δ ” עם $w \in L(N)$ ויתקיים $w \in L(N) \setminus \{q_{acc}, q_{rej}\} \times \Gamma \rightarrow 2^{Q \times \Gamma \times \{L, R\}} \setminus \{\emptyset\}$ אם “ \exists ריצה מקבלת של N על w .

בהתנן מיליה $w \in L^*$, רץ הרצה של מ “ δ ” א “ δ ” N על w הוא $T_{N,w} = \langle V, E \rangle$ המוגדר כך: תהי קבוצה כל הקונפ’ האפשריות בריצה כלשהי של N על w .

- כלומר כל קודקוד מגדיר קונפ' ומיקום ברייצה. $V \subseteq C \times (\mathbb{N} \cup \{0\})$.
 - שורש העז הוא $\langle q_0 w, 0 \rangle$.
 - $E \subseteq \bigcup_{i \geq 0} (C \times \{i\}) \times (C \times \{i+1\})$ כאשר $E(\langle c, i \rangle, \langle d, i+1 \rangle)$ אם $d \leq c$ והוא קונפ' עוקבת של c .
 - $f : \Sigma^* \rightarrow \Sigma^*$ היא פונקציה ניתנת לחישוב אם קיימת מ"ט M_f שבгинטע קלט x , עוצרת עם $f(x)$ על הסרט.
 - עבור שתי שפות $A, B \subseteq \Sigma^*$, נאמר כי $A \leq_m B$ אם קיימת פ' נתן לחישוב $\Sigma^* \rightarrow A$ כך $f(w) \in A \iff f(w) \in B$ מתקיים $w \in \Sigma^*$.
- ### משפטים
1. R סגורה למשלים.
 2. $RE \cap co\text{-}RE = R$. כלומר ניתן להכريع שפה אם וונת להוות אותה ואת המשלים שלה.
 3. מ"ט עם שני סורטיים היא מודל חישובי שקול למ"ט כללי.
 4. R סגורה לאיחוד.
 5. $L(E) = L$ ש-ספרן $\iff E \in RE, \forall L \subseteq \Sigma^*$.
 6. יש שפה L כך $L \notin R$.
 7. $REG_{TM} \notin R$.
 8. $L_1 \cdot L_2 \in RE$ אז $L_1, L_2 \in RE$ אם $L_1 \cdot L_2 \in RE$.
 9. לכל מ"ט א"ד N קיימת מ"ט דטרמיניסטיבית M ששקולה לה.
 10. (הרדוקציה) לכל $A \in R$ או $B \in R$ -ו $A \leq_m B$, $A, B \in RE$ אם (RE, R) מושפעת מ- A .
 11. אם $B \leq_m A$ אז B מ- A קלחה.
 12. (הרדוקציה, גרסה נוספת) $A \in co\text{-}RE$ או $B \in co\text{-}RE$ אם $A \in RE$ או $B \in RE$ -ו $A \leq_m B$.
 13. אם ניתן להכريع את L ב- $O(n \log n)$ (פחות מש- $O(n \log n)$) או L רגולרית.

סיבוכיות זמן

הגדרות

1. לכל $\mathbb{N} \rightarrow \mathbb{N}, t$, נגידר מחלוקת

$TIME(t(n)) = \{L : \text{זמן } O(t(|w|)) \text{ צעדים שמכריעת } L \text{ ועוצרת על כל קלט } w \text{ תוך}$

. $NP = NPTIME$, כלומר כל השפות שניתן להכריע בזמן פולינומיائي, ונסמן $PSPACE = \bigcup_{i \geq 0} TIME(n^i)$

2. נגידר את המחלוקת $t : \mathbb{N} \rightarrow \mathbb{N}$

$NTIME(t(n)) = \{L : \text{זמן } O(t(|w|)) \text{ צעדים שמכריעת } L \text{ ועוצרת על כל קלט } w \text{ תוך}$

4. נגידר את המחלוקת $NPTIME = \bigcup_{i \geq 0} NTIME(n^i)$, כלומר כל השפות שניתן להכריע בזמן פולינומיائي באמצעות נירוחשים, ונסמן $NP = NPTIME$.

5. $EXPTIME = \bigcup_{i \geq 0} TIME(2^{n^i})$ כלומר כל שפה שניתנת בסיבוכיות אקס' להכריע אותה עם מ"ט דטר.

6. מודוא V עבור שפה L הוא מ"ט דטר. כך ש- V קיים c כך ש- V מקבלת את $L = \{w : (w, c) \in V\}$

7. שפה L היא NP-שלמה אם $L \in NP$ ואם $L \in NP$ או $P = NP$, כלומר שפה L ניתנת להכריעים בזמן פוליאי עם מ"ט א"ד, ואם נמצא אלג'ריה בזמן פוליאי דטר' להכרעת L נפתר בעיה פתוחה במדמ"ח $P \stackrel{?}{=} NP$.

8. משתנה בוליאני הוא משתנה שמקבל ערכים מ- $\{T, F\}$.

נוסחה בוליאנית היא משתנה בוליאני, או $\varphi_1 \wedge \varphi_2$ כאשר φ_1, φ_2 נוסחאות בוליאניות.

בהתנאי השמה $f : X \rightarrow \{T, F\}$ למשתני הנוסחה, ניתן לחשב את ערך האמת של הנוסחה (באינדוקציה).

נוסחה θ היא b-CNF אם θ ממחזורה $\ell_i^j \in \{x_1, \dots, x_n, \bar{x}_1, \dots, \bar{x}_n\}$ כאשר $\left(\ell_1^1 \vee \dots \vee \ell_1^{k_1}\right) \wedge \dots \wedge \left(\ell_m^1 \vee \dots \vee \ell_m^{k_m}\right)$

9. תכונה סמנטית של מ"ט היא קבוצה P של מ"ט, כך שלכל זוג מ"ט M_1, M_2 ואם $M_1 \in P \iff M_2 \in P$

10. תהי V מ"ט דטר. נאמר כי V מודוא לשפה L אם

$$L = \{w : (\exists c : \langle w, c \rangle \in L(V))\}$$

ונאמר ש- V מודוא פוליאי אם

$$L = \{w : (\exists c : |c| \leq \text{בגודל פולינומי}-\text{ו-} \langle w, c \rangle \in L(V))\}$$

ו- V רצה בזמן פוליאי- w על $\langle w, c \rangle$

11. $f(x) = \Sigma^* \rightarrow \Sigma^*$ היא פ' ניתנת לחישוב בזמן פוליא אם קיימת מ"ט M_f של קלט x , עוצרת תוך מספר פוליא ב- x של צעדים עם על הסרט.

12. יהיו $A, B \subseteq \Sigma^*$. נאמר כי A ניתנת לרדוקציה פוליא ל- B אם קיימת $f : \Sigma^* \rightarrow \Sigma^*$ ונסמן $A \leq_p B$ אם f ניתנת לחישוב בזמן פוליא כך $w \in A \iff f(w) \in B, w \in \Sigma^*$.

13. נאמר ששפה $L \subseteq \Sigma^*$ היא NP-שלמה אם:

• (חסם עליון) $L \in \text{NP}$.

• (חסם תחתון) L היא NP-קשה, כלומר שלכל שפה $L' \leq_p L, L' \in \text{NP}$.

14. יהיו $G = \langle V, E \rangle$ גרף. נאמר כי $C \subseteq V$ כיסוי קודקודי ב- G אם לכל צלע $e = \{u, v\} \in E$, לפחות אחד הקודקודים של e נמצא ב- C .

15. $\text{VC} = \{\langle G, k \rangle : G$ גראף לא מכובן ויש ב- G כיסוי קודקודי מוגדל לכל היותר k

16. יהיו $G = \langle V, E \rangle$ גרף. נאמר כי $D \subseteq V$ היא Dominating Set אם לכל $v \in V$ או ש- v חלק מצלע שהקצה השני שלה ב- D , כלומר D קבוצה של קודקודים כך שכל קודקודה במרחב לכל היותר 1 מקודקודה כלשהו ב- D .

17. בעיית subset sum מתקבלת כקלט קבוצה (יתכן עם חזרות) של טבעיים $A = \{a_1, \dots, a_n\} \subseteq \mathbb{N}$ ומספר יעד s , וצריכה לענות כפלט

$$\text{האם ישsubset sum such that } \sum_{a_i \in B} a_i = s.$$

$$\text{SS} = \left\{ \langle A, s \rangle \in 2^{\mathbb{N}} \times \mathbb{N} : \left(\exists B \subseteq A : \sum_{a_i \in B} a_i = s \right) \right\}$$

18. שפת הנוסחאות שלא ניתנות לסיפוק היא

$$\overline{\text{SAT}} = \text{CONTRADICTION} = \{\langle \varphi \rangle : \text{CNF} \text{ לא ספיקה}\}$$

ושפת הטאוטולוגיות היא $\{\langle \varphi \rangle : \text{CNF} \text{ טאוטולוגיה בצורת Tautology}\}$

19. השפות המרכזיות לגרפים המילטוניים הן

$\text{D-ST-HAMPATH} = \{\langle G, s, t \rangle : G$ גראף מכובן ויש מסלול המילטון מ- s ל- $t\}$

$\text{D-HAMPATH} = \{\langle G \rangle : G$ מכובן ויש ב- G מסלול מכובן המילטוני

$\text{D-HAMCYCLE} = \{\langle G \rangle : G$ מכובן ויש ב- G מעגל מכובן המילטוני

$\text{SAT} \in \text{NP}$.1

. $L_P \notin \text{R}$ עבור P תכונה סמנטית לא טריויאלית, אזי $L_P = \{\langle M \rangle : M \in P\}$.2. (ריביס) נגיד $L_P \notin \text{R}$

. $(L_P \notin \text{co-RE})$ תכונה סמנטית לא טריויאלית של מ"ט כך ש- $T_\emptyset \notin P$ (כלומר $A_{TM} \leq L_P$ (המכונה עם השפה הריקה), אזי $A_{TM} \leq P$)

.4. (שקלות הגדרת $L \in \text{NP}$ (NP אם ו- $L \in \text{NP}$)) קיימים לה מודוא פולי.

.5. (הרדווקציה עבור P אם $A \in P$ או $B \in P$ -ו $A \leq_p B$ אם P)

.6. אם $A \notin P$ אז $B \notin P$ (קונטרה-פוזיטיב על משפט הרדווקציה).

.7. אם $L \in \text{P-קשה}$ אז $L \in \text{NP-קשה}$.

.8. תהי L'' שפה $L'' \leq_p L$ ואם $L \subseteq \Sigma^*$ - NP-קשה (מטרזיטיביות של רדווקציות).

.9. אם $B \neq \emptyset$, Σ^* לכל $A \leq_p B$ אם $A \in P$ או

.10. $\text{3SAT} \leq_p \text{CLIQUE}$

.11. $L \leq_p \text{3SAT}$ הינו NP-קשה , כלומר $L \leq_p \text{3SAT}$ לכל $L \in \text{NP-קשה}$.

.12. הינו NP-שלמה .

.13. הינו NPC DS .

.14. הינו NP-שלמה .

.15. הינו NP-שלמה אם $\bar{L} \in \text{coNP}$ הינו NP-שלמה .

.16. coNPH הינו TAUTOLOGY .

.17. הינו $\text{NPC D - ST - HAMPATH}$.

.18. הינו $\text{NPC U - ST - HAMPATH}$.

סיבוכיות מקום

הגדרות

.1. תהי M מ"ט דטר', חד סרטית שעוצרת על כל קלט. סיבוכיות הזיכרון של M היא $f : \mathbb{N} \rightarrow \mathbb{N}$ כך שעל קלט באורך n , M משתמש בכל היותר ב-(n) תאים, ונאמר ש- M -רזה בשטח (n)

2. עברו $\mathcal{P}^{\mathcal{S}}$, נגדיר

$$\text{SPACE}(s(n)) = \{L : L \in \mathcal{O}(s(n)) \text{ שמכריע את } \mathcal{O}(s(n))\}$$

ואז NSPACE המקבילה הא"ד להגדירה הנ"ל.

$$\text{NPSPACE} = \bigcup_k \text{NSPACE}(n^k) \text{ ו-} \text{PSPACE} = \bigcup_k \text{SPACE}(n^k)$$

4. נאמר כי $L \leq_p L, K \in \text{coNP}$ קשה אם לכל $L \in \text{coNP}$ -שלמה אם הוא $\bar{L} \in \text{NP}$ או $L \in \text{coNP}$ -קשה וגם $\bar{L} \in \text{NP}$.

5. המחלקות המתאימות לביעית הריקנות והאוניברסליות הן

$$\text{EMPTY}_{\text{NFA}} = \{\langle A \rangle : L(A) = \emptyset \text{ NFA } A\}$$

$$\text{ALL}_{\text{NFA}} = \{\langle A \rangle : L(A) = \Sigma^* \text{ NFA } A\}$$

6. נאמר כי שפה שלמה ב- PSPACE אם $L \in \text{PSPACE}$ •

$L' \leq_p L, L' \in \text{PSPACE}$ (רזרקציה בזמן פוליאורדרם) •

7. נוסחה ב- QBF היא נוסחה (לא בהכרח CNF) שכל המשתנים שלה מכומתיים (יש להם או \exists או \forall , בסדר מסוים) ונגידר את השפה

$$\text{TQBF} = \text{QSAT} = \{\langle \varphi \rangle : \text{True } \varphi \in \text{QBF}\}$$

8. סיבוכיות הזיכרון של M היא $s(n)$ אם סרט העבודה של M מכיל (n) תאים בעיבוד של קלט באורך n .

משפטים

1. עברו $\text{TIME}(2^{\mathcal{O}(f(n))}) \subseteq \text{SPACE}(f(n))$

2. $\text{P} \subseteq \text{PSPACE}$

3. $\text{P} \subseteq \text{NP} \subseteq \text{PSPACE}$

4. $\overline{\text{ALL}_{\text{NFA}}} \in \text{NPSPACE}$ (אוטומטים הא"ד עם שפה לא אוניברסלית).

5. $\overline{\text{ALL}_{\text{NFA}}} \in \text{PSPACE}$ קשה.

. $\text{NSPACE}(s(n)) \subseteq \text{SPACE}(s^2(n))$, $s(n) \geq \log n$.6. (סביר'ן) לכל n

. $\text{NPSPACE} = \text{PSPACE}$.7

. TQBF היא PSPACE -שלמה .8

סיבוכיות שטח לוגריתמית

הגדרות

. $\text{NL} = \text{NSPACE}(\log n)$ ו $\text{L} = \text{SPACE}(\log n)$.1

.2. נאמר כי A היא שלמה ב- NL אם :

. $A \in \text{NL}$ •

• לכל שפה $B \leq_{\text{logspace}} A, B \in \text{NL}$ -קשה).

.3. log-space transducer (משרף) הוא מ"ט שמחשבת פ' בשטח לוג' (של סרט העבודה) וכותבת את התוצאה על סרט שלישי לכתיבת- בלבד. נאמר כי $f : \Sigma^* \rightarrow \Sigma^*$ שנייתנית לחישוב בשטח לוג' אם קיים משרף M שעל קלט w (בסרט הקלט) יוצר עט (w) על

סרט הפלט ומשתמש ב- $\mathcal{O}(|w| \log |w|)$ תאים בסרט העבודה.

.4. נאמר כי A אם יש פ' f ניתנת לחישוב בשטח לוג', כך שלכל $w \in \Sigma^*$ $f(w) \in A$, $w \in B \iff f(w) \in B$. $B \leq_{\text{logspace}}$

.5. נאמר שפ' $t = \Omega(n \log n)$ (t שעבורה ניתנת לבנייה בזמן t אם הפ' שמניפה את n^t לייצוג הבינארי של (n)) t ניתנת לחישוב בזמן $\mathcal{O}(t(n))$.

.6. G גראף מכובן קשור חזק : $\text{SCC} = \{\langle G \rangle$ כאשר גראף קשור חזק הוא גראף שבו לכל $V \in u, v$, יש מסלול מ- u ל- v וגם מ- v ל- u ב- G .

.7. $\{\langle G \rangle$ בדיקות רכיבי קשרות חזקה : $.2\text{SCC} = \{\langle G \rangle$

משפטים

. $\text{NL} = \text{NSPACE}(\log n) \subseteq \text{SPACE}(\log^2 n) \neq \text{L}$.1

. $B \in \text{L}$ או $B \leq_{\text{logspace}} A$ אם $A \in \text{L}$ (הרצוקציה ל-L) .2

. PATH היא NL -קשה .3

. $\text{NL} \subseteq \text{P}$.4

. $\text{NL} = \text{coNL}$ (אימרמן) .5

.6. (ההיררכיה בזמן) תהי $\mathbb{N} \rightarrow \mathbb{N}$: t : ניתנת לבניה בזמן. אזי קיימת שפה L שמכריעה בזמן $O(t(n))$ אבל לא כריעה בזמן $O\left(\frac{t(n)}{\log t(n)}\right)$.

.7. לכל $1 < \epsilon_1, \epsilon_2$, מתקיים $\text{TIME}(n^{\epsilon_1}) \subsetneq \text{TIME}(n^{\epsilon_2})$ מאשר ב- $(O(n^{\epsilon_1}) \text{ אפשר לפטור יותר ממש בעיות בזמן } O(n^{\epsilon_2}))$.

.8. $P \subsetneq \text{EXPTIME}$.

.9. קיימת מ"ט S כך שבהינתן w מחשבת את הקונפ' בריצת M על w במשך t צעדים תוך זמן $t \log t \cdot p(|\langle M \rangle|)$ פולינום כלשהו.

.10. היא NL-שלמה SCC .