הרצאה 7 – יום רביעי 13.8

רדוקציות פולינומיות

פונקציה $f:\Sigma^* \to \Sigma^*$ תיקרא פולינומית אם קיים *DTM* כך שבהינתן *x*, הוא תמיד עוצר בזמן פולינומי עם $f(x)$ על הסרט.

נאמר ששפה L_1 ניתנת לרדוקציה לשפה L_2 אם קיימת פונקציה פולינומית *f* כך שלכל *x* מתקיים $x \in L_1 \Leftrightarrow f(x) \in L_2$. נסמן $L_1 \leq_p L_2$.

L_1 "קשה לכל היותר כמו" L_2. תכונות של רדוקציות: אם $L_1 \leq_p L_2$, אז:

$$L_2 \in P \Longrightarrow L_1 \in P, \qquad L_2 \in NP \Longrightarrow L_1 \in NP, \qquad L_2 \in coNP \Longrightarrow L_1 \in coNP$$

$$L_1 \notin P \Longrightarrow L_2 \notin P, \qquad L_1 \notin NP \Longrightarrow L_2 \notin NP, \qquad L_1 \notin coNP \Longrightarrow L_2 \notin coNP$$

נוכיח: יהיו שפות כך ש- $L_1 \leq_p L_2$, ונניח $L_2 \in P$. כלומר קיים *DTM* פולינומי *M* עבור L_2, ופונקציה פולינומית *f* שעונה על התנאים לעיל. נוכל לבנות *DTM* פולינומי *N* עבור L_1: בהינתן קלט *x*, נחשב את $M\big(f(x)\big)$ ונחזיר את אותה התשובה. לפי ההגדרות של *M*, *f*, מתקיים:

$$x \in L_1 \Leftrightarrow f(x) \in L_2 \Leftrightarrow M\big(f(x)\big) = 1, \qquad x \notin L_1 \Leftrightarrow f(x) \notin L_2 \Leftrightarrow M\big(f(x)\big) = 0$$

וכל השלבים רצים בזמן פולינומי.

$3\text{-}SAT \leq_p CLIQUE$

(בעיית *3-SAT* נקראה *3-CNF-SAT* באלגו 2. הרדוקציה מופיעה בתרגול 2). בהינתן פסוק בוליאני φ בצורת *CNF* עם 3 ליטרלים בכל פסוקית:

$$\varphi = (x_1 \vee y_1 \vee z_1) \wedge (x_2 \vee y_2 \vee z_2) \wedge \ldots \wedge (x_k \vee y_k \vee z_k)$$

נחזיר $\langle G, k\rangle$, כאשר *G* נבנה כך:

לכל פסוקית, נייצר שלושה קודקודים (אחד לכל ליטרל). נחבר בין כל שני קודקודים שהם לא מאותה פסוקית ולא משלימים $(x, \bar{x})$. כלומר, יש צלע בין כל שני ליטרלים שיכולים לקבל השמה *T*. אז קליקה בגודל *k*, זה *k* ליטרלים מפסוקיות שונות שכולם יקבלו *T*, וזו השמה מספקת.

שלמות *NP*

שפה *L* תיקרא *NP*-קשה (*NP-hard, NPH*) אם לכל $L' \in NP$ מתקיים $L' \leq_p L$. נאמר ש-*L* "קשה לפחות כמו" כל שפה ב-*NP*. אם שפה היא *NP*-קשה וגם בעצמה ב-*NP*, נאמר שהיא *NP*-שלמה (*NP-complete, NPC*). אם יש שפה *L* שהיא *NPC* שנצליח להוכיח שהיא ב-*P*, אז $P = NP$. כי אז נוכל לעשות רדוקציה מכל שפה ב-*NP* ל-*L* (כי היא *NPH*) ולפתור אותה בזמן פולינומי.

כדי להוכיח ששפה *L* היא *NPH*, מספיק לעשות רדוקציה משפה *NPH* אחרת (ולא צריך להוכיח שאפשר לעשות מכל השפות ב-*NP*). כי רדוקציות הן טרנזיטיביות, וההרכבה של פונקציות פולינומיות היא עדיין פולינומית. ואם *L* גם ב-*NP*, אז היא *NPC*.

בעיית *SAT*

בהינתן נוסחה בוליאנית φ, האם היא ספיקה? הבעיה ב-*NP*, כי יש אלגוריתם וידוא: העד הוא ההשמה, ואפשר לבדוק שההשמה תקינה והנוסחה מסופקת בזמן פולינומי.

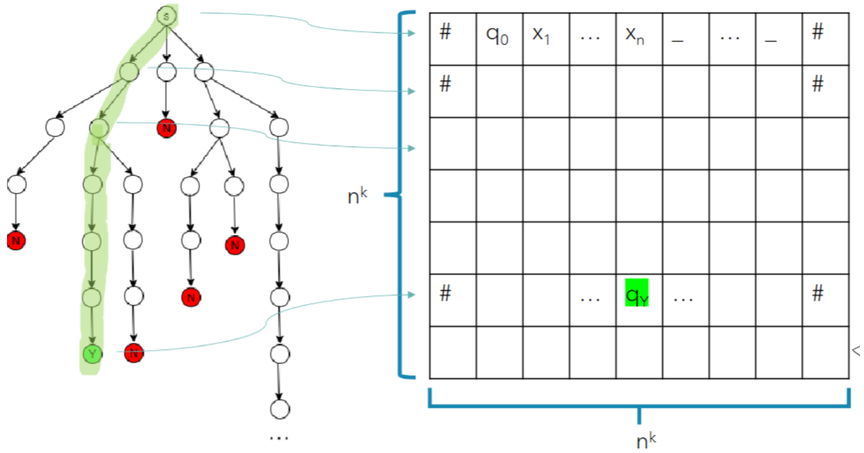
משפט קוק – לוין (*Cook – Levin*)

השפה *NPH* הראשונה. נרצה להוכיח שכל שפה *L* ב-*NP*, ניתנת לרדוקציה בזמן פולינומי ל-*SAT*. בהינתן *N*, *NTM* עבור *L* שמכריע אותה בזמן n^k, וקלט *x*, נתאר נוסחה בוליאנית שה"משמעות" שלה היא "יש סדרה של עד n^k צעדי חישוב של $N(x)$ שמסתיימת במצב מקבל". ואז: $x \in L \Leftrightarrow \varphi \in SAT$.

רעיון ההוכחה: נתאר את החישוב של *N* בטבלה *T*. שורות – הקונפיגורציות של *N* בכל שלב (יש n^k שורות). עמודות – התאים של הסרט של *N*. נכתוב את המצב הנוכחי בתא שהראש נמצא בו. המקום הראשון והאחרון בכל שורה מכיל #. הגבלות:

1. כל תא מכיל בדיוק תו או מצב יחיד.
2. השורה הראשונה מקודדת את הקונפיגורציה ההתחלתית.
3. יש תא כלשהו שמכיל מצב מקבל.
4. כל שורה מניבה את השורה הבאה ע"י צעד חוקי של המכונה.

נחבר את ההגבלות האלה לנוסחת *CNF* Φ. הגודל שלה פולינומי ב- n^k, כלומר פולינומי בגודל הקלט.



פורמלית: לכל תא (i,j), ולכל מצב או תו אפשרי $c \in C \coloneqq Q \cup \Gamma \cup \{\#\}$, נסמן:

$$y_{i,j,c} = 1 \Leftrightarrow T[i,j] = c$$

כלומר, ייצרנו משתנים בוליאניים שמתארים את התוכן של כל תא. נתאר נוסחה שתופסת את הגבלה 1:

$$\varphi_{cell} \coloneqq \bigwedge_{i,j} \left(\underbrace{\bigvee_{c \in C} y_{i,j,c}}_{\substack{no\ empty\\ cell}} \wedge \underbrace{\bigwedge_{s \neq t} (\neg y_{i,j,s} \vee \neg y_{i,j,t})}_{\substack{exactly\ one\ symbol\ in\\ each\ cell}} \right)$$

נדרוש גם את הגבלה 2:

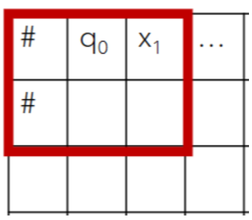
$$\varphi_{start} \coloneqq y_{1,1\#} \wedge y_{1,2,q_0} \wedge y_{1,3,x_1} \wedge y_{1,4,x_2} \wedge \ldots \wedge y_{1,n+1,x_n} \wedge y_{1,n+2,\_} \wedge \ldots \wedge y_{1,n^k,\#}$$

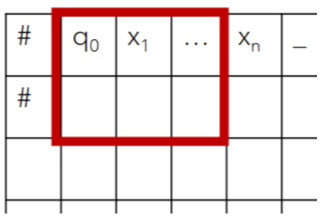
הגבלה 3:

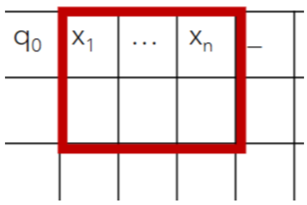
$$\varphi_{accept} \coloneqq \bigvee_{i,j} y_{i,j,q_Y}$$

הגבלה 4:

נשים לב שכדי לבדוק שכל שורה מניבה באופן חוקי את השורה הבאה, מספיק לבדוק כל חלון (תת-טבלה) בגודל 3×2:







כי התאים היחידים שמשתנים זה התא שהראש נמצא בו (כתיבה), ואולי אחד התאים מימין או משמאל (תזוזה).

אז נעבור על כל החלונות האפשריים, ולכל פקודה של המ"ט, נוסיף פסוקית שמייצגת את זה החלון הזה חוקי:

$$\varphi_{legal} \coloneqq \bigwedge_{i,j} \varphi_{i,j,legal}$$

ונגדיר:

$$\varphi_{i,j,legal} \coloneqq \begin{cases} 1, & if\ T[i-1{:}\,i+1, j{:}\,j-1, j+1]\ is\ legal \\ 0, & else \end{cases} = \bigvee_{U \in legal\ configurations} window\ i,j\ holds\ U$$

דוגמאות לחלונות חוקיים:

a	q_1	b
a	c	q_2

q_1	b	a
c	q_2	a

b	a	d
q_2	a	d

d	a	q_1
d	a	c

#	q_1	b
#	a	q_2

#	a	q_1
#	a	c

עבור הדוגמה השמאלית, הקידוד הוא:

$$x_{i-1,j,a} \wedge x_{i,j,q_1} \wedge x_{i+1,j,b} \wedge x_{i-1,j+1,a} \wedge x_{i,j+1,c} \wedge x_{i+1,j+1,q_2}$$

ונחבר הכל ביחד:

$$\Phi \coloneqq \varphi_{cell} \wedge \varphi_{start} \wedge \varphi_{legal} \wedge \varphi_{accept}$$

אם $x \in L$, אז יש טבלה שעונה על כל ההגבלות $\Leftarrow$ Φ ספיקה. אם $x \notin L$, אז אין טבלה שעובדת $\Leftarrow$ Φ לא ספיקה.

הגודל של Φ פולינומי בגודל הקלט: $O\left(n^{2k} \log n\right)$.

- החלק של התאים, φ_{cell}: $O\left(n^k \times n^k\right) = O\left(n^{2k}\right)$, לכל תא.
- הדרישה של ההתחלה, φ_{start}: $O\left(n^k\right)$, עבור התאים של השורה הראשונה.
- הדרישה של החלונות, φ_{legal}: $O\left(n^k \times n^k\right) = O\left(n^{2k}\right)$, לכל חלון.
- הדרישה של מצב מקבל, φ_{accept}: $O\left(n^k \times n^k\right) = O\left(n^{2k}\right)$, לכל תא.
- כפול $\log n$ בשביל הייצוג של כל y.

בסה"כ, הראינו שאפשר לעשות רדוקציה מכל שפה ב-*NP* ל-*SAT*. אז *SAT* היא *NPH*. ובגלל ש-*SAT* ב-*NP*, אז היא *NPC*.

$SAT \leq_p 3\text{-}SAT$

(ההוכחה המפורטת הייתה באלגו 2). בהינתן נוסחה בוליאנית, נייצר מכל פסוקית **גאדג'ט** מקביל. אם יש פחות משלושה ליטרלים, נוסיף ליטרלים חדשים שרירותיים. הגודל קבוע. אם יש יותר משלושה ליטרלים, נצטרך לפצל את הפסוקית. כל ליטרל יקבל פסוקית משלו, ונקשר בין הפסוקיות האלה ע"י ליטרלים חדשים:

$$\ell_1 \vee \ell_2 \vee \cdots \vee \ell_m \to (\ell_1 \vee \ell_2 \vee y_1) \wedge (\overline{y_1} \vee \ell_3 \vee y_2) \wedge (\overline{y_2} \vee \ell_4 \vee y_3) \wedge \cdots \wedge (\overline{y_{m-3}} \vee \ell_{m-1} \vee \ell_m)$$

הגודל של הגאדג'ט הוא פולינומי בגודל הפסוקית.

הנוסחה החדשה ספיקה אמ"מ הנוסחה המקורית ספיקה, אז *3-SAT* היא *NPH*. ומכיוון שהיא ב-*NP*, היא גם *NPC*.