10.5.17 בס״ד

סיבוכיות - תרגול

P/poly:

P/poly - מחלקה זו מכילה את אוסף השפות המוכרעות ע״י מעגלים לוגיים בגודל פולינומי.

* מה ההבדל בין אלגוריתם רגיל למעגל לוגי?

←

קלט לאלגוריתם יכול להיות מכל אורך שהוא ולכן האלגוריתם הוא אחיד לכל אורך קלט. לעומת זאת, מעגל לוגי נבנה והוא ״יחודי״ לאורך קלט מסויים (בהתאם למספר קודקודי הקלט במעגל) ולכן, מדובר בהקשר זה על חישוב לא ״יוניפורמי״.

* הגדרה 1: $L\in P/poly$ אם קיימת סדרה אינסופית של מעגלים $\{C_n\}_{n=1}^{\infty}$ כך שלכל מעגל C_n יש n קודקודי קלט וקיים פולינום $p(.)$ כך ש- $|C_n|\le p(|x|)$ כאשר $|C_n|$ = מס׳ הקשתות במעגל. ולכל $x\in\{0,1\}^n$, מתקיים:

$$C_n(x)=\begin{cases}1, & x\in L\\ 0, & x\notin L\end{cases}$$

* הגדרה 2: $L\in P/poly$ אם קיימת מ״ט הרצה בזמן פולינומי M בעלת שני סרטי קלט וקיימת סדרה אינסופית של ״עצות״ (מחרוזות) $\{a_n\}_{n=1}^{\infty}$, כאשר $|a_n|\le p(|x|)$ לכל n עבור פולינום $p(.)$ כלשהו ולכל $x\in\{0,1\}^n$ מתקיים:

$$M(a_n,x)=\begin{cases}1, & x\in L\\ 0, & x\notin L\end{cases}$$

- משפט 1: $P\subseteq P/poly$
- משפט 2: אם $P\neq NP \Leftarrow NP\not\subseteq P/poly$
- משפט 3: המחלקה $P/poly$ מכילה שפות לא כריעות (ולכן $P/poly\not\subseteq NP$)
- משפט 4: אם $NP\subseteq P/poly$ אזי $PH=\Sigma_2$

תרגיל: נגדיר מחלקה חדשה $P/2^n$ באופן דומה להגדרת $P/poly$, כך שמחרוזת ה״עצה״ באורך אקספוננציאלי ביחס לגודל הקלט. הוכיחו שכל שפה L נמצאת במחלקה זו.

פתרון - הוכחה -

תהי שפה L כלשהי, לכל n נגדיר את a_n להיות המחרוזת שבאינדקס ה-i שבה מופיע 1 אם המחרוזת הבינארית באורך n שמייצגת את המס׳ ה-i שייכת ל-L ו-0 אחרת, קל לראות שלכל n $|a_n|=2^n$ (כמות המחרוזות באורך n היא 2^n)

המכונה M, מקבלת קלט x באורך n ומחרוזת ״עצה״ a_n ותחזיר את ערכו של הביט שנמצא באינדקס המציין את הערך המספרי של x, קל להוכיח שמכונה זו מכריעה את L.

תרגיל: נגדיר מחלקה ~~...~~ P/log בדומה ל- $P/poly$, פרט לעובדה שאורך מחרוזת הייעוץ הוא לוגריתמי באורך הקלט. הוכיחו $NP \subseteq P/log \Rightarrow P=NP$.

פתרון - <u>הוכחה</u> -

מספיק להוכיח $NP \subseteq P/log \Rightarrow 3\text{-}SAT \in P$.

נניח כי $NP \subseteq P/log$ ⟸ קיימת מ"ט פול' דט' M וסדרה אינסופית של מחרוזות ייעוץ $\{a_n\}_{n=1}^{\infty}$ באורך לוגריתמי המכריעות את 3-SAT. נניח שלכל n מתקיים $|a_n| \le c\log(n)$, נבנה אלגוריתם פול' דט' שמכריע את 3-SAT באופן הבא:

בהינתן נוסחה ϕ ~~...~~ באורך n:

(*) אם ϕ לא בפורמט 3-CNF החזר 0.

(*) לכל מחרוזת ייעוץ אפשרית $a_n \in \{0,1\}^{c\log(n)}$:

← אם $M(a_n,\phi)=1$, אזי לכל משתנה x ב- ϕ:

← נציב 0 בערך של המשתנה x ונדאג שאורך הנוסחה לא ישתנה (אם המבטל נוטרל בפסוקית אחת נכפיל אחד אחר וכן אם המבטלה פסוקית נכפיל אחרת).

← נריץ את M על הקלט לאחר ההצבה ושמירת האורך יחד עם מחרוזת הייעוץ a_n

אם M החזירה 1 נמשיך. (עם ההצבה של 0 ב- x) אחרת נציב ב- x 1 ונשמור כמו קודם. (על אורך הנוסחה)

← נציב ~~...~~ את השמת האמת בנוסחה, אם הנוסחה מסופקת, החזר 1, אחרת ← 0.

הוכחת נכונות: אם $\phi \in 3SAT$ ⟸ קיימת מחרוזת ייעוץ a_n עבורה $M(a_n,\phi)=1$

מכיוון שדאגנו לא לשנות את אורך הקלט: - אם a_n היא מחרוזת ייעוץ נכונה

⟸ ברדוקציה העצמית נמצא השמת אמת נכונה ~~...~~ שבאמת מספקת את הנוסחה ונחזיר 1

~~...~~

אם $\phi \notin 3SAT$ ⟸ 1. הנוסחה לא בצורת CNF ואז נחזיר 0 בתחילת האלגו'

או..

2. לא קיימת השמת אמת שמספקת את הנוסחה, מכיוון שאנו בודקים לכל השמת אמת האם היא מספקת את הנוסחה, לפני שאנו מחזירים 1 בהכרח נחזיר 0.

סיבוכיות האלגוריתם: אורך מחרוזת הייעוץ חסום לוגריתמית בגודל הקלט ⟸ מס' המחרוזות של ייעוץ האפשריות הוא: $2^{c\log n}=n^c$, כלומר פולינומי.

בנוסף, M רצה בזמן פולינומי ולולאת הרדוקציה העצמית מתבצעת בזמן פולינומי.

⟸ ריצת האלגוריתם פולינומית באורך נוסחת הקלט.