סיכומים תרגול מס' 7
04.05

$P/Poly$ - הגדרה

מחלקה שמכילה את השפות שניתנות להכרעה ע"י מעגלים לוגיים בגודל פולינומי.

מה ההבדל בין מעגל לוגי לאלגו' רגיל?

קלט לאלגוריתם יכול להיות בכל אורך שהוא ולכן האלגוריתם הוא **אחד** עבור כל האורכי הקלט האפשריים.

לעומת זאת, מעגל לוגי - הוא קבוע לאורך הקלט ספציפי, ולכן נדרש לבנות מעגל **שונה** לכל אורך קלט. ⇐ לכן חישוב זה נקרא חישוב **לא יוניפורמי**.

הגדרה 1: $L \in P/Poly$ אם קיימת סדרה אינסופית של מעגלים לוגיים $\{C_n\}_{n\in\mathbb{N}}$, כך שלכל n ל-C_n יש n קודקודי קלט וקיים פולינום $P(\cdot)$ כך ש: $|C_n| \le P(n)$
(גודל של מעגל לוגי הוא 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 קיימים מ"ט שרצה בזמן פולינומי M בעלת שני סרטי קלט, פולינום $P(\cdot)$ וסדרה אינסופית של מחרוזות "עצה" $\{a_n\}_{n\in\mathbb{N}}$ כך שלכל n $|a_n| \le P(n)$ ולכל $x \in \{0,1\}^n$ מתקיים:

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

משפט 1: $P \subseteq P/Poly$ מחרוזות העצה ריקות.

משפט 2: $P \neq NP \Leftarrow NP \not\subseteq P/Poly$ · נובע ממשפט 1.

משפט 3: המחלקה $P/Poly$ מכילה שפה לא כריעה.
$P/Poly \not\subseteq NP$

משפט 4: $PH = \Sigma_2 \Leftarrow NP \subseteq P/Poly$

· נשים לב שלא מובטח לנו שהעצה היא טובה. כלומר העצה יכול לרמות אותנו, שיש לנו "עצות רעות".
וזהו ההבדל בין NP ל $P/Poly$

NP: אם $x \notin L$ אזי לא קיים עד "עד" שירמה את המוודא.

$P/Poly$: אם $x \notin L$ יכולה להיות עצה שתרמה אותנו.

תרגיל: נגדיר מחלקה חדשה $P/2^n$ באופן דומה להגדרת $P/Poly$ כך שבמחלקה זו אורך מחרוזות העצה הוא 2^n עבור קלט באורך n.
הוכיחו שכל שפה L שייכת ל $P/2^n$.

פתרון: תהי L שפה כלשהי. לכל n נגדיר a_n להיות המחרוזת שבאינדקס ה-i שלה מופיע 1 אם המחרוזת הבינארית באורך n שמייצגת את המס' ה-i שייכת ל-L ו-0 אחרת.
· קל לראות שלכל n, $|a_n| = 2^n$.
· נגדיר מכונה M שבהינתן קלט X באורך n ועצה a_n, המכונה תחשב את הערך המספרי של המחרוזת הבינארית X, ואז תחזיר את הערך של הביט ה-i במחרוזת a_n.
· קל לראות שהמכונה M מכריעה נכונה את השפה L.

תרגיל: נגדיר מחלקה חדשה $P/\log$ באופן דומה ל $P/Poly$ פרט לעובדה שאורך מחרוזת העצה חסום לוגריתמית באורך הקלט.
הוכיחו: אם $P = NP \Leftarrow NP \subseteq P/\log$.

3בב

הוכחה: נניח כי $NP \subseteq P/\log \Leftarrow 3SAT \in P$

נניח כי $NP \subseteq P/\log$ ⇐ קיימת מ"ט M וסדרת מחרוזות "יעוץ" באורך לוגריתמי $\{a_n\}_{n\in\mathbb{N}}$ לכל אורך קלט n המכריעה את 3SAT.
נניח לכל n, $|a_n| = c\log n$

בהינתן קלט ϕ עבור 3SAT באורך n נראה אלג' פולינומי דט' המכריע את 3SAT:

- אם ϕ לא בצורת 3CNF - החזר 0.
- לכל מחרוזת "יעוץ" אפשרית $a_n' \in \{0,1\}^{c\log n}$:
  - אם $M(a_n', \phi) = 1$ ← העצה אומרת שיש הצבה מספקת לϕ
  - לכל משתנה x ב-ϕ:
    - נציב ערך 0 במשתנה x, ונדאג שאורך הנוסחה לא ישתנה (במקום כל פסוקית שהתבטלה נכפיל את אחת הפסוקיות ובמקום כל ליטרל שהתבטל בפסוקית כלשהי נכפיל ליטרל אחר בה). ← בדיקה ע"י רדוקציה עצמית של SAT האם היעוץ הוא נכון ושקר.
    - נריץ את המכונה M על הקלט שקיבלנו לאחר ההצבה עם מחרוזת היעוץ הנוכחית a_n'.
      אם M החזירה 1, נמשיך עם הצבה זו,
      אחרת נציב 1 במקום 0 במשתנה (שוב נדאג שאורך הנוסחה לא ישתנה).
  - נציב את השמת האמת שקיבלנו בנוסחה.
    אם הנוסחה מסופקת - החזר 1.
    אחרת - החזר 0.

הוכחת נכונות: אם $\phi \in 3SAT$ ⇐ קיימת מחרוזת "יעוץ" a_n עבורה $M(a_n, \phi) = 1$.
מכיוון שדאגנו לא לשנות את אורך הקלט:
- אם a_n היא מחרוזת היעוץ הנכונה ⇐ ברדוקציה העצמית נמצא השמת אמת נכונה שאכן מספקת את הנוסחה ונחזיר 1.

אם $\phi \notin 3SAT$ ⇐ 1. הנוסחה לא בצורת 3CNF ואז נחזיר 0 בתחילת האלגוריתם

או

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

סיבוכיות האלגוריתם: אורך מחרוזת היעוץ חסום לוגריתמית בגודל הקלט ⇐ מס' המחרוזות של "יעוץ" האפשריות היא: $2^{c\log n} = n^c$, כלומר פולינומי.
בנוסף, M רצה בזמן פולינומי וגם הרדוקציה העצמית מתבצעת בזמן פולינומי.
⇐ ריצת האלגוריתם פולינומית באורך נוסחת הקלט.

Scanned by CamScanner