סיבוכיות - תרגול

תרגיל: שפה S תיקרא שפה גדולה, אם קיים פולינום $p(.)$, כך שלכל n מתקיים:

$|S\cap\{0,1\}^n| \le p(n)$ הוכיחו ש: $NP \subseteq P/poly \iff$ לכל שפה $L\in NP$ קיימת

רדוקציה קוק מ- L לשפה גדולה S.

פתרון - <u>הוכחה</u> -

מספיק להוכיח: $SAT\in P/poly \iff$ קיימת רדוקציה קוק מ- SAT לשפה גדולה.

$\Leftarrow$ נניח $SAT\in P/poly$ לפיכך קיימת מ"ט פולינומית M וסדרה אינסופית של מחרוזות

יעץ $\{a_n\}_{n\in\mathbb{N}}$, כאשר לכל n, $|a_n|\le q(n)$ עבור פולינום $q(.)$ כלשהו

ולכל $x\in\{0,1\}^n$ מתקיים -

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

נגדיר: $S_i^n = 0^{i-1}10^{q(n)-i}$

וכמו כן, נגדיר: $S=\{1^n0S_i^n \mid$ לכל סדר כאשר הביט ה- i של a_n הוא 1$\}$

← בנקודה נעזרנו בעדות $\{a_n\}_{n\in\mathbb{N}}$ בשביל הפתרון של SAT כי הוא ב- $P/poly$
ונרצה לעשות רדוקציה קוק מ- SAT לשפה גדולה,
כלומר יש לנו קופסא שחורה שפותרת את
השפה הגדולה ונרצה לפתור את SAT.
לא רשותה ש- ← לכן נרצה לגדור את S בדרכה כזו שהיא תשמור לנו בדרכה כלשהי את העדות ל-SAT ?!

קל לראות ש- S שפה גדולה כי לכל n מתקיים $|\{0,1\}^{n+1+q(n)}\cap S| \le |a_n| \le q(n)$

כעת נראה רדוקציה קוק מ- SAT ל- S.

בהינתן נוסחה ϕ באורך n האלגו' של הרדוקציה יפעל באופן הבא:

1) גור את a_n עי $q(n)$ שאילתות אורקל ל- S.

באופן ספציפי השאילתות יהיו על המחרוזות הבאות $1^n0S_1^n, 1^n0S_2^n, \dots, 1^n0S_{q(n)}^n$

אם התקבל 1 עבור השאילתא ה- i בדרישה, סימן שהביט ה- i ב- a_n הוא 1

ו- 0 אחרת.

2) הרץ את $M(a_n,\phi)$ והחזר את תשובתה.

קיבלנו אלגו' שרץ בזמן פולינומי ומבצע כמות פולינומית של שאילתות אורקל ומכריע את
SAT תוך שימוש באורקל לשפה גדולה S.

בס"ד.

$\Leftarrow$ קיימת רדוקציית קוק מ- SAT לשפה בגודל s, לפיכך קיימת מ"ט בגודל פולינומי אורכלי ל- s. נסמנה M^s, המכריעה את SAT.

יהי $t(\cdot)$ פונ' פול' שחוסמת את זמן הריצה של M^s. לכן עבור קלט x, השאילתא שהמכונה M^s מבצעת יהיו באורך לכל היותר $t(|x|)$.

נקרא את a_n באופן הבא:

נשרשר את כל המחרוזות ב- s עד לאורך $t(n)$. מאחר ש- s שפה בגודל, קיים פולינום $p(\cdot)$ כך שלכל n, $|\{0,1\}^n \cap s| \le p(n)$

אורך המחרוזת ב- a_n באורך i הוא לכל היותר $i \cdot p(i)$, לכן נקבל:

$$|a_n| = \sum_{i=1}^{t(n)} i \cdot p(i) < t(n) \cdot t(n) \cdot p(t(n))$$

כלומר, a_n הוא פול' באורך הקלט. כעת ניתן לבנות מ"ט M שמקבלת קלט x באורך n ועצה a_n הוא אמלץ את M^s כאשר M^s מבצעת שאילתא לאורכלי שלה M על מחרוזת z במקום לבצע שאילתא לאורכלי שאין לה, בדיוק הוא z נמצאת ב- a_n, אם כן זה שקול לתשובה 1 מהאורכלי, אם לא זה שקול לתשובה 0 מהאורכלי.

זמן הריצה של M הוא לכל היותר $|a_n| \cdot t(n)$ שהוא זמן פול' והוא כמובן מכריעה את SAT לכן $SAT \in P/poly$ □