תרגיל

שפה S תקרא שפה דלילה, אם קיים פולינום $p(\cdot)$ כך שלכל n מתקיים:

$$|S \cap \{0,1\}^n| \le p(n)$$

ג': $NP \subseteq P/Poly$ $\Leftrightarrow$ לכל $L \in NP$ קיימת רדוקציה קוק מ-L לשפה דלילה

הוכחה

מספיק להוכיח $SAT \in P/Poly$ $\Leftrightarrow$ קיימת רדוקציה קוק מ-SAT לשפה דלילה.

$\Leftarrow$ נניח ש $SAT \in P/Poly$ לפיכך קיימת סדרה של מחרוזות "עזר" $\{a_n\}_{n\in\mathbb{N}}$ וקיים פולינום $q(\cdot)$ כך שלכל n: $|a_n| \le q(n)$ וקיימת מכ"ט פולינומית דטרמיניסטית M כך שלכל n ולכל $x \in \{0,1\}^n$ מתקיים:

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

נגדיר $S_i^n = 0^{i-1}10^{q(n)-1}$

כמו כן, נגדיר: $S = \{1^n 0 S_i^n \mid$ לכל $n \ge 0$ כאשר הביט ה-i של a_n הוא $1\}$

קל לראות ש-S דלילה מכיוון ש $|S \cap \{0,1\}^{n+1+q(n)}| \le |a_n| \le q(n)$

כעת, נראה רדוקציה קוק מ-SAT ל-S. נילוח אלגוריתם M^S שבהינתן נוסחא ϕ באורך n פועל באופן הבא:

1. בור את a_n עפ"י $q(n)$ שאלות לאורקל.
השאילתות לאורקל יהיו המחרוזות הבאות: $1^n0S_1^n$, $1^n0S_2^n$, ..., $1^n0S_{q(n)}^n$. אם קבלנו תשובה 1 עבור שאלת $1^n0S_i^n$ סימן שהביט ה-i ב a_n הוא 1, אחרת הוא 0.
2. הרץ את $M(\phi, a_n)$ והחזר את תשובתה.

האלגוריתם M^S מבצע מס' פולינומי של שאילתות לאורקל, ויתר הפעולות מתבצעות אף הן בזמן פולינומי לכן קבלנו רדוקציה קוק תקינה מ-SAT ל-S כנדרש.

$\Rightarrow$ נניח שקיימת רדוקציה קוק מ-SAT לשפה דלילה S. לפיכך, קיימת מכ"ט פולינומית דטרמיניסטית M^S שמכריעה את SAT.

תהי $t(\cdot)$ פונקציית חסימה של זמן הריצה של M^S. הפונקציה t פולינומית.
לכן עבור קלט באורך n, M^S מבצעת שאילתות באורך עד $t(n)$.
נגדיר את a_n כך שהיה שרשור של כל המילים ב-S עד לאורך $t(n)$.
מכיוון ש-S שפה דלילה, קיים פולינום $p(\cdot)$ כך ש $|S \cap \{0,1\}^n| \le p(n)$ לכל n.
לכן אורך כל המילים באורך i ב-S הוא לכל היותר $i \cdot p(i)$.
לכן יתקיים: $|a_n| \le \sum_{i=0}^{t(n)} i \cdot p(i) \le t^2(n) \cdot p(t(n))$

לכן האורך של a_n חסום פולינומית, כעת, ניתן לילוח מכ"ט M שמקבלת קלט ϕ באורך n ועצה a_n ופועלת באופן הבא:

האלגוריתם מסמלץ את הריצה של M^S, כאשר M^S מבצעת שאילתות לאורקל עם מחרוזת כלשהי y, האלגוריתם יעבור על a_n:
אם המחרוזת y נמצאת ב-a_n, הדבר שקול לתשובה של האורקל (חיובי)
אחרת הדבר שקול לתשובה שלילית של האורקל.

המכונה M מכריעה את SAT ופועלת בזמן פולינומי כיוון ש M^S רצה בזמן פולינומי והאורך של a_n חסום פולינומית. לכן קיבלנו ש $SAT \in P/Poly$.