

P/poly

הגדרה 1

$L \in P/poly$ אם קיימת סדרה אינסופית של מעגלים $\{C_n\}_{n \in \mathbb{N}}$, כך שלכל n , C_n יש n קוי קלט וקיים פולינום $P(\cdot)$ כך שלכל n ולכל $x \in \{0, 1\}^n$ $|C_n| \leq P(n)$ ולכל $x \in \{0, 1\}^n$

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

נשים

מכיוון שדורשים סדרה אינסופית של מעגלים, מעגל לכל אורך קלט, יש לנו בעצם חישוב שונה לכל אורך קלט. זה נותן לחישוב תכונה של non-uniform

הגדרה 2

$L \in L/poly$ אם קיימת מ"ט פולינומית M בעלת שני סרטי קלט, קיים פולינום $P(\cdot)$ וסדרה אינסופית של מחרוזות יעוץ $\{a_n\}_{n \in \mathbb{N}}$, כאשר $|a_n| \leq P(n)$ כך שלכל n ולכל $x \in \{0, 1\}^n$

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

הערה

אפשר לחשוב על מחרוזת היעוץ a_n כעל תיאור של המעגל C_n .

משפט 1

$$P \subseteq P/poly$$

משפט 2

$P/poly$ מכילה שפות לא כריעות

משפט 3

(כנראה $NP \not\subseteq P/poly$)
אם $NP \subseteq P/poly$, אז $PH = \Sigma_2$

תרגיל

נגדיר מחלקה חדשה בדומה ל $P/poly$, אבל נאפשר ייעוצים באורך אקספוננציאלי (2^{n^c}) . הראו שכל שפה שייכת למחלקה זו.

פתרון

תהי L שפה כלשהי. נגדיר את a_n להיות טבלה שמכילה 2^n שורות, שורה לכל קלט באורך n , ולכל קלט רשום ליד את התשובה לאותו קלט.

תרגיל

נגדיר את המחלקה P/\log בדומה ל $P/poly$, פרט לעובדה שלכל n : $|a_n| \leq c \cdot \log n$ עבור קבוע c .

הוכיחו: אם $NP \subseteq P/\log$ אזי $P = NP$

פתרון

נניח $3SAT \in P/\log \iff NP \subseteq P/\log$. צ"ל $P = NP$ כלומר $3SAT \in P$.
 $3SAT \in P/\log \iff$ קיימת מ"ט פולינומית M ו $\{a_n\}_{n \in \mathbb{N}}$ כך ש $|a_n| \leq c \cdot \log n$ ולכל $\varphi \in \{0, 1\}^n$:

$$M(a_n, \varphi) = \begin{cases} 1 & \varphi \in 3SAT \\ 0 & \varphi \notin 3SAT \end{cases}$$

נבנה אלגוריתם פולינומי M' שבהינתן קלט φ :

1. אם φ לא בצורת $3CNF$, החזר 0.

2. יהי $n = |\varphi|$. לכל $a^* \in \{0, 1\}^{c \cdot \log n}$:

2.1 אם $m(a^*, \varphi) = 1$