סיבוכיות- תרגול 8

<u>תזכורת:</u> $S \in P/Poly$ אם קיימת מ"ט פולינומית דטרמיניסטית M, פולינום p וסדרה אינסופית של מחרוזות עצה $\{a_n\}_{n=1}^{\infty}$, כך שלכל n, $|a_n| = p(n)$ ולכל x מתקיים $x \in S \Leftrightarrow M(a_{|x|}, x) = 1$.

<u>תרגיל:</u> קבוצה A תקרא <u>דלילה</u> (Sparse) אם קיים פולינום p כך שלכל n, $|A \cap \{0,1\}^n| \le p(n)$. הוכיחו כי $S \in P/Poly$ אמ"ם קיימת רדוקצית קוק מ-S לקבוצה דלילה (במילים אחרות, $P/Poly = P^{Sparse}$).

<u>פתרון:</u>

($\Leftarrow$): תהי $S \in P/Poly$. לכן, קיימת מ"ט דטר' פולינומית M, פולינום p וסדרה אינסופית של מחרוזות עצה $\{a_n\}_{n=1}^{\infty}$ כך שלכל n, $|a_n| = p(n)$, ולכל x מתקיים $x \in S \Leftrightarrow M(a_{|x|}, x) = 1$. נראה מ"ט דטר' פולינומית עם גישת אורקל לקבוצה דלילה המכריעה את S.

לכל n ולכל $1 \le i \le p(n)$, נגדיר את השלשה $a_n^i = (1^n, 0^{i-1}10^{q(n)-i}, \sigma_i)$ כאשר σ_i הינו הביט ה-i במחרוזת העצה a_n. ונגדיר את השפה $A = \{a_n^i \mid n \in \mathbb{N}, 1 \le i \le q(n)\}$.

נשים לב ש-A קבוצה דלילה, שכן לכל m מהצורה $m = n + q(n) + 1$ מתקיים

$$|A \cap \{0,1\}^m| = |a_n| = q(n) \le q(m),$$

ולכל m אחר מתקיים $|A \cap \{0,1\}^m| = 0$.

כעת, נראה מ"ט דטר' פולינומית N^A המכריע את S:

<u>$N^A(x)$:</u>

1. לכל $1 \le i \le p(|x|)$, בצע שאילתא לאורקל $(1^{|x|}, 0^{i-1}10^{q(|x|)-i}, 1) \overset{?}{\in} A$. אם התשובה היא כן, $\sigma_i \leftarrow 1$, אחרת, $\sigma_i \leftarrow 0$.
2. $a_{|x|} \leftarrow \sigma_1 \dots \sigma_{p(|x|)}$.
3. סמלץ את $M(a_{|x|}, x)$ והחזר את תשובתה.

קיבלנו מ"ט דטר' פולינומית עם גישת אורקל ל-$A \in Sparse$ המכריעה את S ולכן $S \in P^{Sparse}$.

($\Rightarrow$): תהי $S \in P^{Sparse}$. לכן, קיימת מ"ט דטר' פולינומית M^A עם גישת אורקל ל-$A \in Sparse$ המכריעה את S. נסמן ב-t את הפולינום החוסם את זמן הריצה של M. נשים לב כי עבור קלט באורך n, M מבצעת שאילתות לאורקל באורך לכל היותר $t(n)$. נרצה שהעצה a_n תכיל את כל המידע הדרוש עבור הרצת M ללא גישה לאורקל. לשם כך נגדיר את העצה a_n להיות שרשור של כל המילים ב-A באורך לכל היותר $t(n)$. כלומר, $a_n = x_1\#x_2\# \dots \#x_m$, כך ש-$x_1, \dots x_m$ הן כל המילים ב-A המקיימים $|x_i| \le t(n)$.

מהו האורך של a_n? A שפה דלילה ולכן קיים פולינום p כך שלכל n, $|A \cap \{0,1\}^n| \le p(n)$. לכן, מתקיים כי $m = \sum_{i=1}^{t(n)} |A \cap \{0,1\}^i| \le \sum_{i=1}^{t(n)} p(i) \le t(n)p(t(n))$. בנוסף, לכל i, $|x_i| \le t(n)$, ולכן

$$|a_n| \le m \cdot (t(n) + 1) \le (t(n) + 1)(t(n)p(t(n)))$$

שזהו פולינום ב-n. כעת, נראה מ"ט דטר' פולינומית המקבלת קלט x ומחרוזת עצה $a_{|x|}$ ומכריעה את S. המכונה תסמלץ את M^A, ועבור כל שאילתא לאורקל $z \overset{?}{\in} A$, המכונה תסרוק את מחרוזת העצה ותבדוק אם z מופיע בה.

אם כן, תמשיך כפי ש-M^A ממשיכה עבור תשובה חיובית, ואם לא, תמשיך כפי ש-M^A ממשיכה עבור תשובה שלילית. זמן הריצה של המכונה הוא לכל היותר $|a_n| \cdot t(n)$, שזה פולינומי ב-n. כלומר, קיבלנו כי $S \in P/Poly$.

סיבוכיות מקום

נרצה למדוד את המקום הדרוש על מנת לבצע חישוב כלשהו. מכיוון שנעסוק גם בסיבוכיות מקום תת-לינארי באורך הקלט, נרצה להפריד בין המקום הנדרש לאחסון את הקלט/פלט, לבין המקום הנדרש לביצוע החישובים. לשם כך נעסוק במ"ט בעלת 3 סרטים:

1) סרט קלט- קריאה בלבד.
2) סרט פלט- כתיבה בלבד (חד כיוונית).
3) סרט עבודה- קריאה וכתיבה.

<u>הגדרה:</u> תהי M מ"ט דטר'. נאמר כי M בעלת סיבוכיות מקום $s: \mathbb{N} \to \mathbb{N}$, אם לכל $n \in \mathbb{N}$, M משתמשת בלכל היותר $s(n)$ תאים מסרט העבודה עבור קלטים באורך n.

<u>הגדרה:</u> תהי $s: \mathbb{N} \to \mathbb{N}$. נאמר כי בעית הכרעה כלשהי שייכת למחלקה $DSPACE\big(s(n)\big)$, אם קיימת מ"ט דטר' בעלת סיבוכיות מקום s המכריעה את הבעיה.

הקשר בין סיבוכיות מקום וסיבוכיות זמן

<u>טענה 1:</u> לכל פונקציה $t: \mathbb{N} \to \mathbb{N}$ מתקיים $DTIME\big(t(n)\big) \subseteq DSPACE\big(t(n)\big)$.

<u>טענה 2:</u> לכל פונקציה $s: \mathbb{N} \to \mathbb{N}$ מתקיים $DSPACE\big(s(n)\big) \subseteq DTIME\big(n2^{O(s(n))}\big)$, ועבור $s(n) \geq \log n$ מתקיים $DSPACE\big(s(n)\big) \subseteq DTIME\big(2^{O(s(n))}\big)$.

חישוב לא דטרמינסטי

ראינו שני מודלים שקולים לסיבוכיות זמן ל"ד:

1) מודל אונליין: במכונה יש מעברים שלא מוגדרים באופן יחיד. הקלט מתקבל אמ"ם קיים מסלול מקבל.
2) מודל אופליין: המכונה היא למעשה דטר', אך מקבלת קלט נוסף (עד). הקלט מתקבל אמ"ם קיים עד שגורם למכונה לקבל.

מה ההבדל העקרוני בין המודלים? במודל האונליין, ברגע שהמכונה מבצעת בחירה ל"ד וממשיכה הלאה היא כבר לא "זוכרת" מה הייתה הבחירה הנ"ל. לעומת זאת, במודל האופליין, הבחירות הל"ד מתקבלות כחלק מהקלט ולכן המכונה יכולה לחזור שוב ושוב ו"להזכר" בבחירה שנעשתה בעבר.

ברור אם כן, שמודל האונליין מוכל במודל האופליין. בהקשר של סיבוכיות זמן המודלים שקולים, מכיוון שגם במודל האונליין המכונה יכולה "לשמור" את כל הבחירות שמתבצעות לאורך הריצה ולחזור אליהן לאחר מכן (אין הגבלת מקום). לעומת זאת, בהקשר של סיבוכיות מקום מסתבר שמודל האופליין חזק יותר ממודל האונליין, מכיוון שלא תמיד קיים מספיק מקום לשמור את הבחירות הל"ד שנעשו.

נראה בתרגול הבא שעבור $s(n) \geq \log n$ מתקיים כי $NSPACE_{online}\big(s(n)\big) \subseteq NSPACE_{offline}\big(O(\log s(n))\big)$ ועבור $s(n) \geq n$ מתקיים $NSPACE_{online}\big(s(n)\big) = NSPACE_{offline}\big(\theta(\log s(n))\big)$