# סיבוכיות- תרגול 12

**גרסה הסתברותית של NP**

<u>הגדרה:</u> נאמר כי $S \in MA$ אם קיימת מ"ט פולינומית הסתברותית $V$ כך ש:

$$x \in S \Longrightarrow \exists y, \Pr[V(x,y) = 1] = 1$$

$$x \notin S \Longrightarrow \forall y, \Pr[V(x,y) = 0] \geq 1/2$$

<u>תרגיל:</u> נגדיר את המחלקה $MA'$ באופן הבא: נאמר כי $S \in MA'$ אם קיימת מ"ט פולינומית הסתברותית $V$ כך ש:

$$x \in S \Longrightarrow \exists y, \Pr[V(x,y) = 1] \geq 2/3$$

$$x \notin S \Longrightarrow \forall y, \Pr[V(x,y) = 0] \geq 2/3$$

הוכיחו כי $MA = MA'$.

<u>פתרון:</u> הכיוון $MA \subseteq MA'$ קל (פשוט מריצים את המוודא פעמיים ומחזירים 1 אם"ם שתי ההרצות החזירו 1).

נראה כי $MA' \subseteq MA$. תהי $S \in MA'$. לכן קיימת מ"ט פולינומית הסתברותית $V$ העונה על הדרישות של $MA'$.
נסמן ב-$p = p(n)$ את מס' הטלות המטבע של $V$ עבור קלטים באורך $n$. נגדיר את המוודא $V^*$ כך שמריץ את $V$ $k$ פעמים ומחזיר את תשובת הרוב. נסמן ב-$q = kp(n)$ את מס' הטלות המטבע של $V^*$. לפי חסם צ'רנוף מתקיים:

$$x \in S \Longrightarrow \exists y \Pr_{r \in \{0,1\}^q}[V^*(x,y,r) = 0] \leq e^{-\frac{k}{18}}$$

$$x \notin S \Longrightarrow \forall y \Pr_{r \in \{0,1\}^q}[V^*(x,y,r) = 1] \leq e^{-\frac{k}{18}}$$

נבחר $k = 18\ln(2p^2)$ ונקבל כי ההסתברות לטעות $\leq \frac{1}{2p^2} \leq \frac{1}{2q}$.

<u>טענה 1:</u> עבור $x \in S$, קיים $y$ וקיימת סדרה של מחרוזות $s_1, \dots, s_q \in \{0,1\}^q$ כך שלכל $r \in \{0,1\}^q$ קיים $i$ עבורו

$$V^*(x,y,r \oplus s_i) = 1$$

<u>טענה 2:</u> עבור $x \notin S$, לכל $y$ ולכל סדרה של מחרוזות $s_1, \dots, s_q \in \{0,1\}^q$ מתקיים

$$\Pr_{r \in \{0,1\}^q}\left[\bigvee_{i=1}^{q} V^*(x,y,r \oplus s_i) = 0\right] \geq \frac{1}{2}$$

נניח כי הטענות נכונות. נגדיר $y' = y||s_1, \dots, s_q$ כך ש-$y$ הינו אותו $y$ של המוודא $V^*$ והמחרוזות $s_1, \dots, s_q$ כנ"ל.
נגדיר את המוודא $V'$ באופן הבא: $V'(x,y',r) = \bigvee_i V^*(x,y,r \oplus s_i)$. מטענה 1 נקבל:

$$x \in S \Longrightarrow \exists y', \Pr_{r \in \{0,1\}^q}[V'(x,y',r) = 1] = 1$$

ומטענה 2 נקבל:

$$x \notin S \Longrightarrow \forall y', \Pr_{r \in \{0,1\}^q}[V'(x,y',r) = 0] \geq 1/2$$

<u>הוכחת טענה 2:</u> נקבע $s_1, \dots, s_q$ כלשהן. נשים לב כי לכל $i$ המחרוזת $r \oplus s_i$ הינה מחרוזת אקראית. לכן

$$\Pr_{r\in\{0,1\}^q}\left[\bigvee_i V^*(x,y,r\oplus s_i)=0\right]=1-\Pr_{r\in\{0,1\}^q}[\exists i, V^*(x,y,r\oplus s_i)=1]$$
$$\geq 1-\sum_{i=1}^{q}\Pr_{r\in\{0,1\}^q}[V^*(x,y,r\oplus s_i)=1]\geq 1-q\cdot\frac{1}{2q}=\frac{1}{2}$$

<u>הוכחת טענה 1:</u> נראה כי עבור סדרה אקראית $s_1,\dots,s_q$, מתקיים:

$$\Pr_{s_1,\dots,s_q}[\exists r\forall i, V^*(x,y,r\oplus s_i)=0]<1$$

ומזה נסיק כי

$$\Pr_{s_1,\dots,s_q}[\forall r\exists i, V^*(x,y,r\oplus s_i)=1]>0$$

$$\Pr_{s_1,\dots,s_q}[\exists r\forall i, V^*(x,y,r\oplus s_i)=0]\leq\sum_{r\in\{0,1\}^q}\Pr_{s_1,\dots,s_q}[\forall i, V^*(x,y,r\oplus s_i)=0]$$
$$\leq\sum_{r\in\{0,1\}^q}\prod_{i=1}^{q}\Pr_{s_i}[V^*(x,y,r\oplus s_i)=0]\leq\sum_{r\in\{0,1\}^q}\left(\frac{1}{2q}\right)^q\leq 2^q\left(\frac{1}{2q}\right)^q=\left(\frac{1}{q}\right)^q<1$$

לכן קיימת סדרת מחרוזות המקיימת את הדרישה. (למעשה, כמעט כל סדרת מחרוזות היא טובה.)

<u>הגדרה:</u> עבור יחס $R$, נגדיר את $f_R$ כך ש-$f_R(x)=|\{y\mid(x,y)\in R\}|$.

<u>הגדרה:</u> $\#P=\{f_R\mid R\in PC\}$.

<u>תרגיל:</u> הוכיחו כי $P^{\#P}\subseteq PSPACE$.

<u>הוכחה:</u> תהי $S\in P^{\#P}$. לכן קיימת מ"ט פולינומית $M$ עם גישת אורקל ל-$f_R\in\#P$ המכריעה את $S$. נסמן ב-$p$ את הפולינום החוסם את זמן הריצה של $M$, ב-$V$ את המוודא עבור היחס $R$ וב-$q$ את הפולינום החוסם אותו.

נבנה מכונה $M'$ המכריעה את $S$ ללא גישת אורקל ובסיבוכיות מקום פולינומית. $M'$ תפעל בדיוק כמו $M$ למעט המקרים בהם $M$ פונה לאורקל. עבור כל גישת אורקל מהצורה $f_R(a)$, $M'$ תעבור על כל מחרוזת $y\in\{0,1\}^{q(|a|)}$ ותספור עבור כמה $y$ מתקיים $V(a,y)=1$.

ברור ש-$M'$ מכריעה את $S$ ללא גישת אורקל. נותר רק להראות שסיבוכיות המקום היא פולינומית:

1. המכונה $M$ רצה בזמן פולינומי, ולכן גם סיבוכיות המקום פולינומית.
2. עבור כל שאילתא לאורקל מהצורה $f_R(a)$, לכל $y$ מתקיים $|y|\leq q(|a|)\leq q\big(p(|x|)\big)$. כלומר, המקום הנדרש לשמירת כל מחרוזת $y$ הוא פולינומי באורך הקלט. הבדיקה האם $V(a,y)=1$ מתבצעת בזמן פולינומי ולכן גם במקום פולינומי. בנוסף, יש לאחסן מונה. לכל $a$, $f_R(a)\leq 2^{q(p(|x|))}$ ולכן מספיק מונה באורך $q\big(p(|x|)\big)$.