22.06

תרגיל

המחלקה MA מוגדרת באופן אנלוגי לNP כאשר המוודא הוא מ"ט הסתברותית.
נגדיר את המחלקה $MA_{\frac{2}{3},\frac{1}{3}}$ להיות המחלקה שמכילה את השפות L כך שקיימת מ"ט הסתברותית פולינומית המכריעה את L כך שמתקיים:

$$x\in L \Rightarrow \exists y \; Pr[M(x,y,r)=1] \geq \frac{2}{3}$$

$$x\notin L \Rightarrow \forall y \; Pr[M(x,y,r)=1] \leq \frac{1}{3}$$

באופן דומה, נגדיר את המחלקה $MA_{1,\frac{1}{3}}$ להיות המחלקה שמכילה את השפות L כך שקיימת מ"ט M פולינומית שמכריעה הסתברותית את L כך שמתקיים:

$$x\in L \Rightarrow \exists y \; Pr[M(x,y,r)=1] = 1$$

$$x\notin L \Rightarrow \forall y \; Pr[M(x,y,r)=1] \leq \frac{1}{3}$$

הוכח: $MA_{\frac{2}{3},\frac{1}{3}} = MA_{1,\frac{1}{3}}$

פתרון

כיוון אחד ברור $(MA_{1,\frac{1}{3}} \subseteq MA_{\frac{2}{3},\frac{1}{3}})$.
נראה שאם $L\in MA_{\frac{2}{3},\frac{1}{3}}$ אז $L\in MA_{1,\frac{1}{3}}$
מכיוון ש $L\in MA_{\frac{2}{3},\frac{1}{3}}$, אז קיים מוודא פולינומי הסתברותי V שמתקיים:

$$x\in L \Rightarrow \exists y \; Pr[V(x,y,r)=1] \geq \frac{2}{3}$$

$$x\notin L \Rightarrow \forall y \; Pr[V(x,y,r)=1] \leq \frac{1}{3}$$

ע"י הרצת V מס' פולינומי של פעמים ובחירה ע"פי רוב, ניתן לייצר מוודא V^* שהסתברות השגיאה שלו לא עולה על $\frac{1}{2^n}$.
בדומה להוכחה ש $BPP \subseteq \Sigma_2$, ניתן להראות כי עבור $x\in L$ קיימות $poly(n)=k$ מחרוזות $r_1, r_2, \dots, r_n$ באורך m (קטן מ kn) כך שמתקיים:

$$\forall r_0 \; \exists i\in\{1,2,\dots,k\} \; s.t \; V^*(x,y,r_0\oplus r_i)=1$$

ניתן להראות זאת באמצעות שיטה הסתברותית ע"י שנראה:

$$\circledast \quad Pr\left[\forall r_0 \left(\bigvee_{i=1}^{k} V^*(x,y,r_0\oplus r_i)=1\right)\right] > \frac{1}{2}$$

מישהו מבינהם יתן לנו 1

כדי להראות זאת נתבונן במאורע המשלים:

$$Pr\left[\exists r_0 \left(\bigvee_{i=1}^{k} V^*(x,y,r_0\oplus r_i)\right)=0\right]$$

$$\leq \sum_{r_0\in\{0,1\}^m} Pr\left[\left(\bigvee_{i=1}^{k} V^*(x,y,r_0\oplus r_i)\right)=0\right] \quad \text{חסם האיחוד}$$

$$= \sum_{r_0\in\{0,1\}^m} Pr\left[\bigwedge_{i=1}^{k} \left(V^*(x,y,r_0\oplus r_i)=0\right)\right]$$

$$= \sum_{r_0\in\{0,1\}^m} \prod_{i=1}^{k} Pr\left[V^*(x,y,r_0\oplus r_i)=0\right] \quad \text{המאורעות הינם בת.}$$

$$\leq \sum_{r_0\in\{0,1\}^m} \prod_{i=1}^{k} \frac{1}{2^n} = \sum_{r_0\in\{0,1\}^m} \frac{1}{2^{nk}} = 2^m\cdot\frac{1}{2^{nk}} < \frac{1}{2^n}$$

⇐ ⊛ ההסתברות נכונה ולכן קיים r_0 שמקיים זאת (שיטה הסתברותית)

בס"ד

לכן ניתן לבנות מוודא V' שמקבל r_0, y', x כאשר: $y' = y | r_1 | \dots | r_k$

ומריץ k פעמים את V^* כל פעם עם $x, y, r_0 \oplus r_i$ עבור i שונה.

אם באחת ההרצות החזר 1 V' יחזיר 1,

אחרת יחזיר 0

- עבור $x \in L$ לפי מה שהוכחנו לעיל לפחות אחת ההרצות חייבת להחזיר 1 ללא קשר לערך r_0.
  לכן תמיד V' יחזיר 1 עבור $x \in L$.

- עבור $x \notin L$ מתקיים לכל i:

$$Pr\,[V^*(x, y, r_0 \oplus r_i) = 1] \le \frac{1}{2^n}$$

לכן:

$$Pr\,[V^*(x, y, r_0 \oplus r_i) = 1 \text{ for some } i] \le k \cdot \frac{1}{2^n} \le \frac{1}{3}$$