סיבוכיות – תרגול 7

כל העולם הוא חישוב אחד גדול

5.4.11

מחלקות סיבוכיות הסתברותיות

נדגיש שוב שהכוונה שלכל קלט המכונה תחזיר תשובה נכונה בהסתברות גבוהה. ולא תהיה לנו רשימת קלטים שעבורם המכונה לא תעבוד.

הגדרה. $BPP_{\alpha,\beta}$ היא מחלק השפות $L \subseteq \{0,1\}^*$ עבורן קיימת מ"ט דטרמיניסית עם זמן ריצה פולינומיאלי M כך שלכל $x \in \{0,1\}^*$:

$$x \in L \Rightarrow \mathbb{P}_y\Big(M(x,y)=1\Big) \geq \beta$$

$$x \notin L \Rightarrow \mathbb{P}_y\Big(M(x,y)=1\Big) \leq \alpha$$

כאשר y מסמן את סדרת המטבעות האקראיים של המכונה וכן $|y| = poly(|x|)$. לעיתים נסמן $BPP(\alpha,\beta)$.

למשל: $BPP = BPP(\frac{1}{3},\frac{2}{3})$. $RP = BPP(0,\frac{1}{2})$ באותו אופן נוכל להגיד $RP = BPP(0,\frac{2}{3})$. מדוע? נראה בהמשך.
בקלות $RP \subseteq BPP$, $RP \subseteq NP$.

תרגיל.

1. האם $BPP(\frac{1}{3},\frac{2}{3}) = BPP(2^{-n^{10}}, 1-2^{-n^{10}})$?
2. האם $BPP(\frac{1}{2}-\frac{1}{n^{10}},\frac{1}{2}+\frac{1}{n^{10}}) = BPP(2^{-n^{10}}, 1-2^{-n^{10}})$?
3. האם $BPP(\frac{1}{2}-\frac{1}{2^{n^{10}}},\frac{1}{2}+\frac{1}{2^{n^{10}}}) = BPP(2^{-n^{10}}, 1-2^{-n^{10}})$?

הערה. נובע מידית מההגדרה שבשלושת הסעיפים ההכלה מימין לשמאל מתקיימת.

פתרון. נתחיל מהמחלקה $BPP(\frac{1}{2}-q,\frac{1}{2}+q)$ ואח"כ נעבור מקרה מקרה ונראה מה יקרה. השיטה שבא נשתמש נקראת אמפליפיקציה (הגברה) . תהא $L \in BPP(\frac{1}{2}-q,\frac{1}{2}+q)$ אזי קיימת מכונת טיורינג, דטרמיניסטית פולינומיאלית M כך שלכל קלט x עונה נכון בהסתברות $\frac{1}{2}+q$ על פני המטבעות האקראיים y.
נגדיר מכונת טיורינג M' שבהינתן קלט x וסדרת מחרוזות אקראיות בלתי תלויות $y_1, y_2, \ldots, y_T$ מריצה את $M(x,y_i)$, M' תחזיר את התשובה שמופיעה יותר פעמים.
נגדיר: $Y_i = 1$ אם $M(x,y_i)$ החזירה תשובה נכונה ונגדיר $Y_i = 0$ אחרת. נסמן $Y = \sum_{i=1}^{T} Y_i$. נשים לב ש- M' עונה נכון כאשר $Y \geq \frac{T}{2}$. רוצים לאמוד: $\mathbb{P}(Y \leq \frac{T}{2}) \leq ?$.

משפט. *Chernoff* יהיו $Y_1, Y_2, \ldots, Y_T$ משתנים מקריים בוליאניים ב"ת ש"ה $\mathbb{P}(Y_i) = \mathbb{E}(Y_i) = p$. נסמן $Y = \sum_{i=1}^{T} Y_i$, $\mu = \mathbb{E}(Y) = p \cdot T$. אזי לכל $\alpha \in (0,1)$:

$$\mathbb{P}(|Y - \mu| \geq \alpha\mu) \leq 2 \cdot e^{-\frac{\alpha^2}{4} \cdot \mu}$$

נחזור למכונה M': $p = \frac{1}{2} + q$, $\mu = (\frac{1}{2} + q) \cdot T$.

$$\mathbb{P}(Y \leq \frac{T}{2}) = \mathbb{P}(Y - \mu \leq \frac{T}{2} - \mu) = \mathbb{P}(Y - \mu \leq -q \cdot T) \leq \mathbb{P}(|Y - \mu| \geq \underbrace{q \cdot T}_{\alpha \cdot \mu})$$

ואז נבחר $\alpha = \frac{q}{\frac{1}{2}+q}$. נציב במשפט:

$$\mathbb{P}(|Y - \mu| \geq q \cdot T) \leq 2 \cdot e^{-\frac{1}{4}\frac{q^2}{(\frac{1}{2}+q)^2}(\frac{1}{2}+q) \cdot T} \underbrace{\leq}_{q \in [0, \frac{1}{6}]} 2^{-\Omega(q^2 \cdot T)}$$

נחזור לשאלה:

1. $q = \frac{1}{6}$. נבחר $T = n^{11}$ ונקבל ש- M' רצה בזמן פולינומיאלי וסיכוי השגיאה שלה $\leq 2^{-n^{10}}$.
2. $q = \frac{1}{n^{10}}$. נבחר $T = n^{31}$ ונקבל ש- M' רצה בזמן פולינומיאלי וסיכוי השגיאה שלה $\leq 2^{-n^{10}}$.
3. $q = \frac{1}{2^{n^{10}}}$. כדי לקבל סיכוי הצלחה $\geq \frac{2}{3}$ יש לדרוש $T \geq 2^{n^{10}}$ אך זמן הריצה של M' יהיה פולינומיאלי. לכן ההוכחה הזאת לא תעבוד במקרה הזה.

טענה. הטענה בסעיף השלישי היא שאלה פתוחה ששקולה לשאלה "האם $SAT \in BPP$?" או באופן שקול $NP \subseteq BPP$.

הוכחה. נראה:

$$SAT \in BPP(\frac{1}{2} - \frac{1}{2^{n^{10}}}, \frac{1}{2} + \frac{1}{2^{n^{10}}})$$

ואמנם, נסתכל על האלגוריתם הבא: בהינתן נוסחאת CNF φ באורך n:

- בהסתברות $\frac{1}{2^{n^{10}}}$ נקבל $\frac{1}{2}$.
- אחרת, (כלומר בהסתברות $\frac{1}{2} + \frac{1}{2^{n^{10}}}$) נגריל השמה ונבדוק אם היא מספקת את φ. אם כן נקבל ואחרת נדחה.

ניקח נוסחא $\varphi \notin SAT$. אז ההסתברות שהאלגוריתם מקבל את φ היא: $\frac{1}{2} - \frac{1}{2^{n^{10}}}$.
ניקח נוסחא $\varphi \in SAT$. ההסתברות שהאלגוריתם מקבל את φ:

$$(\frac{1}{2} - \frac{1}{2^{n^{10}}}) + (\frac{1}{2} + \frac{1}{2^{n^{10}}}) \cdot \frac{1}{2^n} \geq \frac{1}{2} - \frac{1}{2^{n^{10}}} + \frac{1}{2^{n+1}} \geq \frac{1}{2} + \frac{1}{2^{n^{10}}}$$

□