

מחלקות סיבוכיות הסתברותיות

הגדרה: עבור $p_1, p_2 \in [0, 1]$, נגדיר את $BPP(p_1, p_2)$ כמחלקת השפות L עבורן קיימת מכונת טיורינג M דטרמיניסטית שרצה בזמן פולינומי, כך שלכל $x \in \{0, 1\}^*$, אם $x \in L$ אזי $\Pr_r[M(x, r) = 1] \geq p_2$ ואם $x \notin L$ אזי $\Pr_r[M(x, r) = 1] \leq p_1$, כאשר r מציינן סדרה של הטלות מטבע, $|r| = \text{Poly}(|x|)$.
הערה: נשים לב שההסתברות היא על פני המטבעות האקראיים r ולא על פני הקלטים.
הערה: ניתן להגדיר את ה"ל" בעזרת מכונת טיורינג הסתברותית שמטילה מטבעות אקראיים. מספרם יהיה פולינומי כי זמן הריצה פולינומי.

מחלקות סטנדרטיות

טעות דו-צדדית: $BPP = BPP\left(\frac{1}{3}, \frac{2}{3}\right)$.

טעות חד-צדדית: $RP = BPP\left(0, \frac{1}{2}\right)$, $coRP = BPP\left(\frac{1}{2}, 1\right)$.

נשים לב: $RP \subseteq NP$.

תהא $L \in RP$, ותהא M מ"ט המתאימה לה. נחשוב על r כעל עד במכונת NP . אם $x \in L$, אזי קיים r שמוביל את המכונה לקבל (בעצם לפחות $\frac{1}{2}$ מהעדים האפשריים עושים זאת), ואם $x \notin L$, אזי לא קיים r כזה.

אפשר להראות: $BPP\left(2^{-n^{10}}, 1 - 2^{-n^{10}}\right) = BPP = BPP\left(\frac{1}{2} - n^{-10}, \frac{1}{2} + n^{-10}\right)$.

שאלה פתוחה: האם $SAT \in BPP$?

טענה: אם $SAT \in BPP$ אזי $NP = RP$.

כזכור, $RP \subseteq NP$, ולכן די להראות ש- $NP \subseteq RP$. נראה ש- $SAT \in RP$.
 מההנחה, $SAT \in BPP$, ולכן קיימת מ"ט פולינומית דטרמיניסטית M , שבהינתן נוסחה וסדרת מטבעות אקראיים r , מחזירה אם הנוסחה ספיקה בהסתברות שגיאה לכל היותר 2^{-n} (על פני r).
 נבנה מ"ט M' , שבהינתן נוסחה ϕ מבצעת: לכל משתנה x_i נקבע ערך T , נציב אותו ב- ϕ ונריץ את M על הנוסחה המתקבלת, כדי לדעת אם הנוסחה שקיבלנו ספיקה. אם כן, נקבע את x_i להיות T , ואחרת F (בכל שלב ממשיכים עם הנוסחה שהתקבלה). כעת, נבדוק אם ההשמה שקיבלנו מספקת את ϕ . אם כן, נחזיר כן. אחרת, נחזיר לא.

אם $\phi \notin SAT$, אזי ההשמה בסוף האלגוריתם בהכרח לא תספק את ϕ , כדרוש.
 אם $\phi \in SAT$, וכל הפעולות המכונה M החזירו תשובה נכונה, אזי האלגוריתם ימצא השמה מספקת ויחזיר כן. ההסתברות שלפחות אחת מבין n ההרצות של M החזירה תשובה לא נכונה היא לכל היותר $n \cdot 2^{-n} \leq \frac{1}{2}$, ובהסתברות לפחות $\frac{1}{2}$ תוחזר תשובה נכונה (הסתמכנו על

זה ש- $\Pr[A \cup B] \leq \Pr[A] + \Pr[B]$).

זמן הריצה של M' הוא n פעמים זמן הריצה של M , ולכן פולינומי.

כמו כן, לכל $L \in NP$ ניתן להפעיל רדוקציה פולינומית ל- SAT , ואז להפעיל את האלגוריתם RP ה"ל על התוצאה.
 מש"ל.

האם $SAT \in BPP\left(\frac{1}{2} - n^{-10}, \frac{1}{2} + n^{-10}\right)$? שאלה פתוחה, השקולה ל- $SAT \in BPP$.

האם $SAT \in BPP\left(\frac{1}{2} - 2^{-n^{10}}, \frac{1}{2} + 2^{-n^{10}}\right)$? כן.

האלגוריתם:

בהסתברות $p = \frac{1}{2} - 2^{-n^{10}}$, החזר כן.

בהסתברות $1 - p = \frac{1}{2} + 2^{-n^{10}}$, הגרל השמה לנוסחה. אם מספקת, החזר כן, ואחרת לא.

ניתוח:

אם $\phi \notin SAT$, נחזיר שהיא ספיקה בהסתברות $p \leq \frac{1}{2} - 2^{-n^{10}}$.

אם $\phi \in \text{SAT}$, נחזיר שהיא ספיקה בהסתברות לפחות $\frac{1}{2^n} \left(\frac{1}{2} - 2^{-n^{10}} \right) + \left(\frac{1}{2} + 2^{-n^{10}} \right) \cdot \frac{1}{2^n}$, וזה
 לפחות $\frac{1}{2} + 2^{-n^{10}}$.