

אלגוריתמים ראנדומיים

BPP - טעות דו צדדית

משפט

$$BPP \subseteq P/poly$$

הוכחה

תהי $A \in BPP$. ע"פ הדין בפעם קודמת, קיימת מכונת טיורינג הסתברותית M^* אשר על כל קלט x מקיימת

$$\Pr_r (M^*(x, r) = \chi_A(x)) \geq 1 - \frac{1}{2^{2|x|}}$$

כלומר

$$\Pr_r (M^*(x, r) \neq \chi_A(x)) \leq \frac{1}{2^{2|x|}}$$

ויהי $p(|x|)$ הפולינום החוסם את זמן ריצת M^* על x . עבור $|x| = n$, M^* משתמשת במחרוזת של הטלות מטבע $\{0, 1\}^{p(n)}$ מהי ההסתברות ש r גורם ל M^* לטעות על קלט כלשבו באורך n ? מטרה:

$$\begin{aligned} \Pr_r [\exists x \in \{0, 1\}^n M^*(x, r) \neq \chi_A(x)] &< 1 \leq \\ &\leq \sum_{x \in \{0, 1\}^n} \Pr_r [M^*(x, r) \neq \chi_A(x)] \leq 2^n \cdot \frac{1}{2^{2n}} = \frac{1}{2^n} \ll 1 \end{aligned}$$

r יקרא "טוב" אם

$$\forall x \in \{0, 1\}^n M^*(x, r) = \chi_A(x)$$

ולמעשה הוכחנו כי קיים r טוב(למעשה, הראנו כי כמעט כל ה r הם טובים).
כעת נטען כי $A \in P/poly$:

המכונה הדטרמיניסטית שתכריע את A תהי M^* שרצה בזמן פולינומי, כאשר עבור קלט x באורך n העצה ש M^* תקבל היא r_n , עבור r_n שהינו "טוב" ל x באורך n . מהעובדה ש r_n הינו טוב עבור $n = |x|$ מקבלים ש $M^*(x, r_n)$ הינה מכונה פולינומית המכריעה את A ע"י שימוש בעיצה באורך פולינומי, ולכן מתקיימות דרישות $P/poly$ ולכן $A \in P/poly$.

הערה

$BPP \subsetneq P/poly$ כי $P/poly$ מכיל שפות לא כריעות.

הוכחה בשיטה הסתברותית

משפט

$$BPP \subseteq \Sigma_2 \cap \Pi_2$$

$$RP \subseteq BPP \quad RP \subseteq NP = \Sigma_1 \quad \text{ניזכר:}$$

הוכחה

תהיה $A \in BPP$. נרצה להראות כי קיים פרדיקט $\varphi(x, r, s)$ כך ש

$$\exists_s \forall_r \prod_{|s|, |r| < p(|x|)} \varphi(x, r, s) = 1 \iff x \in A$$

צעד ראשון יהיה להראות קיום של מכונת טיורינג הסתברותית M^* שהסתברות השגיאה שלה תהיה תלויה במספר הטלות המטבע שלה. כלומר, אם עבור קלט x , M^* מבצעת l הטלות מטבע, אזי נראה שעבור M^* מתקיים

$$\Pr_r [M^*(x, r) \neq \chi(x)] < \frac{1}{3l}$$

כזכור, $A \in BPP$, ותהי M המכונה ההסתברותית המובטחת מהוכחת BPP . M^* (כמו בשיעור הקודם) תהיה מכונה המריצה את M k פעמים (k יקבע בהמשך) ומחזירה תשובה ע"פ תוצאת רוב ההרצות. אם נסמן ב- w_i את המשתנה המקרי המציין שהייתה טעות בהרצה ה- i של M אזי:

$$\Pr_r [M^*(x, r) \neq \chi_A(x)] = \Pr_r \left[\frac{\sum_{i=1}^k w_i}{k} \geq \underbrace{\frac{1}{3} + \frac{1}{6}}_{=\frac{1}{2}} \right] \stackrel{\text{Chernof}}{\leq} e^{-2(\frac{1}{6})^2 \cdot k} = e^{-\frac{k}{18}}$$

נבחר $k = 18 \ln(3p^2(n))$ כאשר $p(n)$ הוא מספר הטלות המטבע של M . לכן מספר הטלות המטבע של M^* (שסימנו אותו בתור $l(n)$):

$$l(n) = k \cdot p(n) = 18p(n) \ln(3p^2(n))$$

נשים לב ש- $k \leq p(n)$ עבור n גדול די. לכן סה"כ:

$$\Pr_r [M^*(x, r) \neq \chi_A(x)] \leq e^{-\frac{k}{18}} = e^{-\ln(3p^2(n))} = \frac{1}{3p^2(n)} \leq \frac{1}{3kp(n)} = \frac{1}{3l(n)}$$

בהנתן $A \in BPP$, נתאר כעת בעיית הכרעה $\pi(\dots)$ באופן הבא: נסמן $s_i \in \{0, 1\}^l$,
 נתבונן בזוגות: $s = s_1, \dots, s_l$

$$\Pi_{\text{yes}} = \left\{ (x, s) \mid \forall_{r \in \{0, 1\}^l} \left[\bigvee_{i=1}^l (M^*(x, r \oplus s_i)) = 1 \right] \right\}$$

במילים: הגדרנו אוסף זוגות x, s כך שלכל r קיים s_i כך ש $M^*(x, r \oplus s_i) = 1$.
 נגדיר גם:

$$\Pi_{\text{no}} = \left\{ (x, s) \mid \Pr_{r \in \{0, 1\}^l} \left[\bigvee_{i=1}^l (M^*(x, r \oplus s_i)) = 0 \right] \geq \frac{1}{2} \right\}$$

עבור קלט x ל A נגדיר פונקציית מיפוי אקראית $f(x)$ המחזירה זוג (x, s) באופן הבא:
 בחר באקראי $s = s_1, \dots, s_l \in \{0, 1\}^l$ והחזר (x, s) .
 נרצה לטעון:

טענה 1: אם $x \in A$, $\Pr_s [f(x) \in \Pi_{\text{yes}}] > \frac{1}{2}$

טענה 2: אם $x \notin A$, $\Pr_s [f(x) \in \Pi_{\text{no}}] = 1$

ע"פ טענה 1:

$$x \in A \implies \Pr_s [\forall_r \varphi(x, r, s) = 1] > \frac{1}{2}$$

↓

$$\exists_s \forall_r [\varphi(x, r, s) = 1]$$

ע"פ טענה 2:

$$x \notin A \implies \forall_s \left[\Pr_r (\varphi(x, r, s) = 0) \geq \frac{1}{2} \right]$$

↓

$$\forall_s \exists_r \varphi(x, r, s) = 0$$

וכל זה אס"ם

$$\exists_s \forall_r \varphi(x, r, s) \implies x \in A$$

$x \oplus y^1$ משמעותו $x \text{ xor } y$

ולכן

$$x \in A \iff \exists_s \forall_r \varphi(x, r, s)$$

ולכן $A \in \Sigma_2$
 נשים \heartsuit שאם $A \in BPP$ אזי גם $\bar{A} \in BPP$. לכן ע"פ מה שראינו $\bar{A} \in \Sigma_2$ ולכן $a \in \Pi_2$, ולכן סה"כ קיבלנו

$$A \in BPP \implies A \in \Sigma_2 \cap \Pi_2$$

ולכן

$$BPP \subseteq \Sigma_2 \cap \Pi_2$$

נותר להראות נכונות טענות 1 ו 2 כדי לסיים.

הוכחת טענה 1

$$\begin{aligned} \Pr_s [f(x) \notin \Pi_{\text{yes}}] &= \Pr_s \left[\exists_r \left[\bigwedge_{i=1}^l M^*(x, r \oplus s_i) = 0 \right] \right] \leq \\ &\leq \sum_{r \in \{0,1\}^l} \Pr_{s=s_1, \dots, s_l} \left[\bigwedge_{i=1}^l M^*(x, r \oplus s_i) = 0 \right] = \dots \end{aligned}$$

כזכור $x \in A$

$$\begin{aligned} \dots &= \sum_{r \in \{0,1\}^l} \prod_{i=1}^l \Pr_{s_i} [M^*(x, r \oplus s_i) = 0] \leq \\ &\leq \sum_{r \in \{0,1\}^l} \left(\frac{1}{3l} \right)^l = 2^l \cdot \frac{1}{(3l)^l} < \frac{1}{2} \end{aligned}$$

(עבור $[M^*(x, \tilde{r}) = 0] < \frac{1}{3l}, x \in A$
 כלומר הראנו כי:

$$x \in A \implies \Pr_s [f(x) \in \Pi_{\text{yes}}] \geq \frac{1}{2}$$

הוכחת טענה 2

$x \notin A$, צ"ל שלכל s

$$\Pr_r \left(\underbrace{\bigvee_{i=1}^l (M^*(x, r \oplus s_i) = 0)}_{=\varphi(x, r, s)} \right) \geq \frac{1}{2}$$

יהי $s = s_1, \dots, s_l$ כלשהו.

$$\Pr_r [\varphi(x, r, s) = 0] = 1 - \Pr_r [\varphi(x, r, s) = 1] =$$

$$= 1 - \Pr_r \left[\left(\bigvee_{i=1}^l M^*(x, r \oplus s_i) \right) = 1 \right] \geq$$

$$\geq 1 - \sum_{i=1}^l \Pr_r (M^*(x, r \oplus s_i) = 1) \geq$$

$$\geq 1 - l \cdot \frac{1}{3l} \geq \frac{2}{3}$$

■

הערה

באופן אינטואיטיבי, ב BPP יש שגיאה דו צדדית, ולכן היינו צריכים להוסיף שני כמתים, שכן אחד הוריד את השגיאה מצד אחר.