

הבעיה: נתון מספר N . האם N ראשוני?

עובדה 1: לכל מספר ראשוני p ולכל $r \in \{1, \dots, p-1\}$, למשוואה $x^2 = r^2 \pmod{p}$ יש בדיוק שני פתרונות: $r, -r \pmod{p}$.

עובדה 2: לכל מספר פריק אי זוגי שאיננו חזקה של ראשוני N , למשוואה $x^2 = r^2 \pmod{N}$ יש לפחות 4 פתרונות שונים.

נתון אלגוריתם sqrt:

קלט: מספר ראשוני p ומספר $r^2 \pmod{p}$

פלט: פתרון אפשרי למשוואה $x^2 = s \pmod{p}$

אלגוריתם A בהנתן קלט $N > 2$:

1. אם N מספר זוגי או חזקה של ראשוני, החזר 0.

2. בחר בצורה רנדומית $r \in \{1, \dots, N-1\}$ וחשב $s = r^2 \pmod{N}$.

3. $r' = \text{sqrt}(N, s)$. אם $r' = r$ או $r' = -r \pmod{N}$ החזר 1. אחרת החזר 0.

מקרה א: N הוא מספר ראשוני. לפי עובדה 1, הפלט של sqrt הוא r או $-r \pmod{N}$, ולכן בהכרח נחזיר 1.

מקרה ב: N לא ראשוני.

מקרה ב.1: N הוא זוגי או חזקה של ראשוני. במקרה הזה היינו מחזירים 0 כבר בצעד 1.

מקרה ב.2: N איננו זוגי ואיננו חזקה של ראשוני. עבור כל s חשוב בצעד 2, קיימים r_1, r_2, r_3, r_4 שונים שיכולים לייצר את s .

$$\Pr[r = \text{sqrt}(N, s) \vee r = -\text{sqrt}(N, s)] \leq \frac{2}{4} = \frac{1}{2}$$

הגדרה - RP

$L \in RP$ אם קיימת מכונת טיורינג הסתברותית M כך ש:

$$x \in L \iff \Pr_r[M(x, r) = 1] \geq \frac{1}{2}$$

$$x \notin L \iff \Pr_r[M(x, r) = 0] = 1$$

הערות

1. $P \subseteq RP \subseteq NP$

2. אפשר להקטין את הסתברות השגיאה במקרה $x \in L$ ל $\frac{1}{2^{p(n)}}$ (כלומר את הסתברות ההצלחה ל $1 - \frac{1}{2^{p(n)}}$) ע"י הרצת M פעמים, והחזרת 1 אם לפחות אחת ההרצות החזירה 1 אחרת. כל עוד $p(n)$ פולינומי המכונה נשארת פולינומית.

הגדרה - BPP

$L \in BPP$ אם קיימת מכונת טיורינג הסתברותית M כך ש:

$$\forall_x \Pr_r [M(x, r) = \chi_L(x)] \geq \frac{2}{3}$$

כאשר

$$\chi_L(x) = \begin{cases} 1 & x \in L \\ 0 & x \notin L \end{cases}$$

הערות

1. $RP \subseteq BPP$

2. $BPP = coBPP$ כאשר $coBPP = \{L | \bar{L} \in BPP\}$

3. $NP = BPP?$ - הקשר לא ידוע, זו שאלה פתוחה.

תרגיל

הוכיחו שאם $NP \subseteq BPP$ אזי $NP = RP$.

פתרון

ידוע ש $RP \subseteq NP$. נראה שאם $NP \subseteq BPP$ אזי $NP \subseteq RP$.
נניח $NP \subseteq BPP \iff SAT \in BPP$. צ"ל $NP \subseteq RP$, מספיק להוכיח $SAT \in RP$.

\iff קיימת מ"ט פולינומית M' כך ש:

$$\forall_\varphi \Pr_r [M'(\varphi, r) = \chi_{SAT}(\varphi)] \geq \frac{2}{3}$$

ע"י הרצות חוזרות, נקבל אלגוריתם M כך ש:

$$\forall_\varphi \Pr_r [M(\varphi, r) = \chi_{SAT}(\varphi)] \geq 1 - \frac{1}{4n}$$

נבנה אלגוריתם M^* שבהינתן קלט φ :

1. אם $M(\varphi) = 0$, החזר 0 וסיים.

2. עבור כל משתנה x_i :

2.1 הצב $x_i = T$, צמצם את φ ל φ_T .

2.2 אם $M(\varphi_T) = 1$, המשך עם φ_T

2.3 אחרת, הצב $x_i = F$ וצמצם את φ ל φ_T .

3. הצב את השמת האמת שהתקבלה ב φ . אם היא מספקת - החזר 1. אחרת - החזר 0.

- אם $\varphi \notin SAT$ - האלגוריתם מחזיר 0 בהסתברות 1
- אם $\varphi \in SAT$ - אם כל הריצות של M החזירו תשובה נכונה, M^* בהכרח תחזיר תשובה נכונה.

$$\Pr \left[\begin{array}{c} \text{Some run of } M \\ \text{returns a wrong answer} \end{array} \right] \leq (n+1) \cdot \frac{1}{4n} = \frac{n+1}{4n} \leq \frac{1}{2}$$

לכל n .