תרגיל

הוכיחו שאם $NP \subseteq BPP$ אז $NP = RP$

פתרון

עלינו להראות ש $NP = RP$ כלומר: $NP \subseteq RP$, וגם $RP \subseteq NP$.

$NP \subseteq RP$: נכון באופן כללי שהוכח בהרצאה.

$RP \subseteq NP$: מספיק להראות לפי כך ששפה שהיא NP - שלמה נמצאת ב RP.
נראה זאת עבור SAT.

מהנתון ש $NP \subseteq BPP$ נובע כי $SAT \in BPP$ לכן קיימת מכ"ט הסתברותי M' הרצה בזמן פולינומי ומכריעה את SAT כך שמתקיים לכל x:

$$Pr[M'(x,r) = \chi_{SAT}(x)] \geq \frac{2}{3}$$

ע"י מספר פולינומי של הרצות חוזרות של M' ובחירה לפי רוב, ניתן לקבל מכ"ט הסתברותי M שרצה בזמן פולינומי ומכריעה את SAT כך שלכל x מתקיים:

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

כעת, נבנה מכ"ט הסתברותי M^* המכריעה את SAT בהכרעה הסתברותית של RP.
בהינתן קלט x ומחרוזת תדמית $r = (r_1, r_2, \dots, r_{n+1})$ המכונה M^* תפעל באופן הבא:

1. בדוק האם $M(x, r_1) = 0$ אם כן החזר 0.
2. אחרת, הצב 0 במשתנה v_i בנוסחה x ולמצא אותה ל x_0
אם $M(x_0, r_{i+1}) = 1$ המשך עם x_0
אחרת הצב 1 במשתנה v_i בנוסחה x ולמצא אותה ל x_1
והמשך עם x_1.
* אם שלב זה עושים עבור כל משתנה v_i בנוסחה x.
3. הצב את השמת האמת שהתקבלה מהשלב הקודם בנוסחה המקורית x. אם הנוסחה מסופקת החזר 1 אחרת החזר 0.

אם $x \notin SAT$ מכיוון שבכל מקרה M^* בודקת את השמת האמת שהתקבלה מהרצוקליה הרנדומית, הרי שבהכרח נחזיר 0 כיוון שלא ניתן לספק את x.

אם $x \in SAT$ אם בכל $n+1$ ההרצות של M החוצרה התשובה הנכונה נקבל השמת אמת שמספקת את x ולכן בשלב 3 נחזיר 1.
ההסתברות ש M^* תחזיר תשובה שגויה במקרה זה היא לכל היותר
ההסתברות ש M תטעה באחת מ $n+1$ ההרצות שלה ב M^*.
ההסתברות לטעות של M בהרצה בודדת היא לכל היותר $\frac{1}{4n}$.
לכן ההסתברות שנטעה באחת מ $n+1$ ההרצות של M במסגרת M^* היא לכל היותר $\frac{n+1}{4n} \leq \frac{1}{2}$ לפי חסם האיחוד.

לכן קיבלנו שעבור $x \in SAT$ מתקיים הדרוש.

סה"כ קיבלנו: $x \in SAT$ $\quad Pr[M^*(x,r) = 1] \geq \frac{1}{2}$

$x \notin SAT$ $\quad Pr[M^*(x,r) = 0] = 1$

$\Leftarrow SAT \in RP \Leftarrow NP \subseteq RP$.

בהינתן קלט $x = (A,B,C)$ האלגוריתם M פועל באופן הבא:

1. בחר וקטור בינארי r באורך n (מתוקבל על סרט הרנדומיות)
2. חשב: $P = A\cdot(Br) - Cr$
3. אם הוקטור P הוא וקטור האפס - נחזיר 1
אחרת נחזיר 0.

• קל לראות כי זמן הריצה אכן $O(n^2)$

נראה כי מתקיימים תנאי $co-RP$:

עבור $x = (A,B,C) \in MAT\text{-}VERIFY$ מתקיים:

$$P = A(Br) - Cr = (AB)r - Cr = (AB-C)r = 0$$

לכן:

$$\underline{Pr_r[M(x,r)=1] = 1}$$

עבור $x = (A,B,C) \notin MAT\text{-}VERIFY$ נשים $D = AB - C = (d_{ij})$

$$P = Dr = A(Br) - Cr = (p_1, p_2, \dots, p_n)^T$$

מכיוון ש $AB \neq C$, לכן קיים אלמנט ב-D שאינו 0.
נניח ש $d_{ij} \neq 0$ עבור i ו j מסוימים

עפ"י הגדרת כפל מטריצות מתקיים:

$$p_i = \sum_{k=1}^{n} d_{ik} r_k = d_{i1}\cdot r_1 + d_{i2} r_2 + \dots + d_{ij}\cdot r_j + \dots + d_{in} r_n = y + d_{ij}\cdot r_j$$

עבור y קבוע כלשהו

לפי נוסחת Bayes נקבל:

$$Pr[p_i = 0] = Pr[p_i = 0 \mid y = 0]\cdot Pr[y=0] + Pr[p_i = 0 \mid y \neq 0]\cdot Pr[y \neq 0]$$

מתקיים:

$$Pr[p_i = 0 \mid y = 0] = Pr[r_j = 0] = \frac{1}{2}$$

$$Pr[p_i = 0 \mid y \neq 0] = Pr[r_j = 1 \wedge d_{ij} = -y] \leq Pr[r_j = 1] = \frac{1}{2}$$

קיבלנו סה"כ:

$$Pr[p_i = 0] \leq \frac{1}{2}\cdot Pr[y=0] + \frac{1}{2}[y \neq 0]$$
$$= \frac{1}{2} Pr[y=0] + \frac{1}{2}[1 - Pr[y=0]] = \frac{1}{2}$$

לכן

$$\underline{Pr[M(x,r)=0]} = 1 - Pr[P = \vec{0}] = 1 - Pr[p_1 = 0 \wedge p_2 = 0 \wedge \dots \wedge p_n = 0]$$
$$\geq 1 - Pr[p_i = 0] \geq \underline{\frac{1}{2}}$$