אלגוריתמים הסתברותיים

מ"ט הסתברותית M היא:

1. מ"ט לא"ד המחליטה איזה מעבר לבצע ע"י הטלת מטבע אחיד.
2. מ"ט דטרמיניסטית המקבלת קלט נוסף r (על סרט מיוחד - סרט הרנדומיות) שהוא סדרת הטלות מטבע אקראיות שמתפלגות באופן אחיד.

המחלקה RP

$L \in RP$ אם קיימת מ"ט הסתברותית M הרצה בזמן פולינומי ומתקיים:

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

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

<u>הערות</u>:
1. $P \subseteq RP \subseteq NP$
2. ניתן להחליף את הקבוע $\frac{1}{2}$ בהגדרה בכל מספר בין $\frac{1}{p(|x|)}$ ל $1-\frac{1}{2^{p(|x|)}}$ עבור פולינום כלשהו ע"י אמפליפיקציה. (=מספיק שאחד קיבל ונחזיר שx בשפה).

המחלקה co-RP

$L \in co\text{-}RP$ אם קיימת מ"ט הסתברותית M הרצה בזמן פולינומי ומתקיים:

$$x \in L \Rightarrow \Pr_r [M(x,r)=1] = 1$$

$$x \notin L \Rightarrow \Pr_r [M(x,r)=0] \geq \frac{1}{2}$$

המחלקה BPP

נגדיר את הפונקציה האופיינית של x ב-L:

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

$L \in BPP$ אם קיימת מ"ט הסתברותית M שרצה בזמן פולינומי ומתקיים:

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

<u>הערות</u>:
1. $RP \subseteq BPP$
2. היחס בין BPP ו NP היא שאלה פתוחה.
3. ניתן להקטין את ההסתברות ל $1-\frac{1}{2^{p(|x|)}}$ עבור פולינום $p(\cdot)$ כלשהו ע"י הרצות חוזרות ובחירה לפי הרוב.
4. $BPP \subseteq P/Poly$
5. $BPP \subseteq \Sigma_2 \cap \Pi_2$

דוגמה לאלגוריתם הסתברותי - וידוא מכפלת מטריצות

נתונה השפה:

$MAT\text{-}VERIFY = \{ (A,B,C) \mid$ A,B,C מטריצות בגודל n×n כך שמתקיים $A \cdot B = C \}$

ניתן לוודא שייכות לשפה ע"י אלגוריתם שמחשב את מכפלת המטריצות A ו B ומשווה אותו ל C בזמן $O(n^3)$.

נראה אלגוריתם הסתברותי שרץ בזמן $O(n^2)$ ומקיים את התנאים של co-RP.

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

1. גרל וקטור בינארי r באורך n (מתקבל 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 $X = (A, B, C) \in \text{MAT-VERIFY}$ מתקיים:

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

לכן:

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

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

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

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

עפ"י הגדרת כפל מטריצות מתקיים:

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

עבור y קבוע כלשהו

לפי נוסחת Bayes נקבל:

$$Pr[P_i = 0] = Pr[P_i = 0 | y = 0]\cdot Pr[y = 0] + Pr[P_i = 0 | y \neq 0]\cdot Pr[y \neq 0]$$

מתקיים:

$$Pr[P_i = 0 | y = 0] = Pr[r_j = 0] = \frac{1}{2}$$

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

קיבלנו סה"כ:

$$\begin{aligned} Pr[P_i = 0] &\leq \frac{1}{2}\cdot Pr[y = 0] + \frac{1}{2}[y \neq 0] \\ &= \frac{1}{2} Pr[y = 0] + \frac{1}{2}[1 - Pr[y = 0]] = \frac{1}{2} \end{aligned}$$

לכן

$$\underline{Pr[M(x, r) = 0]} = 1 - Pr[P = \vec{0}] = 1 - Pr[P_1 = 0 \wedge P_2 = 0 \wedge \ldots \wedge P_n = 0]$$

$$\geq 1 - Pr[P_i = 0] \geq \underline{\frac{1}{2}}$$