

# אלגוריתמים ראנדומיים

## מודל - מכונת טיורינג הסתברותית

זוהי למעשה **מכונת טיורינג לא דטרמיניסטית** פולינומית כך שבכל מעבר של המכונה שאינו מוגדר באופן יחיד(בה"כ, במקרה זה קיימים בדיוק 2 מעברים אפשריים) המכונה מטילה מטבע, בסיכוי של  $\frac{1}{2}$  מבצעת מעבר ראשון, בסיכוי של  $\frac{1}{2}$  מבצעת מעבר שני. נאמר כי מכונת טיורינג הסתברותית  $M$  מקבלת את הקלט  $x$ , אם  $M(x)$  מחזיר לנו את התשובה הנכונה "בהסתברות גבוהה".

**לעומת זאת:** מ"ט  $M$  לא דטרמיניסטית מקבלת  $x$ , אם קיים מסלול בו  $M$  מקבלת את  $x$ .

המודל שתיארנו הוא מודל on-line.

נאמר כי מ"ט  $M$  הסתברותית, הרצה על קלט  $x$  מחזירה  $M(x)$  משתנה מקרי(מ"מ). בהנתן  $M$  כנ"ל, ניתן לעסוק במודל שקול(off-line): קיימת  $M'$  מ"ט דטרמיניסטית המקבלת כקלט זוג  $(x, r)$ , כאשר  $x$  הינו הקלט המקורי של  $M$  ו- $r$  הינה סדרת הטלות מטבע.  $M'(x, r)$  משתנה מקרי המתפלג באופן זהה ל- $M(x)$ .

## אבחנה

כדי שראנדומיות תהיה מועילה, צריך לשלב עליה מחיר - כלומר סיכוי לטעות.

## טענה

תהי  $M$  מ"ט הסתברותית לפתרון  $A$  אשר לכל  $x$  מחזירה את התשובה הנכונה בהסתברות  $\geq 1 - \epsilon$  (כלומר לא טועה). אזי קיימת מ"ט דטרמיניסטית  $M'$  הרצה בזמן זהה לזה של  $M$  ומכריעה את  $A$ .

## הוכחה

בהנתן  $M$  כנ"ל, נבנה  $M'$  כנ"ל באופן הבא:

$M'$  תבצע סימולציה של  $M$ , וכל פעם ש- $M$  מטילה מטבע,  $M'$  תניח כי התשובה המתקבלת היא 0.

אם קיים  $x$  עבורו  $M'$  מחזירה תשובה שגויה,  $M$  מקבלת את סדרת הטלות המטבע שכולן 0 בהסתברות  $\leq \frac{1}{2^{p(|x|)}}$  כאשר  $p(\cdot)$  הוא הפולינום החוסם את זמן ריצת המכונה  $M$ , ולכן  $M$  מחזירה תשובה נכונה בהסתברות  $> 1 - \frac{1}{2^{p(|x|)}}$ . כלומר  $M$  מחזירה תשובה נכונה בהסתברות  $> 1 - \epsilon$ , בניגוד להנחה שלנו ש- $M$  מחזירה תשובה נכונה בהסתברות  $> 1 - \epsilon$ .

# טעות חד צדדית - RP

## הגדרה

נאמר כי קבוצה  $A$  שייכת למחלקה  $(\text{Randomized Poly})RP$  אם קיימת מכונת טיורינג הסתברותית  $M$  הרצה כזמן פולינומי ומקיימת:

$$\forall x \in A \Pr_r (M(x, r) = 1) \geq \frac{1}{2}$$

$$\forall x \notin A \Pr_r (M(x, r) = 0) = 1$$

## טענה

$$RP \subseteq NP$$

## הוכחה

תהי  $L \in RP$ , צ"ל  $L \in NP$ .

**זכור:** אם  $L \in NP$  אז קיים מודא פולינומי  $v(\cdot)$  ופולינום  $p(\cdot)$  כך ש

$$\exists_y y < p(|x|), v(x, y) = 1 \iff x \in L$$

עבור  $L \in RP$  קיימת מכונת טיורינג דטרמיניסטית  $M$  המקבלת כקלט זוג  $(x, r)$  כך שתמקיים

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

ולכן

$$\boxed{x \in L \implies \exists_r (x, r) = 1}$$

ובאופן דומה

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

ולכן

$$\boxed{x \notin L \implies \forall_r M(x, r) = 0}$$

סה"כ

$$x \in L \implies \exists_r M(x, r) = 1 \quad x \notin L \implies \forall_r M(x, r) = 0$$

וביחד זה אומר ש

$$\boxed{x \in L \iff \exists_r M(x, r) = 1}$$

יהי  $M$  המוודא הפולינומי הנדרש בהגדרת  $NP$ , ו- $p(\cdot)$  הפולינום החוסם את זמן ריצת  $M$ , וכן  $r$  יהיה העד המשמש את המוודא הפולינומי הנדרש בהגדרת  $NP$ , ונשים לב כי למעשה קיבלנו  $L \in NP$ .

### נגדיר $RP1$

$L \in RP1$  אם קיימת מ"ט הסתברותית  $M$  ופולינום  $p(\cdot)$  כך ש:

$$x \in L \implies \Pr_r [M(x, r) = 1] > \frac{1}{p(|x|)}$$

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

### נגדיר $RP2$

$L \in RP2$  אם קיימים  $M$  ו- $p(\cdot)$  כנ"ל כך ש:

$$x \in L \implies \Pr_r [M(x, r) = 1] \geq 1 - 2^{-p(|x|)} = 1 - \frac{1}{2^{p(|x|)}}$$

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

טענה

$$RP1 = RP2$$

## הוכחה

ברור  $RP1 \subseteq RP2$ , צ"ל  $RP2 \subseteq RP1$ , קיימת מ"ט הסתברותית  $M_1$  ופולינום  $p(\cdot)$  כך ש:  
 תהי  $L \in RP1$ , אזי ע"פ הגדרת  $RP1$ , קיימת מ"ט הסתברותית  $M_1$  ופולינום  $p(\cdot)$  כך ש:

$$\forall x \in L \Pr_r [M_1(x, r) = 1] \geq \frac{1}{p(|x|)}$$

נגדיר מ"ט הסתברותית  $M_2$  באופן הבא:  
 $M_2(x)$  תריץ את  $M_1(x)$  פעמים (כל פעם עם  $r$  חדש), ואם אחת ההפעלות של  $M_1(x)$  החזירה 1 אזי  $M_2(x)$  תחזיר 1, אחרת תחזיר 0.  
 ההסתברות לטעות היא:

$$x \in L \implies \Pr_r [M_2(x, r) = 0] = (\Pr_r [M_1(x, r) = 0])^{t(|x|)} \leq \underbrace{\left(1 - \frac{1}{p(|x|)}\right)^{t(|x|)}}_{\text{probability of } M_2(x) \text{ mistake}} \leq \frac{1}{2^{p(|x|)}}$$

$$\left(1 - \frac{1}{p}\right)^{p \cdot \frac{t}{p}} \leq \left(\frac{1}{2}\right)^p$$

$$\left(1 - \frac{1}{p}\right)^{\frac{t}{p}} \leq \frac{1}{2}$$

$$2 \leq \left(1 - \frac{1}{p}\right)^{-1 \cdot \frac{t}{p}}$$

$$\boxed{1 \leq \frac{t}{p} \log_2 \left(1 - \frac{1}{p}\right)^{-1}}$$

$$t \geq p \cdot \frac{1}{\log_2 \left(1 - \frac{1}{p}\right)^{-1}} = \frac{p}{-\log_2 \left(1 - \frac{1}{p}\right)^{p \cdot \frac{1}{p}}} = \frac{p}{\underbrace{-\frac{1}{p} \log_2 \left(1 - \frac{1}{p}\right)^p}_{=\log_2 e^{-1}}} \geq \frac{p}{-\frac{1}{p} \cdot (-\log_2 e)} = \frac{p^2}{\log_2 e}$$

$$t(x) \geq \frac{p^2(x)}{\log_2 e}$$

מסקנה -  $L \in RP2$ .

# אלגוריתמים הסתברותיים עם טעות דו צדדית

## הגדרה

נאמר כי קבוצה  $A$  שייכת ל  $BPP$  (Bounded error Probability Polynomial time) אם קיימת מכונת טיורינג הסתברותית פולינומית  $M$  המקיימת:

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

כאשר

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

## אבחנות

$$RP \subseteq BPP$$

$$BPP \subseteq PSPACE \subseteq EXP$$

לא ידוע מה הקשר בין  $BPP$  ו  $NP$   
כזכור,  $RP \subseteq NP$

## טענה

תהי  $A \in BPP$ , אזי לכל פולינום  $p(\cdot)$  ישנה מכונת טיורינג הסתברותית  $M^*$  העוזרת בזמן פולינומי ומקיימת

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

## הוכחה

$A \in BPP$ , לכן קיימת  $M$  מכונת טיורינג הסתברותית שהסתברות ההצלחה שלה  $\leq \frac{2}{3}$  לפי המובטח בהגדרת  $M$ .  
נגדיר  $M^*(x)$ :

$$1. T \leftarrow 0$$

2. הרץ את  $M(x)$  פעמים  $k$  (קבע אח"כ) וקדם את  $T$  כל פעם שהתוצאה של  $M(x)$  היא 1.

3. אם  $T > \frac{k}{2}$  החזר 1, אחרת 0.

**חסם צ'רנוף:** יהיו  $x_1, \dots, x_k$  משתנים מקריים בלתי תלויים שווי התפלגות המקבלים ערכים ב  $\{0, 1\}$ , ותהי  $\mu$  התוחלת של כל אחד מהמשתנים. אזי עבור כל  $\varepsilon > 0$  מתקיים

$$\Pr \left[ \frac{\sum_{i=1}^k x_i}{k} \geq \mu + \varepsilon \right] \leq e^{-2\varepsilon^2 k} \approx \frac{1}{2^{2\varepsilon^2 k}}$$

נסמן ב  $\omega_1, \dots, \omega_k$  את המשתנים המקריים הבאים:

$$\omega_i = \begin{cases} 1 & M(x, r_i) \neq \chi_A(x) \\ 0 & \text{otherwise} \end{cases}$$

כלומר  $\omega_i = 1$  אם"ם בהרצה ה  $i$   $M(x, r_i)$  נתנה תשובה שגויה.  $\omega_i$  משתנים מקריים בלתי תלויים שווי התפלגות המקבלים ערכים ב  $\{0, 1\}$ , ו  $\mu(\omega_i) \leq \frac{1}{3}$

כדי ש  $M^*$  תטעה צריך להתקיים  $\frac{\sum \omega_i}{k} > \frac{1}{2}$ , כלומר

$$E \left[ \frac{\sum \omega_i}{k} \right] \leq \frac{1}{3}$$

כעת ע"פ צ'רנוף:

$$\Pr [M^*(x, r) \neq \chi_A(x)] = \Pr \left[ \frac{\sum \omega_i}{k} > \frac{1}{2} \right] = \Pr \left[ \frac{\sum \omega_i}{k} > \underbrace{\frac{1}{3}}_{\mu} + \underbrace{\frac{1}{6}}_{\varepsilon} \right] \leq e^{-2 \cdot \left(\frac{1}{6}\right)^2 \cdot k} = e^{-\frac{k}{18}}$$

אנו רוצים

$$e^{-\frac{k}{18}} \leq 2^{-p(|x|)}$$

למשל, אם נבחר  $k = 18p(|x|)$ , נקבל

$$e^{-\frac{k}{18}} = e^{-p(|x|)} < 2^{-p(|x|)}$$

■