

שיעור 6 - 13.04.2010

חשוב יעיל: כל שפה שאפשר לפתור על ידי מ"ט דטרמיניסטית שרצה בזמן פולינומי.
הגדרה: מ"ט הסתברותית:

- Q - סט מצבים.
- q_{init} - מצב התחלתי.
- q_{acc} - מצב מקבל.
- q_{rej} - מצב דוחה.
- סרטים:

- סרט קלט (כרגיל).
- סרט עבודה (כרגיל).

◦ סרט מטבעות: סרט אינסופי, מאוחל במחרוזות אקראיות.

סימון: אם M מ"ט הסתברותית, נסמן ב- $M(x, r)$ את התשובה ש- M נותנת על הקלט x , כשנותנים לה את המטבעות r . בה"כ, האורך של r הוא זמן הריצה של המכונה על הקלט x : $r \in \{0, 1\}^{T(n)}$.

הגדרה: נאמר ששפה L שייכת למחלקה $BPP_{\alpha, \beta}$, $0 \leq \alpha < \beta \leq 1$, אם קיימת מ"ט הסתברותית $M(x, r)$ שרצה בזמן פולינומי, ולכל $x \in L$, $\Pr_r[M(x, r) = 1] \geq \beta$, ולכל $x \notin L$, $\Pr_r[M(x, r) = 1] < \alpha$.

הגדרה:

$$BPP = BPP_{\frac{1}{3}, \frac{2}{3}}$$

$$RP = BPP_{0, \frac{1}{2}}$$

מה הסתברות הקבלה?

$x \notin L$	$x \in L$	
0	1	P חישוב דטרמיניסטי
0	> 0	NP חישוב לא דטרמיניסטי
$\leq \frac{1}{3}$	$\geq \frac{2}{3}$	BPP
0	$\geq \frac{1}{2}$	RP

דוגמה לאלגוריתם הסתברותי: PM (Perfect matching)

הבעיה: האם קיים זיווג מושלם בגרף דו-צדדי?

הקלט: גרף דו-צדדי $G = (V_1, V_2, E)$, $E \subseteq V_1 \times V_2$, $|V_1| = |V_2| = n$.
הקלט בשפה $\Leftrightarrow$ יש זיווג מושלם בגרף.

אפשר לפתור בעיה זו עם אלגוריתם זרימה, ולכן היא ב- P.
נראה שהיא ב- RP (למרות שזה ברור כי $P \subseteq RP$):

האלגוריתם:

1. בונים מטריצה $B_{n \times n}$, כך ש- $B_{ij} = \begin{cases} 0 & (i, j) \notin E \\ x_{ij} & (i, j) \in E \end{cases}$, כאשר x_{ij} משתנה.

2. לכל i, j בוחרים $a_{ij} \in_{\mathbb{R}} \{1, 2, \dots, 2n\}$ (באופן אקראי), ואנחנו מחליפים כל x_{ij} ב- a_{ij} .
מקבלים מטריצה $A_{n \times n}$.

3. מחשבים את $\det A$. אם היא 0, אזי אין זיווג מושלם. אחרת, יש זיווג מושלם.

נכונות:

$\det B = \sum_{\pi \in S_n} \text{sign}(\pi) \cdot x_{1, \pi(1)} \cdots x_{n, \pi(n)}$. כלומר, $\det B$ הוא פולינום במשתנים $x_1, \dots, x_n$, מולטי-

לינארי מדרגה טוטלית לכל היותר n .

משפט (שורץ-ציפלי): אם $p(x_1, \dots, x_m)$ פולינום ב- m שאינו זהותית 0 משתנים מדרגה

טוטלית לכל היותר D מעל שדה F , ואם $S \subseteq F$, אז $\Pr_{a_1, \dots, a_m \in S} [p(a_1, \dots, a_m) = 0] \leq \frac{D}{|S|}$.

נוכיח את המשפט בהמשך.

מצב 1: אין זיווג מושלם בגרף.
 לכל π יש i כך ש- $(i, \pi(i)) \notin E$, ואז $b_{i, \pi(i)} = 0$, ואז המונום נהרג.
 לכן, $(\det B)(x_{11}, \dots, x_{nn}) \equiv 0$.

מצב 2:

קיימת פרמוטציה $\pi: [n] \rightarrow [n]$, כך ש- $(i, \pi(i)) \in E$ לכל $i \in [n]$.
 לכן, כל פרמוטציה π שמייצגת זיווג מושלם בגרף G , תורמת את מונום המתאים לה:
 $\text{sign}(\pi) \cdot x_{1, \pi(1)} \cdots x_{n, \pi(n)}$.
 המונומים לא יכולים לבטל אחד את השני, בגלל שלכל פרמוטציה כזו יהיו משתנים שונים,
 ולכן הפולינום לא יהיה זהותית 0.

בהינתן $S = \{1, \dots, 2n\}$, לפי שוורץ-ציפיל, $\Pr_{a_1, \dots, a_{2n} \in S}[(\det B)(a_1, \dots, a_{2n})] \leq \frac{n}{|S|} = \frac{1}{2}$.
 לכן: אם אין זיווג מושלם בגרף, $\Pr_r[M(x, r)] = 0$. אם יש זיווג מושלם בגרף, $\Pr_r[M(x, r)] \geq \frac{1}{2}$.
 לכן, $PM \in RP$.

מעבר לזה: יודעים לחשב דטרמיננטה במקביל מהר, ולכן זה נותן אלגוריתם הסתברותי מקבילי
 ל- PM . לא ידוע אלגוריתם דטרמיניסטי מקבילי מהיר ל- PM .

טענה: $P \subseteq RP \subseteq NP$.

הוכחה:

1. $P \subseteq RP$ - כל אלגוריתם דטרמיניסטי הוא גם הסתברותי.
2. $RP \subseteq NP$: $L \in RP$ נפתרת על ידי מ"ט $M(x, r)$. M היא פתרון NP ל- L : אם $x \in L$ אזי
 $\Pr_r[M(x, r) = 1] \geq \frac{1}{2} > 0$, כלומר $\exists w. M(x, w) = 1$. ואם $x \notin L$ אזי $\Pr_r[M(x, r) = 1] = 0$, ולכן
 $\forall w. M(x, w) = 0$.

אמפליפיקציה של שגיאה חד-צדדית

טענה: אם $L \in BPP_{0, \frac{1}{n}}$, אזי $L \in BPP_{0, 1-e^{-n^2}}$.

הוכחה:

תהי $L \in BPP_{0, \frac{1}{n}}$. אזי יש מ"ט M , $M(x, r)$ פולינומית כך ש- $\Pr_r[M(x, r) = 1] \geq \frac{1}{n}$ ל- $x \in L$
 ו- $\Pr_r[M(x, r) = 1] = 0$ ל- $x \notin L$.
 נבנה אלגוריתם חכם M' על קלט x : יבחר $\bar{r} = r_1, \dots, r_T$ באופן ב"ת, יריץ את $M(x, r_i)$
 ל- $i = 1, \dots, T$, ויקבל אם ורק אם אחד מהם קיבל.
 אם $x \notin L$, אזי $\Pr_r[M'(x, \bar{r}) = 1] = 0$, כי לכל i , $M(x, r_i) = 0$. אם $x \in L$,
 $\Pr_{\bar{r}}[M'(x, \bar{r}) = 0] = \Pr_{r_1, \dots, r_T}[\forall i. M(x, r_i) = 0] \stackrel{\text{בלתי תלויים}}{=} \prod_{i=1}^T \Pr_{r_i}[M(x, r_i) = 0] \leq \left(1 - \frac{1}{n}\right)^T \approx e^{-\frac{T}{n}}$.
 ניקח $T = n^3$, ונקבל $\Pr_{\bar{r}}[M'(x, \bar{r}) = 0] \leq e^{-n^2}$ מש"ל.

אמפליפיקציה לשגיאה דו-צדדית

טענה: אם $L \in BPP_{\alpha, \alpha + \frac{1}{n}}$, אזי $L \in BPP_{2^{-n^2}, 1-2^{-n^2}}$.

הוכחה:

ניקח $L \in BPP_{\alpha, \alpha + \frac{1}{n}}$, הנפתרת על ידי מ"ט $M(x, r)$, כך שמקבלת או דוחה בהסתברויות
 המתאימות.
 נבנה מ"ט חדשה M' : מטילה $\bar{r} = r_1, \dots, r_T$ באופן ב"ת, ומחשבת את $M(x, r_i)$. היא רואה את
 האחוז β של ההרצות שקיבלו. אם $\beta > \alpha + \frac{1}{2n}$ - תקבל. אחרת, תדחה.

משפט (צ'רנוף): אם $X_1, \dots, X_n$ מ"מ בינריים ב"ת, ו- $E(X_i) = p$ $\forall i$ (באופן שקול:

$$\Pr\left[\left|\sum_{i=1}^n X_i - pn\right| > \delta \cdot (pn)\right] \leq e^{-\frac{\delta^2 pn}{4}}, \text{ אזי } (\Pr[X_i=0]=1-p \text{ ו- } \Pr[X_i=1]=p)$$

ההסתברות שכשעושים n ניסיונות ב"ת, נסטה מהממוצע יורדת אקספוננציאלית ב- $\delta^2 p$.

נחזור לניתוח של המכונה M' .

נניח $x \in L$. נסמן מ"מ: $X_i = \begin{cases} 1 & M(x, r_i) = 1 \\ 0 & \text{אחרת} \end{cases}$. נקבל מ"מ $X_1, \dots, X_T$ בינריים, ב"ת, כך

ש- $E(X_i) = \Pr[X_i=1] = p \geq \alpha + \frac{1}{n} \geq \alpha + \frac{1}{2n}$. M' טועה עם עונה לא, וזה קורה אם

$$\sum X_i \leq \left(\alpha + \frac{1}{2n}\right) \cdot T = \Pr\left[\sum X_i \leq \left(\alpha + \frac{1}{2n}\right) T\right] \leq \Pr\left[\left|\sum X_i - p \cdot T\right| > \frac{1}{2n} \cdot T\right] \stackrel{\text{צ'רנוף}}{\leq} 2^{-\Omega\left(\frac{T}{n^2}\right)}$$

$$. p T - \sum X_i \geq \frac{1}{2n} T \text{ ולכן } p T \geq \left(\alpha + \frac{1}{n}\right) \cdot T$$

ובפרט, $BPP_{\frac{1}{3}, \frac{2}{3}}$, $BPP_{2^{-n}, 1-2^{-n}}$ ו- $BPP_{\frac{1}{10}, \frac{1}{10} + \frac{1}{n}}$ כולם מבטאים את אותה מחלקה.

כל עוד הפער לא זניח ($\frac{1}{\text{Poly}}(n)$), אפשר לעשות אמפליפיקציה ולהוריד את השגיאה להיות אקספוננציאלית קטנה.

טענה: $RP \subseteq BPP$.

$$L \in BPP_{\frac{1}{3}, \frac{2}{3}} \Leftrightarrow L \in BPP_{2^{-n}, 1-2^{-n}} \Leftrightarrow L \in BPP_{0, \frac{1}{2}} \Leftrightarrow L \in RP$$

נוכיח את משפט צ'רנוף:

אי שוויון מרקוב: אם X מ"מ, $X \geq 0$, אזי $\Pr[X \geq A] \leq \frac{E(X)}{A}$.

$$E(X) = \sum_i i \cdot \Pr[X=i] \geq \sum_{i \geq A} i \cdot \Pr[X=i] \geq A \cdot \sum_{i \geq A} \Pr[X=i] = A \cdot \Pr[X \geq A]$$

משפט: אם $X_1, \dots, X_n$ מ"מ בינריים ב"ת, $E(X_i) = p$, $\mu = p \cdot n$, ואם $\delta > 0$, ו- $X = \sum_{i=1}^n X_i$, אזי

$$\Pr[X \leq (1-\delta)\mu] \leq e^{-\frac{\delta^2 \mu}{2}}$$

$$\Pr[X \leq (1-\delta)\mu] = \Pr[-X \geq -(1-\delta)\mu] \stackrel{\forall t}{=} \Pr[-tX \geq -(1-\delta)t\mu] =$$

$$= \Pr\left[e^{-tX} \geq \underbrace{e^{-(1-\delta)t\mu}}_A\right] \stackrel{\text{מרקוב}}{\leq} \frac{E(e^{-tX})}{e^{-(1-\delta)t\mu}}$$

באופן כללי: $e^{-tX_i} = e^{-t(X_1 + \dots + X_n)} = \prod e^{-tX_i}$, וכל e^{-tX_i} ב"ת. לכן:

$$\Pr[X \leq (1-\delta)\mu] \leq \dots \leq \frac{E(e^{-tX})}{e^{-(1-\delta)t\mu}} = \frac{\prod_{i=1}^n E(e^{-tX_i})}{e^{-(1-\delta)t\mu}}$$

$$. e^{-t} - 1 = -\delta \Leftrightarrow e^{-t} = 1 - \delta \Leftrightarrow t = \ln \frac{1}{1-\delta} \text{ נבחר } t > 0 \text{ באופן הבא:}$$

נתונים לנו $X_1, \dots, X_n$ מ"מ בינריים, ויכול להיות שהם תלויים. $E(X_i) = p$. שואלים: מה ההסתברות ש-

$X = \sum_{i=1}^n X_i$ שונה מהותית מהתוחלת $p \cdot n$? אם אין נתונים נוספים על $X_1, \dots, X_n$, אפשר להשתמש רק

במרקוב: $\Pr[X \geq A] \leq \frac{E(X)}{A}$. אם אנחנו יודעים שהם לחלוטין ב"ת, אז אפשר להשתמש בצ'רנוף.

הגדרה: $X_1, \dots, X_n$ בלתי תלויים בזוגות אם לכל $X_i, X_j, i \neq j$ ב"ת.
דוגמה:

	X_1	X_2	X_3
$\frac{1}{4}$	0	0	0
$\frac{1}{4}$	0	1	1
$\frac{1}{4}$	1	0	1
$\frac{1}{4}$	1	1	0

אזי $\forall i. E(X_i) = \frac{1}{2}$. כל זוג מתפלג אחיד על $[0, 1]^2$. השלישייה לא אחידה, מחמיצה 4 מחרוזות

מ-8 אפשרויות.

הגדרה: מ"מ $X_1, \dots, X_n$ הם **ב"ת ב-k-יות** אם לכל $1 \leq i_1 < \dots < i_k \leq n$, המ"מ $X_{i_1}, \dots, X_{i_k}$ הם ב"ת.

צ'בישב: אם $X_1, \dots, X_n$ ב"ת בזוגות, δ קבוע, אזי $\Pr\left[\left|\sum X_i - \mu\right| \geq \delta \cdot \mu\right] \leq \Omega\left(\frac{1}{\mu}\right)$.

צ'רנוף דורש שהם יהיו ב"ת לחלוטין.