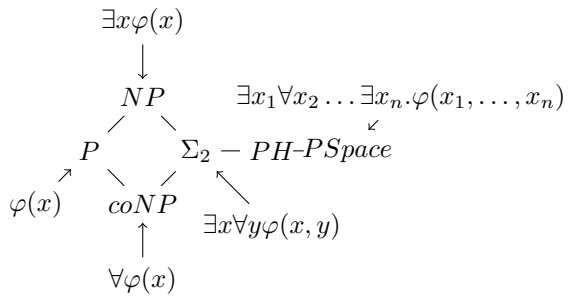
סיבוכיות – הרצאה 6

כל העולם הוא חישוב אחד גדול

29.3.11



ראינו $TQBF \in PSpace$.

משפט. $TQBF$ היא שלמה ב- $PSpace$.

הוכחה. נקבע $A \in PSpace$ כלשהי. צריכים להראות $A \leq_{\mathrm{p}} TQBF$. נראה אפילו $A \leq_L TQBF$. בהינתן קלט $x \in \{0,1\}^n$ ל- A נבנה נוסחאת $TQBF$ φ כך ש- $x \in A \Leftrightarrow \varphi \in TQBF$.
נסתכל על A והקלט $x \in \{0,1\}^n$. מגדיר את גרף הקונפיגורציות $G = (V, E)$ של A על x. $|V| = 2^{p(n)}$, $p(n)$ פולינום,

$$Reach(q_{init}, q_{acc}, \underbrace{p(n)}_{\text{צעדים } 2^{p(n)}}) \Leftrightarrow x \in A$$

תזכורת. $Reach(v_1, v_2, t) = 1 \Leftrightarrow$ יש מסלול בגרף הקונפיגורציות מ- v_1 ל- v_2 תוך $2^t \geq$ צעדים.

ננסה לתרגם לפסוק.
ניסיון 1: עבור $t = 0$, $Reach(v_1, v_2, 0) = 1 \Leftrightarrow$ אפשר לעבור מ- v_1 ל- v_2 בגרף הקונפיגורציות בצעד 1. וזה אפשר לתרגם לפסוק במשתנים: x, v_1, v_2 ותאור של A.
עבור t:

$$Reach(v_1, v_2, t+1) = \exists v_{mid} : Reach(v_1, v_{mid}, t) \wedge Reach(v_{mid}, v_2, t)$$

הפרוצדורה יוצרת פסוק SAT. הפסוק ספיק $\Leftrightarrow$ יש מסלול מ- v_1 ל- v_2 באורך לכל היותר 2^t.

מה הבעיה? אין כאן כמתי לכל (אם היינו מצליחים היינו עושים רדוקציה ל- SAT ואז היינו מקבלים $PSpace = NP$). נסמן $L(t)$ פלט של הפסוק שנוצר ב- $Reach(v_1, v_2, t)$:

$$L(t) = 2L(t-1) + p(n)$$

$$L(t) \geq 2^{p(n)}$$

לכן הרדוקציה שלנו אקספוננציאלית.
נסיון :

$$\begin{aligned} Reach(v_1, v_2, t+1) = \exists v_{mid}\ \forall i\ \exists A, B \\ ((i=0) \rightarrow (A = v_1) \wedge (B = v_{mid})) \wedge \\ ((i=1) \rightarrow (A = v_{mid}) \wedge (B = v_2)) \wedge \\ Reach(A, B, t) \end{aligned}$$

נראה: נכונות, אורך הפסוק קצר, אפשר לייצר אותו מהר.
נכונות של $Reach$:
$t = 0$ ברור.
נניח ל- t נוכיח ל- $t+1$.
יש מסלול מ- v_1 ל- v_2 באורך $2^{t+1} \geq$ $\Leftrightarrow$ יש קודקוד v_{mid} באמצע כך ש- $Reach(v_1, v_{mid}, t) \wedge Reach(v_{mid}, v_2, t)$.
אם יש כזה v_{mid} הפסוק ספיק (בודקים).
אם הפסוק ספיק אז יש v_mid כך ש- $v_{mid} \rightsquigarrow v_2$ ו- $v_1 \rightsquigarrow v_{mid}$ ולכן גם הכיוון השני נכון.
לכן, הרדוקציה מ- A ל- $TQBF$ נכונה.
נסמן ב- $L(t)$ את אורך הפסוק.

$$L(t) = O(p(n)) + L(t-1)$$

$$L(t) = O(t \cdot p(n))$$

$$L(p(n)) = O(p^2(n))$$

לכן נוסחא בגודל פולינומי.
נכתוב תכונית שתיצור את הפסוק ב- $LogSpace$.
נסמן:

$$\begin{aligned} S(t) = \exists v_{mid}\ \forall i\ \exists v_{t-1}, w_{t-1} \\ ((i=0) \rightarrow (v_{t-1} = v_t) \wedge (w_{t-1} = v_{mid})) \wedge \\ ((i=1) \rightarrow (v_{t-1} = v_{mid}) \wedge (w_{t-1} = w_t)) \end{aligned}$$

□

$v_{p(n)} = q_{init}$
$w_{p(n)} = q_{acc}$
for $t = p(n), \ldots, 1$ **do**
  print $S(t)$ ב- $\log$
end for
$Reach(v_1, w_1, 0)$ דורש מחשבה שאכן אפשר לחשב ב- $O(\log(|v|)$ מקום

יש חומרה שמייצרת אקראיות אמיתית ולכן מ"ט שמשתמשת באקראיות זו מכונה פיזיבילית.
האם ייתכן שהכוח של מכונות כאלה הוא יותר חזק? האם ייתכן שפותרות את SAT?

נעשה ניסיון ראשון לפתור את $3SAT$ עם אלגוריתם הסתברותי. Schöning 1999.
$\varphi = \bigwedge_{i=1}^{m} c_i$ כאשר $c_i = (l_{i1} \vee l_{i2} \vee l_{i3})$.
אפשר לעבור על כל ההשמות האפשריות וזה ייקח 2^n זמן. רוצים אלגוריתם הסתברותי שירוץ בזמן $(\frac{4}{3})^n \sim (\frac{4}{3})^n$ (כלומר כפול איזשהו פולינום ב- n). לכל קלט נרצה שהסתברות השיגאה תהיה אקספוננציאלית קטנה.
נסתכל על השפה הבאה: $L = Prime$, $x \Leftrightarrow x \in L$ ראשוני. נסתכל על אלגוריתם שתמיד עונה לא. כמעט תמיד (כמעט לכל קלט) הוא צודק. כי יש בערך $\theta(1/n)$ ראשוניים. אבל עדיין זה אלגוריתם לא טוב כי לא באמת נותן תשובה מעניינת. מצד שני הוא לא באמת בוחר משהו הסתברותי.
האלגוריתם:
נבחר השמה $a_1, \ldots, a_n$ באקראי. נריץ לולאה $3n$ פעמים. אם ההשמה הנוכחית מספקת, נעצור ונקבל. אחרת נמצא פסוקית שלא מסתפקת בהשמה (למשל הראשונה שלא מספתקת) נבחר משתנה באקראי מהמשתנים בפסוקית ונהפוך את הערך שלו.

טענה. האלגוריתם לוקח $O(n)$ זמן. אם הפסוק לא ספיק תמיד עונה לא. אם הפסוק ספיק אז נענה כן בהסתברות $\Omega(\frac{1}{\sqrt{n}}(\frac{3}{4})^n)$ שזה בכל זאת יותר טוב להגריל השמה שזה יצליח בהסתברות $O(2^{-n})$.

אם הוכחנו את הטענה, נחזור $(\frac{4}{3})^n poly(n)$ פעמים על האלגוריתם ונקבל $\Leftrightarrow$ אלת מההשמות קיבלה.
זמן ריצה: $(\frac{4}{3})^n poly(n)$. אם $x \notin L$ תמיד נענה לא.
אם $x \in L$:

$$\mathbb{P}(\text{נענה כן בניסיון בודד}) \geq \frac{1}{\sqrt{n}}(\frac{3}{4})^n$$

נסמן: $p := \frac{1}{\sqrt{n}}(\frac{3}{4})^n$.

$$\mathbb{P}(\text{נענה לא בניסיון בודד}) = 1 - p$$

$$\mathbb{P}(\text{נענה לא ב-}T\text{נסיונות ב"ת}) \leq (1-p)^T \leq e^{-pT} \underset{T=\frac{n}{p}}{=} e^{-n}$$

הוכחה. אם הפסוק לא ספיק ברור שהאלגוריתם לא ימצא השמה מספקת.
נניח ש- φ ספיק. תהי a^* השמה מספקת. נגדיר מרחק בין השמות $d(a,b)$ - מספר המשתנים שמקבלים ערך שונה בשתי ההשמות.
עבור $0 \leq t \leq n$ בהסתברות $p_t = \frac{\binom{n}{k}}{2^n}$ נגריל השמה a כך ש- $d(a, a^*) = t$.

אם לא ספיק, האלגוריתם בוחר פסוקית ארביטררית שלא מסתפקת ב- a. הפסוקית כמובן מסתפקת ב- a^*. לכן יש משתנה (משלושת המשתנים של הפסוקית) שעליו a, a^* נותנים ערכים שונים.
בהסתברות לפחות $\frac{1}{3}$ נבחר אותו ואז המרחק יתקצר ב-1. בהסתברות לכל היותר $\frac{2}{3}$ נבחר משתנה והמרחק יגדל ב- 1.
מה ההסתברות שב- $3t$ צעדים עברנו ב- 0 (כלומר מצאנו את a^*)?
יש לנו $3t$ צעדים. מותר לנו לטעות t פעמים ולצדוק $2t$ פעמים.

$$\mathbb{P}(\text{נצליח ב-}3t\text{ עצדים}) \geq \binom{3t}{t}(\frac{2}{3})^t(\frac{1}{3})^t$$

מנוסחאת סטירלינג:

$$\binom{3t}{t} \approx \frac{1}{\sqrt{t}}\frac{3^{3t}}{2^{2t}}$$

ואז

$$\mathbb{P}(\text{הצלחנו}|t\text{ התחלנו ממרחק}) \geq \binom{3t}{t}(\frac{2}{3})^t(\frac{1}{3})^t \approx \frac{1}{\sqrt{t}}\frac{3^{3t}}{2^{2t}}\frac{2^t}{3^{3t}} = \frac{1}{\sqrt{t}2^t}$$

$$\mathbb{P}(\text{הצלחנו} = \sum_{t=0}^{n}\frac{\binom{n}{t}}{2^n}\frac{1}{\sqrt{t}}2^{-t} = \frac{1}{\sqrt{n}}2^{-n}\sum_{t=0}^{n}\binom{n}{t}2^{-t} = \frac{1}{\sqrt{n}} = \frac{1}{2^n}(\frac{3}{2})^n = \frac{1}{\sqrt{n}}(\frac{3}{4})^n$$

□

אחרי שראינו דוגמא, נגדיר באופן פורמלי:

הגדרה. מכונת טיורינג הסתברותית:

- סרט קלט $(\leftrightarrow, R)$.
- סרט עבודה $(\leftrightarrow, RW)$.
- סרט אקראיות (שיודע להגריל דברים).

נאמר שמכונת טיורינג הסתברותית מקבל קלט x עם אקראיות y אם $M(x,y)$ מקבל במצב מקבל.

הגדרה. נאמר ששפה $L \in RTime(T(n))$ אם קיימת מכונת טיורינג הסתברותית M כך ש-

$$x \in L \Rightarrow \mathbb{P}_y(M(x,y) = 1) > \frac{1}{2}$$

$$x \notin L \Rightarrow \mathbb{P}_y(M(x,y) = 1) = 0$$

ומתקיים:

1. $|y| \leq T(|x|)$.
2. זמן הריצה של M על x עם אקראיות y הוא לכל היותר $T(|x|)$.

הערה. נשים לב שההסתברות תלויה רק במטבעות ולא בקלט עצמו.

הגדרה. נאמר כי $L \in \underset{\alpha,\beta}{BPTime}(T(n))$ אם יש מכונת טיורינג הסתברותית M כך ש-

- $|y| \leq T(|x|)$.
- זמן הריצה $\geq T(|x|)$.
-

$$x \in L \Rightarrow \mathbb{P}_y(M(x,y)=1) \geq \beta$$

$$x \notin L \Rightarrow \mathbb{P}_y(M(x,y)=1) \leq \alpha$$

הגדרה.

$$RP = RTime(poly) = \underset{0,\frac{1}{2}}{BPTime}(poly)$$

$$BPP_{\alpha,\beta} = \underset{\alpha,\beta}{BPTime}(poly)$$

נרצה להשוות בין P, NP, RP, BPP.
ברור מאוד ש- $P \subseteq NP$.
כמו כן, קל להבחין $P \subseteq RP$, $P \subseteq BPP$. למעשה P פותר עם הסתברות לשגיאה 0 והסתברות להצלחה 1. אז פשוט נתעלם לגמרי מסרט האקראיות.
לא קשה לוודא ש- $BPP_{0,\frac{2}{3}} \subseteq BPP_{\frac{1}{3},\frac{2}{3}}$. מדוע? נשתמש באותו האלגוריתם. אם הוא פותר בהסתברות שגיאה 0 בפרט התסברות השגיאה שלו קטנה מ- $1/3$.

טענה. אס $L \in BPP_{0,\frac{1}{n}}$ אז $L \in BPP_{0,1-2^{-n}}$.

כלומר בהינתן הסתברות קטנה להצלחה נוכל למצוא אלגוריתם עם הסתברות אקפסוננציאלית קטנה לכישלון.

הוכחה. נניח M פותרת את L ב- $BPP_{0,\frac{1}{n}}$.

$$x \in L \Rightarrow \mathbb{P}_y(M(x,y)=1) \geq \frac{1}{n}$$

$$x \notin L \Rightarrow \mathbb{P}_y(M(x,y)=0) = 0$$

נבנה אלגוריתם חדש M'. נריץ את M $T = O(n)$ פעמים ב"ת. נקבל $\Leftrightarrow$ אחרת ההרצות מקבלת

$$x \notin L \Rightarrow \mathbb{P}_{y_1,\ldots,y_T}(M' \text{ מקבלת}) = 0$$

כי לכל y_i $M(x,y_i)$ דוחה.

$$\begin{aligned} x \in L \Rightarrow \mathbb{P}_{y_1,\ldots,y_T}(M'(x,y_1,\ldots,y_T)=0) = \\ = \mathbb{P}(\forall 1 \leq i \leq T(M'(x,y_i)=0) \underset{\text{ב"ת}}{=} \prod \mathbb{P}(M'(x,y_i)=0) \leq \\ \leq \prod(1-\frac{1}{n}) = (1-\frac{1}{n})^T \leq e^{-T/n} \end{aligned}$$

נבחר $T = n + \frac{1}{\varepsilon}$. אז $e^{-T/n} \leq \varepsilon$. □

נרצה להראות:

טענה. $RP \subseteq NP$.

נשים לב:

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

$$NP = BPP_{0,2^{-m}}$$

כאשר m הוא מספר המטבעות.
נוכל לחשוב על סרט העד של המכונה שפותרת את הבעיה ב- NP כסרט הניחוש של BPP.
נכתוב:

$$L \in NP$$

אז:

$$x \notin L \Rightarrow \mathbb{P}_y[M(x,y) = 1] = 0$$

$$x \in L \Rightarrow \exists y[M(x,y) = 1]$$

נרכז הכל בטבלה:

	$x \notin L$	$x \in L$
NP	0	≥ 1
RP	0	$\geq \frac{1}{2}2^m$
BPP	$\leq \frac{1}{3}2^m$	$\geq \frac{2}{3}2^m$
P	0	2^m

הוכחה. תהי $L \in RP$. אז קיימת $M(x,y)$ כך ש- $M \in P$, $|y| = p(|x|)$.

$$x \notin L \Rightarrow \forall y M(x,y) = 0$$

$$x \in L \Rightarrow \mathbb{P}(M(x,y) = 1) \geq 0.5 \Rightarrow \exists y.M(x,y) = 1$$

□

אמפליפיקציה לשגיאה של מוכנות עם שגיאה דו צדדית

נתנונה לנו מכונה הסתברותית $M(x,y)$ שפותרת שפה L ב- $BPP_{\frac{1}{3},\frac{2}{3}}$. רוצים למצוא מכונה הסתרותית חדשה $M'(x,\bar{y})$ שפותרת את L ב- $BPP_{2^{-n},1-2^{-n}}$.
ואכן, נבנה M': M' תריץ את M T פעמים ב"ת: תבחר $y_1, \ldots, y_T \in \{0,1\}^m$ צחשב $M(x,y_i)$ ותענה לפי הרוב.

נניח $x \in L$. נסמן: Y_i תוצאת הניסוי ה- i. כלומר, $Y_i = 1$ אם $M(x, y_i) = 1$ ו- $Y_i = 0$ אם $M(x, y_i) = 0$. אלה הם מ"מ ב"ת כך ש- $\mathbb{P}(Y_i) = \mathbb{E}(Y_i) \geq \frac{2}{3}$. M' תבדוק האם $\sum Y_i \geq \frac{T}{2}$. כעת:

$$\mathbb{P}(\text{תטעה } M') = \mathbb{P}(\sum_{i=1}^{T} < \frac{T}{2}) \leq \mathbb{P}(|\sum_{i=1}^{T} Y_i - \frac{2}{3}T| \geq \frac{T}{6}) \leq 2^{-\Omega(T)}$$

כאשר אי השוויון האחרון נובע ממשפט צ'רנוב:

משפט. נניח $Y_1, \ldots, Y_T$ מ"מ בולאניים ב"ת ואס $\mathbb{E}(Y_i) = p$ וכן נסמן את סכום התוחלות ב- $\mu = p \cdot T$ אז

$$\mathbb{P}(|\sum Y_i - \mu| \geq \alpha\mu) \leq 2^{-\alpha^2/2}$$