

סיבוכיות מקום פולינומית

הגדרה

$$\text{PSPACE} = \bigcup_{k=1}^{\infty} \text{DSPACE}(n^k)$$

$$\text{NPSpace} = \bigcup_{k=1}^{\infty} \text{NSpace}(n^k)$$

ע"פ משפט Savitch:

$$\text{NSpace}(n^k) \subseteq \text{PSPACE}$$

$$\text{NSpace}(n^k) \subseteq \text{DSPACE}(n^{2k}) \subseteq \text{PSPACE}$$

מסקנה

$$\boxed{\text{PSPACE}} = \text{NPSpace}$$

הגדרה

$$\boxed{\text{EXP}} = \bigcup_c \text{DTIME}(2^{p_c})$$

$$p_c(n) = n^c$$

ראינו

$${}^N/D\text{SPACE}(s(n)) \subseteq \text{DTIME}(2^{O(s(n))})$$

$$s(n) > \log n$$

באופן כללי:

$${}^N/D\text{SPACE}(s(n)) \subseteq \text{DTIME}(n \cdot 2^{O(s(n))})$$

מסקנה

$$\text{PSPACE} \subseteq \text{EXP}$$

אם $A \in PH$ קיים $k \in \mathbb{N}$, $A \in \Sigma_k$, קיים מוודא פולינומי v ופולינום $p(\cdot)$ כך ש

$$\exists_{y_1} \forall_{y_2} \dots Q_{ky_k} v(x, y_1, \dots, y_k) = 1 \iff x \in A \quad |y_i| < p(|x|)$$

$$PH \subseteq \text{PSPACE}$$

נראה כעת בעיה A שהיא שלמה ב-PSPACE - כלומר A שייכת ל-PSPACE, וכן עבור כל $B \in \text{PSPACE}$ קיימת רדוקציית קארפ מ B ל A .
נגדיר את הבעיה הבאה:

$$QBF = \left\{ \varphi \mid \begin{array}{l} \varphi \text{ is a boolean formula that has} \\ \text{a quantifier for each variable} \\ \text{and has the value } T \end{array} \right\}$$

דוגמה:

$$QBF \ni \varphi = \exists_{x_1} \forall_{x_2} (x_1 \vee x_2)$$

$$QBF \not\ni \psi = \forall_{x_1} \forall_{x_2} \exists_{x_3} (x_1 \vee x_3) \wedge (x_2 \vee \neg x_3)$$

טענה

QBF היא PSPACE-שלמה

הוכחה

$QBF \in \text{PSPACE}$ - עבור קלט ל QBF באורך n מספר המשתנים בנוסחא האמורה חסום ע"י n , צריך לעבור על פני כל ההשמות האפשריות למשתנים ולבדוק שהנוסחא מסתפקת עבורן. לכן כמות הזיכרון הפנימי בשימוש חסומה ע"י $p(n)$.
כעת, עבור כל $B \in \text{PSPACE}$ קיימת רדוקציית קארפ f כך ש

$$f(x) \in QBF \iff x \in B$$

$B \in \text{PSPACE}$, לכן קיימת מ"ט M_B המכריעה את B בסיבוכיות מקום פולינומית - כלומר עבור קלט x $M_B(x)$ משתמשת בזיכרון עבודה $|x|^c \geq$ עבור קבוע c כלשהו.

גרף הקונפיגורציות $G_{B,x}$ של ריצת $M_B(x)$ מכיל לכל היותר $2^{O(|x|^c)}$ קונפיגורציות. (נניח בלי הגבלת הכלליות כי קיימת קונפיגורציה מקבלת אחת) ולכן $M_B(x)$ מקבלת אס"ם קיים מסלול מכוון ב $G_{B,x}$ מקונפיגורציה התחלתית לקונפיגורציה מקבלת (S_{acc}).
 כזכור, הגדרנו פונקציה $\Phi(u, v, k)$ המקבלת כאשר u, v הם קודקודים בגרף k ו k הינו מספר כלשהו. $\Phi(u, v, k) = 1$ אם קיים בגרף מסלול מ u ל v באורך $k \geq 1$. לכן $M_B(x)$ מקבלת את x אס"ם $\Phi_{G_{B,x}}(S_{init}, t_{acc}, 2^m) = 1$.

$$(*) \quad \Phi(s, t, 2^m) = \exists_w \Phi(s, w, 2^{m-1}) \wedge \Phi(w, t, 2^{m-1})$$

את $\Phi(s, t, 2^m)$ ניתן לתרגם לנוסחא בוליאנית עם כמתים באורך $O(2^m)$. זאת נעשה ע"י הפעלה חוזרת ונשנית של שוויון (*), ונשים \heartsuit שבנוסחא הסופית הנוצרת ישנם 2^m ביטויים מהצורה $\Phi(\cdot, \cdot, 1)$, ולכן סה"כ קיבלנו נוסחא באורך אקספוננציאלי - וזו בעיה! כדי להתגבר על הבעיה הזו נשתמש ברעיון הבא:

$$\Phi(s, t, 2^m) = \exists_{w \in \{0,1\}^m} \forall_{(x,y) \in \{(u,w), (w,v)\}} \Phi(x, y, 2^{m-1})$$

נשים לב ש

$$\forall_{(x,y) \in \{(u,w), (w,v)\}} \Phi(x, y, 2^{m-1}) \equiv \Phi(s, w, 2^{m-1}) \wedge \Phi(w, t, 2^{m-1})$$

אז מצד אחד הצלחנו להתגבר על ההכפלה - אבל מצד שני הנוסחא החדשה היא לא לפי החוקים!

ניתן לתקן את הנוסחא לעיל ולהפוך אותה לבוליאנית באופן הבא:

$$\odot \quad \exists_{w \in \{0,1\}^m} \forall_{b \in \{0,1\}} \exists_{x \in \{0,1\}^m} \exists_{y \in \{0,1\}^m} \left(\begin{array}{l} [(b=0) \rightarrow (x=s \wedge y=w)] \wedge \\ [(b=1) \rightarrow (x=w \wedge y=t)] \wedge \\ \Phi(x, y, 2^{m+1}) \end{array} \right)$$

נשים לב שאם מפתחים את $\Phi(s, t, 2^m)$ ע"פ הכלל החדש, אזי הנוסחא המתקבלת לאחר סיום הפיתוח מכילה $O(m)$ משתנים עם כמתים וכן היא מכילה $O(m)$ ביטויים מהצורה \odot וביטוי אחד מהצורה $\Phi(\cdot, \cdot, 1)$. את הביטויים מהצורה \odot וגם את הביטוי $\Phi(\cdot, \cdot, 1)$ ניתן לבדוק באופן ברור ע"י פונקציה בוליאנית באורך $O(m)$, ולכן סה"כ מקבלים נוסחא שאורכה $O(m^3)$ שמכילה $O(m)$ משתנים(כזכור, $m = |x|^c$ כלומר פולינום באורך הקלט), ולכן סה"כ בהנתן $x \in B$ עבור $\exists B \in \text{PSPACE}$ הראינו פונקציה $\delta(x)$ המחזירה נוסחא באורך $|x|^c \geq$ עם כמתים כך שמתקיים

$$\delta(x) \in QBF \iff x \in B$$

אלגוריתמים הסתברותיים

מכונת טיורינג הסתברותית

מכונת טיורינג הסתברותית היא מכונה המוגדרת באופן דומה למכונת טיורינג לא דטרמיניסטית, כאשר ההבדל הוא שעבור מעבר של המכונה שאינו מוגדר באופן יחיד(בה"כ בכל מעבר שאינו

יחיד ישנו שתי אפשרויות) המכונה מטילה מטבע שבהסתברות $\frac{1}{2}$ מחזיר 1 ובהסתברות $\frac{1}{2}$ מחזיר 0, וע"פ הרוך ההטלה המכונה מחליטה איזה מעבר לבצע. כזכור, מ"ט לא דטרמיניסטית ניתן לתאר בשני מודלים שקולים:

• מודל on-line, מכונה לא דטרמיניסטית המבצעת את החלטותיה בזמן אמת. במודל זה מכונה מקבלת את הקלט אם קיים מסלול מקבל.

• מודל off-line, מכונה **דטרמיניסטית** המקבלת שני קלטים, קלט מקורי ועד, ובמקרה זה מכונה מקבלת את הקלט אם קיים עד הגורם למכונה לקבל.

גם על מכונת טיורינג הסתברותית אפשר לחשוב באחד משני המודלים השקולים. מודל on-line ומודל off-line.

נשים לב כי במודל on-line כאשר M רצה על x התושבה $M(x)$ היא **משתנה מקרי**. כאשר המכונה רצה במודל off-line, עם סדרת בחירות אקראיות r המתפלגות באופן אחיד, $M(x, r)$ אינו משתנה מקרי המתפלג כמו $M(x)$.