

סיבוכיות

© ארזים

4 באפריל 2017

1 מעגלים בוליאנים

הגדרה 1.1 מעלג בוליאני הוא גרף חסר מעגלים. קודקוד שדרגת הכניסה שלו היא 0 יסומן במשתנה x_i , אם קבוע 0, 1. שיערים אחרים מסומנים בקשר בוליאני $\{\neg, \vee, \wedge\}$. שער עם דרגת יציאה 0 נקרא שער פלט.

מעגל מחשב באופן טבעי פונקציה. מעגל בו כל דרגת יציאה היא לכל היותר 1 נקרא נוסחה. נגדיר גודל של מעגל בתור סכום כמות הקשתות וכמות הקודקודים, ועומק של מעגל להיות אורך (בקשתות) של מסלול ארוך ביותר מקלט לפלט.

בהרצאה ראינו שכמעט כל פונקציה $f : \{0, 1\}^n \rightarrow \{0, 1\}$ דורשת מעגל בגודל $\Omega\left(\frac{2^n}{n}\right)$, וכן כי לכל f יש מעגל בגודל $O(n2^n)$.

בעיה פתוחה: להראות f מפורשת שדורש מעגל בגודל $\Omega(n)$.

תרגיל לכל f מעגל בגודל $O(2^n)$ (ואפילו נוסחא שכזו).

הוכחה: נסמן S_n את גודל המעגל המקסימלי של פונקציות עם n משתנים. נראה כי $S_n = O(2^n)$. ברור כי $S_1 = O(1)$. כעת נוכיח באינדוקציה עבור $n > 1$. תהי $f : \{0, 1\}^n \rightarrow \{0, 1\}$ נגדיר

$$f_0(x_2, \dots, x_n) = f(0, x_2, \dots, x_n)$$

ובאופן דומה נגדיר f_1 . שתי אלה הן פונקציות של $n-1$ משתנים, ולכן יש להן מעגלים בגודל S_{n-1} לכל היותר. אזי

$$f \equiv (f_0 \wedge (\neg x_1)) \vee (f_1 \wedge x_1)$$

ומכאן נוכל בקלות לבנות נוסחה שמחשבת את f . אם כן,

$$S_n \leq 2S_{n-1} + 20$$

$$S_n = O(2^n)$$

■

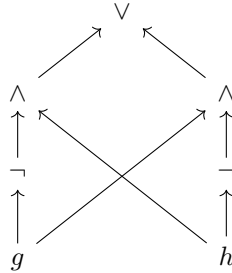
דוגמא למעגל עבור הפונקציה $Parity$:

$$f_n(x_1, \dots, x_n) = \sum_{i=1}^n x_i \bmod 2 = f_{\frac{n}{2}}(x_1, \dots, x_{\frac{n}{2}}) \oplus f_{\frac{n}{2}}(x_{\frac{n}{2}+1}, \dots, x_n)$$

וכך נקבל גודל $O(n)$. ניפטר משערי xor :

$$\alpha \oplus \beta = (\alpha \wedge \neg \beta) \vee (\neg \alpha \wedge \beta)$$

אפשר לבנות את המעגל הבא:



נסמן בתור T_n את גודל המעגל המינימלי של $Parity$:

$$T_n \leq 2T_{\frac{n}{2}} + O(1)$$

ולכן $T_n = O(n)$. אם היינו נוקטים בגישה נאיבית, היינו בונים נוסחה בגודל n^2 (משכפלים את g, h). ברור כי $T_n = \Omega(n)$, כי העומק הוא לפחות $O(\log n)$.

2 מכונות עם אורקל

הגדרה 2.1 תהי A שפה. מכונת טיורינג עם אורקל לשפה A , שנסמנה M^A , היא מכונת טיורינג עם סרט שאילתא ושלושה מצבים מיוחדים: כאשר M^A מגיע למצב q_{query} , היא עוברת מיד (צעד חישוב יחיד) למצב q_{yes} או q_{no} , בהתאם להיות תוכן סרט השאילתא בשפה A .

הגדרה 2.2 תהי $\mathcal{C}$ קבוצת מכונות טיורינג, ותהי B שפה. מסמנים $\mathcal{C}^B$ את קבוצת השפות שניתן לחשבן בעזרת מכונה מתוך $\mathcal{C}$ עם אורקל לשפה B . תהי $\mathcal{B}$ מחלקה (קבוצת שפות). מסמנים

$$\mathcal{C}^{\mathcal{B}} = \bigcup_{B \in \mathcal{B}} \mathcal{C}^B$$

תרגיל הוכיחו כי $\mathcal{P}^{\mathcal{P}} = \mathcal{P}$.

פתרון ברור כי $\mathcal{P} \subseteq \mathcal{P}^{\mathcal{P}}$. בכיוון השני, תהי $A \in \mathcal{P}^{\mathcal{P}}$. יש $B \in P$ ומכונה פולינומית M^B שרצה בזמן $O(n^c)$. שמכריעה את A . בנוסף, עבור B יש מכונה N שרצה בזמן $O(n^d)$ ומכריעה את B . נבנה כעת מכונה M' שתכריע את A . M' תסמלץ את ריצת M^B . כאשר M^B מבצעת שאילתה, תופסק הסימולציה, ותסומלץ ריצת N על תוכן סרט השאילתה. בהתאם לקבלת או דחיית N , נעביר את הסימולציה של M^B למצב המתאים, ונמשיך. נחשב את זמן הריצה, שכן הנכונות ברורה. M^B עושה $O(n^c)$ צעדים. הסימולציה של N מתבצעת בזמן לכל היותר $O((n^c)^d) = O(n^{cd})$. בסך הכל זמן הריצה הוא

$$O(n^c) O(n^{cd}) + O(n^c) = O(n^{(d+1)c})$$

לכן מצאנו מכונה פולינומית שמכריעה את A , ולכן $A \in \mathcal{P}$ וסיימנו.

תרגיל הראו כי

$$\overline{\text{SAT}} \in \mathcal{P}^{\mathcal{NP}}$$

פתרון נראה מכונה פולינומית עם אורקל לשפה SAT שמכריעה את $\overline{\text{SAT}}$. בהנתן קלט x , נשאל את האורקל על x , ונענה הפוך.

מסקנה 2.3 אם $\mathcal{P}^{\mathcal{NP}} = \mathcal{NP}$, אזי $\mathcal{NP} = \text{coNP}$.

הוכחה: $\overline{\text{SAT}}$ היא coNP שלמה.

■