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 $0,1$.שערים אחרים מסומנים בקשר בלויאני $\{\neg,\vee,\wedge\}$. 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 $f:\{0,1\}^n\to\{0,1\}$ דורשת מעגל בגודל $\Omega\left(\frac{2^n}{n}\right)$, וכן כי לכל f יש מעגל בגודל $O\left(n2^n\right)$.

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

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

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

$$f_0\left(x_2,\ldots,x_n\right)=f\left(0,x_2,\ldots,x_n\right)$$

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

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

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

$$\begin{aligned}S_n&\leq 2S_{n-1}+20\\S_n&=O\left(2^n\right)\end{aligned}$$

■

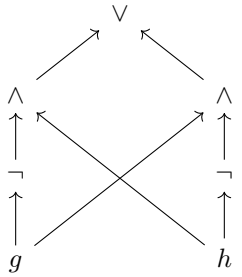
דוגמא למעגל עבור הפונקציה $Parity$:

$$f_n\left(x_1,\ldots,x_n\right)=\sum_{i=1}^{n}x_i \mod 2 = f_{\frac{n}{2}}\left(x_1,\ldots,x_{\frac{n}{2}}\right)\oplus f_{\frac{n}{2}}\left(x_{\frac{n}{2}+1},\ldots,x_n\right)$$

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

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

אפשר לבנות את המעגל הבא:



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

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

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

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 $O\left(n^c\right)$. שמכריעה את A. בנוסף, עבור B יש מכונה N שרצה בזמן $O\left(n^d\right)$ 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 $O\left(n^c\right)$ צעדים. הסימולציה של N מתבצעת בזמן לכל היותר $O\left(\left(n^c\right)^d\right) = O\left(n^{cd}\right)$. בסך הכל זמן הריצה הוא

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

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

תרגיל הראו כי

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

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

מסקנה 2.3 אם $\mathcal{P}^{\mathcal{NP}} = \mathcal{NP}$, אזי $\mathcal{NP} = \mathrm{co}\mathcal{NP}$.

הוכחה: $\overline{\mathrm{SAT}}$ היא $\mathrm{co}\mathcal{NP}$ שלמה. ■