סיבוכיות

© ארזים

25 באפריל 2017

בשיעור שעבר דיברנו על השפה CVAL. כקלט, השפה מקבלת מעגל בוליאני C עם n קלטים, וקלט אליו $\overline{\alpha}=(\alpha_1,\ldots,\alpha_n)$. מתקיים $(C,\overline{\alpha})\in\mathrm{CVAL}$ אם ורק אם $C(\overline{\alpha})=1$.

משפט 0.1 CVAL שלמה למחלקה $\mathcal{P}$ תחת רדוקציות $\leq_L$.

הוכחה: ראשית נראה כי $\mathrm{CVAL}\in\mathcal{P}$. בהינתן מעגל C וקלט $\overline{\alpha}$, תחילה נשערך את כל השערים שאנחנו יודעים את ערכי שני בניהם. נמשיך כך, כשברור שלכל שער נגיע בזמן מסויים. גודל המעגל נתון לנו, ולכן ברור שזמן הריצה כאן הוא פולינומיאלי.

כעת נראה כי CVAL שלמה. תהי $L\in\mathcal{P}$ כלשהי, ותהי M מכונת טיורינג המכריעה את L כך שעל קלט x, ריצת M תיקח לכל היותר $|x|^c$. הרעיון יהיה לבנות את טבלת החישוב, כלומר מטריצה $n^c\times n^c$, שבתא i,j שלה נמצא ערך התא j בסרט בשלב i, יחד עם סימון מיוחד אם הראש הקורא נמצא בתא הזה, ואם הוא נמצא, אז גם המצב הפנימי של המכונה. נשים לב שערך תא מסויים תלוי אך ורק בערכי שלושת התאים שמעליו (ישר, באלכסון לימין ובאלכסון לשמאל). כל תא הוא בגודל קבוע. נבנה מעגל שבהנתן הערך של שלושה תאים צמודים, מחשב, לפי δ של M, את ערך התא שמתחת לתא האמצעי.

הרדוקציה שלנו תחשב מעגל ששעריו מסודרים ברמות, כך שהשערים ברמה i מתארים את הקונפיגורציה (סרט, מיקום ראש, מצב מכונה) אחרי i שלבי חישוב. השערים ברמה i יאוגדו לתאים, כשכל תא מתאים לתא בסרט המכונה. ברמה 0 יהיו הקלט לשפה L ומידע על מיקום הראש והמצב ההתחלתי. כדי לחשב את השערים ברמה $i+1$, נשים לב שכל תא תלוי אך ורק בשלושת התאים מעליו (ישר, שמאל וימין). בהינתן פונקציית המעברים δ של M, יש מעגל קבוע המחשב את ערך התא בהינתן שלושת התאים הללו. כקונבנציה אפשר לומר שכאשר M נכנסת למצב מקבל/דוחה היא מזיזה את הראש שמאלה ומוחקת את הסרט, ולבסוף כותבת 0 או 1. שער הקלט ייחשב בדיוק את הערך הזה.

למעגל יש n^c תאים בכל שכבה, n^c שכבות. כדי לחשב את החלק במעגל שמתאים לתא במיקום j ברמה i, בסך הכל צריך להוציא את המעגל הקבוע שדיברנו עליו, שתלוי בפונקציה δ, ולומר מי הקלטים אליו (השערים שחישבו את התאים $j-1,j,j+1$ ברמה i.

יחד עם המעגל הזה, הרדוקציה תתן את הקלט x. מהתיאור שלנו ברור כי הרדוקציה נכונה, וכן כי היא רצה בזיכרון לוגריתמי. ■

הערה 0.2 הרדוקציה מחשבת מעגל בעומק n^c. כפי שראינו בתרגיל, ניתן להעריך מעגלים בעומק d בזיכרון $O(d)$. לכן, אם המעגל היה מעומק $O(\log n)$היינו מקבלים $\mathcal{P}=\mathcal{L}$. מאמינים כי $\mathcal{P}$ אינה מוכלת בזכרון פולי־לוגריתמי.

הגדרה 0.3 NC^k היא מחלקת כל השפות $A\subseteq\{0,1\}^k$ כך שיש סדרת מעגלים (עם fan-in לכל היותר 2) בגודל פולינומיאלי ועומק $O\left(\log^k n\right)$ עבור A.

הגדרה 0.4 $\mathrm{uniform}-\mathrm{NC}^k$ היא מחלקת כל השפות בתוך NC^k כך שיש מכונת טיורינג מתוך $\mathrm{DSPACE}\left(O\left(\log n\right)\right)$ כך שבהינתן 1^n מוציאה את המעגל המתאים.

הגדרה 0.5 AC^k היא מחלקת כל השפות $A\subseteq\{0,1\}^k$ כך שיש סדרת מעגלים פולינומיאלית בעומק $O\left(\log^k n\right)$ המכריעה את A (מרשים כל fan-in).

הגדרה 0.6 $\mathrm{uniform}-\mathrm{AC}^k$ מוגדרת בדומה למחלקה $\mathrm{uniform}-\mathrm{NC}^k$.

הגדרה 0.7 (נוסחאות בוליאניות מכומתות - Qunatified Boolean Formulas - QBF)
נוסחא בוליאנית מכומתת היא נוסחה מהצירה הבאה:

$$Q_1x_1Q_2x_2\dots Q_nx_n\varphi\left(x_1,\dots,x_n\right)$$

כאשר $Q_i\in\{\forall,\exists\}$, וכן $\varphi\left(x_1,\dots,x_n\right)$ היא נוסחא בוליאנית.

כיוון שכל המשתנים מכומתים, ערך הנוסחא הוא T או F.

הגדרה 0.8 אוסף הנוסחאות מצורת QBF שערכן T מסומן TQBF.

דוגמא

$$\exists x_1\forall x_2\left(x_1\vee x_2\right)\in\mathrm{TQBF}$$
$$\forall x_1\exists x_2\left(x_1\wedge x_2\right)\notin\mathrm{TQBF}$$

"לא למדתם שח מט אף פעם? אתם לא חנונים מספיק!" - המרצה.

משפט 0.9 השפה TQBF שלמה למחלקה PSPACE תחת $\le_L$.

הוכחה: ראשית נראה כי $\mathrm{TQBF}\in\mathrm{PSPACE}$. הרעיון הוא כזה - נבנה נוסחה גדולה, בעומק פולינומיאלי, שמתארת את הנוסחה המכומתת. במקום כמתי $\exists$ נבנה שער $\vee$ בין שתי אפשרויות, כשהמשתנה הוא 0 וכשהוא 1. במקום כמתי $\forall$ נבנה שער $\wedge$ בין שתי אפשרויות, כשהמשתנה הוא 0 וכשהוא 1.

פורמלית - יהי $\psi=Q_1x_1\dots Q_nx_n\varphi\left(x_1,\dots,x_n\right)$ קלט של TQBF. נגדיר

$$\psi_0=Q_2x_2\dots Q_nx_n\varphi\left(0,x_2,\dots,x_n\right)$$
$$\psi_1=Q_2x_2\dots Q_nx_n\varphi\left(1,x_2,\dots,x_n\right)$$

נעריך באינדוקציה את ערכה של ψ_0 ונזכור אותו. נחשב גם את ערכה של ψ_1, ואז לפי Q_1 נוציא את התוצאה המתאימה.

ננתח את הזכרון על ידי רקורסיה:

$$S\left(n\right)=O\left(1\right)+S\left(n-1\right)=O\left(n\right)$$

ראינו שאפשר לחשב ערך של נוסחה בזכרון לוגריתמי - זה בסיס האינדוקציה.

כעת, תהי $A \in \mathrm{PSPACE}$, ונראה רדוקצית $\leq_L$ ממנה אל TQBF. תהי M מכונת טיורינג המכריעה את A כל שעל קלט באורך n היא משתמשת בזיכרון לכל היותר $S(n) = n^{O(1)}$.

ניזכר בגרף הקונפיגורציות של M על קלט x, שבו כל קודקוד מתאים לקונפיגורציה מסויימת של המכונה. מספר הקודקודים הוא לכל היותר

$$2^{O(S(n))} = \exp(S(n))$$

יש קשת מקודקוד u לקודקוד v אם בצעד חישוב אחד של M אפשר לעבור מקונפיגורצייה u לקונפיגורציה v. בהינתן קלט x, M מקבלת אותו אם ורק אם בגרף הקונפיגורציות יש מסלול מהקונפיגורציה ההתחלתית לקונפיגורציה המקבלת (בלי הגבלת הכלליות יש אחת מסויימת כזו).

הרדוקציה של A אל TQBF תטען שיש מסלול מהקודקוד ההתחלתי לקודקוד המקבל. היינו מרוצים לכתוב משהו בסגנון הבא:

נסמן $\mathrm{Reach}(u,v,t)$ ביטוי שיאמר שיש מסלול מכוון מקודקוד u אל קודקוד v באורך לכל היותר 2^t, ואז מתקיים

$$\mathrm{Reach}(u,v,t) = \exists w\left(\mathrm{Reach}(u,w,t-1) \wedge \mathrm{Reach}(w,v,t-1)\right)$$

אם נמשיך ונפתח כך נקבל גודל אקספוננציאלי. לכן נעשה את הדבר הבא:

$$\exists w \forall \sigma \exists a \exists b\left(((\sigma=0) \to (a=u \wedge b=w)) \wedge ((\sigma=1) \to (a=w \wedge b=v) \wedge \mathrm{reach}(a,b,t-1))\right)$$

הרדוקציה שלנו תכתוב את הנוסחה המתאימה לכך שיש מסלול באורך לכל היותר $\exp(S(n))$ בין הקודקוד ההתחלתי לסופי. נוציא את כל הכמתים עבור כל השלבים כדי לקבל מבנה חוקי:

$$\exists w_1 \forall \sigma_1 \exists a_1 \exists b_1 \ldots \exists w_t \forall \sigma_t \exists a_t \exists b_t \varphi(w_1,\sigma_1,a_1,b_1,\ldots,w_t,\sigma_t,a_t,b_t)$$

כאשר φ מכילה את הנוסחאות לאורך השלבים, עד האחרונה שהיא $\mathrm{Reach}(a_t,b_t,0)$. נשים לב שהשוויונים, למשל $a_t = u$, הם בין מחרוזות (שמות של קונפיגורציות), שניתן לבדוק עם $O(S(n))$ ביטים (כי כל מחרוזת כזו אורכה $O(S(n))$). את הנוסחה המתארת את $\mathrm{Reach}(a_t,b_t,0)$ ניתן לחשב בזכרון לוגריתמי על ידי תיאור M והקלט. ■