תורת הסיבוכיות — תרגול 9
מעגלים בוליאניים ונוסחאות בוליאניות

נוסחה בוליאנית — הגדרה ובעיית ההכרעה המתאימה

בהרצאה ראינו את מודל החישוב של מעגלים בוליאניים. בתרגול זה נרצה לעסוק במודל חישוב דומה אך מוחלש יותר, של נוסחאות בוליאניות, ולהבין את הקשר בינו ובין המודל הכללי.

פורמלית, נוסחה בוליאנית היא מעגל בוליאני כך שה־ fan-out שלו (דרגת היציאה של הצמתים) חסום על ידי 1. דהיינו, כל תת־חישוב שמתבצע בתוך המעגל הבוליאני מניב תוצאה "חד פעמית" שנזרקת מייד לאחר השימוש. זה מקנה לנוסחאות פשטות רבה יותר ביחס למעגלים במובן שנראה כעת: כזכור, CVAL הוגדרה כשפת כל הזוגות של מעגל בוליאני והשמה מספקת עבורו, והוכח כי שפה זו היא P־שלמה ביחס לרדוקציות logspace; דהיינו אם $\mathrm{CVAL} \in \mathrm{DL}$ אז $\mathrm{DL} = \mathrm{P}$, ובפרט זוהי שפה "קשה" בהקשר שבו אנו עוסקים. לעומת זאת, נראה כי FVAL, שפת כל הזוגות של נוסחה והשמה שמספקת אותה, היא ב־ DL.

אם כן, נגדיר פורמלית:

$$\mathrm{FVAL} := \{(F, x) \mid F\left(x\right) = 1 \text{ ו־ } ,F \text{ השמה למשתני } x \text{ ,נוסחה בוליאנית } F\}$$

נתאר כעת אלגוריתם הפועל בזכרון לוגריתמי ומכריע את השפה. הרעיון הוא זה: ניתן לחשוב על F כעל עץ ששורשו הוא צומת הפלט של הנוסחה ועליו הם המשתנים. מתן ערכים לעלים קובע את ערכם של שאר הצמתים בעץ כשהמידע "מפעפע" מעלה. אם כן, די בביצוע DFS כדי לחשב את ערכו של השורש. לרוע המזל, עומק העץ יכול להיות פולינומי בגודל הקלט (שהוא גודל הנוסחה F), ולכן ה־ DFS יצרוך יותר מדי זיכרון, בהינתן שאכן יישמר מידע כלשהו במהלך הריצה. התעלול הוא בכך שאין צורך לזכור כמעט מידע במהלך הריצה, עקב האופי הפשוט של הערך שאותו רוצים לחשב. האלגוריתם שלנו יטייל באופן כמעט "עיוור" בעץ, אך מובטח שבסופו של דבר יעבור על כולו ויחזיר את הפלט הנכון.

ההנחה הבסיסית שלנו היא שבהינתן מספר של צומת, ניתן לחשב בזכרון לוגריתמי הן את המספר של אביו, הן את המספר של בנו השמאלי ביותר, והן את המספר של אחיו הקרוב מימין (אם קיים). הדבר תלוי בייצוג של F אך ניתן לביצוע בכל ייצוג סביר.

נעבור כעת לתיאור האלגוריתם:

- אם אתה נמצא בצומת עלה, חשב את ערכו מתוך ההשמה, וחזור לאב של הצומת שלך עם ערך העלה.
- אם חזרת לצומת $\wedge$ מאחד מבניו, אז: אם הבן החזיר 0 החזר גם 0; אם הבן החזיר 1 וזהו הבן הימני ביותר, החזר 1; ואחרת, היכנס לבן הבא בתור והמשך את הריצה כרגיל.
- אם חזרת לצומת $\vee$ מאחד מבניו, אז: אם הבן החזיר 1 החזר גם 1; אם הבן החזיר 0 וזהו הבן הימני ביותר, החזר 0; ואחרת, היכנס לבן הבא בתור והמשך את הריצה כרגיל.
- אם האלגוריתם חזר מהשורש עם הערך 1 — קבל, ואחרת — דחה.

הסיבה שבגללה פתרון זה אינו עובד גם עבור CVAL היא שצומת לא יכול רק להחזיר את ערכו "למעלה" וחסל; יכולים להיות לו כמה אבות ולכן המידע חייב לפעפע לכולם, ולכן חלק מהמידע יצטרך להישמר בצד, מה שמוביל לסיבוכיות זכרון גדולה מדי.

קשר בין מעגלים ונוסחאות

כזכור, ישנם שני מדדי סיבוכיות למעגלים — גודל ועומק. עומק מתאר את המהירות שבה ניתן לחשב את הפונקציה שמתאר המעגל בחישוב מקבילי. כזכור, כל פונקציה ניתן לתאר באמצעות מעגל (או נוסחה) מעומק 2 על ידי שימוש בצורה קנונית כלשהי (CNF או DNF) שמתארת את טבלת האמת של הפונקציה. לכן נגביל את הדיון מראש למעגלים שבהם ה־ fan-in של כל צומת חסום על ידי 2.

נציג כעת את אחד מהאופנים שבו העיסוק ספציפית בנוסחאות עשוי לשפוך אור כללי על מעגלים. בהינתן פונקציה בוליאנית f:

- נסמן ב־ $L\left(f\right)$ את <u>הגודל</u> המינימלי של <u>נוסחה</u> עבור f (עם fan-in 2).
- נסמן ב־ $D\left(f\right)$ את <u>העומק</u> המינימלי של <u>מעגל</u> עבור f (עם fan-in 2).

שימו לב כי הגדרת הגודל נוגעת לנוסחאות בעוד שהגדרת העומק מתייחסת למעגלים כלליים. באופן כללי, לכל פונקציה מתקיים שהעומק המינימלי של נוסחה עבורה שווה לעומק המינימלי של מעגל עבורה.

טענה: $D(f)=\Theta\left(\log L\left(f\right)\right)$.

במילים אחרות, הבנה של גודל הנוסחה המינימלית עבור f אומרת לנו משהו על עומק המעגל הכללי המינימלי עבור f (ובפרט ניתן לקבל חסמים תחתונים ועליונים על מעגלים בעזרת נוסחאות).

הכיוון הראשון של ההוכחה: ראשית נוכיח את הכיוון הקל יותר, ש־ $D\left(f\right)=\Omega\left(\log L\left(f\right)\right)$, או במילים אחרות, ש־ $\log L\left(f\right)=O\left(D\left(f\right)\right)$.

בהינתן מעגל עבור f מעומק $D\left(f\right)$ נרצה לבנות נוסחה שקולה שאיננה גדולה מדי. נתרגם את המעגל לנוסחה באמצעות כוח גס: עבור כל צומת שדרגת היציאה שלו היא $n>1$ נשכפל את כל תת העץ שלו n פעמים ונחליף את הצומת בכל n העותקים הללו כשכל אחד מחובר לאחת מהקשתות היוצאות שהיו מחוברות לצומת המקורית. בצורה הזו הגדלנו את המעגל, אך לא שינינו את העומק שלו.

הנוסחה המתקבלת היא עץ בינארי שעומקו $D\left(f\right)$ ולכן בעלת $2^{O(D(f))}$ צמתים, כלומר $\log L\left(f\right)=O\left(D\left(f\right)\right)$ כנדרש.

הכיוון השני של ההוכחה: זהו הכיוון המורכב יותר. אנו רוצים להראות כי $D\left(f\right)=O\left(\log L\left(f\right)\right)$, כלומר בהינתן נוסחה φ עבור f שגודלה $L\left(f\right)$ לבנות ממנה מעגל עבור f שעומקו לכל היותר $O\left(\log L\left(f\right)\right)$. למעשה נצליח לבנות נוסחה שקולה מהעומק המתאים.

האינטואיציה הבסיסית היא זו: אם φ הייתה עץ בינארי מאוזן, הבעיות שלנו היו נפתרות מאליהן, שכן העומק של עץ בינארי מאוזן אינו יכול להיות גדול מדי. על כן נראה איך ניתן להמיר את φ בנוסחה φ' שקולה שהעץ שלה הוא מאוזן, וזאת מבלי לגרום לתקורה משמעותית.

(קל לראות שאם הנוסחה אינה מאוזנת העומק יכול להיות לינארי בגודל העץ — כך זה בשרוך שבו לכל צומת מחובר בנוסף עלה).

לצורך פשטות נסמן $L=L\left(f\right)$. איזון העץ יבוצע בשלבים כשבכל שלב אנו מוצאים צומת "באמצע" ומטפלים בו. צומת כזה הוא בעל התכונה שבתת העץ שלו יש לפחות $L/3$ צמתים, ובכל אחד מתתי העצים של בניו יש לכל היותר $L/3$ צמתים. ניתן למצוא כזה באופן רקורסיבי: השורש ודאי מקיים את התכונה שבתת העץ שלו יש לפחות $L/3$ צמתים, וכל עוד הצומת הנוכחי שלנו הוא בעל בן שיש לו יותר מ־ $L/3$ צמתים, נעבור הלאה לבן הזה. כאשר לא יהיה בן מתאים, סיימנו (וזה בהכרח יקרה כי עבור העלים לא מתקיימת התכונה שבתת העץ שלהם יש לפחות $L/3$ צמתים).

נסמן את תת העץ של צומת אמצעי כזה ב־ S. נשים לב כי $\frac{1}{3}L\le\left|S\right|\le\frac{2}{3}L+1$. נסמן ב־ φ_0 וב־ φ_1 את הנוסחה המתקבלת מ־ φ על ידי החלפת S בתת־נוסחה המייצגת את הקבועים 0 ו־ 1, בהתאמה. נשים לב שניתן לתאר קבוע שכזה על ידי נוסחה מגודל 3 (משתנה ושלילתו שמחוברים על ידי שער $\wedge$ או שער $\vee$, בהתאמה).

אם כן, $\left|\varphi_0\right|=\left|\varphi_1\right|=\left|\varphi\right|-\left|S\right|+3\le L-\frac{1}{3}L+3=\frac{2}{3}L+3$.

כעת ניתן לכתוב נוסחה שקולה ל־ φ: $\varphi\equiv\left(\neg S\wedge\varphi_0\right)\vee\left(S\wedge\varphi_1\right)$. זוהי φ' שלנו.

יש לבנות פורמלית את $\neg S$ באופן שלא ישנה את העומק; הדבר מבוצע בדומה להוספת שערי NOT מבלי לשנות את עומק המעגל (בונים את $\neg S$ אינדוקטיבית כמעין "תמונת ראי" דה־מורגנית של S).

מה העומק של הנוסחה החדשה? $D\left(\varphi'\right)=2+\max\left\{D\left(S\right),D\left(\varphi_0\right),D\left(\varphi_1\right)\right\}$. ניתן לחזור באופן רקורסיבי על השיפור שלנו הן עבור S והן עבור φ_0 ו־ φ_1. גודלן של שלוש הנוסחאות הללו, כפי שראינו, הוא בערך $\frac{2}{3}L$. קיבלנו (בערך) את נוסחת הנסיגה הבאה לעומק המעגלים: $D\left(L\right)=2+D\left(\frac{2}{3}L\right)$. פתרון הנוסחה מניב $D\left(L\right)=2\cdot\log_{3/2}L=O\left(\log L\right)$, כנדרש.

מסקנה אחת מהמשפט היא שמחלקת השפות המתקבלות על ידי משפחת <u>נוסחאות</u> מגודל פולינומי שקולה למחלקה NC^1, שהיא מחלקת השפות המתקבלות על ידי משפחת <u>מעגלים</u> מגודל פולינומי, עומק $O\left(\log n\right)$, ו־ fan-in חסום.