מודלים חישוביים ־ הרצאה 10

שרון מלטר, אתגר 17

21 במאי 2024

תזכורת:

- הגדרנו $\leqslant_p$
- ראינו הגדרה של שפה NP שלמה; L היא NP שלמה אם $L \in NP$ ולכל $L' \in NP$ מתקיים $L' \leqslant_p L$
- אם L היא NP שלמה, אז מתקיים $NP = P \Leftrightarrow L \in P$
- $3-SAT$ היא שפת כל קבוצות הנוסחאות הבוליאניות עם לכל היותר 3 ליטרלים, שקיים להן פיתרון (שקיימת להן השמה ספיקה)
- משפט קוק־לוין: $3 \cdot SAT$ היא NP שלמה
- ראינו שאם $L_1 \leqslant_p L_2$ ו־ L_1 NP שלמה אזי L_2 NP שלמה.

היום נוכיח את משפט קו־לוין, אך לפני כן נתאמן עוד קצת ברדוקציות.

1 רדוקציות

הבעיה: $VERTEX - COVER$ בגודל k. (אתם מכירים את הבעיה־ רוצים למצוא קבוצת צמתים בגרף כך שכל קשת מחוברת ללפחות אחד מהם)
טענה: $3 - SAT \leqslant_p VERTEX - COVER$

הוכחה:
נגדיר את הפונקציה R: $R(<\phi>) = <G, k>$ כך ש־ ϕ הוא קידוד של 3 נוסחאות בוליאניות.
נרצה לבנות גרף G המקיים: ϕ ספיקה אם"ם ל־ G יש כיסוי בצמתים בגודל k.
הערה: נסמן ב־ n את מספר המשתנים וב־ m את מספר הפסיקות.

הבנייה תיראה כך:
לכל פסוקית $(l_1 \vee l_2 \vee l_3)$ נבנה מעגל (משולש) בין צמתים של l_1, l_2, l_3. מהקצה של אחד מהם נוסיף קשת לצומת השני שמייצג משתנה (משתנה שאליו מתייחסים בפסוקית)
לכל משתנה x_i נוסיף קשת בין צומת המייצגת אותו (x_i) לצומת שני שמייצג אותו $(\overline{x}_i)$. לרכיב זה נקרא "רכיב ההשמה".

רעיון: אם אני אסביר לכם שאתם צריכים לכסות את רכיב ההשמה ב־ n קודקודים, מי שיכסה ב־ n צמתים את רכיב ההשמה בעצם "בוחר השמה".

כיוון 1:
נניח ש־ ϕ ספיקה, כלומר קיימת השמה α שמספקת אותה, ונוכיח שקיים כיסוי בקודקודים בגודל k.
איך נבחר את קבוצת הקודקודים?
לכל i נבחר את הקודקוד x_i אם $x_i = 1$ ואם $x_i = 0$ נבחר לקבוצה את $\overline{x}_i$.
כמו כן, לכל פסוקית יש ליטרל ש־ α מספק. נבחר את שני הצמתים שאינם שכנים של הצומת שלו (שכמובן נבחר ל־ S)
כלומר, נבחר מבין שני הליטרלים $x_i, \overline{x}_i$ את האחד ש־ α מספקת.
בצורה זו בחרנו לכל n קודקודים לכל פסוקית $l_1 \vee l_2 \vee l_3$ ישנו ליטרל ש־ α מספקת ואנו בוחרים ל־ S (קבוצת

כיסוי הקודקודים) שני קודקודים אחרים. בצורה זו לכל $2m$ נוסף עוד קודקוד ולכן בסך הכל $|S| = 2m + n = k$.
האם כל הקשתות מכוסות?
הקשתות שברכיב ההשמה מכוסות (ע"י x_i או $\overline{x}_i$), הקשתות שבמשולשים מכוסות, הקשתות שמחברות בין המשולשים לרכיבי ההשמה מכוסות... כלומר קיבלנו כיסוי, כנדרש (:

כיוון 2:
נניח שקיים כיסוי בגודל k לגרף, ונוכיח שקיימת השמה ספיקה α. *

2 הוכחת משפט קוק־לוין

נוכיח ש־ $3-SAT$ היא NP שלמה.

בשביל ההוכחה, נגדיר שפה חדשה ומרגשת - $CIRCUIT-SAT$ ונוכיח שהיא NP שלמה.
לאחר מכן, נוכיח ש־ $CIRCUIT-SAT \leqslant_p 3-SAT$.

מעגל בוליאני הוא גרף מכוון (חסר מעגלים) שבו בתחתית יש משתנים ובקודקודים יש שערים $\vee, \wedge, \hat{}$ ומלמעלה יוצא פלט (או פלטים, אם בונים כמה חוטי פלט)
בהנתן מעגל C והשמה α אפשר להציב את α ב־ C ולקבל את $C(\alpha)$.
היתרון של גרף בוליאני על פני נוסחה הוא שבגרף ניתן למצוא תתי־ערכים, לפני שמקבלים את ערך הפלט הסופי.
כמו כן, קל לראות איך לוקחים נוסחה והופכים אותה לגרף בוליאני.
אם זאת, איך הופכים גרף כזה לנוסחה? הרי יש בו מספר תתי־פתרונות (ערכי ביניים), איזה מהם בא לפני השני? מדובר בהמרה שלוקחת זמן אקספוננציאלי.

ניזכר קצת במעגלים ממבוא לחומרה.
כל מעגל / נוסחה על n משתנים מחשבים פונקציה $f : \{0,1\}^n \to \{0,1\}$
ומה אם הכיוון השני, האם כל פונקציה בוליאנית ניתנת לחישוב ע"י מעגל / נוסחה? - כן!
אבל, אנו יודעים להבטיח שזה נכון רק למספר עצום של שערים.

משפט:
לכל מ"ט דטרמיניסטית M שרצה בזמן $t(\cdot)$ ולכל מספר n, קיים מעגל בוליאני C על n משתנים ועם $O(t(n)^2$ כך שלכל $x \in \{0,1\}^n$ מתקיים $C(x) = M(x)$.
כלומר, ניתן לקמפל כל מ"ט (כל תוכנה) במעגל (חומרה).
מעבר לכך, ישנו אלגוריתם שבהנתן $< M >$ ו־ n בונה את C בזמן $O(t(n)^2)$ (יש אף זמן טוב יותר, אך הוכחתו מסובכת יותר)

בהינתן מ"ט M שרצה בזמן $t(\cdot)$ מספר n וקלט $x \in \{0,1\}^n$ נגדיר מבנה נתונים שמסכם את הריצה של M על x, $Table$. הוא יהי מערך דו מימדי $t(n) \times t(n)$ שכל תא בו מכיל את השדות הבאים:

- $flag$ - האם הראש הקורא / כותב היה בזמן i במקום j
- $character$ - תוכן התא ה־ i על הסרט בזמן j
- $state$ - אם $flag = 0$ אז בערך זה לא שמור כלום ואם $flag = 1$ אז זהו המצב של M בזמן j.

נשים לב שכל שהשורה ה־ j במערך $Table_M(x)$ מקודדת את הקונפיגיורציה של M על x בזמן j.
נשים לב לתכונה נושמת של מבנה הנתונים: נניח שאנו יודעים את M ולא את x, אך מבקשים ממני את $Table_M[i,j](x)$. כביכול לא נוכל למצוא ערך זה. אך אם ייתנו לנו את התווים הבאים־ $Table_M[i-1,j-1](x)$ $Table_M[i,j-1](x)$, $Table_M[i-1,j](x)$ כלומר התאים שבצדדי ומעל התא הנדרש, נוכל למצוא אותו.
לכל מ"ט M קיימת פונקציה $Next_M$, כך שאם ניתן לה את שלושת התאים שצוינו, נקבל:

$$Next_M(Table_M[i-1,j-1](x), Table_M[i,j-1](x), Table_M[i-1,j](x)) = Table_M[i,j]$$

כל תא ניתן לקודד באמצעות מספר קבוע a של ביטים (נכון לכל דבר בגודל קבוע). לכן אפשר לחשוב על $Next_M$ בתור פונקציה שמקבלת $3a$ ביטים ומחזירה a ביטים. ל־ $Next_M$ יש מעגל בוליאני בגודל קבוע שתלוי ב־ a ונקרא לו D (ניתן גם לבנות אותו)
לכל $2 \leqslant i,j \leqslant t(n)$ נשים עותק של D מתחת לתא (i,j). בצורה זו, אם יכניסו את x מלמטה, ייצאו מלמעלה

הבאים אל השורה האחרונה.
כעת נעבור לשאר חלקי התכנית.

אנו יודעים ש־ $CIRCUIT-SAT \in NP$, כך שכדי להוכיח ש־ $CIRCUIT-SAT$ היא NP שלמה, נותר להוכיח שלכל $L' \in NP$ מתקיים $L' \leqslant_p CIRCUIT-SAT$.
תהי $L' \in NP$ אז יש לה מוודא פולינומי $V(x,y)$ וקיים קבוע c כך שלכל x' מתקיים;

$$x' \in L' \Leftrightarrow \exists y: \quad |y| \leqslant |x'|^c, V(x',y) = 1$$

נגזור את הקלטים בהם x ונקודד אותם לערכים x' (הקלט שלי). נקרא למעגל שמתקבל מכך C.
נרצה מ"ט שרצה בזמן פולינומי. נגדיר אותה כך:

$$R(x') =< C >$$

כך ש־ $x' \in L' \Leftrightarrow$ C ספיק.
נשים לב גם ש־ C ספיק אם"ם קיים y כך ש־ $C(y) = 1$
וכמו כן מתקיים $x' \in L'$ אם"ם $\exists y: \quad V(x',y)(= C(y)) = 1$
נבנה את R כך:
בהינתן קלט x' נחשב את $n = |x'|$ ונפעיל את הקומפיילר מתוכנה לחומרה על V ועל n, נקבל מעגל A כך שלכל x, y מהאורכים הנכונים $A(x,y) = V(x,y)$.
קיבלנו את התנאי השני להיות שפה NP שלמה.
כעת נוכל לעבור לחלק האחרון והקשה ביותר בהוכחה.

נוכיח ש־ $CIRCUIT-SAT \leqslant_p 3-SAT$
רעיון: ϕ לא תהיה שקולה לוגית ל־ C, אפילו נעשה כך של־ ϕ יהיו יותר משתנים מל־ C.

אנו זקוקים למ"ט R שרצה בזמן פולינומי כך ש־

$$R(< C >) =< \phi >$$

ומתקיים C ספיק אם"ם ϕ ספיקה.
נעשה זאת בכך שנתרגם את המעגל הנתון C לנוסחה שקולה ב־ $3-CNF$. זה ניתן לביצוע, אבל אנחנו לא בטוחים שניתן לעשות זאת בזמן פולינומי... ייתכן שקיים מעגל באורך פולינומי, אבל נוסחה עבורו היא בגודל אקספוננציאלי, לכן הרדוקציה לא תוכל לרוץ בזמן פולינומי.
איך נפתור את הבעיה?
R מקבל בתור קלט מעגל C, בעל n משתנים ו־ m שערים והיא אמורה להוציא נוסחה ϕ. נבנה נוסחה כזו עם $n+m$ משתנים ונסמנם $x_1, ..., x_n \ y_1, ..., y_n$ נמספר את השערים של C ונניח שהמספור הוא לפי מיון טופולוגי.
נסמן את ההשמות ל־ C ב־ α ואת ההשמות ל־ ϕ ב־ β.
בהינתן השמה α למשתני C, מוגדרים ערכי אמת לכל השערים ונתאים ל־ α השמת β למשתני ϕ שבה לכל x_i מתקיים $\beta(x_i) = \alpha(x_j)$ ולכל y_j, $\beta(y_j)$ שווה לערך שהשער מקבל תחת ההשמה α.
נאמר שהשמה β עבור משתני ϕ (למשל $01...1$) היא קונסיסטנטית אם היא ההשמה המותאמת למה ש־ β נותנת ל־ $x_1, ..., x_n$ (משתני C)
נשים לב שישנן 2^{n+m} השמות מסוג β ו־ 2^n מהן קונסיסטנטיות.

בסך הכל נקבל ש־

$$R(C) = \phi(x_1, ..., x_n, y_1, ..., y_m)$$

כך ש־ $\phi'(\beta) = 1$ אם"ם β קונסיסטנטית.
כלומר השמה קונסיסטנטית ביחס לשער ה־ 1. אם $y_1 = \hat{}x_7$ נתחיל בלבנות את הנוסחא, ניעזר בסימון הבא;
$a \to b \equiv \hat{}a \vee b$

$$\phi'_1 = (y_1 \to \hat{}x_y) \wedge (\hat{}x_7 \to y_1)$$

כעת אנו צריכים נוסחה ϕ'_2 כך ש־ $y_2 = x_2 \vee x_3$ אם"ם $\phi'_2 = 1$.
נוכל למצוא נוסחת $3-CNF$ שכופה זאת.
לאחר מכן נרצה נוסחה ϕ'_3 עבורה $y_3 = y_2 \wedge x_4$ וגם $g_3 = g_2 \wedge x_4$.
נסתכל בהשמה β המותאמת ל־ α זוהי השמה קונסיסטנטית ולכן $\phi'(\beta) = 1$. כמו כן, כיוון ש־ α מספקת את C אז ב־ g_m יוצא 1 ולכן כיוון ש־ β קונסיסטנטית $\beta(y_m) = 1$ כך ש־ β מספקת את y_m ולכן היא מספקת את ϕ.
וזוהי ההוכחה ♡