סיבוכיות – הרצאה 3

כל העולם הוא חישוב אחד גדול

8.3.11

כיצד הופכים מכונת טיורינג למעגל?

רוצים לעשות המרה ממכונת טיורינג למעגל. בעיה כזאת נקראת $TM-To-Circuit$.
כמובן שנעשה את זה באמצעות מכונת טיורינג.
המכונה מקבלת מ"ט M, קבוע c ואת אורך הקלט 1^n (הרי מעגל יכול לפעול רק לקלט באורך נתון). פלט המכונה יהיה מעגל C עם n קלטים כך שלכל קלט $x \in \{0,1\}^n$ מתקיים $M(x) = C(x)$ כאשר זמן הריצה של המכונה אינו עולה על n^c.

הצעה: נבנה טבלת אמת. נתרגם ל- CNF. עכשיו אפשר בקלות לבנות מעגל כנ"ל.
ברור שזה נכון. מה עם זמן הריצה?

$2^n \cdot$ (זמן הריצה של המכונה הנתונה על קלטים באורך n)

מהגורם של זמן הריצה לא נוכל להתחמק. אבל 2^n זה המון, ואם נאמר המכונה המקורית היתה פולינומיאלית אז בניית המעגל רחוקה מאוד מזה.

הערה. אם המכונה שלנו לא עוצרת, קשה לצפות שנצליח לבנות מעגל הגיוני. המעגל יעבוד עבור הקלטים עבורם המכונה עובדת.

מטרה: בהינתן מכונת טיורינג $M \in Time(n^c)$ האלגוריתם ל- $TM-To-Circuit$ ירוץ בזמן $poly(n)$.

האלגוריתם: הרעיון הוא לקחת את טבלת החישוב של המכונה ולבנות מעגל המחשב אותה.
נבנה מעגל מחולק לרמות. איך? הקלטים יהיו ברמה הראשונה ועומק יוגדר כמרחק לרמה הראשונה. העומק יהיה $t(n) = n^c$ – הזמן שיקח למכונה לרוץ. כל רמה תקבל זמן חישוב $1, \ldots, t(n)$. ברמה יהיו $s(n) \leq t(n)$ בלוקים ב- $s(n)$ גודל הזכרון.
בבלוק: קודקוד אחד שיחזיק האם הראש הקורא נמצא בתא או לא. קבוצה של קודקודים $\log \Sigma$ שתחזיק את ערך התא וקבוצת קודקודים בגודל $\log S$ קודקודים שתחזיק את מצב המכונה אם הראש הקורא נמצא שם.
הרמה הראשונה עמורה לשקף מצב תחילי של המכונה. הראש הקורא נמצא בתא הראשון לכן נשים 1 בקודקוד המתאים. אז יופיע משתנה x_1 (חלק ממשתנה הקלט) ואז הקידוד של q_{start}. אח"כ יהיה 0 (הראש הקורא לא בתא השני) אח"כ x_2 משתנה קלט שני ואז "לא משנה מה" כי הראש ממלא לא נמצא שם, ונדאג לשים משהו הגיוני רק כשנגיע לשם. כך נשמיך עד שנסיים עם משתני הקלט. בסוף יהיה בלוק המורכב מ- 0, הסימן המיוחד שאומר שכאן הסתיים הקלט ולא משנה מה נוסף.
שאר הרמות מורכבות מקודקודים דומים: עם בלוק של מיקום הראש, תוכן התא ומצב המכונה. המטרה היא לחבר בין הרמות עם שערים לוגיים כדי שהמעגל באמת יעבוד.

אבחנה. בלוק כלשהו ברמה $i+1$ במקום j תלוי רק בשלושה בלוקים מרמה i במיקומים $j-1, j, j+1$. מדוע? אם לא שינינו את ערך התא הנוכחי (לדוגמא בגלל שהראש בכלל במקום אחר) אז ערך הבלוק הוא פשוט כמו הבלוק המתאים רמה למטה. אם לעומת זאת שינינו את הערך, אז בוודאי עברו על-ידי פונקציית המעברים מאחד התאים הסמוכים רמה אחת למטה.

אנחנו רוצים לממש את זה אבל בלי לכתוב באמת את כל הנוסחאות כשערים לוגיים. כיצד נעשה את זה? ראשית, בשלושת הבלוקים $j-1, j, j+1$ יש לנו - $\log\Sigma+\log S+1 = O(1)$ קודקודים. כעת נוכל להשתמש ברעיון הקודם.
מ"ט שפותרת את $TM-To-Cricut-M$ תבנה טבלת אמת לכל סדרה של ערכים של שלוש בלוקים ותוציא את הערך של הבלוק הבא. מספר השורות בטבלה קובע. חישוב עבור הבלוק הבא הוא גם בגודל קבוע (כי צריך לעבור על פונקצית המעברים ולכן קבוע בגודל הקלט). כעת מתרגמים את טבלת האמת למעגל בעומק קבוע. זהו נותר רק לחבר כל שלשה של מצבים עם המעגל לבלוק מרמה מעל.
נכונות: זה קל. באינדוקציה על i הרמה i נכונה. באיזה מובן?

- לכל בלוק ברמה הערך שאומר האם הראש הקורא נמצא בתא וערך הסימבול בתא תואמים למצב בהרצת מכונת הטיורינג M על הקלט x לזמן ה- i ולמקום b.
- לכל בלוק b ברמה אם הראש הקורא נמצא עליו אז המצב של המכונה נכון.

זמן ריצה: $t(n)$ רמות. $t(n)$ בלוקים ברמה ולכל בלוק $O(1)$ זמן.
למרות שבנינו מ"ט פולינומיאלית שמקבלת מכונת טיורינג כקלט, לרוב נניח שמכונת הטיורינג M נתונה מראש ונוכל לבנות מכונת טיורינג מתרגמת ספציפית. לבעיה כזאת נקרא $TM-To-Circuit-M$.

כיצד מתרגמים מעגל למכונת טיורינג?

לבעית תרגום מעגל למכונת טיורינג נקרא $Circut-To-SAT$.
היא תקבל כקלט מעגל C על n קלטים ותוציא כפלט: נוסחאת SAT φ על $x_1,\ldots,x_n$ כך ש- $C(x)=1 \Leftrightarrow \varphi(x_1,\ldots,x_n)$ ספיק.
מן הסתם נרצה שכל העסק יהיה פולינומיאלי.
אלגוריתם: גם מעגל הוא משהו לוקלי. נכניס משתנה עבור כל קודקוד של המעגל. עבור כל שער נעשה פסוקית בין המשתנים המתאימים. בסוף נתרגם הכל ל-SAT. על כל הפסוקיות בסוף ניקח כמת "וגם". רוצים שהפסוק יהיה פסוק אמת רק אם הקלט מקבל, אז נוסיף "וגם" עם שער הפלט.
נוסחא סופית:

$$\bigwedge(\text{כל הפסוקיות שבנינו}) \wedge z_{output}$$

משפט קוק־לווין

משפט. קוק-לוין
SAT היא NP קשה.

תזכורת. SAT: קלט: נוסחאת SAT $\varphi(x)$. פלט: האם יש x כך ש- $\varphi(x)$ ספיקה.

אכן עשינו את ההוכחה במודלים. נראה הוכחה אחרת:

הוכחה. תהי L ב- NP. נרצה להראות $L \leq_{\text{p}} SAT$. כלומר צריך להראות $\psi \in P$, $\psi : \{0,1\}^* \to \{0,1\}^*$ כך ש- $x \in L \Leftrightarrow \psi(x) \in SAT$.
בניה של ψ:
בהינתן $x \in \{0,1\}^*$
$L \in NP$ לכן יש מ"ט $M(x,y)$ כך ש-

$$x \in L \Leftrightarrow \exists y M(x,y) = 1$$

וגם $|y| = poly(|x|)$, $M \in P$.
ψ תקח את M תריץ $TM - To - Circuit - M$ ומקבלת כפלט מעגל C.
תיקח את המעגל C ותריץ $Circuit - To - SAT$. נקבל נוסחא χ.
מיהם קלטי χ? $\chi_x(y_1, \ldots, y_m) = \chi(\underbrace{x_1, \ldots, x_n}_{\text{המשתנה של נוסחאת } SAT \text{ שהרדוקציה } \psi \text{ קיבלה } x} , \underbrace{y_1, \ldots, y_m}_{})$.
נכונות:
$x \in L \Leftrightarrow \exists y M(x,y) = 1 \Leftrightarrow \exists y C(x,y) = 1 \Leftrightarrow \exists y \chi(x,y) = T \Leftrightarrow \chi_x \in SAT$.
□

למעשה עשינו משהו חזק יותר. יש פה שתי רדוקציות. הראשונה שמעתיקה למעגל היא מאוד פשוטה ואינטואיטיבית יכולה לעבוד עם מעט זכרון. גם המעבר מהמעגל היה לוקלי וגם לא צריכה הרבה זכרון.
למעשה הראינו גם:

משפט. $CVAL$ הוא P-קשה.

מה זה אומר בכלל? נראה בהמשך.
השלכה של זה היא ש $CVAL$ כנראה שלא תתמקבל. אם כן, נוכל למקבל את כל P ותהיה רעידת אדמה.
עד עכשיו לא התייחסנו לזכרון. נשלים פער מצער זה.

הגדרה. $CVAL$ מקבלת כקלט מעגל C וקלט $x = x_1, \ldots, x_n$ והפלט הוא $C(x)$. כלומר לחשב את ערך המעגל עבור קלט נותן.

$CSAT$ לעמות זאת מקבל רק מעגל C על n קלטים והפלט הוא כן אם ורק אם יש קלט שיגרום ל- C לקבל.
$CVAL$ היא ב- P. זה ברור. בהינתן קלט מעגל C על n קלטים ו- $x_1, \ldots, x_n$. יודעים את הערך של שערי הקלט $x_1, \ldots, x_n$. כעת נרוץ בלולאה ולכל קודקוד ששני השערים תחתיו כבר נקבעו נחשב את הערך שלו.

חישוב מוגבל זיכרון

הגדרה. חישוב מוגבל זיכרון
נגדיר מכונת טיורינג עם שלושה סרטים: סרט קלט, סרט עבודה וסרט פלט. סרט הקלט הוא לקריאה בלבד, לא נוכל לשנות אותו אלא רק נוכל להזיז עליו את הראש כדי לקרוטא. סרט עבודה הוא סרט רגיל, אפשר לכתוב ואפשר לזוז ימינה או שמאלה. סרט הפלט יכול להיות יותר מהזכרון שלנו אפשר רק לכתוב אליו ויש לו כיוון (כלומר אחרי שרשמנו בהכרח זזים).

ככה אפשר להתייחס למצבים בהם זיכרון החישוב קטן מזכרון הקלט. איפה בכלל רואים דברים כאלה? Streaming video.

הגדרה. נאמר כי מכונת טיורינג משתמשת ב- S זכרון על קלט x אם בהרצה של M על x אנחנו משתמשים בלכל היותר s תאים של סרט העבודה. נספור רק את סרט העבודה, לא את סרט הקלט ולא את סרט הפלט.

דוגמא. כפל מטריצות. קלט- מטריצות A, B $n \times n$ $a_{i,j}, b_{i,j} \in \{0,1\}$ הפלט: AB בשלמים.
כמה זיכרון באמת נצטרך על סרט העבודה?
לכל $1 \leq i, j \leq n$ נחשב $c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$ ונפלוט אותו למדפסת. ל- i, j נצטרך $\log$ ביטים של זיכרון.למעשה יש שתי ללואות שרצות על האינדקסים. הסכום הוא למעשה ללואלה נוספת. אז נצטרך בערך $4 \log n$ זכרון. לשמור i, j, k את התוצאה וחישובי ביניים.

טענה. אפשר לממש פתרון ל- $TM - To - Circuit - M$ ע"י מ"ט שרצה $Logspace$.

הוכחה. זאת בדיוק הרדוקציה שעשינו קודם. המכונה פולינומיאלית.

1. חישבה את הטבלה. זה קבוע. נקצה $O(1)$ זכרון ונכתוב את המעגל המתאים לטבלה.
2. נרוץ בלולאה על כל רמה, ונרוץ בלולאה על כל הבלוקים ונעתיק את המעגל בגודל $O(1)$ שכבר עכשינו. צריך לשמור שני רגיסטרים ללולאות $t(n) = n^c$ לכו $\log(t(n)) = c \log n$ ולכן סה"כ המכונה תרוץ בזכרון לוגריתמי.

□

הגדרה. $A \leq_L B$ אם יש $\varphi : \{0,1\}^* \to \{0,1\}^*$ כך ש-

$$x \in A \quad \Leftrightarrow \quad \varphi(x) \in B \wedge \varphi \in Logspace$$

הגדרה. נאמר ששפה A היא P שלמה אם $A \in P$ וגם לכל $B \in P$, $B \leq_L A$.

הכוח של הרדוקציה צריך להיות קטן מכוח המחלקה כדי שנוכל לעבור בין שפות עם תרגומים פשוטים ושלא נקבל שכל השפות שלמות.

משפט. $Logspace \subseteq P$.

הוכחה. מכונת $Logspace$ לא יכולה להיות ביותר מדי מצבים שונים. נקבע לה את הקלט. יש לה s ביטים של זיכרון אז היא יכולה להיות ב- 2^s מצבים (אחרת היא נכנסת ללולאה אינסופית).
תהי $A \in Logspace$ ונניח נפתרת ע"י מכונה $M \in Logspace$. לכן $M \in P$ ונקבל $A \in P$. מדוע $M \in P$? יהי $x \in \{0,1\}^n$. יודעים ש- M עוצרת על x. השאלה כמה זמן יקח לה. נניח שלוקח לה יותר מ- $2^s \cdot n \cdot s \cdot |Q|$ צעדים על x. סרט הקלט לא משתנה. המיקום של הראש יכול להשתנות ויכולות להיות לו n אפשרויות. סרט העבודה עליו אפשר לכתוב מה שרוצים. אורכו s לכן יש 2^s אפשרויות מה כתוב עליו, וכן s אפשרויות למיקום הראש הקורא. סרט הפלט בכלל לא מעניין אותנו "שגר ושכח" כי הוא לא משפיע על כלל ההתקדמות. יש עוד $|Q|$ אפשרויות למצבים של מכונת טיורינג. בסה"כ $2^s \cdot n \cdot s \cdot |Q|$ אפשרויות. אם זמן הריצה של M על x יותר גדול מזה אז בהכרח יש מצב שמופיע פעמיים. המכונה דטרמיניסטית ולכן תיכנס ללולאה אינסופית ולא תעצור וזו סתירה כי הנחנו ש- M עוצרת.
לכן זמן הריצה של M על x הוא $2^s ns|Q|$ והיות ו- $s = O(\log n)$ אז $2^s ns|Q| = poly(n)$.
□

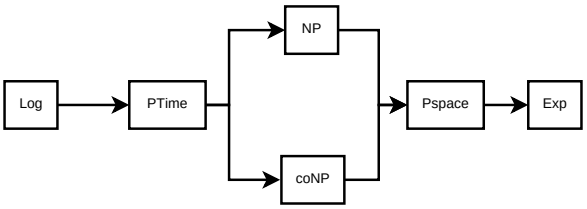
ההוכחה הזאת מראה גם ש-

משפט. לכל $S(n) \geq \log n$ אז $Space(S(n)) \subseteq Time(2^{O(s(n))})$

M רצה בזכרון $s(n)$ ועוצרת אז היא עושה זאת תוך $2^{s(n)}s(n)n|Q|$

הגדרה. $EXP = \bigcup_c Time(2^{n^c})$

טענה. $NP \subseteq Pspace$.



החצים מסמלים הכלה כמובן.

הגדרה. בהינתן מ"ט M עם זכרון s וקלט $x \in \{0,1\}^n$. הקונפיגורציה של M על x מכילה את המידע הבא: מיקום ראש קורא סרט קלט, מיקום ראש קורא סרט עבודה, ערכי סרט העבודה, מצב המכונה.

את התקדמות המכונה אפשר לתאר בגרף הקונפיגרוציות:
הקודקודים הם כל הקונפיגורציות האפשריות. הקשתות – יש קשת בין קונפיגורציה c_1 לקונפיגורציה c_2 אם"ם המכונה מקונפיגורציה c_1 עוברת בשלב הבא לקונפיגורציה c_2.
אם M פותרת את x בגרף הקונפ יש לכל היותר $2^{s(n)}s(n)n|Q|$ קודקודים. דרגת היציאה של כל קודקוד היא 1 כי המכונה דטר'.
אזהרה: חישוב מוגבל זיכרון מרשים פלט הרבה יותר ארוך משטח העבודה. התייחסנו לזה כאילו שזה לא מהווה בעיה. אבל, אנחנו מצפים שאם $A \leq_L B$, $B \leq_L C$ אז $A \leq_L C$. באיזה רדוקציה היינו רוצים להשתמש? $\varphi(x) = \varphi_1(\varphi_2(x))$. אבל זאת בעיה כי איך בדיוק φ_2 אמורה לתפוס את הקלט שהמכונה של φ_1 פולטת?
נראה בהמשך שזה נכון אבל רק למספר הכלות סופי.