תורת הסיבוכיות – תרגול 10
תכניות מתפצלות ומשפט ברינגטון

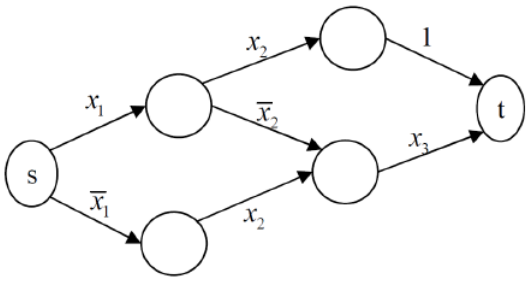
תכנית מתפצלת – הגדרה

תכנית מתפצלת (Branching Program) היא רביעיה $\pi = (G, s, t, \phi)$ כאשר G הוא DAG, s צומת התחלה, t צומת יעד, ו־ ϕ פונקציה המתאימה לכל קשת ליטרל חיובי, ליטרל שלילי או קבוע. כל השמה x למשתנים משרה תת גרף G_x המכיל רק את הקשתות שסימוניהן מסתפקים על ידי x.

π נקראת **דטרמיניסטית** אם תחת כל השמה x, דרגת היציאה של כל צומת ב־ G_x היא לכל היותר 1; אחרת π היא **אי דטרמיניסטית**.

π מקבלת את x אם בגרף G_x קיים מסלול מ־ s אל t ("מסלול מקבל"). בכך היא למעשה מגדירה פונקציה $f : \{0,1\}^n \to \{0,1\}$ (1 מותאם לקלט שמתקבל ו־ 0 לקלט שאינו מתקבל).

דוגמה:



גרף זה מחשב את $\text{Majority}(x_1, x_2, x_3)$, כלומר מקבל 1 אם ורק אם לפחות שניים מהמשתנים מקבלים 1.

אם הגרף G של תכנית מתפצלת הוא גרף שכבות (כלומר, ניתן לחלק את צמתיו לשכבות כך שכל קשת היא בין שתי שכבות עוקבות), אז ה**רוחב** של π הוא גודל השכבה הגדולה ביותר, וה**אורך** הוא מספר השכבות פחות 1.

בדוגמה שלנו הרוחב הוא 2 והאורך הוא 3.

משפט ברינגטון

כרגיל בתורת הסיבוכיות, העניין בתכניות מתפצלות נובע מהיותן מודלים פשוטים יחסית של חישוב, ומכאן מקור לתקווה שיהיה ניתן להוכיח עליהן חסמים תחתונים בקלות (ולהסיק מהם חסמים תחתונים על מודלים אחרים). לרוע המזל מציאת חסמים תחתונים לתכניות מתפצלות כלליות התגלתה כמאתגרת, ולכן החוקרים פנו לתקיפת בעיה מוגבלת יותר. בשנת 1983 הועלתה השערה (על ידי שתי קבוצות חוקרים שונות) לפיה אם מגבילים את <u>הרוחב</u> של תכנית מתפצלת לרוחב קבוע, אז תכנית מתפצלת עבור פונקציית ה־ Majority (ובהכללה, פונקציות NC^1) דורשת אורך סופר־פולינומי. במאמר נוסף הוכח חסם תחתון סופר־לינארי עבור תכניות מתפצלות מרוחב קבוע, ולאחר מכן תוצאה זו שופרה על ידי הסרת הדרישה לרוחב קבוע. נראה היה שהמחקר מתקרב למציאת חסמים תחתונים משופרים אף יותר, אך אז בשנת 1989 הבעיה נקברה לחלוטין כאשר ברינגטון הוכיח את התוצאה המפתיעה לפיה ההשערה שגויה.

<u>משפט</u>: $L \in \mathsf{NC}^1$ אם ורק אם קיימות ל־ L תכניות מתפצלות בעלות רוחב 5 ואורך פולינומי.

כזכור, NC^1 היא מחלקת השפות שקיימת עבורן משפחת מעגלים בעלי דרגת כניסה חסומה, בגודל פולינומי, ובעומק $O(\log n)$.

אנו עוסקים כאן במשפחות לא יוניפורמיות (הן של מעגלים והן של תכניות מתפצלות); אם מצטמצמים לעיסוק במשפחות יוניפורמיות לא חל שינוי מהותי בהוכחה.

הוכחת הכיוון הקל

תהא L עבורה קיימת משפחת תכניות מתפצלות ברוחב 5 ובאורך פולינומי, ונראה ש־ $L \in \mathsf{NC}^1$.

נבנה באופן רקורסיבי נוסחה $\Psi_{v_1,v_2}(x)$ שהיא 1 אם ורק אם קיים מסלול מ־ v_1 ל־ v_2 ב־ G_x, באופן שדומה באופיו להוכחת משפט סביץ'.

הבסיס ברור: אם v_2 בשכבה העוקבת ל־ v_1 אז $\Psi_{v_1,v_2}(x) = \begin{cases} 0 & (v_1,v_2) \notin E \\ \phi(v_1,v_2) & (v_1,v_2) \in E \end{cases}$.

אם v_2 נמצא לפחות במרחק שתי שכבות מ־ v_1 אז נגדיר $\Psi_{v_1,v_2}(x) = \bigvee_{u \in U} (\Psi_{v_1,u}(x) \wedge \Psi_{u,v_2}(x))$.

כאן U היא השכבה שבאמצע הדרך בין v_1 ל־ v_2 (קרובה יותר ל־ v_1 אם מספר שכבות הביניים הוא זוגי).

הנוסחה המובקשת היא $\Psi_{s,t}(x)$.

ניתוח:

נסמן ב־ $s(m)$ את גודל המעגל המתקבל בשיטה שלעיל לתכנית מתפצלת באורך m.

נשים לב שבנוסחה הרקורסיבית אנו בונים את המעגל של $\Psi_{v_1,v_2}(x)$ באמצעות 10 תתי־מעגלים לכל היותר (כי גודל U הוא לכל היותר 5 שכן רוחב התכנית המתפצלת הוא 5, ולכל $u \in U$ יש שתי תתי־נוסחאות), ונשים לב שכל תת־מעגל כזה מתאים לתכנית מתפצלת באורך $\frac{m}{2}$.

מכאן ש־ $s(m) \leq 10 \cdot s\left(\frac{m}{2}\right) + 9$, ואחרי פתרון נוסחת הנסיגה נקבל $s(m) = O\left(10^{\log_2 m}\right) = O\left(m^{\log_2 10}\right)$ – פולינומי ב־ m.

נסמן ב־ $d(m)$ את עומק המעגל שמתקבל לתכנית מתפצלת בגודל m. בבירור $d(m) = 2 + d\left(\frac{m}{2}\right) = O(\log m)$ (ה־ 2 מגיע משערי ה־ $\vee$ וה־ $\wedge$ שבהם השתמשנו).

הוכחת הכיוון הקשה

הוכחת כיוון זה תתבצע בשני שלבים. ראשית נציג מודל ביניים בין מעגלים ותכניות מתפצלות – **תכניות חבורה** – ונראה כיצד ניתן להמיר מודל זה לתכנית מתפצלת רגילה; ולאחר מכן נראה כי קיימת תכנית חבורה קטנה יחסית עבור כל מעגל.

תכניות חבורה

<u>תזכורת</u>: **פרמוטציה** על קבוצה A היא פונקציה $\sigma : A \to A$ שהיא חד־חד ערכית ועל. בדרך כלל בוחרים את A להיות $A = \{1, 2, \ldots, n\}$ עבור ה־ n שנוח לנו.

אוסף כל הפרמוטציות על $A = \{1, 2, \ldots, n\}$ מסומן ב־ S_n. קבוצה זו מהווה <u>חבורה</u> ביחס לפעולת ההרכבה של פרמוטציות: $\sigma \cdot \tau$ היא הפרמוטציה שמתקבלת על ידי הפעלת τ ומייד לאחר מכן הפעלת σ.

מעגל הוא פרמוטציה המסומנת כ־ $(a_1\ a_2\ \ldots\ a_k)$ שבה $\sigma(a_1) = a_2, \sigma(a_2) = a_3, \ldots, \sigma(a_k) = a_1$ ואת האיברים שאינם במעגל σ מעבירה לעצמם. משפט בסיסי בתורת החבורות מראה כי כל פרמוטציה ב־ S_n ניתנת לתיאור כמכפלה של מעגלים זרים (ללא מספרים משותפים). למשל, $(1\ 3)(2\ 5\ 4)$ היא הפרמוטציה שמעבירה את 1 ל־ 3, את 3 ל־ 1, את 2 ל־ 5, את 5 ל־ 4, ואת 4 ל־ 2.

פרמוטצית הזהות, שנסמנה ב־ e, היא הפרמוטציה שמעבירה כל איבר לעצמו.

תכנית חבורה באורך l מתאימה פרמוטציה לכל השמה למשתנים $x = (x_1, \ldots, x_n)$, כאשר הפרמוטציה נבנית כמכפלה של l פרמוטציות ובכל סיבוב נבחרת אחת משתי פרמוטציות אפשריות להוספה למכפלה על פי אחד מביטי הקלט. פורמלית תכנית פרמוטציות מוגדרת על ידי סדרה של שלשות $\left(g_1^0, g_1^1, k_1\right), \left(g_2^0, g_2^1, k_1\right), \ldots, \left(g_l^0, g_l^1, k_l\right)$ כך ש־ $g_i^b \in S_5$ ו־ $k_i \in \{1, \ldots, n\}$. שימו לב לבחירה שלנו ב־ S_5; ניתן להשתמש גם בחבורות פרמוטציות גדולות יותר אך אנו לא נזדקק לכך ומכאן ההגדרה המצומצמת.

הפלט של התכנית על ההשמה x הוא $\prod_{i=1}^{l} g_i^{x_{k_i}}$.

עבור $f : \{0,1\}^n \to \{0,1\}$ כלשהי אומרים שתכנית חבורה σ־מחשבת את f (עבור פרמוטציה $\sigma \neq e$ כלשהי) אם:

- עבור x כך ש־ $f(x) = 1$, פלט תכנית החבורה הוא σ.
- עבור x כך ש־ $f(x) = 0$, פלט תכנית החבורה הוא e.

מתכנית חבורה לתכנית מתפצלת

נראה כעת כי ניתן לסמלץ תכניות חבורה באמצעות תכנית מתפצלת מרוחב 5 ובעלת l שכבות. הרעיון הוא שכל שכבה תכלול בדיוק 5 צמתים המייצגים את האיברים שעליהם פועלות הפרמוטציות שבתכנית החבורה (כזכור, התכנית מוגדרת באמצעות פרמוטציות מ־ S_5; לסימולציה עבור S_t כללי היה צורך ברוחב t של התכנית המתפצלת).

פורמלית, נניח כי יש לנו תכנית חבורה מאורך l אשר σ־מחשבת את f. נבנה תכנית מתפצלת עבור f באופן הבא:

- $V = \left\{v_1^1, \ldots, v_1^5\right\} \cup \cdots \cup \left\{v_l^1, \ldots, v_l^5\right\}$.
- עבור השלשה $\left(g_i^0, g_i^1, k_i\right)$ שבתכנית החבורה, ולכל $1 \leq r \leq 5$ נוסיף לתכנית המתפצלת שתי קשתות: $\left(v_i^r, v_{i+1}^{g_i^0(r)}\right)$ עם הליטרל $\overline{x_{k_i}}$, ו־ $\left(v_i^r, v_{i+1}^{g_i^1(r)}\right)$ עם הליטרל x_{k_i}.

- נניח בלי הגבלת הכלליות כי $\sigma(1) \neq 1$ (קיים מספר שאותו σ אינה מעבירה לעצמו שכן $\sigma \neq e$), ונבחר את הצומת ההתחלתי להיות $s = v_1^1$ ואת הצומת הסופי להיות $t = v_l^{\sigma(1)}$.

ניתן להוכיח באינדוקציה על l שהבניה עובדת, כלומר שעבור השמה x, אם פלט תכנית החבורה הוא τ, אז בתכנית המתפצלת המתאימה יש מסלול מ־ v_1^r אל $v_l^{\tau(r)}$ לכל $1 \leq r \leq 5$.

ממעגל בוליאני לתכנית חבורה

נוכיח כעת את הטענה (המפתיעה!) הבאה: כל פונקציה $f : \{0,1\}^n \to \{0,1\}$ אשר ניתנת לחישוב באמצעות מעגל בוליאני מעומק d, ניתנת ל־σ־חישוב על ידי תכנית חבורה (עם פרמוטציות מתוך S_5) מאורך $l = 4^d$, כאשר σ הוא 5־מעגל כלשהו. זה יסיים את ההוכחה שכן עבור פונקציות ב־ NC^1 נקבל תכנית חבורה מאורך פולינומי.

<u>**אבחנה**</u>: אם σ, τ הם שני 5־מעגלים ו־ f ניתנת ל־ σ־חישוב על ידי תכנית מאורך l, אז f ניתנת ל־ τ־חישוב על ידי תכנית מאורך l.

כלומר, הזהות הספציפית של המעגל אינה משנה כל עוד הוא 5־מעגל. הסיבה לכך היא שכל שתי פרמוטציות שיש להן אותו מבנה מעגלים (בפירוק שלהן למכפלת מעגלים זרים יש אותה כמות מעגלים ואותם גדלים של מעגלים) הן **צמודות**: קיימת פרמוטציה ρ כך ש־ $\tau = \rho\sigma\rho^{-1}$ (זהו משפט אלמנטרי נוסף מתורת החבורות שלא נוכיח כאן).

אם כן, אם $\left(g_1^0, g_1^1, k_1\right), \left(g_2^0, g_2^1, k_1\right), \ldots, \left(g_l^0, g_l^1, k_l\right)$ היא תכנית ש־ σ־מחשבת את f, אז תכנית מאותו אורך ש־ τ־מחשבת את f היא $\left(\rho g_1^0, \rho g_1^1, k_1\right), \left(g_2^0, g_2^1, k_1\right), \ldots, \left(g_l^0\rho^{-1}, g_l^1\rho^{-1}, k_l\right)$.

זאת מכיוון שפלט התכנית החדשה הוא $\rho^{-1}\left(\prod_{i=1}^{l} g_i^{x_{k_i}}\right)\rho$, ולכן אם פלט התכנית הישנה היה σ אז פלט התכנית החדשה יהיה $\tau = \rho\sigma\rho^{-1}$, ואם פלט התכנית הישנה היה e אז פלט התכנית החדשה יהיה $\rho e \rho^{-1} = e$.

נעבור כעת לבניית תכנית החבורה. נראה בניה אינדוקטיבית – דהיינו, כיצד לכל צומת במעגל ניתן לבנות תכנית חבורה שמחשבת את אותה הפונקציה כמו הצומת הזה. לצורך פשטות נניח כי המעגל כולל שערי $\neg$ ו־ $\wedge$ וליטרלים חיוביים בלבד (את $\vee$ ניתן לסמלץ בעזרת דה־מורגן מבלי לגרום לשינוי מהותי בעומק).

בסיס: עבור צומת ליטרל x_i שמייצג את הפונקציה $f(x) = x_i$ נבנה את תכנית הפרמוטציות (e, σ, i). מכאן שאפשר לבנות תכנית פרמוטציות ש־σ־מחשבת את f לכל $\sigma \neq e$ ובפרט לכזו שהיא 5־מעגל.

צעד – שער NOT: נניח כי יש לנו תכנית P מאורך l אשר σ־מחשבת את הפונקציה f ונבנה תכנית P' מאורך l עבור $\neg f$: P' תהיה זהה ל־ P פרט לשלשה האחרונה. אם ב־ P השלשה הייתה $\left(g_l^0, g_l^1, k_l\right)$ אז ב־ P' השלשה תהיה $\left(g_l^0\sigma^{-1}, g_l^1\sigma^{-1}, k_l\right)$.

כעת, אם $f(x) = 1$ אז $P(x) = \sigma$, ולכן $P'(x) = \sigma\sigma^{-1} = e$; ואילו אם $f(x) = 0$ אז $P(x) = e$, ולכן $P'(x) = e\sigma^{-1} = \sigma^{-1}$. לכן P' σ^{-1}־מחשבת את $\neg f$, ואם σ היה 5־מעגל, כך גם σ^{-1}.

צעד – שער AND: זה החלק המורכב של הבניה (וזה שיגרום לניפוח התכנית). נניח כי P_1 σ_1־מחשבת את f_1 ו־ P_2 σ_2־מחשבת את f_2, אורכיהן הם l_1, l_2 בהתאמה, ו־ σ_1, σ_2 הן 5־מעגלים. נבנה P אשר σ_3־מחשבת את $f_1 \wedge f_2$ כך ש־ σ_3 אף היא 5־מעגל ואורך P הוא $2(l_1 + l_2)$.

קיימים שני 5־מעגלים τ_1, τ_2 אשר גם הקומוטטור $\tau_1\tau_2\tau_1^{-1}\tau_2^{-1}$ שלהם הוא 5־מעגל. למשל, עבור $\tau_1 = (1\ 2\ 3\ 4\ 5), \tau_2 = (1\ 3\ 5\ 4\ 2)$ בדיקה ישירה מראה כי הקומוטטור הוא $\tau = (1\ 3\ 2\ 5\ 4)$. זו הסיבה שבגללה היה עלינו להשתמש בפרמוטציות מאורך 5 ולא קטן יותר; תופעה דומה לא מתקיימת עבור פרמוטציות על 4 איברים או פחות.

ניתן להניח בלי הגבלת הכלליות כי P_1 τ_1־מחשבת את f_1 ו־ P_2 τ_2־מחשבת את f_2, שכן, כפי שכבר ראינו, ניתן להחליף כל 5־מעגל ב־ 5־מעגל אחר מבלי לשנות את אורך התכנית. בדומה, קל לבנות תכניות P_1^{-1} ו־ P_2^{-1} מאותם אורכים של P_1, P_2 כך ש־ P_1^{-1} τ_1^{-1}־מחשבת את f_1 ו־ P_2 τ_2^{-1}־מחשבת את f_2.

כעת נגדיר תכנית חדשה: $P = P_1P_2P_1^{-1}P_2^{-1}$. אורך התכנית הוא $2(l_1 + l_2)$. כמו כן:

- על קלט x שעבורו $f_1(x) = f_2(x) = 1$ יתקיים $P(x) = \tau_1\tau_2\tau_1^{-1}\tau_2^{-1} = \tau$.
- על קלט x שעבורו $f_1(x) = 1$ ו־ $f_2(x) = 0$ יתקיים $P(x) = \tau_1 e \tau_1^{-1} e = e$. באופן דומה יתקיים $P(x) = e$ אם $f_1(x) = 0$ ו־ $f_2(x) = 1$.

מכאן ש־ P אכן τ־מחשבת את $f_1 \wedge f_2$ עבור τ שהיא 5־מעגל.

סיכום: הראינו כי ניתן לקבל באינדוקציה תכנית חבורה אשר σ־מחשבת את f של מעגל כלשהו, עבור σ כלשהי שהיא 5־מעגל. אם $s(d)$ הוא האורך המקסימלי של תכנית החבורה שהבנייה מניבה עבור מעגל מעומק d עם 2 fan-in, ראינו כי $s(d+1) \leq 2(s(d) + s(d)) = 4s(d)$. מכאן ש־ $s(d) \leq 4^d$, כנדרש.