סיבוכיות – הרצאה 7

כל העולם הוא חישוב אחד גדול

5.4.11

PM - Perfect matching

הקלט: גרף דו צדדי $G = (V, W, E)$, $E \subseteq V \times W$, $|V| = |W| = n$.
הקלט בשפה אם יש זיווג מושלם בגרף.
הבעיה ב– P, למשל אפשר לפתור ע"י רשתות זרימה כמו שעושים באלגוריתמים.

אז למה בכלל נתעניין בבעיה? נרצה להסתכל על פתרון אחר ונראה מה אפשר להסיק.
ניקח את הגרף G ונבנה מטריצה $n \times n$ כך שבמקום i, j:

$$A_{ij} = \begin{cases} 0, & (i,j) \notin E \\ x_{ij} (i,j) \in E \end{cases}$$

$x_{i,j}$ הוא סימבול. אם זה היה אחד היינו מקבלים בדיוק את מטריצת השכנויות.

טענה. ב– G יש זיווג מושלם אם ורק אם $det(A)$ כפולינום במשתנים x_{ij} אינו פולינום האפס.

הוכחה.

$$\det A = \sum_{\pi \in S_n} \operatorname{sgn}(\pi) A_{1,\pi(1)} \dots A_{n,\pi(n)}$$

כאשר הסימן של זהות הוא 1 והסימן של חילוף הוא -1 והסימן הוא שומר על הכפל.

תזכורת. מאלגברה, כל תמורה היא מכפלה של חילופים.

אם $n = 1$, $A = \begin{pmatrix} a_{11} \end{pmatrix}$ ואז $\det A = a_{11}$.

אם $n = 2$, $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ ואז $\det A = ad + (-1)bc$.

מהו זיווג מושלם? זה סוג של תמורה על אחד הצדדים שאותה נתאים ע"י קשתות לצד השני.
כלומר, שקיימת קשת בין צומת לצומת שהותאם ע"י הפרמוטציה.
כי לכל מועמד לזיווג מושלם π (שהוא למעשה פרמוטציה על אחד הצדדים) אבל בגלל שאין זיווג מושלם יש i כך ש– $(i, \pi(i)) \notin E$ לכן המכפלה $A_{1,\pi(1)} \dots A_{n,\pi(n)}$ היא זהותית 0, ולכן זה פולינום האפס. באותו האופן גם הכיוון השני. □

באופן כללי יופיעו בסכום $n!$ איברים (כמספר הפרמוטציות). וזה מספר מאוד אקספוננציאלי: $n! = 2^{\theta(n \log n)} = n^{\theta(n)}$.
עכשיו לקלט שלנו גודל הקלט הוא פולינומי ב– n ואם נרצה לחשב ככה נצטרך זמן אקספוננציאלי. אבל, אנחנו יודעים שהדטרמיננטה של מטרציה לא משתנה אם משנים בסיס. בפרט, ניקח את A, נשלש ועכשיו קל לחשב דטרמיננטה – זה פשוט מכפלה של איברי האלכסון. לשנות בסיס זה גם קל, אפשר למשל לדרג וזה בעך $O(n^3)$. חסכנו.
האם סיימנו? זה עובד טוב מאוד כשמדובר בסקלרים. אבל ניזכר שבמטריצה מופיעים בכלל משתנים ואז לדוגמא כשנצטרך להכפיל בהופכי, נקבל פונקציה רציונלית ונתחיל לקבל ביטויים

ענקיים, שהאורך שלהם כל הזמן גדל ואפילו עלולים לקבל ביטויים שאורכם אקספוננציאלי.
אז זה לא יעבוד.
מצד שני, הפולינום שנקבל הוא ב- n^2 משתנים לכל היותר, דרגה של כל משתנה היא לכל היותר 1 והדרגה של הפולינום היא לכל היותר n (כאשר דרגה של פולינום בהרבה משתנים זה דרגת המונום הכבד ביותר בו ודרגת מונום זה סכום דרגות כל המשתנים בו).
נראה אלגוריתם הסתברותי שפותר את PM.

1. ניקח את הגרף ונבנה את המטריצה A:

$$A_{ij} = \begin{cases} 0, & (i,j) \notin E \\ x_{ij} & (i,j) \in E \end{cases}$$

2. נבחר לכל משתנה x_{ij} ערך a_{ij} באקראי מתוך $1, \ldots, 2n$. נסמן $B = (a_{ij})$.
3. נחשב $\det B$, נגיד שיש $PM \Leftrightarrow$ המספר שקיבלנו אינו 0.

נראה נכונות:

הוכחה. מקרה 1: אין בגרף PM. במקרה זה $\det(A) \equiv 0$ (תהיה פולינום האפס). ואז ברור שלא נמצא סקלרים שלא מאפסים אותו.
מקרה 2: יש ב- G PM π. לכל i: $(i, \pi(i)) \in E$. ה- π תורם את המונום:

$$\operatorname{sgn}(\pi) x_{1,\pi(1)} \ldots x_{n,\pi(n)}$$

המונום הזה לא יכול להתבטל בגלל שפרמוטציות אחרות יוצרות מונומים שונים. לכן המסקנה היא שהדטרמיננטה של A כפולינום ב- $x_{11}, \ldots, x_{nn}$ הוא לא זהותית 0.

משפט. שוורץ-זיפל
אם F שדה ו- p פולינום ב- m משתנים מעל F $p(x_1, \ldots, x_m)$ שאינו זהותית 0 ואם $S \subseteq F$ קבוצה כלשהי של איברים אז:

$$\mathbb{P}_{a_1,\ldots,a_m \in S}(p(a_1, \ldots, a_m) = 0) \leq \frac{\deg(P)}{|S|}$$

בהינתן המשפט, נסמן $p(x_{11}, \ldots, x_{nn}) = \det A$, אם יש זיווג מושלם אז $p(x_{11}, \ldots, x_{nn}) \neq 0$, ולכן: $\deg(p) \leq n$

$$\mathbb{P}_{\text{מטבעות של האלגוריתם}}(\text{האלגוריתם טועה}) =$$
$$= \mathbb{P}_{a_{11},\ldots,a_{nn} \in [2n]} \left(p(a_{11}, \ldots, p_{nn}) = 0 \right) \leq \frac{\deg(p)}{2n} =$$
$$= \frac{n}{2^n} \leq \frac{1}{2}$$

כלומר האלגוריתם ב- RP. נוכל להפעיל n פעמים ונקבל שגיאה קטנה אקספוננציאלית. □

הערה. בעצם פתרנו בעיה קשה יותר: $Identity - Testing$ שהקלט שלה מטריצה $B_{n \times n}$ של משתנים x_{ij} והפלט הוא כן אם ורק אם $\det(B)$ כפולינום לא זהותית 0.
בעצם הוכחנו $IT \in RP$. כיום לא קיים אלגוריתם דטרמיניסטי שפותר את הבעיה בפחות מזמן אקספוננציאלי).

האם $IT \in NP$? כן. ננחש $a_{11}, \ldots, a_{nn}$, נחליף x_{ij} ב- a_{ij} נקבל מטרציה B ונבדוק האם $\det(B) = 0$. אם הפולינום הוא לא 0 אז יש השמה כך שהפולינום לא יהיה אפס. (ובכלל ראינו $RP \subseteq NP$).
אמרנו שלא ידוע כיום האם $IT \in P$. האם יכול להיות שהיא NP קשה? אם היא באמת NP קשה אז $NP \subseteq RP$ ואז $NP = RP$ ולכן הצלחנו לפתור את כל הבעיות של NP עם אלגוריתם הסתברותי.

נוכיח את משפט שוורץ ציפל:

הוכחה. נוכיח באינדוקציה על מספר המשתנים n. מקרה בסיס $n = 1$: אז $p(x)$ פולינום במשתנה אחד, מדרגה d ואז:

$$\mathbb{P}_{a \in S}(p(a) = 0) \leq \frac{d}{|S|}$$

נניח ל- m ונוכיח ל- $m + 1$.

$$p(x_1, \ldots, x_{m+1}) = \sum_{i=0}^{d_{m+1}} p_i(x_1, \ldots, x_m) \cdot x_{m+1}^i$$

כאשר d_{m+1} דרגה של x_{m+1} בפולינום. כעת,

$$\begin{aligned}\mathbb{P}_{a_1,\ldots,a_{m+1} \in S} \Big(p(a_1, \ldots, a_{m+1} = 0)\Big) \leq \\ \leq \mathbb{P}\left(p_{d_{m+1}}(a_1, \ldots, a_m) = 0\right) + \\ + \mathbb{P}\left(p(a_1, \ldots, a_{m+1}) = 0 | p_{d_{m+1}}(a_1, \ldots, a_m) \neq 0\right)\end{aligned}$$

באינדקוציה:

$$\mathbb{P}(p_{d_{m+1}}(a_1, \ldots, a_m) = 0) \leq \frac{\deg(p_{d_{m+1}}}{|S|}$$

אפילו אם נקבע $x_1, \ldots, x_{m+1}$ כמו שרוצים בהינתן $p_{d_{m+1}}(a_1, \ldots, a_m) \neq 0$ מקבלים פולינום ב- x_{m+1} שאינו אפס מדרגה d_{m+1}. עכשיו כשבוחרים $a_{m+1} \in S$ באקראי, חזרנו למקרה $n = 1$ ולכן ההסתברות לקבל 0 $\geq \frac{d_{m+1}}{|S|}$. בסה"כ:

$$\begin{aligned}\mathbb{P}_{a_1,\ldots,a_{m+1} \in S}(p(a_1, \ldots, a_{m+1} = 0)) \leq \frac{\deg(p_{d_{m+1}}}{|S|} + \frac{d_{m+1}}{|S|} \leq \\ \leq \frac{\deg(p) - d_{m+1}}{|S|} + \frac{d_{m+1}}{|S|} = \frac{\deg(p)}{|S|}\end{aligned}$$

□

דוגמא. לפולינום ממשתנה אחד יש מספר סופי של שורשים. לפולינום משני משתנים יכול להיות אינסוף שורשים: למשל $x_1 x_2$ כל המספרים $x_1 = 0$, x_2 כלשהו שורשים שלו. המשפט חוסם את אחוז השורשים, כלומר בתוך S^m אחוז השורשים $\geq \frac{\deg}{|S|}$.

הצעה: אלגוריתם יותר מוצלח ל- PM. ניקח את הגרף G, נבנה מטריצה

$$A_{ij} = \begin{cases} 1 & (i,j) \in E \\ 0 & (i,j) \notin E \end{cases}$$

גרף השכונויות.
נחשב:

$$\mathrm{perm}(A) = \sum_{\pi \in S_n} A_{1,\pi(1)} \dots A_{n,\pi(n)}$$

אם π זיווג מושלם הוא יתרום 1, ואם לא זיווג מושלם יתרום 0. נקבל את מספר הזיווגים המושלימים בגרף ובפרט נדע האם יש. הבעיה שאנחנו לא יודעים לחשב פרמננטה.

משפט. *Valiant*
אם אפשר לחשב לחשב את מספר הזיווגים המושלמים בגרף זו צדדי אז אפשר לחשב את מספר ההשמות המספקות של SAT. בפרט, פותר את כל NP.

לכן הפרמננטה היא בעיה NP קשה, למרות שהיא לא בעיית הכרעה. לא רק זה, אלה היא גם $co-NP$ קשה.

משפט. *Toda* מי שיודע לפתור את הנ"ל הוא יודע לפתור את כל ההיררכיה. לכן PH קשה.

למעשה הפרמננטה $\#P$ קשה, כלומר יכולה לפתור את כל בעיות הספירה של פרדיקטים ב-NP. וזה למעשה מה שמשפט Valiant אומר.

$$L \subseteq NL \subseteq Det \subseteq NC \subseteq P \begin{array}{c} \nearrow NP \searrow \\ \searrow coNP \nearrow \end{array} PH \subseteq \#P\text{-}PSpace$$

עובדה: $\det(A)$ A מטריצה של סקלרים אפשר לחשב במקביל עם $poly(n)$ מעבדים וזמן $O(\log^2 n)$.
כיום לא ידוע שום אלגרויתם מקבילי דטרמיניסטי יעיל ל- PM. וראינו אלגוריתם מקבילי מהיר לבעיה. זה מסמנים: $PM \in RNC$.
במקום להשוות בין BPP ל- P ננסה להשוות בין BPP למעגלים פולינומים לא אוניפורמיים.
(מחלקה אוניפורמיט - תוכנית אחת פותרת כל גודל קלט, BPP כזאת, במעגלים לעומת זאת אנחנו מרשים מעגל אחר לכל גודל קלט).

הגדרה. שפה L שייכת למחלקה $PSize$ ($P|poly$) אם קיימת סדרה מעגלים $\{c_n\}_{n\in\mathbb{N}}$, $\forall n, |c_n| \le p(n)$, p פולינום, שמשתמשת בשערי $\wedge, \vee, \neg$, ל- c_n יש n קלטים ו- $\forall n \forall x \in \{0,1\}^n$:

$$x \in L \Leftrightarrow c_n(x) = 1$$

נשווה בין BPP ל- $PSize$. נראה $BPP \subseteq PSize$. כלומר אם בעיה היא ב- BPP אנחנו לא באמת יודעים האם אפשר לפתור אותה ב- P, אבל בוודאות יש סדרת מעגלים בגודל פולינומי שפותרת. זה סוג של אינדיקציה (למרות שעברנו מאוניפורמי ללא אוניפורמי) לא חזק כמו שהוא נראה.
בהמשך אפילו נראה משפט:

משפט. *Karp - Lipton*
אם $NP \subseteq PSize$ אז ההיררכיה PH קורסת ל- $\Sigma_2 \cap \Pi_2$.

וזאת תוצאה על מחלקות אוניפורמיות. אם ההיררכיה לא קורסת אז $BPP \subseteq PSize$ ו- $BP \nsubseteq PSize$.

משפט. *Adelman 1977*
$BPP \subseteq PSize$.

הוכחה. יש מכונת טיורינג $M(x,y)$ שרצה בזמן פולינומי, $x \in \{0,1\}^n$, $y \in \{0,1\}^m$, $m = p(n)$, p פולינום ופותרת את L במובן ש-

$$x \in L \Rightarrow \mathbb{P}_y\left(M(x,y)=1\right) \geq \frac{2}{3}$$

$$x \notin L \Rightarrow \mathbb{P}_y\left(M(x,y)=1\right) \leq \frac{1}{3}$$

אפשר להוריד את השגיאה: נעשה $O(n)$ חזרות ונענה לפי הרוב. נקבל מכונת טיורינג $\tilde{M}$ חדשה $\tilde{M}(x,\bar{y})$ שרצה בזמן פולינומי, $\bar{y} = y_1, \ldots, y_{O(n)}$. ואז

$$x \in L \Rightarrow \mathbb{P}_{\bar{y}}\left(\tilde{M}(x,y)=1\right) \geq 1 - 2^{-2n}$$

$$x \notin L \Rightarrow \mathbb{P}_{\bar{y}}\left(\tilde{M}(x,y)=1\right) \leq 2^{-2n}$$

נתסכל על אורך קלט מסויים n. נבנה טבלה שהשורות הן כל הקלטים מאורך n ויש 2^n כאלה והעמודות הן המטבעות האפשריות ובתא x,y בטבלה נכתוב האם $\tilde{M}(x,y)$ עונה נכון או לא.
אנחנו יודעים שלכל שורה בטבלה אחוז השיגאות $\leq 2^{-2n}$. בפרט, אחוז השגיאות בטבלה קטן מ- 2^{-2n}. לכן, חייבת להיות עמודה בה אחוז השגיאה הוא 0 (למעשה רוב העמודות הן כאלה), אחרת לכל עמודה שהיא באורך 2^n יש לפחות שגיאה אחת ואז אחוז השגיאות $\geq 2^{-n}$, סתירה. ניקח $\bar{y}$ כזאת כלשהי, נעשה לה hard-wiring לתוך האלגוריתם ונתרגם את החישוב $\tilde{M}(x, \underbrace{\bar{y}}_{\text{קבוע}})$ למעגל $c_n(x)$. המעגל הוא בגדול פולינומי ולכל $x \in \{0,1\}^n$,

$$c_n(x) = \tilde{M}(x,\bar{y}) = \begin{cases} 1 & x \in L \\ 0 & x \notin L \end{cases}$$

□

הערה. איך נמצא $\bar{y}$ כזה? לא אכפת לנו. אנחנו מוכיחים קיום אז מספיק לנו שיש כזה.

משפט. *Karp - Lipton*
אם $NP \subseteq PSize$ אז $\Pi_2 \subseteq \sigma_2$ וממלא $\Pi_2 = \Sigma_2$ וממלא $PH = \Sigma_2$.

הוכחה. נקח בעיה Π_2 שלמה. קלט: פסוק $\forall y \exists z \varphi(y,z)$ פלט: כן אם הפסוק אמת, לא אם הפסוק לא אמת.
ידוע: $NP \subseteq PSpace$, כלומר יש $SAT \in PSize$ שפותרת את SAT כך ש- $|c_n| = poly(n)$ וכן $c_n(\varphi) = \begin{cases} 1 & \varphi \text{ ספיק} \\ 0 & \varphi \text{ לא ספיק} \end{cases}$.
לכן, יש סדרת מעגלים $\{\bar{c}_n\}$ כך ש- $|\bar{c}_n| = poly(n)$ כך ש- $\bar{c}_n(\varphi)$ מחזיר השמה $a_1, \ldots, a_n$ באופן הבא:

$$\varphi \notin SAT \Rightarrow \varphi(a) = F$$

$$\varphi \in SAT \Rightarrow \varphi(a) = T$$

כלומר סדרת המעגלים תמצא ממש את ההשמה המספקת. מדוע? כי כבר ראינו שיש רדוקציה בין חיפוש והכרעה.
בעולם האוניפורמי נרצה להשתמש במעגלים $\{\bar{c}_n\}$ אבל אנחנו לא באמת יודעים למצוא מעגלים כאלה. לכעורה אין לנו דרך לגשת אליהם בצורה מפורשת, אבל נוכל פשוט להשתמש בכמת $\exists$.
נוכל לכתוב פסוק ב- Σ_2:

$$(*)\exists \underbrace{\bar{c}}_{\substack{poly(n) \\ \text{בגודל}}} \quad \forall y \varphi(y, \bar{c}(y))$$

$\bar{c}$ מקבלת פסוק ומחזירה השמה. $\varphi(y)$ שמופיע הוא למעשה $\varphi(y,z)$ שעשינו לו hard-wiring ל- y.
אם הפסוק הוא אמת אז $\forall y \exists z \varphi(y,z)$ אז ננחש את $\bar{c}$ הנכון לכל y, הפסוק $\varphi(y, \underbrace{\cdot}_{\text{המשתנים}})$ (y קבוע) הוא ספיק לכן $\bar{c}(\varphi(y,\cdot))$ תחזיר לנו השמה מספקת z שתספק את $\varphi(y,\cdot)$. אז $\varphi(y, \bar{c}(\varphi(y,\cdot))) = True$ ולכן $(*)$ הוא אמת.
מצד שני, אם פסוק ה- Π_2 הוא שקר אז יש y כך שלכל $\varphi(y,z) = False$ ואז זה לא משנה מי הוא $\bar{c}$ עבור ה- y הזה נקבל $False$. אז הפסוק $(*)$ גם יהיה שקר.
לכן עשינו רדוקציה מפסוק - Π_2 שלם לפסוק ב- Σ_2 ואז $\Pi_2 \subseteq \Sigma_2$. □