תורת הסיבוכיות – תרגול 11
רדוקציות הסתברותיות

השפה USAT

הדוגמה שבה נשתמש בתרגול זה היא השפה USAT (קיצור של Unique SAT) של כל נוסחאות ה־ CNF שקיימת להן השמה מספקת אחת בדיוק.

נתחיל באבחנה כי שפה זו אינה קשה משמעותית מ־ SAT; בפרט, היא ניתנת לרדוקציית טיורינג ל־ SAT (במילים אחרות, מתקיים $\mathrm{USAT} \in \mathsf{P}^{\mathrm{SAT}}$).

מכונה M עם אוב ל־ SAT עבור USAT תפעל כך על קלט φ:

- תשאל את האוב על φ. אם התשובה שלילית, תדחה (אם אין השמה מספקת כלל, ודאי שאין השמה מספקת יחידה).
- תשאל את האוב על $\varphi' = \varphi(x) \wedge \varphi(y) \wedge (x \neq y)$ ותענה הפוך ממנו.

בבירור φ' ספיקה אם ורק אם יש ל־ φ שתי השמות מספקות לפחות, מה שמראה את נכונות הרדוקציה.

נשאלת השאלה כיצד ניתן לתאר את $\overline{x} \neq \overline{y}$ באמצעות CNF. ניתן לעשות זאת באמצעות משתני עזר. ראשית נשים לב לכך ש־ $x_i \neq y_i$ ניתן לתיאור באמצעות $(x_i \vee y_i) \wedge (\overline{x_i} \vee \overline{y_i})$. כעת נשתיל משתני עזר בפסוקיות אלו שיאפשרו "להציל" את ספיקות הפסוק כולו במקרה של שוויון, אך נעשה זאת באופן כזה שמשתני העזר לא יוכלו להציל את כל n המקרים בו זמנית.

פורמלית הפסוק ייראה כך:

$$[(x_1 \vee y_1 \vee z_1) \wedge (\overline{x_1} \vee \overline{y_1} \vee z_1)] \wedge [(\overline{z_1} \vee x_2 \vee y_2 \vee z_2) \wedge (\overline{z_1} \vee \overline{x_2} \vee \overline{y_2} \vee z_2)] \wedge \quad \dots \quad \wedge [(\overline{z_{n-1}} \vee x_n \vee y_n) \wedge (\overline{z_{n-1}} \vee \overline{x_n} \vee \overline{y_n})]$$

רדוקציות העתקה הסתברותית

כאשר אנו מגדירים רדוקציות תמיד עומדת מחלקה כלשהי לנגד עינינו, כשהמטרה היא לגרום לכך שאם L_2 שייכת לאותה מחלקה ו־ L_1 ניתנת לרדוקציה אליה (תחת ההגדרה המתאימה של "רדוקציה") אז גם L_1 תהיה שייכת לאותה מחלקה. כל הרדוקציות שראינו עד כה (רדוקציות העתקה רגילות, רדוקציות העתקה בזמן פולינומי, רדוקציות העתקה במקום לוגריתמי, רדוקציות טיורינג) קיימו תכונה זו. אנו מעוניינים להגדיר סוג חדש של רדוקציה שיתאים למחלקה BPP. הרדוקציה תהיה רדוקציית העתקה, במובן זה שהיא ממפה מילים ב־ L_1 למילים ב־ L_2 ומילים שאינן ב־ L_1 למילים שאינן ב־ L_2 (ולא, למשל, משתמשת באוב ל־ L_2 כקופסה שחורה, כפי שעושים עם רדוקציות טיורינג). ההבדל הוא שכעת נרשה לרדוקציה לטעות.

בהגדרת מכונות טיורינג הסתברותיות ראינו שני סוגי טעויות אפשריים: טעות דו צדדית, שמובילה למחלקה BPP, וטעות חד צדדית, שמובילה למחלקה RP. זה מוביל לשתי ההגדרות הבאות:

1. $L_1 \leq_r^{\mathsf{BPP}} L_2$, ונהוג לסמן בקצרה $L_1 \leq_r L_2$ (r עבור randomized), אם יש M פולינומית הסתברותית ופולינום $p(n)$ כך שלכל x מתקיים:

$$\mathbf{Pr}\left[x \in L_1 \iff M(x) \in L_2\right] \geq \frac{1}{2} + \frac{1}{p(|x|)}$$

2. $L_1 \leq_r^{\mathsf{RP}} L_2$ אם יש M פולינומית הסתברותית ופולינום $p(n)$ כך ש־

$$x \in L_1 \implies \mathbf{Pr}\left[M(x) \in L_2\right] \geq \frac{1}{p(|x|)}$$
$$x \notin L_1 \implies \mathbf{Pr}\left[M(x) \notin L_2\right] = 1$$

לא קשה לראות כי הרדוקציות מקיימות את משפט הרדוקציה המתאימים: אם $L_2 \in \mathsf{BPP}$ ו־ $L_1 \leq_r L_2$ אז $L_1 \in \mathsf{BPP}$, וכנ"ל עבור RP. כמו כן, שימו לב שמתקיים $L_1 \leq_r^{\mathsf{RP}} L_2 \implies L_1 \leq_r L_2$.

משפט וליאנט-וזירני

נרצה כעת להוכיח כי $\mathrm{SAT} \leq_r^{\mathsf{RP}} \mathrm{USAT}$ (מה שיראה כי אם $\mathrm{USAT} \in \mathsf{RP}$ אז $\mathsf{NP}=\mathsf{RP}$, שכן כבר ידוע כי $\mathsf{RP} \subseteq \mathsf{NP}$). תוצאה זו משנת 1985 מכונה **משפט Valiant–Vazirani** (ליתר דיוק, התוצאה חזקה מעט יותר: אנו מראים רדוקציה f כך שאם $\varphi \notin \mathrm{SAT}$ אז $f(\varphi) \notin \mathrm{SAT}$ ולא רק $f(\varphi) \notin \mathrm{USAT}$).

מה שנעשה בהינתן φ הוא להוסיף ל־ φ אילוצים אקראיים נוספים בתקווה לחסל את רוב ההשמות המספקות של φ אבל לא את כולן. לצורך כך נשתמש ב־ Universal Hashing.

פורמלית מה שעושה הרדוקציה, בהינתן φ על n משתנים, זה להגריל מספר $k \in \{2,\ldots,n+1\}$ ופונקציית תמצות $h:\{0,1\}^n \to \{0,1\}^k$, ולהגדיר פסוק $\varphi'(x)=\varphi(x) \wedge (h(x)=0)$.

הפונקציה h תהיה מהצורה $h(x)=A\cdot x+\vec{b}$ כאשר $A \in \mathrm{GF}(2)^{k\times n}$ היא מטריצה בינארית מעל $k\times n$, ו־ $\vec{b} \in \mathrm{GF}(2)^k$ הוא וקטור. זה מאפשר לנו, בהינתן A, לקודד עם נוסחת CNF מגודל פולינומי את הפרדיקט $A\cdot x+\vec{b}=0$.

<u>דוגמה</u>: אם $A=\begin{bmatrix}0&1&0\\1&1&1\end{bmatrix}$ ו־ $\vec{b}=\begin{bmatrix}1\\0\end{bmatrix}$ אז הנוסחה שמתקבלת עבור התנאי $h(x)=0$ היא $(x_2=1)\wedge(x_1\oplus x_2\oplus x_3=0)$, ונוסחה שכוללת $\oplus$ ניתן להמיר בעזרת משתני עזר ל־ CNF.

אם כן, פורמלית הרדוקציה פועלת כך:

1. בחר $k \in_R \{2,3,\ldots,n+1\}$ באקראי.
2. בחר $A \in_R \mathrm{GF}(2)^{k\times n}$ ו־ $\vec{b} \in_R \mathrm{GF}(2)^k$ באקראי עבור הפונקציה $h(x)=A\cdot x+\vec{b}$.
3. החזר את $\varphi'(x)=\varphi(x)\wedge(h(x)=0)$.

ברור כי אם φ אינה ספיקה כך גם φ'.

הרעיון הוא זה: כל שורה ב־ A מגדירה אילוץ שבהסתברות $\frac{1}{2}$ "מחסל" השמה מספקת ובהסתברות $\frac{1}{2}$ משאיר אותה בחיים. ככל שנוסיף שורות ל־ A (נגדיל את k) נחסל יותר השמות מספקות. לכן, אם בחרנו k שהוא בערך מסדר הגודל המתאים לכמות ההשמות המספקות של φ, יש סיכוי סביר שתשרוד בדיוק הכמות שאנו מקווים לה.

נעבור להוכחה הפורמלית. מרחב ההסתברות שלנו הוא כל הבחירות של h, בהתפלגות אחידה.

נסמן ב־$S \subseteq \{0,1\}^n$ את קבוצת ההשמות המספקות של φ.

נגדיר משתנה מקרי N שסופר את ההשמות ששורדות את האילוץ שמוגדר על ידי h, כלומר $N=\left|\left\{x\in S \,\middle|\, A\cdot x+\vec{b}=0\right\}\right|$ (כאן $A,\vec{b}$ הם הגורמים האקראיים).

לכל $x\in\{0,1\}^n$ בדיוק עבור מחצית מהזוגות $(\vec{a},b)$ כך ש־ $\vec{a}\in\{0,1\}^n$ ו־ $b\in\{0,1\}$ מתקיים $\vec{a}\cdot x=b$, פשוט כי היפוך ערכו של b נותן לנו זוג שעבורו בהכרח המשוואה לא מתקיימת, כלומר $(\vec{a},b)\leftrightarrow(\vec{a},1-b)$ היא התאמה חח"ע ועל, ומכאן ש־ $\mathbf{Pr}_{\vec{a},b}[\vec{a}\cdot x=b]=\frac{1}{2}$. לכן $\mathbf{Pr}_{A,\vec{b}}\left[A\cdot x+\vec{b}=0\right]=2^{-k}$ (הסתברות $\frac{1}{2}$ לכל שורה בנפרד, ולכן הסתברות $\frac{1}{2^k}$ עבור כולן יחד). נסמן $p=2^{-k}$.

כעת, מה קורה עבור זוג $x\neq y\in S$? מהי ההסתברות $\mathbf{Pr}_{A,\vec{b}}\left[A\cdot x+\vec{b}=0\ \wedge\ A\cdot y+\vec{b}=0\right]$?

מכיוון ש־ $x\neq y$ קיים ביט, נאמר i, כך ש־ $x_i\neq y_i$, ונניח בלי הגבלת הכלליות כי $x_i=0$ בעוד $y_i=1$. כעת, יהיו $\vec{a},b$ כך ש־ $\vec{a}\cdot x=b$. נגדיר $\vec{c}$ להיות זהה ל־ $\vec{a}$ פרט להיפוך הקואורדינטה ה־ i. מכיוון ש־ $x_i=0$ הרי ש־ $\vec{c}\cdot x=\vec{a}\cdot x=b$, אבל מכיוון ש־ $y_i=1$ הרי ש־ $\vec{c}\cdot y\neq\vec{a}\cdot y$, ולכן בדיוק עבור אחד מהם מתקיים שוויון ל־ b. המסקנה היא ש־ $\Pr_{\vec{a},b}[\vec{a}\cdot x+b=0\ \wedge\ \vec{a}\cdot y+b=0]=\frac{1}{4}$, כלומר $\mathbf{Pr}_{A,\vec{b}}\left[A\cdot x+\vec{b}=0\ \wedge\ A\cdot y+\vec{b}=0\right]=4^{-k}=p^2$.

כעת נשתמש בעקרון ההכלה וההפרדה כדי לחסום מלמטה את $\mathbf{Pr}[N\geq 1]$. נזכור כי $\mathbf{Pr}[N\geq 1]$ הוא בדיוק מספר הבחירות של h שעבורן לפחות x אחד מקיים $h(x)=0^k$, אחרי חלוקה בנרמול מתאים (מספרן הכולל של ה־ h). נפעיל את עקרון ההכלה וההפרדה כאשר על התכונות "$h(x)=0$" המוגדרות לכל $x\in S$ ונקבל את החסם התחתון הבא:

$$\begin{aligned}\mathbf{Pr}[N\geq 1] &\geq \sum_{x\in S}\mathbf{Pr}\left[h(x)=0^k\right]-\sum_{x<y\in S}\mathbf{Pr}\left[h(x)=0^k\ \wedge\ h(y)=0^k\right]\\ &= |S|\,p-\binom{|S|}{2}p^2\end{aligned}$$

מצד שני, ננסה לחסום מלעיל את $\mathbf{Pr}[N\geq 2]$ על ידי union bound על <u>כל</u> הזוגות $x,y\in S$, כך ש־ $\mathbf{Pr}[N\geq 2]\leq\binom{|S|}{2}p^2$.

מכאן נקבל:

$$\begin{aligned}\mathbf{Pr}[N=1] &= \mathbf{Pr}[N\geq 1]-\mathbf{Pr}[N\geq 2]\\ &\geq |S|\,p-\binom{|S|}{2}p^2-\binom{|S|}{2}p^2\\ &= |S|\,p-2\binom{|S|}{2}p^2\geq |S|\,p-(|S|\,p)^2\end{aligned}$$

כעת, את הפונקציה $f(t)=t-t^2$ קל לחקור: $f'(t)=1-2t$ ולכן יש לנו נקודת קיצון ב־ $t=\frac{1}{2}$, שם ערכה של הפונקציה הוא $\frac{1}{2}-\frac{1}{4}=\frac{1}{4}$. הנגזרת השניה היא -2 ולכן זוהי נקודת מקסימום; מכאן ש־ $f(t)$ עולה בקטע $\left[\frac{1}{4},\frac{1}{2}\right]$ וערכה המינימלי מתקבל ב־ $t=\frac{1}{4}$, שם הוא $\frac{1}{4}-\frac{1}{16}=\frac{3}{16}$. מכאן שאם $|S|\,p\in\left[\frac{1}{4},\frac{1}{2}\right]$ אז $\mathbf{Pr}[N=1]\geq\frac{3}{16}$. נוכיח שההסתברות לכך ש־ $|S|\,p\in\left[\frac{1}{4},\frac{1}{2}\right]$, כשהיא נלקחת על הגרלת ערכו של k, היא $\frac{1}{n}$ ובכך נסיים כי זה יוכיח שהסתברות ההצלחה של הרדוקציה היא לפחות $\frac{3}{16n}$.

כדי שיתקיים $|S|\,p\in\left[\frac{1}{4},\frac{1}{2}\right]$, צריך שיתקיים $\frac{1}{4}p^{-1}\leq|S|\leq\frac{1}{2}p^{-1}$, כלומר $2^{k-2}\leq|S|\leq 2^{k-1}$. עבור $k\in\{2,3,\ldots,n+1\}$, כל S המקיימת $1\leq|S|\leq 2^n$ תיפול לאחד מהתחומים, וכמובן שכאשר S היא קבוצת ההשמות המספקות של פסוק ספיק עם 2^n משתנים היא מקיימת $1\leq|S|\leq 2^n$, כך שהסתברות ההצלחה שלנו היא לפחות ההסתברות לבחור את k מתוך $\{2,3,\ldots,n+1\}$, כלומר בדיוק $\frac{1}{n}$, מה שמסיים את ההוכחה.