תורת הסיבוכיות — תרגול 8
מערכות הוכחה אינטראקטיביות

IP $\subseteq$ PSPACE

בהרצאה ראינו כי PSPACE $\subseteq$ IP. כעת נראה את הכיוון "הפחות מפתיע".

בהינתן קלט w שאנו רוצים לבדוק את שייכותו ל־ $L \in$ IP, היינו רוצים לסמלץ את התנהלות הדיאלוג בין המוודא V ובין המוכיח P ולענות כמו V, אך יש בגישה זו שתי בעיות: ראשית, אם V מקבל זה אינו מבטיח כי $w \in L$, שכן הנאותות של V אינה מושלמת; ושנית, אין לנו שום יכולת לסמלץ את P בגלל כוחו החישובי הבלתי מוגבל.

הפתרון יהיה שונה. בהינתן w ננסה לבדוק מהי ההתנהגות של מוכיח P שיבטיח הסתברות קבלה מקסימלית של w, ואם נראה כי הסתברות הקבלה של V היא גבוהה, נקבל (שכן מובטח לנו ש־ V דוחה את w בהסתברות גבוהה אם $w \notin L$ ללא תלות במוכיח שמולו). האופן שבו נעשה זאת יהיה סימולציה של ריצת V "מול כל המוכיחים בבת אחת".

פורמלית, ניתן לחשוב על הפרוטוקול כעל עץ משחק שמשחקים המוודא והמוכיח לסירוגין, כשכל מהלך אפשרי הוא הודעה שאחד הצדדים שולח לשני. העלים מסומנים ב־ 0 או 1 בהתאם לתשובת המוודא.

כל צומת בעץ ניתן לייצוג על ידי תוכן כל ההודעות שנשלחו עד כה (פולינומי ב־ $|w|$). חזרה למעלה בעץ מבוצעת פשוט על ידי "גדימת" ההודעה האחרונה שנשלחה.

בכל צומת בעץ שמתאים למהלך של המוודא, לכל אחת מהקשתות היוצאות מתאימה הסתברות כלשהי, בהתאם לאופן פעולת המוודא. בהינתן המידע שמייצג את הצומת, ניתן לחשב בזכרון פולינומי את ההסתברות הזו על ידי סימולציה של המוודא על כל מחרוזות האקראיות האפשריות, ובדיקה האם הן מיצרות את הפרוטוקול עד לקשת הזו.

האלגוריתם שלנו יהיה אם כן בסך הכל DFS על עץ הפרוטוקול שיבצע את החישוב הבא שמתאים ערך מספרי לכל צומת:

1. אם הצומת הוא עלה, ערכו שווה להסתברות שהמוודא מקבל בתום הפרוטוקול שמיוצג על ידי המסלול אל העלה.
2. אם הצומת הוא פנימי ושייך למוכיח, אז ערכו הוא המקסימום מבין ערכי בניו.
3. אם הצומת הוא פנימי ושייך למוודא, אז ערכו הוא <u>הממוצע המשוקלל</u> של הבנים (משוקלל על בסיס ההסתברות של כל בן).

לאחר סיום הרצת ה־ DFS יש להשוות את ערכו של השורש ל־ $\frac{2}{3}$. אם ערכו של השורש גדול או שווה לערך זה מקבלים, ואחרת דוחים. כפי שניתן לראות, אין כאן הסתמכות על כך ש־ $w \in L$ מתקבל בהסתברות 1, ובאותה מידה היינו יכולים להקל על דרישות השלמות מהפרוטוקול.

עומק עץ הפרוטוקול חסום על ידי $\mathcal{O}\left(p\left(|w|\right)\right)$ (כאשר p הוא הפולינום שחוסם את סיבוכיות הזמן של V בפרוטוקול), הזכרון שנדרש כדי לייצג כל צומת בפרוטוקול הוא פולינומי ב־ $|w|$, מספר הבנים של כל צומת בפרוטוקול הוא לכל היותר $2^{p(|w|)}$ (אין טעם במחרוזות ארוכות יותר ששולח המוכיח למוודא כי המוודא לא יספיק לקרוא אותן, והמוודא בוודאי שאינו יכול לשלוח למוכיח מחרוזות ארוכות יותר שכן עליו לכתוב אותן) ולכן ניתן לעבור על כולם בזכרון פולינומי ב־ $|w|$, והסימולציות של המוודא הן כולן בזכרון פולינומי ב־ $|w|$. מכאן שהאלגוריתם כולו דורש זכרון פולינומי ב־ $|w|$.

coNP $\subseteq$ IP

לכאורה זוהי תוצאה מיותרת שכן ראינו כי PSPACE $\subseteq$ IP. מצד שני, אפשר לחשוב על ההוכחה של coNP $\subseteq$ IP כעל דוגמת צעצוע של ההוכחה הכללית, ולכן הצגה שלה היא הזדמנות טובה לחזור על הרעיונות המרכזיים שהיו בהוכחה הכללית.

מספיק לנו להראות כי $\overline{3\mathrm{SAT}} \in$ IP.

למעשה, נוכיח שייכות ל־ IP של שפה חזקה מעט יותר: $\#\mathrm{SAT}_D = \{(\varphi, k) \mid \varphi$ הוא פסוק 3CNF בעל k השמות מספקות בדיוק$\}$.

אריתמטיזציה

הכלי המרכזי שבו אנו משתמשים הוא **אריתמטיזציה של נוסחאות**. הרעיון באריתמטיזציה הוא לחשוב על נוסחאות בוליאניות כעל נוסחאות חשבוניות (עם פעולות החיבור והכפל) מעל שדה גדול יותר, שבו ניתן לשכן את הערכים 0 ו־ 1. הכוח הנוסף שאריתמטיזציה מניבה נובע בדיוק מכך שניתן להציב בנוסחאות אלו גם ערכים שונים מ־ 0 ו־ 1.

יהא $\mathbb{F}$ שדה סופי כלשהו. לכל נוסחה φ נסמן ב־P_φ את הייצוג שלה באמצעות פולינום במספר משתנים, שיוגדר אינדוקטיבית באופן הבא:

- $P_{x_i} = X_i$ לכל משתנה בוליאני x_i (X_i הוא משתנה שמקבל ערכים מתוך $\mathbb{F}$).
- $P_{\varphi\wedge\psi} = P_\varphi \cdot P_\psi$
- $P_{\neg\varphi} = 1 - P_\varphi$
- $P_{\varphi\vee\psi} = 1-(1-P_\varphi)\cdot(1-P_\psi)$ (זהו למעשה יישום של כלל דה־מורגן ושני הכללים הקודמים).

כך למשל:

- הפסוק $(x_1 \vee \overline{x_2}) \wedge (\overline{x_1} \vee x_3)$ יהפוך לפולינום $((1-X_1)\cdot X_2)\cdot(X_1\cdot(1-X_3))$.
- הפסוק $(x_1 \vee x_2 \vee x_3)$ יהפוך לפולינום $1-(1-X_1)(1-X_2)(1-X_3)$ (נשים לב שדרגתו היא 3).

קל להוכיח (באינדוקציה) שכאשר מציבים במשתנים $X_1,\dots,X_n$ רק ערכי 0 ו־ 1, הפולינום יקבל ערכי 0 ו־ 1 בהתאם לערכים שהנוסחה המקורית הייתה מקבלת.

כאשר הבניה לעיל מופעלת על פסוק 3CNF בעל m פסוקיות מתקבל פולינום בעל דרגה לכל היותר $3m$ (כי דרגת כל פסוקית היא 3 ואנו כופלים את כל הפסוקיות).

$\#\mathrm{SAT}_D \in \mathsf{IP}$

בהינתן קלט (φ, k), ראשית ניתן לבנות את $P_\varphi(X_1,\dots,X_n)$ באופן שהוצג לעיל. כעת, אם נסמן ב־ $\#\varphi$ את מספר ההשמות המספקות של φ, ברור כי מתקיים:

$$\#\varphi \quad = \quad \sum_{b_1\in\{0,1\}}\cdots\sum_{b_n\in\{0,1\}} P_\varphi(b_1,\dots,b_n)$$

מטרת המוכיח היא לשכנע את המוודא ש־ $\#\varphi = k$. לצורך כך נראה כי המוכיח יוכל אפילו להוכיח משהו כללי יותר: בהינתן פולינום $g(X_1,\dots,X_n)$ בעל ייצוג יעיל (דהיינו, בהינתן $b_1,\dots,b_n$ ניתן לחשב ביעילות את $g(b_1,\dots,b_n)$) ומספר ראשוני p, המוכיח ירצה לשכנע את המוודא כי

$$k \quad = \quad \sum_{b_1\in\{0,1\}}\cdots\sum_{b_n\in\{0,1\}} g(b_1,\dots,b_n)$$

מעל השדה הסופי $\mathbb{F}_p$.

הוכחה לטענה זו מאפשרת למוכיח להוכיח את הטענה המקורית באופן הבא: הוא בוחר ראשוני גדול, אך לא גדול מדי, $p \in (2^n, 2^{n+1})$ ושולח למוודא, שבודק שזהו אכן ראשוני באמצעות אלגוריתם יעיל כלשהו (קיום ראשוני בתחום הזה נובע ממשפט מתמטי בשם "השערת ברטרנד", לפיו יש תמיד ראשוני בקטע $(n,2n)$ לכל n). כעת נשים לב שבגלל גודל הראשוני p, השוויון שלעיל נכון ב־ $\mathbb{F}_p$ אם ורק אם הוא נכון במספרים שלמים (שכן הסכום הוא על 2^n מחוברים שכל אחד מהם הוא 0 או 1). מצד שני, p קטן דיו כדי שחישובים מודולו p יוכלו להתבצע ביעילות.

המרנו את הבעיה המקורית שכללה נוסחאות בוליאניות לבעיה אריתמטית מעל שדות סופיים. כעת נציג פרוטוקול בשם Sumcheck עבורה.

פרוטוקול Sumcheck

נתונים פולינום $g(X_1,\dots,X_n)$ ומספר k. מטרת המוכיח היא לשכנע את המוודא ש־

$$k = \sum_{b_1\in\{0,1\}}\cdots\sum_{b_n\in\{0,1\}} g(b_1,\dots,b_n)$$

הפרוטוקול פועל באופן רקורסיבי, כשבכל איטרציה הוא מקטין את n (מספר המשתנים) ב־ 1 ומייצר "אתגר" חדש עבור המוכיח, תוך ניצול העובדה שהחישובים מבוצעים בשדה גדול $\mathbb{F}_p$.

לכל $g(X_1,\dots,X_n)$ אפשר לבנות פולינום במשתנה יחיד $h(X_n)$ שמתקבל כאשר מחשבים את הסכום של g "כמעט עד הסוף":

$$h(X_n)=\sum_{b_1\in\{0,1\}}\cdots\sum_{b_{n-1}\in\{0,1\}}g(b_1,b_2,\dots,b_{n-1},X_n)$$

פולינום זה ישמש את המוודא בבניית האתגר החדש.

ניתן לתאר את הפרוטוקול כך:

- אם $n=1$, המוודא בודק בעצמו ש־ $g(0)+g(1)=k$; אם לא אז דוחה, ואחרת מקבל.
- אם $n\geq 2$, המוודא מבקש מהמוכיח שישלח לו ייצוג יעיל של הפולינום $h(X_n)$ כפי שהוגדר לעיל (למשל, את רשימת המקדמים של הפולינום).
- המוכיח שולח פולינום $s(X_n)$.
- המוודא בודק האם $s(0)+s(1)\neq k$, ודוחה מייד אם כן. אחרת, הוא בוחר $a\in\mathbb{F}_p$ באקראי ומריץ רקורסיבית את הפרוטוקול על מנת להשתכנע ש־

$$s(a)=\sum_{b_1\in\{0,1\}}\cdots\sum_{b_{n-1}\in\{0,1\}}g(b_1,b_2,\dots,b_{n-1},a)$$

השלב האחרון הוא עיקר הרעיון: החלפנו את הפולינום g בפולינום דומה שבו הוצב a במקום X_n, ולכן הוא פשוט יותר.

ברור כי אם המוכיח דובר אמת, הפרוטוקול יסתיים בהצלחה; האתגר הוא לראות שהסתברות הרמאות אינה גדולה.

הוכחת הנאותות

נרצה להראות באינדוקציה על n כי אם טענת המוכיח היא שקרית, המוודא ידחה בהסתברות $\left(1-\frac{d}{p}\right)^n$ לפחות, כאשר d היא דרגת g; מבחירת p, נקבל שהסתברות זו קרובה מאוד ל־ 1.

עבור $n=1$ המוודא דוחה בהסתברות 1, שכן אופן פעולותו הוא דטרמיניסטי ומתקיים $k\neq g(0)+g(1)$.

נניח נכונות עבור $n-1$ ונוכיח עבור n. אם ה־ s שאותו שולח המוכיח שווה ל־ $h(X_n)$ והטענה המקורית אינה נכונה, אז יתקיים $k\neq s(0)+s(1)$ והמוודא ידחה מייד. על כן, נניח שהמוכיח רימה ושלח $s(X_n)\neq h(X_n)$. על כן, לפולינום $s(X_n)-h(X_n)$, שהוא פולינום מדרגה d לכל היותר, יש לכל היותר d שורשים, כלומר לכל היותר d איברים $a\in\mathbb{F}_p$ עבורם $s(a)=h(a)$. אם כן, ההסתברות שהמוודא יבחר a אקראי שעבורו אין שוויון היא גדולה או שווה ל־ $1-\frac{d}{p}$.

אם אכן נבחר a עבורו $s(a)\neq h(a)$ אז תרמית המוכיח נכשלה, שכן הוא עדיין צריך להוכיח טענה שאינה נכונה, שבמקרה זה נתונה על ידי $s(a)=\sum_{b_1\in\{0,1\}}\cdots\sum_{b_{n-1}\in\{0,1\}}g(b_1,b_2,\dots,b_{n-1},a)$. על פי הנחת האינדוקציה, ההסתברות שהמוודא ידחה בהמשך הדרך היא לפחות $\left(1-\frac{d}{p}\right)^{n-1}$, ולכן ההסתברות הכוללת לדחייה של המוודא היא לפחות $\left(1-\frac{d}{p}\right)^n=\left(1-\frac{d}{p}\right)\cdot\left(1-\frac{d}{p}\right)^{n-1}$, כנדרש.