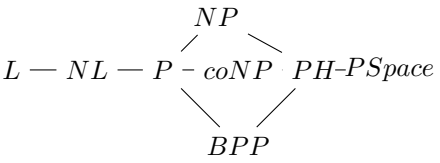
סיבוכיות – הרצאה 9

כל העולם הוא חישוב אחד גדול

3.5.11

תמונת העולם שלנו:



אנחנו דנים בשאלה מה מוכיח כל יכול, יכול להוכיח לבודק הסתברותי יעיל. ואז מגיעה בעיית ה GNI שלא ידועה להיות ב- BPP. אפשר להוכיח אותה לבודק יעיל (עם מטבעות סודיים וגם עם מטבעות פומביים).
דיברנו גם על שיחה בין בודק יעיל למוכיח: הבודק שואל אשלות את המוכיח והמוכיח עונה לו. על סמך השאלות והתשובות הבודק יחליט אם לקבל או לדחות. אפשרות ראשונה היא שהבודק מטיל מטבעות r, מחשב שאלה q ושולח רק את q למוכיח (ולא את המטבעות). כאן יש לבודק סודות. זה נקרא private coins. האפשרות השניה היא שהבודק תמיד שולח למוכיח גם את המטבעות. זה נקרא public coins.
GNI לא ידועה להיות ב- BPP ולא ידועה להיות ב- NP אבל יש לה הוכחה שבודק הסתברותי יכול לבדוק. עכשיו אנחנו הולכים לראות הכללה.

הגדרה. – מחלקת כל השפות שיש להם פרוטוקול אינטרקטיבי עם בודק הסתברותי יכיח במספר פולינומי של סיבובים עם public coins, perfect completeness (וזה אומר שהסתברות לצדוק אם המילה בשפה היא 1).

אם $x \in L$ אז קיים מוכיח כך ש:

$$\mathbb{P}_{\text{מטבעות}}[\text{הבודק יקבל בשיחה עם המוכיח}] = 1$$

ואם $x \notin L$ אז קיים מוכיח כך ש:

$$\mathbb{P}_{\text{מטבעות}}[\text{הבודק יקבל בשיחה עם המוכיח}] \leq \frac{1}{2}$$

משפט. $IP = PSpace$.

לא נוכיח את המשפט, אלא נראה את שני הדברים הבאים: נראה:

1. $IP \subseteq PSpace$ (וזה פחות מפתיע).

2. $\#3SAT \in IP$.

כאשר $\#3SAT$ היא בעיה שמקבלת כקלט פסוק $3SAT$ $\varphi = \bigwedge_{i=1}^{n} c_i$ וגם k והקלט הוא בשפה אם מספר ההשמות המספקות של φ הוא בדיוק k.
ואז למשל, $coNP \in IP$.
בטכניקות דומות (אך כמובן עם עוד עבודה) אפשר להוכיח את המשפט במלואו.

משפט. $IP \subseteq PSpace$.

הוכחה. תהי שפה $L \in IP$. יש פרוטוקול אינטרקטיבי שפותר אותה עם מטבעות פומביים. המוכיח תמיד יבחר את התשובה שתגרום לבודק "הכי לקבל".
נבנה "עץ משחק": נתחיל מהמצב ההתחלתי עם הקלט. ישנם שני סוגי צמתים: אלה שמתאימים לצעד של הבודק ואלה שמתאימים לצעד של המוכיח. צמתים מסוגים שונים מופיעים לסירוגין. המעבר בין רמות מתבצע ע"י שאלה שהבודק שואל (עם עוברים מבודק למוכיח) או ע"י תשובה שהמוכיח עונה לבודק(עם עוברים בין מוכיח לבודק).
נסמן

$$\mathrm{Val}(\text{עלה}) = \begin{cases} 1 & \text{הבודק מקבל} \\ 0 & \text{הבודק דוחה} \end{cases}$$

כאשר העלה הוא ההחלטה של הבודק אחרי התשובה האחרונה של המוכיח עבור קודקוד V עם בנים V_i שבו המוכיח משחק, נקבע $\mathrm{Val}(v) = \max_i \mathrm{Val}(v_i)$. עבור קודקוד V עם בנים V_i שבו הבודק משחק נגדיר $\mathrm{Val}(V) = \mathrm{avg}\, \mathrm{Val}(V_i)$.
לכל קודקוד V, $V = (x, r_1, a_1, \ldots)$ אם ניקח את המוכיח "הכי רע" p^* אז:

$$\mathrm{Val}(V) = \mathbb{P}[p^* \text{המוכיח יקבל אחרי השיחה עם} \mid V \text{ ההיסטוריה עד כה היא}]$$

את זה אפשר להוכיח באינדוקציה. הבסיס (עלה) ברור. המעבר: עם זה קודקוד מוכיח עם בנים V_i, באינדוקציה $Val(V_i)$ היא בדיוק ההסתברות שהבודק יקבל בהינתן שנגיע ל- V_i אז כדי למקסם את ההסתברות שהוא יקבל הוא יקח בדיוק את המקסימום. עבור קודקוד בודק הוא מטיל מטבעות ואז ההתסברות לקבל היא בדיוק הממוצע של כל ההסתברויות של הבנים.
כדי לדעת אם $x \in L$ מספיק לנו לקבל את $\mathrm{Val}(root)$ כאשר $root$ הוא שורש העץ. אם אנחנו בשפה הערך הוא 1 ואחרת הערך $\geq \frac{1}{2}$.
אז נחשב את ה- Val של השורש.
נתחיל מהעלים. נריץ את הפרדיקט של V על $(x, r_1, a_1, \ldots)$. זה ב- P ובפרט ב- $PSpace$.
בקודקוד אחר ניקח את ערכי ה- Val של הבנים ונעשה מקסימום או ממוצע בהתאמה לסוג הקודקוד.
סיבוכיות המקום: נסמן $S(i)$ הזכרון שנדרש לפתור פרוטוקול עם i סיבובים.
$S(i) = poly(n)$ עבור עלה.
$S(i+1) = S(i) + poly(n)$ כאשר $poly(n)$ נדרש בשביל "אדמיניסטרציה" (למשל לשמור באיזה שאלה אנחנו עכשיו). נפתח ונקבל $S(t) = tpoly(n)$.
□

עכשיו המטרה שלנו להראות $\#3SAT \in IP$.
הקלט הוא פסוק $3SAT$ $\varphi(x_1, \ldots, x_n) = \bigwedge_{i=1}^{n} c_i$ כאשר כל $c_i = (l_{i_1} \vee l_{i_2} \vee l_{i_3})$ כאשר $l_{i_j} \in \{T, F, x_m, \neg x_m\}$ ומספר k.
הקלט בשפה אם ורק אם מספר ההשמות המספקות את φ הוא בדיוק k.
נעשה ארתמיזציה של הקלט: $A(T) = 1$, $A(F) = 0$, $A(x_i) = x_i$, $A(\neg x_i) = 1 - x_i$, $A(l_1 \wedge l_2) = A(l_1) \cdot A(l_2)$.
למשל:

$$(x_1 \vee \overline{x_2}) = \overline{\neq x_1 \wedge \neg\overline{x}_2} = \overline{\neg x_1 \wedge x_2} = 1 - (1 - x_1)x_2$$

אחרי תרגום של פסוק מקבלים פולינום. $A(\varphi(a_1, \ldots, a_n)) \mapsto p(A(a_1), \ldots, A(a_n))$. p הוא פולינום ב- n משתנים.
כעת אם $\varphi(a_1, \ldots, a_n) = T$ אז $p(A(a_1), \ldots, A(a_n)) = 1$, ואם $\varphi(a_1, \ldots, a_n) = F$ אז $p(A(a_1), \ldots, A(a_n)) = 0$
כעת מספר ההשמות המספקות הוא בדיוק:

$$\sum_{x_1 \in \{0,1\}} \sum_{x_2 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} p(x_1, \ldots, x_n)$$

את הסכום הזה עדיין קשה לחשב. אבל יש לנו מוכיח כל יכול.
פרוטוקול אינטרקטביבי: ההתחלה: $p(x_1, \ldots, x_n)$ כתוב על השולחן בצורה

$$p(x_1, \ldots, x_n) = \prod_{i=1}^{m} A(c_i(x_1, \ldots, x_n))$$

המוכיח טוען ש- $\sum_{x_1,\ldots,x_n \in \{0,1\}} p(x_1, \ldots, x_n) = k$. אנחנו מבקשים מהמוכיח לשלוח לנו את $f_1(x_1) = \sum_{x_2,\ldots,x_n \in \{0,1\}} p(x_1, \ldots, x_n)$. זה פולינום במשתנה אחד מדרגה $3n \geq$ כי p הוא מכפלה על האריתמזציה של c_i וכל c_i מדרגה ≥ 3 לכל היותר. כלומר אנחנו מבקשים מהמוכיח את כל $3n$ המקדמים.
נניח הוא שלח לנו פולינום $\tilde{f}_1$ (כי אנחנו לא יודעים אם הוא נכון). נבדוק ש- $\underbrace{k}_{k_0} = \tilde{f}_1(1) + \tilde{f}_1(0)$. אם זה לא נכון, נדחה. הבודק בוחר $a_1 \in F$ ושולח את a_1 למוכיח, והטענה החדשה לבדיקה היא

$$\sum_{x_2,\ldots,x_n} p(a_1, x_2, \ldots, x_n) = \underbrace{\tilde{f}_1(a_1)}_{k_1}$$

המוכיח אמור לשלוח לנו את $f_2(x_2) = \sum_{x_3,\ldots,x_n \in \{0,1\}} p(a_1, x_2, x_3, \ldots, x_n)$. נקבל $\tilde{f}_2$ מדרגה $3n \geq$ נבדוק שאכן $\tilde{f}_2(0) + \tilde{f}_2(1) = k_1$. נבחר $a_2 \in F$ נשלח למוכיח. נשאל האם $\tilde{f}_2(a_2) = \sum_{x_3,\ldots,x_n} p(a_1, a_2, x_3, \ldots, x_n)$. נמשיך עד שניתן ערכים לכל x_i. בסוף הטענה שעומדת לדיון היא האם:

$$p(a_1, \ldots, a_n) \stackrel{?}{=} k_n$$

הבודק מחשב, מקבל אם כן ודוחה אם לא. נסכם:
קלט: $\varphi(x_1, \ldots, x_n)$ מתורגם ל- $p(x_1, \ldots, x_n) = \prod_{i=1}^{m} A(c_i(x))$. p מדרגה $3m \geq$ בכל משתנה ומספר k_1.
רוצים להוכיח $\sum_{x_1,\ldots,x_n \in \{0,1\}} p(x_1, \ldots, x_n) = k_0$.
בוחרים שדה סופי F שיש בו לפחות $6mn$ איברים (כאשר n מספר המשתנים, n מספר הפסוקיות). נצטרך לדרוש גם $|F| > 2^n$ כדי לייצג את כל ההשמות.
שלב 0: טענה - $\sum_{x_1,\ldots,x_n \in \{0,1\}} = k_1$.
בשלב ה- i בחרנו $a_1, \ldots, a_{i-1} \in F$. הטענה שעומדת לדיון היא: $\sum_{x_i,\ldots,x_n \in \{0,1\}} = k_i$.
הבודק בוחר $a_i \in F$ ושלוח למוכיח. המוכיח שולח פולינום $\tilde{f}_i$ מדרגה $3n \geq$. הבודק בודק ש- $\tilde{f}_i(0) + \tilde{f}_i(1) = k_{i-1}$. בוחרים $a_i \in F$ ומגדירים $k_{i+1} = \tilde{f}_i(a_i)$ וממשיכים לסיבוב הבא.
בסיבוב ה- $n+1$ הבודק בודק אם $p(a_1, \ldots, a_n) = k_n$.

דוגמא. למען ההדגה נפר את המבנה של $3SAT$.
נניח $p(x_1,x_2,x_3) = x_1^2x_2 - 3x_1x_3 - x_1x_2$. המוכיח טוען ש- $\sum_{x_1,x_2,x_3} p(x_1,x_2,x_3) = 17$.

$$f_1(x_1) = \sum_{x_2,x_3} p(x_1,x_2,x_3) = 0 + 3x_1 + x_1^2 - x_1 + x_1^2 + 2x_1$$

המוכיח החזיר פולינום $\tilde{f}_1$. אם זה היה נכון אז $\tilde{f}_1(0) + \tilde{f}_1(1) = 17$. נבדוק את זה. נבחר $a_1 \in F$. ונראה האם $f(x_2) = \sum_{x_3} p(a_1,x_2,x_3) = \tilde{f}_1(a_1)$. איך נבדוק? נבקש מהמוכיח פולינום ב- x_2 נוודא שהוא בסדר ונבדוק שנקודה אקראי. וכו'.

הוכחה. שלמות: אם $x \in L$ מספר ההשמות המספקות את φ הוא k. לכן, יש מוכיח כך שהבודק תמיד יקבל, המוכיח שתמיד ישלח $\tilde{f}_i$ נכון, כלומר $\tilde{f}_i = f_i$. ואז

$$f_i(x_i) = \sum_{x_{i+1},\ldots,x_n} p(a_1,\ldots,a_{i-1},x_i,\ldots,x_n)$$

החלק המעניין הוא מה קורה כאשר הטענה לא נכונה. נניח $\sum_{x_1,\ldots,x_n} p(x_1,\ldots,x_n) \neq k_1$.
המוכיח מחזיר איזשהו $\tilde{f}_1$. האפשרות הראשונה היא $\tilde{f}_1 = f_1$ אבל אז כאשר נחשב $\tilde{f}_1(0) + \tilde{f}_1(1) = f_1(0) + f_1(1) = \sum_{x_1,\ldots,x_n} p(x_1,\ldots,x_n) \neq k_1$. ואז פשוט נדחה.
האפשרות השנייה היא ש- $\tilde{f}_1 \neq f_1$. כעת, $f_1, \tilde{f}_1$ פולינומים שונים מדרגה $3m \geq$. כשנבחר $a_1 \in F$ באקראי, חוץ מהסתברות $\frac{3m}{|f|} \geq$ מתקיים $\tilde{f}_1(a_1) \neq f_1(a_1)$.
לכן בהסתברות גבוהה נבחר a_1 כך שהם שונים. הטענה בשלב הבא אומרת:

$$\underbrace{\sum_{x_2,\ldots,x_n} p(a_1,\ldots,x_n)}_{=f(a_1)} = \tilde{f}_1(a_1)$$

אבל כמעט תמיד זאת תהיה טענה לא נכונה. זה טוב כי נפתרנו ממשתנה והטענה עדיין לא נכונה.
אם המוכיח ינסה לשלוח פולינום נכון, באופן דומה לשלב הראשון אנחנו נבדוק ונדחה. אז כדי שלא נדחה המוכיח צריך שוב לשלוח פולינום לא נכון. הטיעון הזה נכון גם באופן כללי: בצעד ה- i, אם הטענה לא נכונה אז אם $\tilde{f}_{i+1} = f_{i+1}$ נבדוק ונדחה מייד. לעומת זאת, אם $\tilde{f}_{i+1} \neq f_{i+1}$ חוץ משגיאה בגודל $\frac{3m}{|F|}$ הטענה בשלב הבא שוב לא נכונה.
לכן, חוץ משגיאה $\frac{3m}{|F|}$ בכל סיבוב, הטענה בסוף לא נכונה. בסוף הבודק כבר בודק את הפולינום כולו בעצמו ויגלה את השגיה. יש n סיבובים לכן השגיאה הכוללת תהיה $\frac{3mn}{|F|}$ והיות ובחרנו $|F| \geq 6mn$ אז השגיאה תהיה לכל היותר $\frac{1}{2}$.
□

נדבר על פרוטוקול עם מספר מוכיחים כל יכולים. Multiprove IP או בקיצור $MIP(k,s)$ כאשר k מספר המוכיחים ו- s מספר הסיבובים. נתאר את הפרוטוקול $MIP(2,1)$:
הפרוטוקול: הקלט x מונח על השולחן. הבודק V מטיל r מטבעות סודיים, על סמך המטבעות מחשב שאלות q_1, q_2 ושולח את q_1 למוכיח הראשון p_1 ואת q_2 למוכיח השני p_2. נשים לב, שהמוכיחים לא יודעים איזה שאלה קיבל המוכיח השני. כל אחד מהם מחזיר לו תשובה, הראשון a_1 והשני a_2. על סמך השאלות הבודק יחליט האם לקבל או לדחות:

$$V(x,q_1,q_2,a_1,a_2) \in \{accept, reject\}$$

הערה. אם המטבעות לא סודיים, היות והבודק הוא דטרמיניסטי, המוכיחים ידעו בדיוק איזה שאלה הוא שואל כל אחד מהמוכיחים ואז זה שקול לשיחה אינטרקטיבית אם מוכיח יחיד.

משפט. $MIP(2,1) = NExp$, $IP = MIP(1, poly) = PSpace$.

ללא הוכחה.
יתר על כן:

משפט. לכל $\varepsilon > 0$, קייס: $NP = PCP_{\frac{3}{4}+\varepsilon,1}(O(\log n), 3)$.

נתאר את הפרוטוקול החדש PCP.
הקלט $x \in \{0,1\}^n$ מונח על השולחן. המוכיח מניח הוכחה π מכוסה על השולחן. הבודק מטיל r מטבעות ולפי r הוא מחליט על איזה k ביטים מההוכחה הוא רוצה להסתכל. הוא בודק את הביטים האלה, ובהתאם לזה מחליט אם לקבל או לדחות.
נסמן את הפרוטוקול $PCP_{\alpha,\beta}(r,q)$ אם הבודק מטיל r מטבעות ומסתכל על q ביטים מההוכחה לכל היותר.

$$x \in L \Rightarrow \exists p \, \mathbb{P}(p \text{ יקבל בשיחה עם } v) \geq \beta$$

$$x \notin L \Rightarrow \forall p \, \mathbb{P}(p \text{ יקבל בשיחה עם } v) \leq \alpha$$

בהגדרות האלה נוכל לכתוב $NP = PCP_{0,1}(0, polyn)$.

משפט. לכל $\varepsilon > 0$, קייס: $NP = PCP_{\frac{3}{4}+\varepsilon,1}(O(\log n), 3)$.

זה מראה על קושי לקירוב בעיות NP קשות. בזה נעסוק לכמה שיעורים.

Set-Cover

נתון עולם U וקבוצות $S_1, \ldots, S_n \subseteq U$. המטרה היא למצוא קבוצה $F \subseteq \{S_1, \ldots, S_n\}$ שמכסה את כל העולם, כלומר $\bigcup_{S \in F} S = U$. כמובן שנרצה קבוצה קטנה ככלה האפשר. זאת בעיה NP שלמה.
אמנם קשה למצוא הפתרון המינימלי אבל אולי קל למצוא פתרון שיקרב אותו. למשל את פתרון הבעיה של Set-Cover אפשר לקרב עד כדי פקטור של $\ln |U|$ במהירות.
וזה יהיה הנושא הבא שלנו. אולם לא נראה את הקירוב של Set-Cover אבל נתבונן בקירוב בעיות אחרות.