# סיבוכיות – הרצאה 11

כל העולם הוא חישוב אחד גדול

24.5.11

$\mathrm{Gap}_{[\alpha,\beta]}\, max3SAT$ היא בעיית אבטחה. הקלט הוא פסוק $3SAT$. הפלט הוא $Yes$ אם הפסוק $\varphi = \bigwedge_{i=1}^{m} c_i$ יש השמה שמספקת $\alpha m \geq$ פסוקיות והפלט הוא $No$ אם לכל השמה, היא מספקת לכל היותר $\beta m$ פסוקיות. למעשה זאת רלקסציה של בעיית $3SAT$.
בבעית Gap יש לנו הבטחה על הקלט. יש לנו יותר אינפורמציה, ופוטנציאלית הבעיה קטנה יותר. אבל, המשפט אומר שהאינפורמציה הנוספת לא עוזרת לנו. כלומר, יש קבוע $\alpha$ כך שגם הבעיה $\mathrm{Gap}_{[\alpha,1]}\, max3SAT$ היא $NP$ קשה.
ראינו שאם יודעים ש- $\mathrm{Gap}\, max3SAT$ היא $NP$ קשה אז ע"י רדוקציות משמרות פער, אפשר להראות שקשה לקרב עוד בעיות. למשל ראינו שקשה לקרב $Clique$, $VC$, $IS$. למעשה כמעט כל בעיות ה- $NP$ המעניינות, $NP$ קשה לקרב אותן.

**תזכורת.** שפה $L$ שייכת ל- $PCP_{\alpha,\beta}(r,q)$ אם קיים פרוטוקול בין מוכיח כל יכול לבודק הסתברותי יעיל, שבו עבור $x \in \{0,1\}^n$, המוכיח כותב הוכחה מכוסה $w_1,\ldots,w_n$ (באורך פולינום) על השולחן. הבודק מטיל $r$ מטבעות $y \in \{01,\}^r$. לפי המטבעות מחליט על איזה $q$ ביטים מההוכחה להסתכל. קורא את הביטים $w_{i_1},\ldots,w_{i_q}$. מחשב את הפרדיקט $V(x,y,w_{i_1},\ldots,w_{i_q})$ ומחליט האם לקבל או לדחות כך שאם $x \in L$ אז יש $w$ כך ש- $\mathbb{P}_y[v \text{ מקבל}] > \beta$ ואם $x \notin L$ אז לכל $w$, $\mathbb{P}_y[v \text{ מקבל}] < \alpha$.

**טענה.** יש $\alpha > 1$ כך ש- $NP \subseteq PCP_{\alpha,1}\big(O(\log n), \underbrace{O(1)}_{=3}\big)$.

כלומר אפשר לתת הוכחה ל-$NP$ שמספיק להסתכל על $O(1)$ ביטים (שנבחר באקראי) ממנה.

**טענה.** יש $\alpha' < 1$ כך ש- $\mathrm{Gap}_{[\alpha',1]}\, max3SAT$ הוא $NP$ קשה.

כלומר יש בעיות אוטימיזציה של $NP$ שהקירוב שלהן $NP$ קשה.
לא הוכחנו אותן ולא נוכיח אבל נרצה להראות ששתי הטענות שקולות.

**טענה.** אם יש $\alpha < 1$ כך ש- $\mathrm{Gap}_{[\alpha,1]}\, max3SAT$ היא $NP$ קשה אז $NP \subseteq PCP_{\alpha,1}\big(O(\log n), 3\big)$.

הוכחה. תהי $L \in NP$. אנחנו יודעים $L \leq \mathrm{Gap}_{[\alpha,1]}\, max3SAT$. הרדוקציה $f$ לוקחת $x \in \{0,1\}^n$ ובונה פסוק $3SAT$ $f(x) = \varphi(w) = \bigwedge_{i=1}^{n} c_i(w)$ באורך פולינומיאלי כך ש- $x \in L \Rightarrow$ יש השמה $w$ כך שכל הפסוקיות $c_i$ ספיקות עם $w$ ו- $x \notin L \Leftarrow$ לכל השמה $w$ מספר הפסוקיות שלא מסתפקות $\geq \alpha m$.
נראה שלשפה $L$ יש מערכת $PCP_{\alpha,1}\big(O(\log n), 3\big)$ וזה יסיים את ההוכחה. עבור $x \in \{0,1\}^n$, $y \in \{1,\ldots,m\} = \{0,1\}^r$ המוכיח נותן $w$, $|w| = poly(n)$ והבודק בוחר $|y| = r = O(\log n)$. הוא מסתכל הפסוקים ה- $y$: $c_y = (l_{i_1} \vee l_{i_2} \vee l_{i_3})$ מסתכל על $w_{i_1}$, $w_{i_2}$, $w_{i_3}$, מחשב ערך $c_i(w)$ אם $T$ מקבל ואם $F$ דוחה.
זאת מערכת $PCP\big(O(\log n), 3\big)$.
נכונות: אם $x \in L$ אז יש $w$ כך שכל $c_i$ מסתפקת ואז $V$ תמיד מקבל. אם $x \notin L$ אז לכל מוכיח $w$ יש $(1-\alpha)m$ פסוקיות שלא יסתפקו, ולכן בהסתברות $> 1-\alpha$ בהסתברות הבודק יבחר פסוקית כזו וידחה. □

**טענה.** אם $NP \subseteq PCP_{\alpha,1}\big(O(\log n), O(1)\big)$ אז יש $\alpha' M1$ כך ש- $\mathrm{Gap}_{\alpha',1}\ NP$ קשה.

הוכחה. נגדיר בעיה חדשה, $\mathrm{Gap}_{\alpha,\beta} CSP(q)$. הקלט: לכל $i = 1, \ldots, m$ יש פונקציה בסיסית $f : \{0,1\}^q \to \{0,1\}$. ותת קבוצה $S_i$ של $\{1, \ldots m\}$ שכל קבוצה היא בגודל $q$.
$Yes$: $(f_1, \ldots, f_m, S_1, \ldots, S_m)$ כך שיש $w \in \{0,1\}^n$ כך שעבור לפחות $\beta m$ אילוצים $i$ כך ש- $S_i = \{j_1, \ldots, j_q\}$ מתקיים $f_i(\underbrace{w_{j_1}, \ldots, w_{j_q}}_{w\big|_{S_i}}) = 1$.
$No$: $(f_1, \ldots, f_m, S_1, \ldots, S_m)$ כך שלכל $w \in \{0,1\}^n$ עבור לכל היותר $\alpha m$ים האילוץ $i$ מתאפס.
כלומר עבור לפחות $(1-\alpha)m$, $f_i(w\big|_{S_i}) = 0$ כאשר $S_i = \{j_1, \ldots, j_q\}$, $w\big|_{S_i} = w_{j_1}, \ldots, w_{j_q}$.

**דוגמא.** $q = 3$. נקודד את הפסוק

$$\varphi(w_1, \ldots, w_{50}) = \underbrace{(w_{17} \vee \neg w_1 0 \vee w_7)}_{i=1} \wedge \underbrace{(w_5 \vee \neg w_1 \vee \neg w_2)}_{i=2} \wedge \ldots$$

ניקח את $m$ להיות מספר הפסוקיות. $S_1 = \{17, 10, 7\}$, $S_2 = \{3, 1, 2\}$ וכו'. $f_1(a,b,c) = a \vee \neq b \vee \neg c$, $a \vee \neg b \vee c$. $f_2(a,b,c) =$.

**טענה.** $\mathrm{Gap}_{\alpha,\beta} 3SAT \leq \mathrm{Gap}_{\alpha,\beta} CSP(3)$.

כי בהינתן מופע $\varphi(w) = \bigwedge c_i(w)$ של $3SAT$. הרדוקציה תבנה מופע של $CSP$, תבחר $q = 3$ ו- $m$ מספר הפסוקיות ב- $\varphi$. תבחר את $n$ להיות מספר המשתנים ב- $w$, תבחר את $S_i$ להיות האינדקסים של המשתנים ב- $c_i$, נבחר $f_i$ להיות הפונקציה ש- $c_i$ מפעיל (סה"כ 8 אפשרויות).
נכונות: מספר הפסוקיות המקסימלי שמסתפרות בו זמנית ב- $\varphi$ =מספר האילוצים הספיקים בו זמנים במערכת שבחרנו.

**טענה.** (ו) אם $NP \subseteq PCP_{\alpha,1}\big(O(\log n), q\big)$ אז $\mathrm{Gap}_{\alpha,1} CSP(q)$ היא $NP$ קשה.

**טענה.** (ג) לכל $\alpha < 1$ יש $\alpha' < 1$ כך ש- $\mathrm{Gap}_{\alpha,1} CSP(q) \leq \mathrm{Gap}_{\alpha',1} 3SAT$.

נוכיח את טענה 1:

הוכחה. מניחים ש- $NP \subseteq PCP_{\alpha,1}\big(O(\log n), q\big)$. תהי $L \in NP$ בעיה $NP$ קשה. רוצים להראות $L \leq \mathrm{Gap}_{\alpha,1} CSP(q)$.
$L \in PCP_{\alpha,1}\big(\underbrace{O(\log n)}_{=r}, q\big)$. ז"א יש מוכיח שנותן $w_1, \ldots, w_{\overline{n}}$ כאשר $\overline{n} = poly n$. הבודק מטיל $y \in \{0,1\}^r$, לפיהן בוחר $j_1, \ldots, j_q \subseteq [\overline{n}]$ ומבצע בדיקה $V(x, y, w_{j_1}, \ldots, w_{j_q})$.
נבנה מערכת $CSP$ ושפה. נמשיך עם $q$. נבחר $m = 2^r$. עבור $y = 1, \ldots, m$, $y \in \{0,1\}^r$, $S_y$ יהיה הסט של האינדקסים $j_1, \ldots, j_q$ שהבודק בוחר להסתכל עליהם. $f_y(w_{j_1}, \ldots, w_{j_q}) = V(x, y, w_{j_1}, \ldots, w_{j_q})$.
הרדוקציה היא ב- $P$. זמן הריצה הוא $2^r$ לכל $y$, וחישוב הסט המתאים $S_y$ וחישוב הפרדיקט פולינומיאלי (לחשב את טבלאות האמת). הרדקוציה פולינומית כי $\log n$ מטבעות לכן אפשר לעבור על כולם וכן הבודק הוא יעיל.
נכונות: אם $x \in L$ אז יש $w$ כך שלכל $y$ שהבדוק מטילף $V(x, y, w_{j_1}, \ldots, w_{j_q}) = 1$. לכן, $f_i(w\big|_{S_i}) = 1$ לכל $i$. לכן, הרדוקציה מעבירה $YES$ של $L$ ל- $YES$ של $CSP$. מצד שני, אם $x \notin L$ לכל $w$ לפחות $(1-\alpha)m$ הטלות $y$ יקימו $V(x, y, w_{j_1}, \ldots, w_{j_q}) = 0$ ולכן לכל $w$ לפחות עבור $(1-\alpha)m$ $i$ים יתקיים $f_i(w\big|_{S_i}) = 0$ והרדוקציה מעבירה מ- $NO$ של $L$ ל- $NO$ של $CSP$.

□

**טענה.** לכל $\alpha < 1$ יש $\alpha' < 1$ כך ש- $\mathrm{Gap}_{\alpha,1} CSP(q) \leq \mathrm{Gap}_{\alpha',1} 3SAT$.

הוכחה. הרעיון יהיה שכל אילוץ שהוא מהצורה $f_t : \{0,1\}^n \to \{0,1\}$ אילוץ כללי, מובע ע"י טבלת אמת. אפשר להביע אותו ע"י פסוק $q---SAT$ וכל פסוק $q---SAT$ אנחנו יודעים לתרגם לפסוק $3SAT$.

$$(l_1 \vee \ldots \vee l_q) \mapsto \big((l_1 \vee l_2) \Leftrightarrow z_1\big) \wedge \big((z_1 \vee l_3) \Leftrightarrow z_2\big) \wedge \ldots \big((l_q \vee z_{q-2}) \Leftrightarrow z_{q-1}\big) \wedge z_{q-1}$$

כאשר היינו צריכים להוסיף משתני עזר $z$. אם פסוק $qSAT$ ספיק אז יש השמה למשתני העזר כך שפסק ה- $3SAT$ יהיה ספיק. אם פסוק $qSAT$ לא ספיק אז לכל השמה למשתני העזר אז פסוק $3SAT$ לא ספיק.
בהינתן מופע של $\mathrm{Gap}\, CSP(q)$, $S_1, \ldots, S_m \subseteq [n]$, $|S_i| = q$, $f_1, \ldots, f_m : \{0,1\}^q \to \{0,1\}$. ניקח משתנים $w_1, \ldots, w_n$ ומשתני העזר לכל $f_i$ ונגדיר פוסק $3SAT$. כל תנאי $f_i(w\big|_{S_i})$ יפתח לפסק $3SAT$ על משתנים $w\big|_{S_i}$ ומשתני עזר וניקח את $\bigwedge$ של כל הפסוקים האלה.
כמה פסוקיות יש בפסוק $3SAT$?

$$\underbrace{m}_{\text{לכל } f_i} \cdot \underbrace{2^q}_{\text{כל שורה בטבלת האמת של } f_i} \cdot \underbrace{q}_{\text{תרגום מפסוקיות לליטרלים}}$$

הרדוקציה פולינומית, $q$ קבוע.
נכונות: אם התחלנו ממופע $\varphi$ של $\mathrm{Gap}\, CSP$ יש $w$ כך שלכל $i$, $f_i(w\big|_{S_i}) = 1$. יש $w, z$ כך שלכל פסוקית של $3SAT$ הפסוקית מסתפקת. ואם התחלנו ממופע $NO$ של $\mathrm{Gap}\, CSP$ אז לכל $w \in \{0,1\}^n$ עבור $(1-\alpha)m$ מה- $i$: $f_i(w\big|_{S_i}) = 0$. כל $f_i$ נפתח לפסוק $3SAT$ $\varphi_i$ באורך $2^q \cdot q$. הפסוק $3SAT$ $\varphi_i$ שקול ל- $f_i$ לכן לא ספיק. ולכן לכל השמה למשתני העזר יש לו לפחות פסוקית אחת שלא מסתפקת. לכן בפסוק ה- $3SAT$ יהיו לפחות $(1-\alpha)m$ פסוקיות מתוך $2^q q$ פסוקיות שלא יסתפקו.
לכל השמה לפסוק $3SAT$ אחוז הפסוקיות שלא מסתפקות $\leq \frac{(1-\alpha)}{mq2^q} = \frac{1-\alpha}{q2^q}$. לכן מספר הפסוקיות הספיקות $\leq 1 - \frac{1-\alpha}{q2^q}$ ובפרט $\alpha' < 1$. □

□

בשלב הזה צריך להבין שמערכות הוכחה ו- Gap זה אותו דבר. איך נעשה התרגום?
הוכחה במערכת $PCP$ מתרגמת ל- $w_1, \ldots, w_n$, מספר הביטים שמערכת ה- $CSP$ תסתכל. ב- $PCP$ לו הייתה הוכחה $w$, כיצד בודק הסתברותי היה בודק אותה. ב- $CSP$ לו היו נתונים $w$, כיצד היינו מפעילים $m$ בדיקות $f_i$ עליה. מספר הביטים $q$ שהבודק מסתכל מתתרגם ל- ס $|S_i| = q$ ב- $CSP$. ספר המטבעות $r$ שהבודק מטיל מתרגם למספר הבדיקות ב- $CSP$ $m = 2^r$. $soundness$ מתרגם ללכל היותר אחוז בדיקות שמסתפקות סימולטנית. $completness$ מתרגם ללפחות אחזור בדיוק שמסתפקות סימולטנית. פרדיקט הבדיקה $V(x, y, w|_{S_i})$ מתרגם ל- פרדיקת בדיקה כללי על $q - bit$ $f_i(w\big|_{S_i})$. המקרה הפרטי של $CSP$ שבו רק בודקים פסוקיות $3SAT$ עד כדי הפסד בפרמטרים אומר למעשה אותו דבר.
רצינו לברר מה קל ומה קשה. הסכמנו ש- $L$, $P$,$NL = coNL$, $BPP$ הן קלות. $NP$,$\Sigma_2$, $PH$, $Pspace$, $Exp$, $NExp$ הן קשות לנו.
ניסינו פתור את $NP$ עם אלגוריתמים הסתברותיים $IT \subseteq BPP$ ולא ידועה להיות ב-$P$. אמרנו שכנראה יש ל- $BPP$ דרנדומיזציה ואולי $BPP = P$.
אולי $NP \subseteq PSize$ $Psize$ - מעגלים לא אוניפורמיים בגודל פולינומי. אבל אז מקבלים שההירכיה קורסת.

הרחבנו את מושג ההוכחה לשיחה בין מוכיח כל יכול ובודק הסתברותי. הפתעה: $IP = PSpace$, $MIP = NExp$, $NP = PCP(O(\log n), O(1))$. זה סוג של הצלחה. אבל עכשיו ראינו שיש בעיות אופטימיזציה של $NP$ שהם בעצמן $NP$ קשות. זה אפילו הדוק – למשל ל- $SC$ יש קירוב $\log(n)$ אבל ל- $c < 1$ קירוב $c \log n$ הוא $NP$ קשה.
אולי בכלל $NP$ היא קשה, אבל על כל התפלגות קלטים שקוראת במציאות היא קלה? על זה נחשוב שיעור הבא.
עכשיו נרצה להניח קושי ולנצל אותו לצרכנו. דוגמא אחת היא הצפנה. הדוגמא השנייה היא can flipping. האם $NP \neq P$ גורר הצפנה? איזה קושי גורר הצפנה?
זוג בעל מכונית מחליט להפרד. אבל הם רוצים לחלק את המכונית באופן הוגן, אבל לא רוצים לראות אחד את השני. $A$ תטיל מטבע, אם יוצא עץ היא לוקחת מוכנית, אם יוצא פלי $B$ לוקח את המכונית. היא תתקשר ל-$B$ ותגיד לו. ברור שהיא כל הזמן תגיד עץ. רוצים פרוטוקול טוב יותר ( ספויילר – בסוף הם חוזרים להיות ביחד).