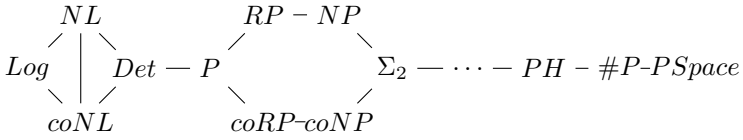
סיבוכיות – הרצאה 8

כל העולם הוא חישוב אחד גדול

12.4.11

מה זה חישוב פיזיבילי? בהתחלת הקורס זה היה P. כעת אנחנו יודעים לעשות גם BP. תמונת העולם שלנו נכון להיום:



איפה BPP בכל התמונה הזאת? אנחנו יודעים:

1. $RP \subseteq BPP$.
2. $BPP \subseteq PSize$.
3. אם $NP \subseteq PSize$ אז ההירכיה קורסת ל- Σ_2 ($\Sigma_2 = \Pi_2$).
4. שפת IT ב- RP אבל לא ידועה להיות ב- P.

משפט. *Sipser 1984* $BPP \subseteq \Sigma_2$.

כלומר אם $NP = P$ אז $\Sigma_2 = P$ ואז גם $BPP = P$. מצד שני אם $BPP = P$ אנחנו עדיין לא יכולים להסיק כלום לגבי הקשר בין NP ל- P.

הוכחה. נניח $L \in BPP$. יש מכונה הסתברותית $M(x,y)$ כך שעבור $x \in \{0,1\}^n$, $y \in \{0,1\}^m$, $m = p(n)$, עבור p פולינום. כך ש-

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

$$x \notin L \Rightarrow \mathbb{P}_y(M(x,y) = 1) \leq \frac{1}{4m}$$

מדוע מותר לקחת את המספרים האלה? בגלל האמפליפיקציה. M רצה ב- P. נבנה רדוקצחה המקבחת קלט $x \in \{0,1\}^n$ ובונה מופע $\varphi(x)$ Σ_2 כך ש- $x \in L \Leftrightarrow \varphi(x) = T$.

$$\varphi(x) = \exists y_1, \ldots, y_n \in \{0,1\}^m \forall z \in \{0,1\}^m$$
$$M(x, y_1 \oplus z) = 1 \vee M(x, y_2 \oplus z) = 1 \vee \ldots \vee M(x, y_{2m} \oplus z) = 1$$

זה לא באמת פסוק אבל אפשר לתרגם את $M(x, y_1 \oplus z) = 1$ לפסוק (כמו במקרה של $CVAL$). עלות הרדוקציה היא כמו ב- $CVAL$, כלומר $logspace$.
נכונות: אם $x \notin L$. M מטילה $y \in \{0,1\}^m$ אז $\mathbb{P}_y(M(x,y) = 1) \leq \frac{1}{4m}$. אם היינו מסמנים את כל ההטלות כנקודות של קבוצה כלשהי במישור, אז אם היינו מסמנים את כל המטבעות שגורמים למכונה לקבל היינו מקבלים קבוצה קטנה.
לכל $y_1, \ldots, y_m \in \{0,1\}^m$ כלשהם. נבנה: $\Gamma_1 = \{z : M(x, y_1 \oplus z) = 1\}$ ... $\Gamma_n = \{z : M(x, y_n \oplus z) = 1\}$
לכל i, $|\Gamma_i| \leq \frac{2^m}{4m} \xrightarrow{\text{התאמה חח"ע}} y_1 \oplus z$ כי $\{0,1\}^m$ כאשר y_1 הוא קבוע ו- z רץ על פני כל $\{0,1\}^m$.
לכן,

$$|\{z : M(x, y_1 \oplus z) = 1 \vee M(x, y_2 \oplus z) = 1 \vee \ldots \vee M(x, y_m \oplus z) = 1\}| =$$
$$= |\Gamma_1 \cup \ldots \cup \Gamma_m| \leq m\frac{2^m}{4m} \leq \frac{2^m}{4} < 2^m$$

ולכן יש- z שלא מספק באף אחת מההזזות הפסוק $\varphi(x)$ הוא $False$. באינטואציה של הקבוצה במישור, הקבוצה שלנו קטנה כל כך שאפילו אם ניקח m עותקים שלו, עדיין אין לו נפח.
מקרה ב': אם $x \in L$, נראה ש- $\varphi(x)$ מקבל ערך T. נראה בשיטה ההסתברותית: נראה שאם נבר $y_1, \ldots, y_{2m} \in \{0,1\}^m$ באופן ב"ת ואקראי אז בהסתברות גבוהה $\forall z \in$ [פסוק יהיה $True$] $\{0,1\}^n$ ובפרט יש כזאת סדרה והפסוק $\varphi(x)$ הוא $True$.
נקבע $z \in \{0,1\}^m$ ספציפי. $\mathbb{P}_y[M(x, y \oplus z) = 1] \geq \frac{1}{2}$
נסמן A_i מאורע, 1 אם $M(x, y_i \oplus z) = 1$ ו- 0 אחרת. $A_1 \ldots A_{2m}$ מ"מ ב"ת בוליאנים ו- $\mathbb{E}(A_i) \geq \frac{1}{2}$ כי x קבועים, y_i ב"ת.

$$\mathbb{P}((A_1 = 0) \wedge \ldots \wedge (A_{2m} = 0)) = \prod_{i=1}^{2} m\,\mathbb{P}(A_i = 0) \leq \left(\frac{1}{2}\right)^{2m}$$

מסקנה. לכל $z \in \{0,1\}^m$ $\mathbb{P}_{y_1,\ldots,y_m}[\text{הפסוק שקר}] \leq 2^{-2m}$.

מסקנה.

$$\mathbb{P}_{y_1,\ldots,y_m}[\exists z \text{ לא מכוסה}] \leq$$
$$\leq \mathbb{P}[1, \ldots, 1 \text{ לא מכוסה}] + \ldots + \mathbb{P}[0 \ldots, 0, 1 \text{ לא מכוסה}] + \mathbb{P}[0, \ldots, 0 \text{ לא מכוסה}]$$
$$\leq \sum_{z \in \{0,1\}^m} \mathbb{P}_{y_1,\ldots,y_m}[z \text{ לא מכוסה}] \leq 2^m 2^{-2m} = 2^{-m} < 1$$

□

משפט. אם יש שפה ב- Exp שאי אפשר לחשב אותה עם מעגלים בגודל תת-אקספוננציאלי אז $BPP = P$.

לא נוכיח את המשפט הזה. את ההוכחה אפשר לראות בקורסי המשך.
P זה כל מה שאלגוריתם דטרמיניסטי יכול לחשב.
BPP זה כל מה שאלגוריתם הסתברותי יכול לחשב.
NP זה מה שאלגוריתם דטראמיניסטי יכול לוודא.
בכלל לא דיברנו לגבי מה אלגוריתם הסתברותי יכול לוודא.

מה היא הוכחה? יש טענה $\varphi(x)$. מישהו מראה עד w שההוכחה נכונה. אם הטענה נכונה אז יש עד שתמיד נקבל. אם הטענה לא נכונה לכל עד לא נקבל.
מאוד הגיוני שהבודק יהיה הסתברותי. אם הטענה נכונה יש עד עך שבודק יקבל בהסתברות (על פני המטבעות) $\leq \frac{2}{3}$. ואם הטענה לא נכונה אז לכל עד נקבל בהסתברות $\geq \frac{1}{3}$. עכשיו נוכל לעשות אמפליפיקציה.
נתחיל עם דוגמא:

דוגמא. GNI - Graph non-isomorphism
$GNI = \overline{GI}$.
הקלט: שני גרפים G_1, G_2 על n קודקודים.
פלט: כן אם $G_1 \not\sim G_2$ ולא אחרת.
מתי שני גרפים איזומורפיים?
$G_1 = (V_1, E_1), G_2 = (V_2, E_2)$, $|V_1| = |V_2| = n$, $G_1 \sim G_2$ אם יש $\pi \in S_n$ כך ש- $(\pi(i), \pi(j)) \in G_2 \Leftrightarrow (i,j) \in E_1$.

טענה. $GI \in NP$.

העדות היא $\pi \in S_n$.
לכן,
$GNI \in coNP$. האם $GNI \in NP$? האם אפשר לתת הוכחה ששני גרפים הם לא איזומורפיים? למשל אם אין אותו מספר קשתות, אם סדרת הדרגות של הקודקודים שונה, אם שני גרפים איזומורפיים אז למטריצות השכנויות יש אותם ערכים עצמיים. הבעיה שכל זה לא עוזר כי יש משפחות של גרפים שיש להם אותם ערכים עצמיים, אותו מספר קשתות ואותה סדרת דרגות אבל הם עדיין איזומורפיים.
האם זה שקול לשאלה $NP = coNP$? כלומר אם $GIsm$ היה NP קשה אז $GIsm \in NP\ coNP \Leftrightarrow NP = coNP$. ואת זה נראה: אם $GIsm$ קשה אז ההירכיה קורסת.
פרוטוקול: G_1, G_2 מונחים על השולחן. הבודק בוחר באקראי $\pi \in S_n$ ואת אחד הגרפים באקראי, כלומר בוחר $b \in \{1,2\}$, ושומר את π, b לעצמו בסוד. הוא שולח למוכיח $\pi(G_b)$ ($\pi(G_b)$ הוא G_b כשהשמות של הקודקדים שונו בהתאם לתמורה). המוכיח עונה $c \in \{1,2\}$. הבודק בודק ש- $b = c$ אם כן מקבל ואם לא דוחה.
נסמן $\Gamma_1 = \{G : G \sim G_1\}$, $\Gamma_2 = \{G : G \sim G_2\}$. אם $G_1 \not\sim G_2$ אז $\Gamma_1 \cap \Gamma_2 = \varnothing$ כי אם $G \in \Gamma_1 \cap \Gamma_2$ אז $G \sim G_1$ וכן $G \sim G_2$, מטרנזיטיביות $G_1 \sim G_2$. לכן קיים מוכיח שבהינתן G_1, G_2, G בודק האם $G \in \Gamma_1$, $G \in \Gamma_2$ ואם $G \in \Gamma_c$ המוכיח יענה c. ואז הבודק תמיד יקבל $\mathbb{P}_{\pi,b}[\text{יקבל } V] = 1$.
אם $G_1 \sim G_2$ אז $\Gamma_1 = \Gamma_2$ טאן $G \in \Gamma_1$ אז $G \sim G_1 \sim G_2$ ולכן $G \sim G_2$:

$$\mathbb{P}_\pi[G \text{ ישלח}|b = 1] = \mathbb{P}_\pi[G \text{ ישלח}|b = 2]$$

ולכן לא משנה מי המוכיח, כשהוא רואה את G אז יש הסתברות שווה לכך ש- $b = 1$ ולכך ש- $b = 2$. אז לכל c $\mathbb{P}_{\pi,b}[\text{יקבל } V] = \frac{1}{2}$.

הגדרה. שיחה אינטרקטיבית בין מוכיח כל יכול P לבודק הסתברותי V היא:
יש קלט $x \in \{0,1\}^n$. השיחה מתקימת בסיבובים. הבודק בוחר $y_1 \in \{0,1\}^{r_1(n)}$ באקראי, מחשב שאלה $q_1 = V_1(x, r_1)$ ושולח את q_1 ל- P. המוכיח מחשב תשובה $a_1 = P_1(x, q_1)$ ושולח אותה ל- V. וממשיכים ככה. V מחשב את השאלה הבאה כפונקציה של מה שראה עד עכשיו: $q_i = V_i(x, y_1, \ldots, y_i, q_1, \ldots, q_{i-1}, a_1, \ldots, a_{i-1})$ והמוכיח עוניה $a_i = P_i(x, q_1, \ldots, q_n)$. בסוף השיחה V מחליט אם לקבל או לא $V(x, y_1, \ldots, y_m, q_1, \ldots, q_m, a_1, \ldots, a_m) \in \{acc, rej\}$. נגיד שהשיחה היא בן מוכיח כל יכול לבודק הסתברותי פולינומי אם הפרקדיקטים $V_1, \ldots, V_m, V$ הם פולינומיים.
נגיד שהשיחה היא ב- k סיבובים אם עוברים k מסרים. כמובן שהמסר האחרון נשלח ל- V. סיבוב אחד זה הכי קרוב ל- NP, המוכיח מחזיר את העד והבודק יבחן האם זה עד טוב. רק שכאן הבודק הסתברותי.

הפרוטוקול שראינו ל- GNI היה שני סיבובים.

הגדרה. נגיד ששפה $L \in IP_{\alpha,\beta}[k]$ אם קיים פרוטוקול אינטרקטיבי בין מוכיח כל יכול לבודק הסתברותי יעיל ב- k סיבובים כך ש-

$$x \in L \Rightarrow \exists \underbrace{P}_{\text{מוכיח}} \mathbb{P}_V[V \text{ יקבל בסוף השיחה}] \geq \beta$$

$$x \notin L \Rightarrow \forall \underbrace{P}_{\text{מוכיח}} \mathbb{P}_V[V \text{ יקבל בסוף השיחה}] \leq \alpha$$

$GNI \in IP_{\frac{1}{2},1}[2]$. נדבר רגע על אמפליפיקציה.

$$GNI \in IP_{\frac{1}{2},1}[2] \Rightarrow GNI \in IP_{\frac{1}{4},1}[4]$$

נעשה אמפליפיקציה ע"י 2 הרצות ב"ת.

תרגיל. אפשר להריץ את שני הניסיונות עם אקראיות ב"ת במקביל ואז $GNI \in IP_{\frac{1}{4},1}[2]$.

הפרוטוקול שלנו ל- GNI היו לו "סודות". פרוטוקול בלי סודות, זה אומר שכש- V_i הוא מכין $y_i \in \{0,1\}^{r_i}$ בונה שאלה ושולח גם את השאלה וגם את y_i ל- P. זה נקרא public coin להבדיל מהפרוטוקול שהיה קודם, שלא שולח את המטבעות ונקרא private coin.

הגדרה. $L \in AM_{\alpha,\beta}[k]$ כמו קודם אבל בפרוטוקול public coin.

האם גם ב- public coin יש הוכחה של GNI? כלומר האם $GNI \in AM_{\frac{1}{2},1}[k]$.

משפט. לכל k קבוע:
$IP_{\alpha,\beta}[k] \subseteq AM_{\alpha,\beta}[k+2] \subseteq AM_{2^{-n},1}[2]$.

השנה לא נראה את ההוכחה.
למעשה אפילו $AM[2] \subseteq \pi_2$ אבל גם את זה לא נראה.
מה קורה אם אנחנו מוכנים ל k פולינומי?

משפט. $Pspace = AM_{2^{-n},1}[poly]$.

אם נסכים להרחיב את מושג הוכחה עוד יותר, ונשאל מה בודק יעיל יכול לוודא כשהוא מנהל שיחה עם שני מוכיחים כל יכולים שלא יכולים לתקשר ביניהם.

הגדרה. $MIP_{\alpha,\beta}[n,k]$ כמו IP אבל עם n מוכיחים ו-k סיבובים. הפרוטוקול הוא כלהלן: הקלט הוא x. V בוחר באקראיות y מחשב שתי שאלות q_1, q_2 ושולח את השאלה q_1 ל- P_1 ושולח את השאלה q_2 ל- P_2. המוכיחים מחזירים תשובות $a_1 = P_1(x, q_1), a_2 = P_2(x, q_2)$ בהתאמה.
לבסוף הבודק מחזיר פרדיקט $V(x, y, q_1, q_2, a_1, a_2) \in \{acc, rej\}$.
המוכיחים יכולים לתאם מראש אבל לא יודעים איזה שאלה קיבל המוכיח השני.

משפט. $NExp = MIP(2^{-n}, 1)[2, 1]$.

בשלב הבא נראה שיש ל NP הוכחה ובודק הסתברותי שקורא רק 3 ביטים מההוכחה:

$$x \in L \Rightarrow \mathbb{P}(\text{ יקבל } V) = 1$$

$$x \notin L \Rightarrow \mathbb{P}(\text{ יקבל } V) \leq \frac{7}{8} - \varepsilon$$