

סיבוכיות

© ארזים

13 ביוני 2017

1 הוכחות אינטראקטיביות

יש כאן שני שחקנים: V (המוודא) הוא מכונה הסתברותית שרצה בזמן פולינומי, P (המוכיח) הוא כל יכול. לשניהם יש קלט משותף x , והם מנהלים שיחה שאורכה פולינומי.

הגדרה 1.1 לשפה A יש פרוטוקול אינטראקטיבי (או הוכחה אינטראקטיבית) אם קיים V שכזה כך שמתקיים:

1. אם $x \in A$, קיים מוכיח P עם $\mathbb{P}(V \text{ accpets } x \text{ while talking to } P) \geq \frac{2}{3}$.

2. אם $x \notin A$, לכל מוכיח P^* מתקיים $\mathbb{P}(V \text{ accepts } x \text{ while talking to } P^*) \leq \frac{1}{3}$.

נסמן IP את מחלקה כל השפות שיש להן הוכחה אינטראקטיבית.

משפט 1.2 (שלא נוכיח) $IP = PSPACE$.

מה אם נדרוש שהמוודא יהיה דטרמיניסטי? נקבל את NP .

דוגמא להוכחה אינטראקטיבית

הגדרה 1.3 $a \in (\mathbb{Z}/p\mathbb{Z})^*$ ייקרא שארית ריבועית אם קיים $r \in (\mathbb{Z}/p\mathbb{Z})^*$ כך שמתקיים $a = r^2$.

דוגמא השאריות הריבועיות מודולו 5 הן $\{1, 4\}$.

נגדיר QNR את אוסף האיברים $a \in (\mathbb{Z}/p\mathbb{Z})^*$ שאינם שאריות ריבועיות. נראה הוכחה אינטראקטיבית עבור QNR .

עובדות

1. יש $\frac{p-1}{2}$ שאריות ריבועיות, ועוד $\frac{p-1}{2}$ שאריות לא ריבועיות.

2. אם x שארית ריבועית וגם y שארית ריבועית אזי xy שארית ריבועית. אם x שארית ריבועית, y שארית לא ריבועית אזי xy לא שארית ריבועית.

3. הפונקציה $x \mapsto ax$ היא פרמוטציה, ולכן אם נבחר $r \in (\mathbb{Z}/p\mathbb{Z})^*$ באופן אקראי ואחיד יתקיים:

(א) r^2 מתפלג אחיד על קבוצת השאריות הריבועיות.

(ב) xr^2 , כאשר x שארית ריבועית, מתפלג אחיד על קבוצת השאריות הריבועיות.

(ג) xr^2 , כאשר x שארית לא ריבועית, מתפלג אחיד על קבוצת השאריות הלא ריבועיות.

הפרוטוקול על קלט (x, p) :

1. מגריל אחיד $r \in (\mathbb{Z}/p\mathbb{Z})^*$ אקראית ואחיד, וכן $b \in \{0, 1\}$ אקראי ואחיד, ושומר אותם בסוד.

2. שולח אל P את $x^b r^2$ ומבקש ממנו לנחש את b .

3. V מקבל אם ורק אם P צודק.

תרגיל כאשר p ראשוני, $\text{QNR} \in P$.

2 בעיות פער

תהי A בעיית מקסימיזציה. בעיית הפער $\text{Gap} - A[\alpha, \beta]$ היא להבחין בין קלטים שעבור $\text{opt}_A(x) \geq \alpha$ וקלאים שעבורם $\text{opt}_A(x) \leq \beta$.

הגדרה 2.1 נאמר כי f היא רדוקציה משמרת פער בין $\text{Gap} - A[\alpha, \beta]$ לבין $\text{Gap} - B[\gamma, \delta]$ אם:

1. ניתן לחשב את f בזמן פולינומי.

2. שלמות - אם $\text{opt}_A(x) \geq \beta$ אז $\text{opt}_B(f(x)) \geq \delta$.

3. נאותות - אם $\text{opt}_A(x) \leq \alpha$ אז $\text{opt}_B(f(x)) \leq \gamma$.

דוגמה הבעיה $\text{Max} - 3\text{LIN}$: הקלט הוא מערכת משוואות לינאריות מעל $\mathbb{F}_2$, כשבכל משוואה יש 3 משתנים. נראה רדוקציה משמרת פער מהבעיה $\text{Gap} - \text{E3SAT}[\frac{7}{8} + \varepsilon, 1]$ אל $\text{Gap} - 3\text{LIN}[\frac{1}{2} + \frac{4}{7}\varepsilon, \frac{4}{7}]$.

הוכחה: יהי φ פסוק בצורת E3CNF. נגדיר את $f(\varphi)$ באופן הבא: לכל פסוקית $C = \alpha \vee \beta \vee \gamma$ (נניח בלי הגבלת הכלליות כי $C = x_1 \vee x_2 \vee x_3$) נגדיר 7 משווא

$$\begin{aligned} y_1 &= 1, y_2 = 1, y_3 = 1 \\ y_1 + y_2 &= 1, y_2 + y_3 = 1, y_1 + y_3 = 1 \\ y_1 + y_2 + y_3 &= 1 \end{aligned}$$

שלמות: נניח כי φ ספיקה. תהי a השמה מספקת. נגדיר השמה של $f(\varphi)$ על ידי $b(y_i) = a(x_i)$. לכל פסוקית C , זו מספקת 4 מתוך 7 המשוואות שמתאימות לה (משיקולי ספירה). לכן b מספקת $\frac{4}{7}$ מהמשוואות.

נאותות: נניח כי בתוך φ אפשר לספק לכל היותר $\frac{7}{8} + \varepsilon$ מהפסוקיות. תהי b השמה כלשהי של $\{y_i\}$. נגדיר השמה a של x_i על ידי $a(x_i) = b(y_i)$. זו מספקת לכל היותר $\frac{7}{8} + \varepsilon$ מפסוקיות φ . לכן, מספר המשוואות שאותן b מספקת הוא לכל היותר

$$\left(\frac{7}{8} + \varepsilon\right) \frac{4}{7} + \left(\frac{1}{8} - \varepsilon\right) \cdot 0 = \frac{1}{2} + \frac{4}{7}\varepsilon$$

■