בסיס

יחס שלא ידוע לו הכרעה אלגוריתם:

(עדיר את היחס הבא: $R = \{ (N, (n_1, n_2)) \mid N = n_1 \cdot n_2,\ n_1, n_2 \in \mathbb{N},\ 1 < n_1, n_2 < N \}$

SR בעיית ההכרעה: לקבוע האם מס' הוא ראשוני או לא. נמצאו אלגו' דטרמינסטי פולינומי $\Leftarrow$ נמצאת ב P.

פתרון נאיבי: רצה עד שורש המספר (= N)

אורך הקלט: $\log N$ $\Leftarrow$ הפתרון אינו פולינומי. באופן הקלט. אקספוננציאלי $\sqrt{N} = 2^{\frac{1}{2}\log N}$

זמן ריצה: $O(\sqrt{N})$

בעיית חיפוש: בהינתן N למצוא $n_1, n_2$ כך ש $(N, (n_1, n_2)) \in R$.
לא יודעים האם קיים פתרון.
חושבים כי הבעיה קשה. (קריפטו מסתמכים על ק..)

שקילות ההגדרות של NP

הגדרה 1: באמצעות מכונת טיורינג לא - תהי $S \subseteq \{0,1\}^*$ בעיית הכרעה/שפה.
$S \in NP$ אם קיימת מ"ט לא פולינומית המכריעה את S.

הגדרה 2: באמצעות מערכת הוכחה - תהי $S \subseteq \{0,1\}^*$ בעיית הכרעה/שפה.
$S \in NP$ אם קיימת מערכת הוכחה מסוג NP ל-S.
כלומר, $S \in NP$ אם קיימים פולינום $p(\cdot)$ ומאמת V פולינומי דטרמינסטי המקיימים:
1. שלמות - אם $x \in S$ אזי קיים "עד" y כך שמתקיים: $|y| \le p(|x|)$ ו $V(x,y) = 1$
2. נאותות - אם $x \notin S$ אז לכל y $V(x,y) = 0$

הוכחה

ביון ראשון: נניח שקיימת מערכת הוכחה מסוג NP ל-S.
נגדיר מ"ט לא פולינומית M שמכריעה את S באופן הבא:
בהינתן קלט x, M תנחש $y \in \{0,1\}^{p(|x|)}$ באופן לא תלוי את V על $(x,y)$ ותציר את תשובת V.

קל לראות, שעבור $x \in S$ קיים ניחוש y שעבורו $(x,y)$ המאמת V יציר 1.
ולכן יש מסלול מקבל של M.
לעומת זאת, עבור $x \notin S$ לכל y המאמת יציר 0 על $(x,y)$ ולכן אין מסלול מקבל של M והיא תציר תמיד 0.

ביון שני: נניח שקיימת מ"ט לא פולינומית M שמכריעה את S.
נגדיר מ"ט דט' פולינומית V שמקבלת צמד $(x,y)$ ופועלת באופן הבא:
V מבצעת סימולציה של המכונה M הלא כאשר M מקבלת את הצעד ה-i הלא שלה, V (שהיא מכונה דטרמינסטית) מסתכלת בבלוק ה-i-י ב-y. אנו מסתכלים על y כמחרוזת של בלוקים שכל אחד מהם מייצג קיפוד של מעבר של המכונה M.
בסופה של הסימולציה המכונה V תציר את מה ש M מחזירה.
• מעבר מוגדר להיות: מה המצב אליו עוברים, מה האות שרושמים על הסרט ולאן מזיזים את הראש הקורא.

קל לראות, שאם $x \in S$ אז קיים מסלול מקבל במכונה M, ולכן קיים y המהווה "מדריך" לבחירות הלא לאורך המסלול הזה מאז ש V יציר 1 על $(x,y)$.
לעומת זאת, אם $x \notin S$ אז לא קיים מסלול מקבל במכונה M ולכן אין מדריך y שעבורו $(x,y)$ המאמת V יציר 1.
ולכן תמיד יציר 0.
• נשים לב שהאורך של $|y| \le p(|x|)$ כיוון ש M היא פולינומית.

## ההיררכיה הפולינומית

1. $S \in \Sigma_k$ אם קיים פולינום $P(\cdot)$ ומודל פולינומי דטרמיניסטי כך ש:

$$x \in S \Leftrightarrow \exists y_1 \in \{0,1\}^{P(|x|)} \forall y_2 \in \{0,1\}^{P(|x|)} \ldots Q\, y_k \in \{0,1\}^{P(|x|)}$$

$$V(x, y_1, y_2, \ldots, y_k) = 1$$

$$Q = \begin{cases} \exists & k \text{ אי זוגי} \\ \forall & k \text{ זוגי} \end{cases}$$

2. $S \in \Pi_k$ אם קיים פולינום $P(\cdot)$ ומודל פולינומי דטרמיניסטי $V$ כך ש:

$$x \in S \Leftrightarrow \forall y_1 \in \{0,1\}^{P(|x|)} \exists y_2 \in \{0,1\}^{P(|x|)} \ldots Q'\, y_k \in \{0,1\}^{P(|x|)}$$

$$V(x, y_1, y_2, \ldots, y_k) = 1$$

$$Q' = \begin{cases} \forall & k \text{ אי זוגי} \\ \exists & k \text{ זוגי} \end{cases}$$

**דוגמה:**

Min-Vertex-Cover מכילה את כל הצמתים $(G,k)$ כך שקיים כיסוי קודקודים מינימלי ל-$G$ שגודלו בדיוק $k$.

**טענה**

$$\text{Min-Vertex-Cover} \in \Sigma_2$$

**הוכחה**

$$(G,k) \in \text{Min-Vertex-Cover} \Leftrightarrow \exists S \in V[G]\ \forall S' \subseteq V[G]$$

$$V((G,k), S, S') = 1$$

כאשר $V$ מקבל גם $(G,k)$ משתי מי קבוצה של קודקודים $S$ ו-$S'$ ומחזיר 1 אם מתקיימים התנאים: (0 אחרת)

1. $|S| = k$
2. $S$ הוא כיסוי קודקודים חוקי של $G$. כלומר לכל $(u,v) \in E(G)$
3. $S'$ לא כיסוי קודקודים חוקי של $G$, או ש $|S'| \geq k$

קל לראות שהמודל $V$ רץ בזמן פולינומי ומקיים את התנאים של $\Sigma_2$ לכן $\text{Min-Vertex-Cover} \in \Sigma_2$.