תזכורת - אלגוריתם לא דטרמיניסטי

בעיות הכרעה

- אם התשובה היא כן, קיים מסלול מקבל.
- אם התשובה היא לא, כל המסלולים מחזירים 0.

בעיות חישוב

- האלגוריתם מחזיר תשובה נכונה או "לא יודע".
- קיימת לפחות ריצה אחת שמחזירה תשובה נכונה.

תרגיל

הראו שהבעיות הבאות בNL:

סעיף א

קלט: גרף G לא מכוון

פלט: האם קיימים בG בדיוק שני רכיבי קשירות המקווים ביחד את כל הגרף?

פתרון לא נכון

1. נבחר קודקוד כלשהו v בצורה שרירותית.
2. לכל קדקד $u \neq v$:
   2.1. אם $\text{st-Conn}\left(G,v,u\right)=0$ עבור לצעד 3.
   2.2. אם עברנו על כל הקודקודים החזר 0 וסיים.
3. לכל קדקד w:
   אם $\text{st-Conn}\left(G,v,w\right)=1$ או $\text{st-Conn}\left(G,u,w\right)=1$ המשך לקדקד הבא.
   אחרת - החזר 0 וסיים.
4. החזר 1

הפתרון לא נכון, כי הוא סומך על תשובה 0 של אלגוריתם בNL(st-Conn) - ואם אלגוריתם לא דטרמיניסטי מחזיר 0 זה לא אומר כלום.

אי אפשר לסמוך על תשובה 0 של אלגוריתם לא דטרמיניסטי!

פתרון נכון

נזכור ש$NL = coNL$ ־ ולכן אם $\text{st-Conn} \in NL$ גם $\text{non-Conn} \in NL$. לכן אפשר להשתמש בnon-Conn:

1. נבחר קודקוד כלשהו v בצורה שרירותית.
2. לכל קדקד $u \neq v$:
   - 2.1. אם $\text{non-Conn}\left(G, v, u\right) = 1$ עבור לצעד 3.
   - 2.2. אם עברנו על כל הקודקודים החזר 0 וסיים.
3. לכל קדקד w:

   אם $\text{st-Conn}\left(G, v, w\right) = 1$ או $\text{st-Conn}\left(G, u, w\right) = 1$ המשך לקדקד הבא.

   אחרת ־ החזר 0 וסיים.
4. החזר 1

הפעם אנו מסתמכים על תשובה 1 של אלגוריתם לא דטרמיניסטי ־ ועל תשובה כזו מותר לסמוך.

סעיף ב

קלט:
- גרף לא מכוון G
- קדקדים s, t
- מספר k

פלט: האם המסלול הקצר ביותר בין s לt הוא באורך k בדיוק.

פתרון

האלגוריתם $\text{reach}\left(G, s, t, d\right)$ בודק האם קיים מסלול בין s לt באורך$\geq d$, והוא בNL. לכן גם ההופכי שלו, non-reach, הוא בNL.

1. אם $\text{reach}\left(G, s, t, k\right) = 1$ וגם $\text{non-reach}\left(G, s, t, k-1\right) = 1$ החזר 1.
2. אחרת החזר 0.

תרגיל

- נגדיר PP_1: $L \in PP_1$ אם קיימת מכונת טיורינג פולינומית M המקיימת:

$$x \in L \quad \Longleftrightarrow \quad \Pr\left[M\left(x\right) = 1\right] > \frac{1}{2}$$
$$x \notin L \quad \Longleftrightarrow \quad \Pr\left[M\left(x\right) = 0\right] \geq \frac{1}{2}$$

- נגדיר PP_2: $L \in PP_2$ אם קיימת מכונת טיורינג פולינומית M המקיימת:

$$\forall_x \Pr\left[M\left(x\right) = \chi_L\left(x\right)\right] > \frac{1}{2}$$

הוכיחו ש$PP_1 = PP_2$

הערה 1

אם היינו מגדירים את PP_1 כך שההסתברות לתשובת 1 נכונה היא <u>גדולה</u> או שווה ל$\frac{1}{2}$, אזי כל השפות היו בPP_1 - שכן אפשר להטיל מטבע.

הערה 2

PP_2 שונה באופן מהותי מBPP, שכן בBPP יש לנו רוב מוחלט לתשובה הנכונה, ואילו בBPP הרוב מאוד קטן - זה יכול להיות הבדל של ריצה אחת מתוך מספר אקספוננציאלי של ריצות, ולכן אי אפשר לעשות אמפליפיקציה במספר פולינומי של ריצות.

פתרון

$PP_2 \subseteq PP_1$ - ברור! נראה ש$PP_1 \subseteq PP_2$:

תהי $L \in PP_1$. קיימת מכונת טיורינג פולינומית M' עם ההסתברות של PP_1. צ"ל $L \in PP_2$. נבנה מכונת טיורינג פולינומית M עם ההסתברות של PP_2.

$$x \in L \iff \Pr\left[M'\left(x\right) = 1\right] > \frac{1}{2} \qquad x \notin L \iff \Pr\left[M'\left(x\right) = 0\right] \geq \frac{1}{2}$$

יהי $p\left(\cdot\right)$ פולינום החוסם את מספר הטלות המטבע של M'. נטען שאת $\Pr\left[M'\left(x\right) = 1\right] > \frac{1}{2}$ אפשר להחליף ב

$$\Pr\left[M'\left(x\right) = 1\right] \geq \frac{1}{2} + \frac{1}{2^{p(|x|)}}$$

שכן אם יש מקסימום $p\left(|x|\right)$ הטלות מטבע, אזי ההסתברות של כל תוצאה היא כפולה שלמה של $\frac{1}{2^{p(|x|)}}$.

נבנה אלגוריתם M שעל קלט x, בהסתברות $\frac{1}{2^{2p(|x|)}}$ מחזיר 0 ומסיים. בהסתברות המשלימה $\left(1 - \frac{1}{2^{2p(|x|)}}\right)$ מריץ את $M'\left(x\right)$ ומחזיר את הפלט שלו.

תזכורת: נוסחת ההסתברות השלמה:

יהיו A וB שני מאורעות, אזי

$$\Pr\left[A\right] = \Pr\left[A|B\right] \cdot \Pr\left[B\right] + \Pr\left[A|\neg B\right] \cdot \Pr\left[\neg B\right]$$

נסמן בE את המאורע שM החזירה 0 בשלב הראשון:

- אם $x \in L$:

$$\Pr\left[M\left(x\right)=1\right]=\Pr\left[M\left(x\right)=1|E\right]\cdot\Pr\left[E\right]+\Pr\left[M\left(x\right)=1|\neg E\right]\cdot\Pr\left[\neg E\right]\geq$$

$$\geq\left(\frac{1}{2}+\frac{1}{2^{p(|x|)}}\right)\left(1-\frac{1}{2^{2p(|x|)}}\right)=\frac{1}{2}+\underbrace{\frac{1}{2^{p(|x|)}}-\frac{1}{2^{2p(|x|)+1}}-\frac{1}{2^{2p(|x|)}}}_{>0}>\frac{1}{2}$$

- אם $x \notin L$:

$$\Pr\left[M\left(x\right)=0\right]=\Pr\left[M\left(x\right)=0|E\right]\cdot\Pr\left[E\right]+\Pr\left[M\left(x\right)=0|\neg E\right]\cdot\Pr\left[\neg E\right]=$$

$$=1\cdot\Pr\left[E\right]+\Pr\left[M'\left(x\right)=0\right]\cdot\Pr\left[\neg E\right]=\frac{1}{2^{2p(|x|)}}+\frac{1}{2}-\frac{1}{2^{2p(|x|)+1}}>\frac{1}{2}$$

תרגיל

מה הi המינימלי עבורו $NP^{BPP} \subseteq \Sigma_i$?

פתרון

ראינו בהצראה ש$BPP \subseteq \Sigma_2$. לכן:

$$NP^{BPP} \subseteq NP^{\Sigma_2} = \Sigma_3$$

נראה ש$NP^{BPP} \subseteq \Sigma_2$:

$$\begin{matrix} BPP = coBPP \\ coBPP \subseteq co\Sigma_2 \end{matrix} \implies BPP \subseteq \Pi_2$$

$$BPP \subseteq \Sigma_2 \cap \Pi_2$$

נוכיח $NP^{\Sigma_2\cap\Pi_2} \subseteq \Sigma_2$:

$$NP^{BPP} \subseteq NP^{\Sigma_2\cap\Pi_2}$$

תהי $L \in NP^{\Sigma_2\cap\Pi_2} \Leftarrow$ קיימת מכונת טיורינג לא דטרמיניסטית פולינומית M^A. עבור $A \in \Sigma_2 \cap \Pi_2$ נראה ש$L \in \Sigma_2$:

ידוע $A \in \Sigma_2 \cap \Pi_2$:

א. $A \in \Sigma_2 \Leftarrow$ קיימת N_A^{SAT}

ב. $\overline{A} \in \Sigma_2 \Leftarrow$ קיימת $N_{\overline{A}}^{\mathrm{SAT}}$

$$NP^{\Sigma_i\cap\Pi_i} \subseteq \Sigma_i$$

תרגיל

יהי $R \in PC \backslash PF$. הראו שאם קיימת רדוקציה עצמית עבור R, אזי הרדוקציה עושה יותר מאשר מספר לוגריתמי של שאילתות לבעיית ההכרעה המתאימה.

פתרון

יהי $R \in PC \backslash PF$. נניח שקיימת רדוקציה עצמית שעושה מספר לוגריתמי של שאילתות לבעיית ההכרעה. נראה ש$R \in PF$.

נריץ את המכונה המשתמשת באורקל, אבל במקום לבצע אורקל - נפצל את הריצה לשני מסלולים בכל שאילתת אורקל. מכיוון שיש רק מספר לוגריתמי של גישות, ניתן לעבור על כל האפשרויות בזמן פולינומי. מכיוון ש$R \in PC$, הבדיקה אם מסלול מחזיר תשובה נכונה היא פולינומית.