הגדרה

תהי M מכונת טיורינג לא דטרמיניסטית העוצרת לכל קלט ולכל בחירה ל"ד. סיבוכיות המקום של M היא $s:\mathbb{N}\to\mathbb{N}$ כאשר $s(n)$ הוא האינדקס הגדול ביותר שM מגיעה אליו על סרט העבודה שלה לכל קלט מאורך n ולכל בחירה ל"ד.

הגדרה

עבור פונקציה s:

$$\mathrm{NSPACE}(s(n)) = \left\{ L \;\middle|\; \begin{array}{c} \text{There exists a non-deterministice} \\ \text{turing machine that determines } L \\ \text{in space complexity } s(n) \end{array} \right\}$$

סימונים

1. $L = \bigcup_c \mathrm{DSPACE}(c \cdot \log n)$
2. $NL = \bigcup_c \mathrm{NSPACE}(c \cdot \log n)$
3. $\mathrm{PSPACE} = \bigcup_c \mathrm{DSPACE}(n^c)$
4. $\mathrm{NPSPACE} = \bigcup_c \mathrm{NSPACE}(n^c)$

משפט Savitch

לכל $s(n) \geq \log n$:

$$\mathrm{NSPACE}(s(n)) \subseteq \mathrm{DSPACE}\left(s^2(n)\right)$$

בפרט:

$$\mathrm{PSPACE} = \mathrm{NSPACE}$$

משפט אימרמן

לכל $s(n) \geq \log n$:

$$\mathrm{NSPACE}(s(n)) = \mathrm{coNSPACE}(s(n))$$

בפרט:

$$\mathrm{NPSPACE} = \mathrm{coNPSPACE}$$

הערה

בעולם של סיבוכיות זמן, יש שתי הגדרות שקולות של NP. בעולם של סיבוכיות מקום הן לא שקולות.

הגדרה

תהיינה L_1, L_2 שתי שפות.
קיימת רדוקציית $\mathrm{SPACE}\left(s\left(\cdot\right)\right)$ מL_1 לL_2 אם קיימת פונקציה f הניתנת לחישוב בסיבוכיות מקום $s\left(\cdot\right)$ כך שלכל x:

$$x \in L_1 \iff f\left(x\right) \in L_2$$

תרגיל

תהיינה L_1 וL_2 שפות. הראו שאם:

א. קיימת רדוקציית $s_1\mathrm{SPACE}$ מL_1 לL_2

ב. $L_2 \in (N)\mathrm{DSPACE}\left(s_2\right)$

אזי:

$$L_1 \in (N)\mathrm{DSPACE}\left(s_1 + s_2'\right)$$

עבור

$$s_2' = s_2\left(2^{s_1(n)+\log s_1(n)} \cdot n\right)$$

פתרון

$L_2 \in \mathrm{DSPACE}\left(s_2\right) \Longleftarrow$ קיימת מכונת טיורינג דטרמיניסטית M_2 המכריעה את L_2 בסיבוכיות מקום $s_2\left(\cdot\right)$.
צ"ל $L_1 \in \mathrm{DSPACE}\left(s_1 + s_2'\right)$, כלומר נבנה מכונט טיורינג דטרמיניסטית M_1 המכריעה את L_1 בסיבוכיות מקום $s_1 + s_2'$.
המכונה M_1 בהינתן קלט x:

א. חשב את $y = f\left(x\right)$

ב. החזר את $M_2\left(y\right)$

נכונות נובעת מהגדרת הרדוקציה.

סיבוכיות מקום: **צעד א**: $s_1\left(n\right)$
צעד ב: $s_2\left(|y|\right)$

טענה: $|y| \leq 2^{s_1(n)+\log s_1(n)} \cdot n$

הוכחה: קיימת רדוקציית s_1SPACE מL_1 לL_2 $\Longleftarrow$ קיימת מכונת טיורינג שבהינתן x מחשבת את $f(x)$ תוך שימוש בסיבוכיות מקום $s_1(n)$.

$|f(x)|$≥סיבוכיות הזמן של M≥מספר הקונפיגורציות$\cdot n$ $2^{s_1(n)+\log s_1(n)}$

לכן, בצעד ב: $s_2(|y|) \leq s_2\left(2^{s_1(n)+\log s_2(n)} \cdot n\right)$

סה"כ: $s_1(n) + s_2\left(2^{s_1(n)+\log s_1(n)} \cdot n\right)$

עכשיו, לכאורה סיימנו, אבל נשים לב שבצעד א' חישבנו את y - אבל לא התחשבנו במקום על סרט העבודה שצריך בשביל לרשום את y!

הפתרון הוא שלא באמת כותבים את y על סרט העבודה. כשמחשבים את $M_2(y)$, אין לנו את y בידיים, אלא החישוב מבוצע ביט־ביט. M_2 מסתכלת על y ביט ביט, ולכן כאשר M_2 רוצה לקרוא ביט מסויים, מריצים את f עד הנקודה שבה מגיעים לאותו ביט ומפסיקים. ברגע שרוצים את הביט הבא, מריצים את f שוב מההתחלה עד שמגיעים אליו.

אלגוריתמים הסתברותיים

דוגמה - בדיקת ראשוניות

בהינתן קלט N, האם N ראשוני או לא?

עובדות:

1. לכל מספר ראשוני p ולכל $r \in \{1, \ldots p-1\}$, למשוואה $x^2 = r^2 \pmod p$ יש בדיוק שני פתרונות:$r, -r$.
2. לכל מספר פריק אי־זוגי ולא חזקה של ראשוני p ולכל $r \in \{1, \ldots p-1\}$, למשוואה $x^2 = r^2 \pmod p$ יש לפחות ארבעה פתרונות$\pmod p$.

נניח שנתון לנו אלגוריתם sqrt: בהינתן קלט מספר ראשוני p ומספר $s = r^2 \pmod p$, האלגוריתם מחזיר איזשהו פתרון ל$x^2 = s \pmod p$.

נבנה אלגוריתם שמקבל כקלט מספר N ומחזיר אם הוא ראשוני או לא:

1. אם N הוא זוגי או חזקה של ראשוני, החזר 0.
2. בחר בצורה רנדומית $r \in \{1, \ldots N-1\}$ וחשב $s = r^2 \pmod p$
3. יהי $r' = \text{sqrt}(N, s)$