

## הגדרה

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

## הגדרה

עבור פונקציה  $s$ :

$$\text{NSPACE}(s(n)) = \left\{ L \mid \begin{array}{l} \text{There exists a non-deterministic} \\ \text{turing machine that determines } L \\ \text{in space complexity } s(n) \end{array} \right\}$$

## סימונים

$$L = \bigcup_c \text{DSPACE}(c \cdot \log n) \quad .1$$

$$NL = \bigcup_c \text{NSPACE}(c \cdot \log n) \quad .2$$

$$\text{PSPACE} = \bigcup_c \text{DSPACE}(n^c) \quad .3$$

$$\text{NPSPACE} = \bigcup_c \text{NSPACE}(n^c) \quad .4$$

## משפט Savitch

לכל  $s(n) \geq \log n$ :

$$\text{NSPACE}(s(n)) \subseteq \text{DSPACE}(s^2(n))$$

בפרט:

$$\text{PSPACE} = \text{NSPACE}$$

## משפט אימרמן

לכל  $s(n) \geq \log n$ :

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

בפרט:

$$\text{NPSPACE} = \text{coNPSPACE}$$

## הערה

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

## הגדרה

תהינה  $L_1, L_2$  שתי שפות. קיימת רדוקציית  $SPACE(s(\cdot))$  מ  $L_1$  ל  $L_2$  אם קיימת פונקציה  $f$  הניתנת לחישוב בסיבוכיות מקום  $s(\cdot)$  כך שלכל  $x$ :

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

## תרגיל

תהינה  $L_1$  ו  $L_2$  שפות. הראו שאם:

א. קיימת רדוקציית  $s_1SPACE$  מ  $L_1$  ל  $L_2$

ב.  $L_2 \in (N)DSPACE(s_2)$

אזי:

$$L_1 \in (N)DSPACE(s_1 + s'_2)$$

עבור

$$s'_2 = s_2 \left( 2^{s_1(n) + \log s_1(n)} \cdot n \right)$$

## פתרון

$L_2 \in DSPACE(s_2) \iff$  קיימת מכונת טיורינג דטרמיניסטית  $M_2$  המכריעה את  $L_2$  בסיבוכיות מקום  $s_2(\cdot)$ .

צ"ל  $L_1 \in DSPACE(s_1 + s'_2)$ , כלומר נבנה מכונת טיורינג דטרמיניסטית  $M_1$  המכריעה את  $L_1$  בסיבוכיות מקום  $s_1 + s'_2$ . המכונה  $M_1$  בהינתן קלט  $x$ :

א. חשב את  $y = f(x)$

ב. החזר את  $M_2(y)$

נכונות נובעת מהגדרת הרדוקציה.

סיבוכיות מקום: צעד א:  $s_1(n)$

צעד ב:  $s_2(|y|)$

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

**הוכחה:** קיימת רדוקציית  $s_1$ SPACE מ  $L_1$  ל  $L_2$   $\Leftarrow$  קיימת מכונת טיורינג שבהינתן  $x$  מחשבת את  $f(x)$  תוך שימוש בסיבוכיות מקום  $s_1(n)$ .

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

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

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

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  $y$  בידים, 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  $r \in \{1, \dots, p-1\}$ , 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  $r \in \{1, \dots, p-1\}$ , 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  $r \in \{1, \dots, N-1\}$  וחשב  $s = r^2 \pmod{p}$

3. יהי  $r' = \text{sqrt}(N, s)$