פתרון תרגיל מספר 3 ־ חישוביות וסיבוכיות

שם: מיכאל גרינבאום, **ת.ז:** 211747639

28 באפריל 2020

שאלה 4:

סעיף 1:

צ"ל: $L = \{v \cdot u \cdot u \mid v, u \in \Sigma^*\}$ אינה רגולרית
הוכחה:
נניח בשלילה ש־ $L \in REG$, נסמן את קבוע הניפוח ב־ p.
נסתכל על המילה $w = a^p \cdot b \cdot a^p \cdot b \in L$ כי $w = u \cdot u$ כאשר $u = a^p \cdot b$,
תהי x, y, z חלוקה המקיימת $w = x \cdot y \cdot z$, $|y| > 0$, $|x \cdot y| \leq p$
נשים לב כי $|w| \geq p$
נסמן $|x| = n, |y| = m$ אזי נקבל כי $x = a^n, y = a^m$ ו־ $z = a^{p-n-m} \cdot b \cdot a^p \cdot b$,
לכן מלמת הניפוח מתקיים כי $x \cdot y^0 \cdot z \in L$, אבל נשים לב כי

$$x \cdot y^0 \cdot z = a^n \cdot a^{0 \cdot m} \cdot a^{p-n-m} \cdot b \cdot a^p \cdot b = a^{p-m} \cdot b \cdot a^p \cdot b \overset{\star}{\notin} L$$

כלומר הראנו שלכל חלוקה של w ו־2 התנאים הראשונים מתקיימים, השלישי לא מתקיים,
כלומר קיבלנו סתירה ללמת הניפוח, ולכן $L \notin REG$.
הערה: $\star$ מתקיים ש־ $w' = a^{p-m} \cdot b \cdot a^p \cdot b \notin L$ בגלל שלכל $v, u \in \Sigma^*$ מתקיים $w' \neq v \cdot u \cdot u$

מ.ש.ל.א.☺

סעיף 2:

צ"ל: $L = \{a \cdot w \cdot a \mid w \in \Sigma^*\}$ זאת שפה רגולרית
הוכחה:
נשים לב כי הביטוי הרגולרי המתאים לשפה הוא $\boxed{\{a\} \cdot \Sigma^* \cdot \{a\}}$ בגלל ש־ $L = \{a \cdot w \cdot a \mid w \in \Sigma^*\} = \{a\} \cdot \{w \mid w \in \Sigma^*\} \cdot \{a\}$

מ.ש.ל.ב.☺

סעיף 3:

צ"ל: $L = \{1^p \mid \text{p is prime}\}$ לא רגולרית
הוכחה:
נניח בשלילה ש־ $L \in REG$, נסמן את קבוע הניפוח ב־ p.
נסתכל על המילה $w = 1^{p'} \in L$ כאשר p' הוא ראשוני גדול מ־ p
תהי x, y, z חלוקה המקיימת $w = x \cdot y \cdot z$, $|y| > 0$, $|x \cdot y| \leq p$
נשים לב כי $|w| = p' \geq p$
נסמן $|x| = n, |y| = m$ אזי נקבל כי $x = 1^n, y = 1^m, z = 1^{p'-n-m}$,
לכן מלמת הניפוח מתקיים כי $x \cdot y^{p'+1} \cdot z \in L$, אבל נשים לב כי

$$x \cdot y^{p'+1} \cdot z = 1^n \cdot 1^{p' \cdot m + m} \cdot 1^{p'-n-m} = 1^{p' + p' \cdot m} = 1^{p' \cdot (1+m)} \overset{\star}{\notin} L$$

כלומר הראנו שלכל חלוקה של w ו־2 התנאים הראשונים מתקיימים, השלישי לא מתקיים,
כלומר קיבלנו סתירה ללמת הניפוח, ולכן $L \notin REG$.
הערה: $\star$ מתקיים ש־ $1^k = 1^{p' \cdot (1+m)} \notin L$ בגלל ש־ $1 + m \geq 2$, כלומר $k = p' \cdot (1+m)$ לא ראשוני כי כתבנו אותו כפירוק של 2 מספרים טבעיים גדולים מ־ 1

מ.ש.ל.ג.☺

סעיף 4:

צ"ל: $\{w \mid w \equiv 0 \mod 3 \wedge w \neq \varepsilon\}$ רגולרית
הוכחה:
ניצור אוטומט שמתאר את השפה הזאת, נגדיר פונקצית עזר $f : \Sigma \to \mathbb{N}$ באופן הבא: $f(i) = i \mod 3$,
נגדיר את $s : \Sigma \to \mathbb{N}$ כסכום הספרות של w
נגדיר אוטומט DFA כ־ $\mathcal{A} = \langle \{q_0, q_1, q_2, q_{start}\}, \Sigma, \delta, \{q_0\}, q_{start} \rangle$, יהיו $\sigma \in \Sigma$, $q \in Q$ נגדיר

$$\delta(q, \sigma) = \begin{cases} q_{f(\sigma)} & q = q_{start} \\ q_{(i+f(\sigma)) \mod 3} & \exists i \in \{0,1,2\} \text{ s.t. } q = q_i \end{cases}$$

נוכיח באינדוקציה שלכל מילה $w \neq \varepsilon$ מתקיים $\delta^*(q_{start}, w) = q_i$ אם"ם $s(w) \equiv i \mod 3$
<u>בסיס:</u> אם $|w| = 1$, נסמן $w = \sigma$ כאשר $\sigma \in \Sigma$, נשים לב כי

$$\delta^*(q_{start}, w) = \delta(q_{start}, \sigma) = q_{f(\sigma)} = q_{\sigma \mod 3}$$

כלומר $\delta^*(q_{start}, w) = q_i$ אם"ם $\sigma \equiv i \mod 3$ אם"ם $s(w) = s(\sigma) \equiv \sigma \equiv i \mod 3$, כנדרש
<u>צעד:</u> נניח שהטענה נכונה ל־ $n-1$ ונוכיח ל־ n,
נסמן $w = \sigma_1 \ldots \sigma_n$ כאשר $\sigma_i \in \Sigma$ ו־ $u = \sigma_1 \ldots \sigma_{n-1}$, כלומר $w = u \cdot \sigma_n$,
נסמן $\delta^*(q_{start}, u) = q_i$ (הוא לא q_{start} כי אי אפשר להגיע אליו לאחר הצעד הראשון)
מהנחת האינודקציה מתקיים כי $s(u) \equiv i \mod 3$ אם"ם $\delta^*(q_{start}, u) = q_i$,
נשים לב כי

$$\delta^*(q_{start}, w) = \delta^*(q_{start}, u \cdot \sigma_n) = \delta(\delta^*(q_{start}, u), \sigma_n) = q_{i+f(\sigma_n) \mod 3}$$

נשים לב כי $s(w) = s(u) + \sigma_n$, ולכן $\delta^*(q_{start}, w) = q_j$ אם"ם $i + f(\sigma_n) \equiv j \mod 3$ אם"ם $s(w) = s(u) + \sigma_n \equiv s(u) + f(\sigma_n) \equiv i + f(\sigma_n) \equiv j \mod 3$, כנדרש
כלומר קיבלנו כי לכל מילה באורך גדול או שווה ל־ 1 מתקיים $\delta^*(q_{start}, w) = q_i$ אם"ם $s(w) \equiv i \mod 3$,
נשים לב כי $\delta^*(q_{start}, \varepsilon) = q_{start} \notin F$ ולכן $\varepsilon \notin L(\mathcal{A})$ וגם $\varepsilon \notin L$, עתה נראה שלכל מילה אחרת מתקיים

$$\begin{aligned} \varepsilon \neq w \in L &\Leftrightarrow (\varepsilon \neq w) \wedge (s(w) \mod 3 \equiv 0) \Leftrightarrow (\varepsilon \neq w) \wedge (\delta^*(q_{start}, w) = q_0) \\ &\Leftrightarrow (\varepsilon \neq w) \wedge (\delta^*(q_{start}, w) \in F) \Leftrightarrow \varepsilon \neq w \in L(\mathcal{A}) \end{aligned}$$

לכן $\boxed{L = L(\mathcal{A})}$ כי $\varepsilon \neq w \in L \Leftrightarrow \varepsilon \neq w \in L(\mathcal{A})$ וגם $\varepsilon \notin L(\mathcal{A})$ וגם $\varepsilon \notin L$,
כלומר הראנו שהשפה רגולרית, ובעזרת האלגוריתם שראינו בתרגול ניתן להמיר את האוטומט לביטוי רגולרי

מ.ש.ל.ד.☺

סעיף 5:

צ"ל: $L = \left\{0^{i_1}10^{i_2}10^{i_3}10^{i_4}10^{i_5}10^{i_6}1 \mid i_6 < i_5 < i_4 < i_3 < i_2 < i_1 < 100\right\}$ רגולרית
הוכחה:
תחילה נשים לב ש־ L סופית בגלל שיש לכל היותר 100^6 אפשרויות למילים.
נסמן $L = \{w_1, \ldots, w_n\}$ אז תחילה נשים לב כי L רגולרית כי היא סופית (הוכח בתרגיל 1),
והביטוי הרגולרי המתאר את השפה הוא $\boxed{\bigcup_{i=1}^{n} \{w_i\}}$

מ.ש.ל.ה.☺

סעיף 6:

צ"ל: $L=\left\{0^{i_1}10^{i_2}10^{i_3}10^{i_4}10^{i_5}10^{i_6}1 \mid i_6<i_5<i_4<i_3<i_2<i_1 \wedge (i_2<100)\right\}$ רגולרית

הוכחה:

נסמן

$$\begin{aligned}
L_1&=\left\{0^{i_1}10^{i_2}10^{i_3}10^{i_4}10^{i_5}10^{i_6}1 \mid i_6<i_5<i_4<i_3<i_2<i_1<100\right\}\\
L_2&=\left\{0^{i_1}10^{i_2}10^{i_3}10^{i_4}10^{i_5}10^{i_6}1 \mid i_6<i_5<i_4<i_3<i_2<i_1 \wedge (i_2<100)\wedge(i_1\geq 100)\right\}\\
L_3&=\left\{0^{i_1}1 \mid i_1\geq 100\right\}\\
L_4&=\left\{0^{i_2}10^{i_3}10^{i_4}10^{i_5}10^{i_6}1 \mid i_6<i_5<i_4<i_3<i_2<100\right\}
\end{aligned}$$

נשים לב כי $L=L_1\cup L_2$, וראינו כי L_1 רגולרית מהסעיף הקודם, נוכיח ש־ L_2 רגולרית.

ועתה נשים לב כי $L_2=L_3\cdot L_4$,

מאותו נימוק של הסעיף הקודם L_4 סופית בגלל שיש לכל היותר 100^5 אפשרויות למילים, ולכן רגולרית.

נשים לב ש־ L_3 רגולרית בגלל שהביטוי הרגולרי המתאים לשפה הוא $\underbrace{\{0\}\cdot\cdots\cdot\{0\}}_{\text{100 times}}\cdot\{0\}^*$, והוכחנו ששפה היא רגולרית אם"ם

קיים ביטוי רגולרי המתאר אותה (אפשר לבנות אוטמט לשפה עם 101 מצבים)

לכן L_2 הוא רגולרי כי הוא שרשור של שפות רגולריות,

ולכן $L=L_1\cup L_2$ רגולרית ונוכל לקבל את הביטוי הרגולרי לפי האלגוריתם שראינו להמרת אוטומט לביטוי רגולרי.

הערה: אפשר לעשות ידנית באופן הבא, נסמן $L_1=\left\{w_1^1,\ldots,w_n^1\right\}$, $L_4=\left\{w_1^4,\ldots,w_m^4\right\}$ ונקבל כי מהנימוק בסעיף הקודם נקבל את הביטוי הרגולרי הבא

$$\begin{aligned}
L=L_1\cup L_2&=\left(\bigcup_{i=1}^{n}\left\{w_i^1\right\}\right)\cup L_2=\left(\bigcup_{i=1}^{n}\left\{w_i^1\right\}\right)\cup(L_3\cdot L_4)=\left(\bigcup_{i=1}^{n}\left\{w_i^1\right\}\right)\cup\left(L_3\cdot\left(\bigcup_{i=1}^{m}\left\{w_i^4\right\}\right)\right)\\
&=\left(\bigcup_{i=1}^{n}\left\{w_i^1\right\}\right)\cup\left(\left(\underbrace{\{0\}\cdot\cdots\cdot\{0\}}_{\text{100 times}}\cdot\{0\}^*\right)\cdot\left(\bigcup_{i=1}^{m}\left\{w_i^4\right\}\right)\right)
\end{aligned}$$

מ.ש.ל.ו.☺

סעיף 7:

צ"ל: $L=\left\{0^{i_1}10^{i_2}10^{i_3}10^{i_4}10^{i_5}10^{i_6}1 \mid i_6<i_5<i_4<i_3<i_2<i_1 \wedge (i_3<100)\right\}$ אינה רגולרית

הוכחה:

נניח בשלילה ש־ $L\in REG$, נסמן את קבוע הניפוח ב־ p.

נחלק ל2 מקרים:

1. אם $p\geq 5$:
   נסתכל על המילה $w=0^{p+1}10^{p}10^{4}10^{3}10^{2}101\in L$
   תהי x,y,z חלוקה המקיימת $w=x\cdot y\cdot z$, $|y|>0$, $|x\cdot y|\leq p$
   נשים לב כי $|w|\geq p+1\geq p$
   נסמן $|x|=n,|y|=m$ אזי נקבל כי $x=0^n,y=0^m,z=0^{p+1-n-m}10^{p}10^{4}10^{3}10^{2}101$,
   לכן מלמת הניפוח מתקיים כי $x\cdot y^0\cdot z\in L$, אבל נשים לב כי

$$x\cdot y^0\cdot z=0^n\cdot 0^{0\cdot m}\cdot 0^{p+1-n-m}10^{p}10^{4}10^{3}10^{2}101=0^{p+1-m}10^{p}10^{4}10^{3}10^{2}101\overset{\star}{\notin} L$$

כלומר הראנו שלכל חלוקה של w ו־2 התנאים הראשונים מתקיימים, השלישי לא מתקיים,
כלומר קיבלנו סתירה ללמת הניפוח, ולכן $L\notin REG$.
הערה: $\star$ מתקיים ש־ $0^{p+1-m}10^{p}10^{4}10^{3}10^{2}101\notin L$ בגלל ש־ $p+1-m\leq p+1-1=p\leq p$, כלומר התנאי $i_1>i_2$ לא מתקיים

2. אם $p<5$:
נסתכל על המילה $w=0^6 10^5 10^4 10^3 10^2 101 \in L$
תהי x,y,z חלוקה המקיימת $w=x\cdot y\cdot z$, $|y|>0$, $|x\cdot y|\le p<5$
נשים לב כי $|w|\ge p+1\ge p$
נסמן $|x|=n, |y|=m$ אזי נקבל כי $x=0^n, y=0^m, z=0^{6-n-m}10^5 10^4 10^3 10^2 101$,
לכן מלמת הניפוח מתקיים כי $x\cdot y^0\cdot z\in L$, אבל נשים לב כי

$$x\cdot y^0\cdot z=0^n\cdot 0^{0\cdot m}\cdot 0^{6-n-m}10^5 10^4 10^3 10^2 101=0^{6-m}10^5 10^4 10^3 10^2 101 \overset{\star}{\notin} L$$

כלומר הראנו שלכל חלוקה של w ו־2 התנאים הראשונים מתקיימים, השלישי לא מתקיים,
כלומר קיבלנו סתירה ללמת הניפוח, ולכן $L\notin REG$.
הערה: $\star$ מתקיים ש־ $0^{6-m}10^5 10^4 10^3 10^2 101\notin L$ בגלל ש־ $6-m\le 6-1=5\le 5$, כלומר התנאי $i_1>i_2$ לא מתקיים

ולכן קיבלנו כי קיבלנו סתירה בכל המקרים ולכן $\boxed{L\notin REG}$, כנדרש

מ.ש.ל.ז.☺