# פתרון תרגיל מספר 5 - חישוביות וסיבוכיות

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

13 במאי 2020

## שאלה 2

**סעיף 1** **צ"ל:** קיים $C \in R$ כך ש- $A \subseteq C$ וגם $C \cap B = \emptyset$

**הוכחה:**

תחילה מהיות $A, B \in coRE$ מתקיים כי $\overline{A}, \overline{B} \in RE$, כלומר קיימים $\mathcal{M}_1, \mathcal{M}_2$ שהם $TM$ כך ש- $L(\mathcal{M}_1) = \overline{A}$, $L(\mathcal{M}_2) = \overline{B}$.

נגדיר $\mathcal{M}$ $TM$ באופן הבא:

1. לכל $i \in \{1, 2, 3 \ldots\}$: (נשמור את המשתנה $i$ בסרט משלו ונריץ מכונות טיורינג כמו שראינו בתרגול)
   (א) נריץ את ה- $i$ הצעדים הראשונים של $\mathcal{M}_1, \mathcal{M}_2$ על הקלט $w$
   (ב) אם $\mathcal{M}_2$ קיבל את $w$, נקבל את $w$
   (ג) אם $\mathcal{M}_1$ קיבל את $w$, נדחה את $w$

תחילה נוכיח ש- $\mathcal{M}$ עוצר על כל קלט.

יהי $w \in \Sigma^*$,

- אם $w \notin A$, אזי $w \in \overline{A}$ ולכן $\mathcal{M}_1$ יקבל את $w$ מתישהו ($\exists t \in \mathbb{N}$ שאחרי $t$ צעדים $\mathcal{M}_1$ צעדים $\mathcal{M}_1$ יקבל את $w$ ואז לאחר $t$ צעדים $\mathcal{M}$ ידחה את $w$)
- אחרת $w \in A$, נשים לב ש- $A \cap B = \emptyset$ וגם $A = (A \cap B) \cup (A \cap \overline{B}) = \emptyset \cup (A \cap \overline{B}) = A \cap \overline{B}$, כלומר $w \in A = A \cap \overline{B} \subseteq \overline{B}$, ולכן $\mathcal{M}_2$ יקבל את $w$ מתישהו ($\exists t \in \mathbb{N}$ שאחרי $t$ צעדים $\mathcal{M}_2$ צעדים $\mathcal{M}_2$ יקבל את $w$ ואז לאחר $t$ צעדים $\mathcal{M}$ יקבל את $w$)

כלומר $\mathcal{M}$ עוצר על כל קלט.

נגדיר $\boxed{C = L(\mathcal{M})}$, נוכיח כי $C$ מקיים את הנדרש.

תחילה נשים לב שהוכחנו ש- $\mathcal{M}$ עוצר על כל קלט ולכן $\boxed{C = L(\mathcal{M}) \in R}$

נשים לב שהוכחנו מלעיל שמתקיים כי $A = A \cap \overline{B} \subseteq \overline{B}$, נשתמש בתכונה זאת שוב,

תהי $w \in A$, אזי $\mathcal{M}_1$ לא יקבל את $w$ אף פעם (אחרת $w \in A \wedge w \notin A$) וגם $w \in A \subseteq \overline{B}$ ולכן מתישהו $\mathcal{M}_2$ יקבל את $w$.

לכן קיימת איטרציה שבה $\mathcal{M}_2$ יקבל את $w$ (ועד איטרציה זאת כולל $\mathcal{M}_1$ לא יקבל), ולכן לפי ההגדרה, $\mathcal{M}$ יקבל את $w$, כלומר $w \in L(\mathcal{M}) = C$.

כלומר $\boxed{A \subseteq C}$

עתה נשים לב כי $B = (B \cap A) \cup (B \cap \overline{A}) = \emptyset \cup (B \cap \overline{A}) = (B \cap \overline{A}) \subseteq \overline{A}$

עתה יהי $w \in B$, אזי $\mathcal{M}_2$ לא יקבל את $w$ אף פעם (אחרת $w \in B \wedge w \notin B$) וגם $w \in B \subseteq \overline{A}$ ולכן מתישהו $\mathcal{M}_1$ יקבל את $w$.

לכן קיימת איטרציה שבה $\mathcal{M}_1$ יקבל את $w$ (ועד איטרציה זאת כולל $\mathcal{M}_2$ לא יקבל), ולכן לפי ההגדרה, $\mathcal{M}$ ידחה את $w$, כלומר $w \notin C$.

כלומר $\boxed{B \cap C = \emptyset}$

כלומר הראנו כי קיים $C \in R$ כך ש- $A \subseteq C$ וגם $C \cap B = \emptyset$

מ.ש.ל.א.☺

**סעיף 2 צ"ל:** אם $\mathcal{M}$ הוא $TM$ שרץ רק ימינה אז $L(\mathcal{M}) \in REG$
**הוכחה:**
יהי $\mathcal{M}$ שהוא $TM$ שרץ רק ימינה, נסמן $\mathcal{M} = \langle Q, \Sigma, \Gamma, \delta, q_0, q_{acc}, q_{rej} \rangle$
נגדיר $F_{helper} = \{q \mid \mathcal{M} \text{ accepts } \varepsilon \text{ when staring the run from state q}\}$
נגדיר $\mathcal{A} = \langle Q, \Sigma, \delta_{\mathcal{A}}, q_0, \{q_{acc}\} \cup F_{helper} \rangle$ באופן הבא,
לכל $q \in Q$, $\sigma \in \Sigma$ נסמן ב־ $\delta(q, \sigma) = \langle q', \sigma', R \rangle$ עתה נגדיר

$$\delta_{\mathcal{A}}(q, \sigma) = \begin{cases} q & (q = q_{acc}) \vee (q = q_{rej}) \\ q' & else \end{cases}$$

תהי $w \in \Sigma^*$, נסמן את הריצה של $\mathcal{A}$ על $w$ ב־ $q_0, q_1, \ldots, q_n$ , ונסמן $w = \sigma_1 \ldots \ldots \sigma_k$
נסמן את הריצה של $\mathcal{M}$ על $w$ ב־ $q'_0, q'_1, \ldots, q'_m$
**הערה:** נשים לב שמכיוון שאנחנו רק רצים שמאלה בשלב ה־ $i$ נגיע לתו $\sigma_i$ גם ב־ $TM$ וגם באוטומט
נוכיח באינדוקציה על $u$ מספר הצעדים בריצה שמתקיים $q_i = q'_i$
<u>בסיס:</u> $i = 0$, כלומר $w = \varepsilon$,
לכן מההגדרה מתקיים ששניהם במצב ההתחלתי שלהם ומתקיים $q_0 = q'_0$, כנדרש
<u>צעד:</u> נניח שטענה נכונה לריצה על $i-1$ צעדים ונוכיח ל־ $i$ צעדים
נשים לב שמתקיים $\delta\left(q'_{i-1}, \sigma_i\right) = \langle q'_i, \sigma', R \rangle$ וגם $\boxed{q_i = \delta_{\mathcal{A}}(q_{i-1}, \sigma_i) \overset{\text{def}}{=} q'_i}$, כנדרש
כלומר הראנו שהריצה של $\mathcal{M}$ על $w$ שהיא $q'_0, q'_1, \ldots, q'_{\min(m,n)} = q_0, q_1, \ldots, q_{\min(m,n)}$
נחלק ל־ 2 מקרים:

1. אם $m \le n$:
נשים לב כי $q_m = q'_m \in \{q_{acc}, q_{rej}\}$ ולכן מהגדרת פונקצית $\delta_{\mathcal{A}}$ נקבל כי $\delta^*_{\mathcal{A}}(q_m, w) = q_m$ לכל $w \in \Sigma^*$, ולכן בפרט מתקיים כי $q_n = q_m = q'_m$,
לכן נקבל שאם $q_n = q'_m = q_{rej}$ אזי מההגדרה $q_n \notin F$ ולכן $w \notin L(\mathcal{A})$ וגם $w \notin L(\mathcal{M})$ כי דחינו את המילה
וגם נקבל שאם $q_n = q'_m = q_{acc}$ אזי מההגדרה $q_n \in F$ ולכן $w \in L(\mathcal{A})$ וגם $w \in L(\mathcal{M})$ כי קיבלנו את המילה
ולכן $w \in L(\mathcal{M})$ אם"ם $w \in L(\mathcal{A})$

2. אם $n < m$:
נשים לב שאם $n < m$ אזי מתקיים כי $q_n = q'_n$ וגם הריצה של $\mathcal{M}$ על המילה $w$ הסתיימה (כי יש $n$ תווים ואי אפשר לחזור אחורה) ולכן הריצה עתה היא ריצה על המילה הריקה עם מצב התחלתי $q_n$.
נשים לב ש־ $q_n \ne q_{acc}, q_{rej}$ אחרת $\mathcal{M}$ היה מסיים את הריצה בצעד ה־ $n$ ולא ה־ $m$.
לכן נקבל שאם $w \in L(\mathcal{M})$ אזי $q_n \in F$ אזי מההגדרה $q_n \in \{q_{acc}\} \cup F_{helper}$ ולכן לפי מה שנאמר בשורה הקודמת, מתקיים כי $q_n \in F_{helper}$. לכן נקבל כי $\mathcal{M}$ מקבל את המילה הריקה כשהריצה מתחילה מהמצב $q_n$ (ההגדרה שמצב $q_n \in F_{helper}$), כלומר $q_m = q_{acc}$, כלומר $\mathcal{M}$ מקבל את $w$, כלומר $w \in L(\mathcal{M})$
וגם נקבל שאם $w \notin L(\mathcal{M})$ אזי $q_n \notin F$, כלומר $q_n \notin F_{helper}$, לכן הריצה של $\mathcal{M}$ על המילה הריקה עם מצב התחלתי $q_n$ לא מקבלת, כלומר $w \notin L(\mathcal{M})$
ולכן $w \in L(\mathcal{M})$ אם"ם $w \in L(\mathcal{A})$

כלומר הראנו שבכל המקרים מתקיים $w \in L(\mathcal{M})$ אם"ם $w \in L(\mathcal{A})$
כלומר קיבלנו ש־ $\boxed{L(\mathcal{M}) = L(\mathcal{A})}$,
כלומר הראנו שקיים אוטומט $\mathcal{A}$ המקיים $L(\mathcal{M}) = L(\mathcal{A})$, כלומר $L(\mathcal{M}) \in REG$

מ.ש.ל.ב.☺

**סעיף 3 חלק $a$ צ"ל:** מכונת טיורינג שמכריעה את השפה $L = \{a^n b^n c^n \mid n \in \mathbb{N}\}$
**הוכחה:**
נגדיר $Q = \{q_0, q_1, q_2, q_3, q_4, q_{acc}, q_{rej}\}$, $\Sigma = \{a, b, c\}$, $\Gamma = \Sigma \cup \{\text{'\_'}, x, X_A\}$
נגדיר $\delta$ באופן הבא:

| | $a$ | $b$ | $c$ | $x$ | $X_A$ | $'\_'$ |
|---|---|---|---|---|---|---|
| $q_0$ | $\langle q_1, X_A, R\rangle$ | $\langle q_{rej}, '\_', R\rangle$ | $\langle q_{rej}, '\_', R\rangle$ | $\langle q_{rej}, '\_', R\rangle$ | $\langle q_4, X_A, R\rangle$ | $\langle q_{acc}, '\_', R\rangle$ |
| $q_1$ | $\langle q_1, a, R\rangle$ | $\langle q_2, x, R\rangle$ | $\langle q_{rej}, '\_', R\rangle$ | $\langle q_1, x, R\rangle$ | $\langle q_{rej}, '\_', R\rangle$ | $\langle q_{rej}, '\_', R\rangle$ |
| $q_2$ | $\langle q_{rej}, '\_', R\rangle$ | $\langle q_2, b, R\rangle$ | $\langle q_3, x, R\rangle$ | $\langle q_2, x, R\rangle$ | $\langle q_{rej}, '\_', R\rangle$ | $\langle q_{rej}, '\_', R\rangle$ |
| $q_3$ | $\langle q_3, a, L\rangle$ | $\langle q_3, b, L\rangle$ | $\langle q_3, c, L\rangle$ | $\langle q_3, x, L\rangle$ | $\langle q_0, X_A, R\rangle$ | $\langle q_{rej}, '\_', R\rangle$ |
| $q_4$ | $\langle q_{rej}, '\_', R\rangle$ | $\langle q_{rej}, '\_', R\rangle$ | $\langle q_{rej}, '\_', R\rangle$ | $\langle q_4, x, R\rangle$ | $\langle q_{rej}, '\_', R\rangle$ | $\langle q_{acc}, '\_', R\rangle$ |

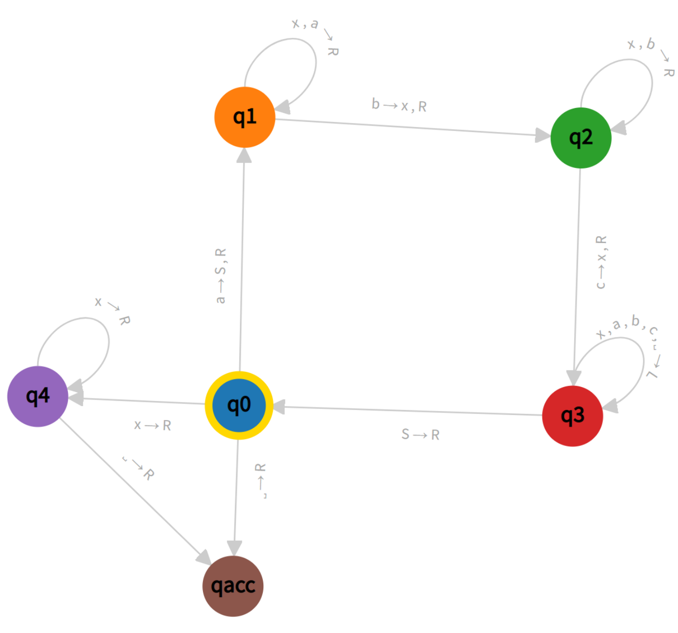
נגדיר $\mathcal{M} = \langle Q, \Sigma, \Gamma, \delta, q_0, q_{acc}, q_{rej}\rangle$
מצורף ציור מתחת לנימוק
הרעיון בתכנות כללי:

1. אם התו הראשון הוא רווח אז המילה היא המילה הריקה ונקבל
2. אם האות הנוכחית היא לא $a$, נקפוץ לשלב 8
3. נמחק את ה־ $a$ הראשונה ונחליפה ב־ $X_A$ (מסמן מקום להתחיל ממנו) ונלך ימינה
4. נדלג ימינה מעבר לכל האותיות שהן $a, x$, וכשנגיע לאות הראשונה שהיא לא $a, x$ אז היא חייבת להיות $b$, אם היא לא, נדחה. אם היא $b$, נחליפה ב־ $x$, נלך ימינה ונעבור לשלב הבא.
5. נדלג ימינה מעבר לכל האותיות שהן $b, x$, וכשנגיע לאות הראשונה שהיא לא $b, x$ אז היא חייבת להיות $c$, אם היא לא, נדחה. אם היא $c$, נחליפה ב־ $x$, נלך ימינה ונעבור לשלב הבא.
6. נלך שמאלה עד שנגיע ל־ $X_A$ (מקום להתחיל ממנו לבדוק שוב).
7. כשנגיע ל־ $X_A$ נלך ימינה ונחזור לשלב 2. (המילה מהצורה $X_A^k \cdot a^{n-k} \cdot x^k \cdot b^{n-k} \cdot x^k c^{n-k}$)
8. נעבור תו תו ונבדוק האם הוא $x$ עד שנגיע לתו רווח. אם כל התווים היו $x$, נקבל את המילה. אחרת, נדחה. המילה מהצורה (המילה מהצורה $X_A^n \cdot x^n \cdot x^n$ כלומר הכל נמחק ואין עוד תווים שלא נבדקו)

אנחנו מוחקים $a$ ואז מוחקים $b$ ואז $c$ וחוזרים להתחלה, ואם הייתה שגיאה, דוחים את המילה, לכן השפה שנקבל היא כל המילים מהצורה $L\left(\mathcal{M}\right) = \{a^n b^n c^n \mid n \in \mathbb{N}\} = L$, נשים לב שאחר $\frac{n}{3}$ ריצות על המילה, נמחק את כל ה־ $a$ ואז נבצע לכל היותר עוד ריצה על המילה ונחליט האם לקבל או לדחות (שלב 8).

לכן הריצה היא תמיד סופית ולכן $\mathcal{M}$ עוצרת על כל קלט ולכן הראנו $\mathcal{M}$ שמכריעה את $L$ כנדרש,
מצורף ציור להבנה יותר פשוטה של התיאור.

בציור כל הפעולות שלא הוגדרו מובילות ל־ $q_{rej}$ וגם מהיות והתוכנה לא אפשרה לכתוב $X_A$, השתמשתי ב־ $S$ גדולה להצגה של $X_A$ וב־ $x$ קטנה להצגה של $x$. (המצב ההתחלתי מסומן עם עיגול צהוב מסביבו)



מ.ש.ל.ג.1.☺

## סעיף 3 חלק $b$

**צ"ל:** מכונת טיורינג שמזהה את השפה $L=\{a^nb^nc^n \mid n\in\mathbb{N}\}$ ולא מכריעה

**הוכחה:**

נעשה אותה בנייה כמו בסעיף הקודם רק שהפעם במקום להעביר במקרה של דחייה ל- $q_{rej}$, ניצור מצב חדש $q_5$ שהוא פשוט "בור דוחה" - כלומר אם מגיעים אליו, אי אפשר לצאת ורצים לנצח

נגדיר $Q=\{q_0,q_1,q_2,q_3,q_4,q_5,q_{acc},q_{rej},\}$, $\Sigma=\{a,b,c\}$, $\Gamma=\Sigma\cup\{\text{'\_'},x,X_A\}$

נגדיר $\delta$ באופן הבא:

| | $a$ | $b$ | $c$ | $x$ | $X_A$ | $\text{'\_'}$ |
|---|---|---|---|---|---|---|
| $q_0$ | $\langle q_1,X_A,R\rangle$ | $\langle q_5,\text{'\_'},R\rangle$ | $\langle q_5,\text{'\_'},R\rangle$ | $\langle q_5,\text{'\_'},R\rangle$ | $\langle q_5,X_A,R\rangle$ | $\langle q_{acc},\text{'\_'},R\rangle$ |
| $q_1$ | $\langle q_1,a,R\rangle$ | $\langle q_2,x,R\rangle$ | $\langle q_5,\text{'\_'},R\rangle$ | $\langle q_1,x,R\rangle$ | $\langle q_5,\text{'\_'},R\rangle$ | $\langle q_5,\text{'\_'},R\rangle$ |
| $q_2$ | $\langle q_5,\text{'\_'},R\rangle$ | $\langle q_2,b,R\rangle$ | $\langle q_3,x,R\rangle$ | $\langle q_2,x,R\rangle$ | $\langle q_5,\text{'\_'},R\rangle$ | $\langle q_5,\text{'\_'},R\rangle$ |
| $q_3$ | $\langle q_3,a,L\rangle$ | $\langle q_3,b,L\rangle$ | $\langle q_3,c,L\rangle$ | $\langle q_3,x,L\rangle$ | $\langle q_0,X_A,R\rangle$ | $\langle q_5,\text{'\_'},R\rangle$ |
| $q_4$ | $\langle q_5,\text{'\_'},R\rangle$ | $\langle q_5,\text{'\_'},R\rangle$ | $\langle q_5,\text{'\_'},R\rangle$ | $\langle q_4,x,R\rangle$ | $\langle q_5,\text{'\_'},R\rangle$ | $\langle q_{acc},\text{'\_'},R\rangle$ |
| $q_5$ | $\langle q_5,\text{'\_'},R\rangle$ | $\langle q_5,\text{'\_'},R\rangle$ | $\langle q_5,\text{'\_'},R\rangle$ | $\langle q_5,\text{'\_'},R\rangle$ | $\langle q_5,\text{'\_'},R\rangle$ | $\langle q_5,\text{'\_'},R\rangle$ |

נגדיר $\mathcal{M}=\langle Q,\Sigma,\Gamma,\delta,q_0,q_{acc},q_{rej}\rangle$

נשים לב שהשפה נשארה זהה ולכן $L(\mathcal{M})=\{a^nb^nc^n \mid n\in\mathbb{N}\}$ אבל הפעם עבור המילה $a$ נגיע למצב $q_5$ ונשאר בו באופן אינסופי, ולכן $\mathcal{M}$ לא בהכרח תעצור על כל קלט ולכן היא רק מזהה את $L$ ולא מכריעה את $L$.

מ.ש.ל.ג.2.☺