חישוביות וסיבוכיות

מועד ב'

ד"ר יוחאי טוויטו, ד"ר ירמיהו מילר .

סמסטר א, תשפ"ה'

מספר העמוד הנוכחי ומספר העמודים הכולל בשאלון מופיעים בתחתית כל עמוד. בהצלחה!

הנחיות למדור בחינות

שאלוני בחינה

☑ לשאלון הבחינה יש לצרף מחברת.

☐ לשאלון הבחינה יש לצרף כריכה בלבד.

☐ יש להחזיר את השאלון ביחד עם המחברת/כריכה.

שימוש במחשבונים

☐ ניתן להשתמש במחשבון.

☑ לא ניתן להשתמש במחשבון.

חומר עזר

☑ לא ניתן להשתמש בחומר עזר כלל.

☐ ניתן להשתמש בחומר עזר/דף נוסחאות, כמפורט:

☐ הבחינה עם חומר פתוח – מותר להשתמש בכל חומר עזר מודפס או כתוב.

הנחיות

נא קראו בעיון את ההנחיות הבאות בטרם תתחילו לפתור את הבחינה. מומלץ לקרוא בקצרה את כלל השאלות לפני שמתחילים לפתור את הבחינה. ניתן לענות על השאלות בכל סדר שתרצו.

1. המבחן כולל 5 שאלות. יש לענות על כולן.
2. שאלות הבחינה שוות משקל - כל שאלה 20 נקודות.
3. כתבו הוכחות מלאות ומפורטות. אל תדלגו על שלבים.
4. המבחן כולל נספחים, לשימושכם. הסתייעו בהם במידת הצורך.
5. הקפידו על כתב יד ברור וקריא.
6. הקפידו לרשום בגדול ובבירור את מספר השאלה / סעיף בראש העמוד.
7. כתבו את פתרונותיכם במחברות שקיבלתם. רק הן נבדקות !
8. ניתן לקחת את השאלון כאשר הבחינה מסתיימת.

בהצלחה!

הבחינה

שאלה 1: מכונות טיורינג (20 נקודות)

סעיף א' (10 נקודות)

נתון אלפבית הקלט $\Sigma = \{a, b, c\}$ ונתונה השפה הבאה:

$$L = \{a^i b^j c^{2i \cdot 3j} \mid i, j \in \mathbb{N}^+\}$$

תארו מכונת טיורינג סטנדרטית (כלומר, במודל הבסיסי) שמכריעה את השפה.

בסעיף זה **עליכם לתאר את המכונה בצורה גרפית בעזרת תרשים** $\backslash$ **דיאגרמת מצבים בלבד**, ולא בדרכים אחרות. כלומר, לא בעזרת טבלת מעברים, לא בעזרת פסאודו -קוד,וכיוצא באלו.

תזכורת, $\mathbb{N}^+$ היא קבוצת הטבעיים החיוביים (כלומר, ללא המספר אפס).

סעיף ב' (10 נקודות)

בנומכונת טיורינג סטנדרטית (כלומר, במודל הבסיסי) **שמכריעה** את השפה הבאה:

$$L = \left\{x_1 \ldots x_k \# y_1 \ldots y_k \# z_1 \ldots z_k \;\middle|\; x_i, y_i, z_i \in \{0, \ldots, 9\} \wedge \forall_i \left(z_i \neq x_i \wedge z_i \neq 2y_i \wedge z_i \geqslant x_i + y_i\right)\right\}$$

אתהמכונה יש לתאר בעזרת **טבלת המעברים בלבד**. אין לתאר את המכונה בעזרת תרשים ו/או פסאודו-קוד(תיאור מילולי).

שאלה 2: וריאציות על מכונות טיורינג (20 נקודות)

נסמן ב-T את מודל מכונת הטיורינג הבסיסי. במודל זה בכל צעד ניתן לזוז ימינה או שמאלה. אך לא ניתן להישאר במקום, באותה המשבצת בסרט. במודל זה ,הסרט הוא אינסופי לשני הכיוונים. בתחילת החישוב הראש נמצא בתחילת הקלט.

נסמן ב-O את מודל מכונת הטיורינג עם סרט ימינה בלבד. במודל זה בכל צעד ניתן לזוז ימינה או שמאלה. אך לא ניתן להישאר במקום, באותה המשבצת בסרט. במודל זה ,הסרט הוא אינסופי לכיוון אחד בלבד - ימינה. בתחילת החישוב, הקלט ממוקם בקצה השמאלי של הסרט והראש נמצאת בתחילת הקלט. החישוב מתנהל כמו במכונה במודל, T למעט כאשר הראש נמצא במשבצת השמאלית ביותר בסרט וצריך לזוז שמאלה - במקרה כזה הראש נשאר במקום ולא זז.

הוכיחו כי המודל T והמודל O שקולים חישובית. כיתבו הוכחה מלאה ומפורטת. אל תדלגו על שלבים .תארו באופן מפורט את פונקציית המעברים בשני כיווני ההוכחה. העזרו בטבלת מעברים בכדי לתאר באופן מלא את פונקציית המעברים.

שאלה 3: התזה של צ'רץ'-טיורינג (20 נקודות)

סעיף א' (10 נקודות)

נתון הדקדוק הבא. מהי השפה שהדקדוק יוצר? כלומר, מהי $L(G)$? כיתבו את השפה בצורה פורמלית, ברורה ומוגדרת היטב. ניתן גם להוסיף תיאור מילולי של השפה.

$$
\begin{aligned}
G &= (V, \Sigma, R, S)\ , \\
V &= \{S, C, D, E, \$, \#\}, \\
\Sigma &= \{a\}\ , \\
R &= \{
\end{aligned}
$$

$$
\begin{array}{ccc}
S & \rightarrow & \$Ca\#\ , \\
S & \rightarrow & a\ , \\
S & \rightarrow & \varepsilon\ , \\
Ca & \rightarrow & aaC\ , \\
\$D & \rightarrow & \$C\ , \\
C\# & \rightarrow & D\#\ , \\
C\# & \rightarrow & E\ , \\
aD & \rightarrow & Da\ , \\
aE & \rightarrow & Ea\ , \\
\$E & \rightarrow & \varepsilon\ .
\end{array}
$$

$$\}$$

סעיף ב' (10 נקודות)

נתון הדקדוק הבא. מהי השפה שהדקדוק יוצר? כלומר, מהי $L(G)$? כיתבו את השפה בצורה פורמלית,

ברורה ומוגדרת היטב. ניתן גם להוסיף תיאור מילולי של השפה.

$$G = (V, \Sigma, R, S) \ ,$$
$$V = \{S, B, C, H\},$$
$$\Sigma = \{a, b, c\} \ ,$$
$$R = \{$$

$$\begin{array}{ccl} S & \rightarrow & aSBC \ , \\ S & \rightarrow & aBC \ , \\ CB & \rightarrow & HB \ , \\ HB & \rightarrow & HC \ , \\ HC & \rightarrow & BC \ , \\ aB & \rightarrow & ab \ , \\ bB & \rightarrow & bb \ , \\ bC & \rightarrow & bc \ , \\ cC & \rightarrow & cc \ . \end{array}$$

$$\}$$

שאלה 4: אי כריעות (20 נקודות)

נתונה השפה הבאה:

$$L_{\geqslant 3} = \left\{ \langle M \rangle \ \middle| \ |L(M)| \geqslant 3 \right\}$$

$L_{\geqslant 3}$ מכילה קידודים של מכונות טיורינג שמקבלות לפחות k מילים שונות.

סעיף א' (10 נקודות)

הוכיחו כי $L_{\geqslant 3}$ שפה קבילה.

סעיף ב' (10 נקודות)

הוכיחו כי $L_{\geqslant 3}$ לא כריעה.

שאלה 5: סיבוכיות זמן (20 נקודות)

בעיית סכום התת קבוצה (subsetSum): בהינתן קבוצת מספרים שלמים $S=\{x_1,x_2,\ldots,x_n\}$ ומספר שלם t, האם קיימת תת קבוצה $Y\subseteq S$ שסכום איבריה הוא בדיוק t.
בעיית סכום התת קבוצה כשפה פורמלית:

$$\text{SubsetSum}=\left\{\langle S,t\rangle \;\middle|\; \text{קבוצת שלמים } S \text{, } t \text{ שלם וקיימת תת-קבוצה } Y\subseteq S \text{ כך ש- } t=\sum_{y\in Y} Y\right\}$$

בעיית החלוקה (Partition): בהינתן קבוצת מספרים שלמים $S=\{x_1,x_2,\ldots,x_n\}$ האם קיימת תת-קבוצה $Y\subseteq S$ כך ש- $\sum\limits_{y\in Y} y=\sum\limits_{y\in S\setminus Y} y$.
בעיית החלוקה כשפה פורמלית:

$$\text{partition}=\left\{S \;\middle|\; \text{קבוצת שלמים, וקיימת תת-קבוצה } Y\subseteq S \text{ כך ש- } \sum_{y\in Y} y=\sum_{y\in S\setminus Y} y\right\}$$

הוכיחו כי קיימת רדוקציית התאמה פולינומיאלית מהשפה SubsetSum לשפה partition. כלומר:

$$\text{SubsetSum}\leqslant_P \text{Partition}\ .$$

בשאלה זו עליכם:

סעיף א' (8 נקודות)

להגדיר במפורש את הרדוקציה.

סעיף ב' (6 נקודות)

להראות שהרדוקציה היא רדוקציית התאמה.

סעיף ג' (6 נקודות)

להראות שהרדוקציה פולינומיאלית.

תוכן העניינים

1 מכונות טיורינג

הגדרה 1: מכונת טיורינג

מכונת טיורינג (מ"ט) היא שביעיה $M = (Q, \Sigma, \Gamma, \delta, q_0, \text{acc}, \text{rej})$.

Q	קבוצת מצבים סופיות	
Σ	א"ב קלט סופי	$\textvisiblespace \notin \Sigma$
Γ	א"ב סרט סופי	$\Sigma \subseteq \Gamma$, $\textvisiblespace \in \Gamma$
δ	פונקציית המעברים	$\delta : (Q\backslash\{\text{rej}, \text{acc}\} \times \Gamma \to Q \times \Gamma \times \{L, R\}$
q_0	מצב התחלתי	
acc	מצב מקבל	
rej	מצב דוחה	

הגדרה 2: קונפיגורציה

תהי $M = (Q, \Sigma, \Gamma, \delta, q_0, \text{acc}, \text{rej})$ מכונת טיורינג.
קונפיגורציה של M הינה מחרוזת

$$uq\sigma \mathsf{v} , \quad u, \mathsf{v} \in \Gamma^*, \ \sigma \in \Gamma, \ q \in Q .$$

משמעות:

- q מצב המכונה,
- σ הסימון במיקום הראש
- u תוכן הסרט משמאל לראש,
- v תוכן הסרט מימין לראש.

הגדרה 3: גרירה

תהי $M = (Q, \Sigma, \Gamma, \delta, q_0, \text{acc}, \text{rej})$ מכונת טיורינג, ותהיינה c_1 ו- c_2 קונפיגורציות של M.
נסמן

$$c_1 \vdash_M c_2$$

(במילים, c_1 גורר את c_2) אם כשנמצאים ב- c_1 עוברים ל- c_2 בצעד בודד.

נסמן

$$c_1 \vdash_M^* c_2$$

אם ניתן לעבור מ- c_1 ל- c_2 ב- 0 או יותר צעדים.

הגדרה 4: קבלה ודחייה של מחרוזת

תהי $M = (Q, \Sigma, \Gamma, \delta, q_0, \text{acc}, \text{rej})$ מכונת טיורינג, ו- $w \in \Sigma^*$ מחרוזת.
נאמר כי:

- M **מקבלת** את w אם $q_0w \vdash_M^* u\ \mathsf{acc}\, \sigma\, \mathsf{v}$
- M **דוחה** את w אם $q_0w \vdash_M^* u\ \mathsf{rej}\ \sigma\ \mathsf{v}$

כאשר $\mathsf{v}, u \in \Gamma^*, \sigma \in \Gamma$ כלשהם.

הגדרה 5: הכרעה של שפה
תהי $M = (Q, \Sigma, \Gamma, \delta, q_0, \mathsf{acc}, \mathsf{rej})$ מכונת טיורינג, ו- $L \subseteq \Sigma^*$ שפה.
נאמר כי M **מכריעה** את L אם לכל $w \in \Sigma^*$ מתקיים

- $L \ni w \Leftarrow M$ מקבלת את w.
- $L \not\ni w \Leftarrow M$ דוחה את w.

הגדרה 6: קבלה של שפה
תהי $M = (Q, \Sigma, \Gamma, \delta, q_0, \mathsf{acc}, \mathsf{rej})$ מכונת טיורינג, ו- $L \subseteq \Sigma^*$ שפה.
נאמר כי M **מקבלת** את L אם לכל $w \in \Sigma^*$ מתקיים

- אם $w \in L$ אז M מקבלת את w.
- אם $w \notin L$ אז M לא מקבלת את w.

במקרה כזה נכתוב ש- $L(M) = L$.

הגדרה 7: חישוב פונקציות
תהי $M = (Q, \Sigma, \Gamma, \delta, q_0, \mathsf{acc}, \mathsf{rej})$ מכונת טיורינג ותהי $f : \Sigma_1^* \to \Sigma_2^*$.
נאמר כי M **מחשבת** את f אם:

- $\Sigma = \Sigma_1$, $\Sigma_2 \subset \Gamma$,
- לכל $w \in \Sigma_1^*$ מתקיים $q_0w \vdash_M^* \mathsf{acc} f(w)$.

2 וריאציות של מכונות טיורינג

הגדרה 8: מודל חישוב
מודל חישובי = אוסף של מכונות שעבורם מוגדרים המושגים של הכרעה וקבלה של שפות.

הגדרה 9: מודלים שקולים חישובית
יהיו A, B מודלים חישוביים. נאמר כי A ו- B שקולים אם לכל שפה L:

- קיימת מכונה במודל A שמכריעה את L אם"ם קיימת מכונה כזו במודל B.
- קיימת מכונה במודל A שמקבלת את L אם"ם קיימת מכונה כזו במודל B.

הגדרה 10: מכונות שקולות חישובית
שתי מכונות הן שקולות חישובית אם הן מקבלות ודוחות בדיוק את אותן המילים.

משפט 1: מכונת טיורינג עם סרט ימינה בלבד
מודל מ"ט עם סרט אינסופי לכיוון אחד בלבד (מודל O) שקול למודל אינסופי בשני הכיוונים (מודל T).
כלומר, לכל שפה L:

- יש מ"ט ממודל O שמקבלת את L אם"ם יש מ"ט במודל T שמקבלת את L.
- יש מ"ט ממודל O שמכריעה את L אם"ם יש מ"ט במודל T שמכריעה את L.

משפט 2: מכונת טיורינג מרובת סרטים
במכונת טיורינג מרובת סרטים:

- יתכנו מספר סטרים.

  מספר הסרטים סופי וקבוע מראש בזמן בניית המ"ט, ואינו תלוי בקלט או במהלך החישוב.
- לכל סרט יש ראש נפרד.
- הפעילות (תנועה וכתיבה) בכל סרט נעשית בנפרד.

  בפרט, הראשים יכולים לזוז בכיוונים שונים בסרטים שונים.
- ישנו בקר מרכזי יחיד, שקובע את הפעילות בכל אחד מהסרטים, על סמך המידע שמתקבל מכל הסרטים.

  לכן, תוכן סרט אחד יכול להשפיע על הפעילות בשאר הסרטים.
- בתחילת החישוב, הקלט נמצא בסרט הראשון ושאר הסרטים ריקים.

משפט 3:
לכל k, המודל של מ"ט עם k סטרים שקול חישובי למודל של מ"ט עם סרט אחד.

משפט 4:
קבלה ודחייה של מחרוזות:
עבור מ"ט לא דטרמיניסטית N ומחרוזת w:

- N **מקבלת** את w אם קיים חישוב של N על w שמגיע למצב מקבל.
- N **דוחה** את w אם כל החישובים של N על w עוצרים במצב דוחה.

הכרעה וקבלה של שפות:
עבור מ"ט לא דטרמיניסטית N ושפה L:

- N **מכריעה** את L אם N מקבלת אך כל המילים ב- L ודוחה את כל המילים שאינן ב- L.
- N **מקבלת** את L אם N מקבלת אך כל המילים ב- L ולא מקבלת את כל המילים שאינן ב- L.

משפט 5:
לכל מ"ט לא דטרמיניסטית קיימת מ"ט דטרמיניסטית שקולה.

3 התזה של צ'רץ'-טיורינג

שמות נרדפים לשפות כריעות ושפות קבילות

שפות כריעות	**Decideable languages**	**שפות קבילות**	**Acceptable languages**
שפות רקורסיביות	Recursive languages	שפות ניתנות לזיהוי	recognizable languages
		שפות כריעות למחצה	Semi-deidable languages
			Partially-deidable languages
		שפות הניתנות למנייה רקורסיביות	Recursively enumerable languages

משפט 6: סגירות שפות כריעות
השפות הכריעות סגורות תחת:
- איחוד
- חיתוך
- משלים
- שרשור
- סגור קלין

משפט 7: סגירות שפות קבילות
- איחוד
- חיתוך
- שרשור
- סגור קלין

משפט 8: היחס בין הכרעה לקבלה
אם שפה הינה כריעה אז היא קבילה.
אם שפה והמשלים שלה קבילות אז היא כריעה.

הגדרה 11: שפת סימפל
<u>משתנים</u>

- טבעיים: `i,j,k,...`

  מקבלים כערך מספר טבעי.
- מערכים: `A[],B[],C[],...` בכל תא ערך מתוך א"ב Γ אין סופיים.
- אתחול: הקלט נמצא בתאים הראשונים של `A[]`.

  כל שאר המשתנים מאותחלים ל- `0`.

<u>פעולות</u>

- השמה בקבוע:

  `i=3, B[i]="#"`
- השמה בין משתנים:

  `i=k, A[k]=B[i]`
- פעולות חשבון:

  `x = y + z , x = y − z , x = y.z`

<u>תנאים</u>

- B[i]==A[j]

(מערכים).

- x >= y

(משתנים טבעיים).

כל משתנה מופיע רק פעם אחת בכל פעולה או תנאי.

<u>זרימה</u>

- סדרה פקודות ממוספרות.
- goto: מותנה ולא מותנה.
- stop עצירה עם ערך חזרה.

```
1  one = 1
2  zero = 0
3  B[zero] = "0"
4  i=0
5  j=i
6  if A[i] == B[zero] goto 9
7  i=j + one
8  goto 3
9  C[one] = A[j]
10 if C[one] ==  A[zero] goto 12
11 stop(0)
12 stop(1)
```

הגדרה 12: קבלה ודחייה של מחרוזת בשפה SIMPLE

עבור קלט

w ותוכנית

P בשפת SIMPLE. נאמר כי

- P **מקבלת** את w אם הריצה של P על w עוצרת עם ערך חזרה 1.
- P **דוחה** את w אם הריצה של P על w עוצרת עם ערך חזרה 0.

הגדרה 13: הכרעה וקבלה של שפות

עבור שפה L ותוכנית P בשפת SIMPLE. נאמר כי

- P **מכריעה** את L אם היא מקבלת את המילים שב- L ודוחה את אלה שלא ב- L.
- P **מקבלת** את L אם היא מקבלת את כל ורק המילים ב- L.

משפט 9:

המודלים של מכונת טיורינג ותוכניות SIMPLE שקולים.

משפט 10: מ"ט ותוכניות מחשב
מ"ט חזקה לפחות כמו תוכנית משחב.
כל תוכנית מחשב ניתנת למימוש במ"ט.
לכן, כל שפה שהינה כריעה ע"י מחשב היא כם כריעה ע"י מ"ט.
וכמו כן, שפה שהינה קבילה ע"י מחשב היא גם קבילה ע"י מ"ט.

הגדרה 14: דקדוקים כלליים
בדקדוק כללי, בצד שמאל של כלל יצירה יכולה להופיע מחרוזת (לא ריקה) כלשהי.
פורמלית, כלל יצירה בדקדוק כללי הוא מהצורה

$$\gamma \to u$$

כאשר $\gamma \in (V \cup \Sigma)^+$, $u \in (V \cup \Sigma)^*$.

משפט 11:
תהי L שפה. L קבילה אם"ם קיים דקדוק כללי G כך ש- $L(G) = L$.

משפחת שפות	דקדוק	מודל חישובי
קבילות	כללי	מכונת טיורינג
חסרות הקשר	חסר הקשר	אוטומט מחסנית
רגולריות	רגולרי	אוטומט סופי

משפט 12:
כל שפה חסרת הקשר הינה כריעה.

משפט 13: התזה של צ'רץ' טיורינג
התזה של צ'רץ' טיורינג מודל מ"ט מגלם את המושג האבסטרקרטי של "אלגוריתם".
כלומר, כל אלגוריתם שניתן לתיאור כתהליך מכניסטי שבו:
- התהליך מתבצע כסדרה של צעדים.
- כל צעד מצריך כמות סופית של "עבודה".

ניתן גם לתיאור כמ"ט.
בפרט, אין מודל מכניסטי / אוטומטי יותר ממ"ט.

4 אי-כריעות

הגדרה 15: השפה ATM

$$ATM = \left\{ (P,w) \mid P(w) = 1 \right\} \ .$$

השפה ATM כוללת את כל הזוגות של מחרוזות P,w כך ש:

- P היא קוד (תקין) של תוכנית.
- w מחרוזת.
- מתקיים שאם מריצים את התוכנית P על הקלט w אז התוכנית עוצרת עם ערך חזרה 1.

הגדרה חלופית:

$$A_{TM} = \left\{ \langle M,w\rangle \mid M \text{ מכונת טיורינג שמקבלת את } w \right\}$$

השפה A_{TM} כוללת את כל הזוגות של מחרוזות $\langle M,w\rangle$ של כל מכונת טיורינג M וכל קלט w כך ש- M מקבלת את w.

סיכום 1: התוכנה U

התוכנה U היא תוכנה שמקבלת כקלט זוג מחרוזות P,w ופועלת כך:

- U מחזירה את ערך החזרה שהתקבל מהריצה של P על w.
- מריצה את התוכנה P על קלט w (במקרה שבו P אינה תוכנית מחשב תקינה אז U מחזירה ערך 0).

נשים לב שאם P לא עוצרת על w אז גם U לא עוצרת על הזוג P,w.
התוכנה U פועלת באופן דומה לאופן שבה מערכת ההפעלה מפעילה תוכנות אחרות.

התוכנה U נקראת גם "תוכנה אוניברסלית" (או, בעולם מכונות טיורינג: "מכונת טיורינג אוניברסלית") כיוון שהיא תוכנה אחת שמדמה כל תוכנה אחרת.

U היא תוכנית שמקבלת את ATM. כלומר:

$$L(U) = ATM \ .$$

מסקנה: ATM קבילה.

שיטת ההוכחה:
אם שפה הינה קבילה אבל לא כריעה, אז המשלים שלה בהכרח אינה קבילה.
לכן, בשביל להוכיח ששפה אינה קבילה, די להוכיח שהשפה לא כריעה, והמשלים שלה כן קבילה.

הגדרה 16: השפה HALT

$$HALT = \left\{ (P,w) \mid P(w) \downarrow \right\} \ .$$

השפה HALT כוללת את כל הזוגות של מחרוזות P,w כך ש:

- P היא קוד (תקין) של תוכנית.
- w מחרוזת.
- מתקיים שאם מריצים את התוכנית P על הקלט w אז התוכנית עוצרת (הסימון $\downarrow$ מסמן עצירה).)

בעיית העצירה קבילה אבל לא כריעה.
כיוון שכך, המשלים שלה לא כריעה ולא קבילה.

הגדרה חלופית:

$$HALT_{TM} = \left\{ \langle M, w \rangle \;\middle|\; \text{מכונת טיורינג שעוצרת על } w \text{ } M \right\}$$

השפה $HALT_{TM}$ כוללת את כל הזוגות של מחרוזות $\langle M, w \rangle$ של כל מכונת טיורינג M וכל קלט w כך ש- M עוצרת על w.

הגדרה 17: השפה E

$$E = \left\{ P \;\middle|\; L(P) = \varnothing \right\}$$

השפה E כוללת את כל המחרוזות P כך ש-

- P היא קוד (תקין) של תוכנית.
- השפה של P ריקה.

כלומר, לכל קלט w, הריצה של P על w לא מחזירה 1.

הגדרה חלופית:

$$E_{TM} = \left\{ \langle M \rangle \;\middle|\; \text{מכונת טיורינג שעומדת בתנאי } L(M) = \varnothing \text{ } M \right\}$$

השפה E_{TM} כוללת את כל מחרוזות $\langle M \rangle$ של כל מכונת טיורינג M כך ש- M לא מקבלת אף מילה.
במילים אחרות, השפה של M ריקה: $L(M) = \varnothing$.

הגדרה 18: השפה EQ

$$EQ = \left\{ (P_1, P_2) \;\middle|\; L(P_1) = L(P_2) \right\} \; .$$

השפה EQ כוללת את כל זוגות המחרוזות P_1, P_2 כך ש:

- P_1, P_2 הינן קודים (תרינים) של תוכניות.
- השפות של P_1, P_2 זהות.

כלומר, P_1, P_2 מקבלות בדיוק את אותן המילים.

הגדרה חלופית:

$$EQ_{TM} = \left\{ \langle M_1, M_2 \rangle \;\middle|\; \text{מכונות טיורינג } L(M_1) = L(M_2) \text{ } M_1, M_2 \right\}$$

השפה EQ_{TM} כוללת את כל זוגות של מכונות טיורינג $\langle M_1, M_2 \rangle$ שמקבלות בדיוק אותן המילים.
במילים אחרות, השפות של M_1 ו- M_2 זהות: $L(M_1) = L(M_2)$.

	כריעה	קבילה
ATM	$\times$	$\checkmark$
$\overline{ATM}$	$\times$	$\times$
$HALT$	$\times$	$\checkmark$
$\overline{HALT}$	$\times$	$\times$
E	$\times$	$\times$
$\overline{E}$	$\times$	$\checkmark$
EQ	$\times$	$\times$
$\overline{EQ}$	$\times$	$\times$

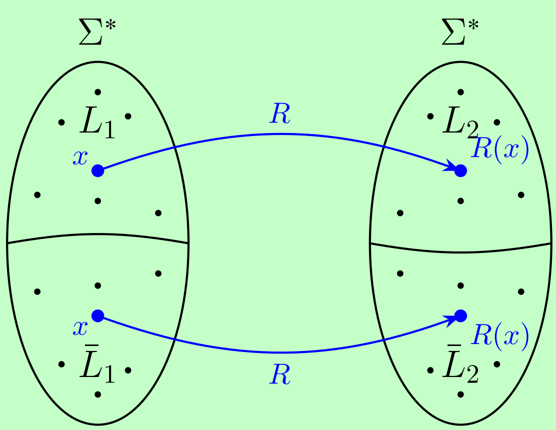
הגדרה 19: הרדוקציה

רדוקציית התאמה (many to one reduction) מקבוצה $L_1 \subseteq \Omega_1$ לקבוצה $L_2 \subseteq \Omega_2$ הינה **פונקציה**

$$R : \Omega_1 \to \Omega_2$$

כך שלכל $x \in \Omega_1$ מתקיים:

$$x \in L_1 \quad \Leftrightarrow \quad R(x) \in L_2 \ .$$



סימון: $L_1 \leqslant_m L_2$ רייסמת רדוקציה התאמה ניתנת לחישוב מ- L_1 ל- L_2.

משפט 14: משפט הרדוקציה

טענה:
אם:
- L_2 כריעה
- $L_1 \leqslant L_2$

אז L_1 כריעה.

מסקנה:
אם:
- L_1 לא כריעה
- $L_1 \leqslant L_2$

אז L_2 לא כריעה.

מתכון להוכחה ששפה L_2 לא כריעה:
1. בחר שפה L_1 לא כריעה.
2. מצא רדוקציית התאמה ניתנת לחישוב מ- L_1 ל- L_2.

טענה:
אם:
- L_2 קבילה
- $L_1 \leqslant L_2$

אז L_1 קבילה.

מסקנה:
אם:
- L_1 לא קבילה
- $L_1 \leqslant L_2$

אז L_2 לא קבילה.

מתכון להוכחה ששפה L_2 לא קבילה:
1. בחר שפה L_1 לא קבילה.
2. מצא רדוקציית התאמה ניתנת לחישוב מ- L_1 ל- L_2.

משפט 15: תכונות של רדוקציות

B	$\leqslant_m$	A
כריעה	$\Leftarrow$	כריעה
לא כריעה	$\Rightarrow$	לא כריעה

B	$\leqslant_m$	A
קבילה	$\Leftarrow$	קבילה
לא קבילה	$\Rightarrow$	לא קבילה

משפט 16: לכל שפה קיימת רדוקציה ל- A_{TM}

מכל שפה כריעה A קיימת רדוקציה חישובית ל- A_{TM}.

כלומר

$$A \leqslant_m A_{TM} \ .$$

משפט 17: רדוקציה משפות כריעות
מכל שפה כריעה קיימת רדוקציה חשיבה לכל שפה אחרת שאינה $\varnothing$ או Σ^*.

הגדרה 20:

$$NOTREG = \{P \mid \text{לא רגולרית } L(P)\} \ .$$

השפה NOT-REG כוללת את כל המחרוזות P כך ש:
- P הינה קוד (תקין) של תוכנית.
- השפה של P לא רגולרית.

הגדרה חלופית:

$$NOTREG_{TM} = \{\langle M\rangle \mid \text{לא רגולרית } L(M)\} \ .$$

השפה $NOTREG_{TM}$ כוללת את כל המחרוזות $\langle M\rangle$ של מ"ט M כך שהפשה של M לא רגולרית.

משפט 18: השפה $NOT-REG$ אינה קבילה.
השפה $NOT-REG$ אינה קבילה.

5 סיבוכיות זמן

הגדרה 21: זמן הריצה
זמן הריצה של מכונת טיורינג M על קלט w הוא מספר צעדי החישוב ש- M מבצעת על w.

הגדרה 22: סיבוכיות זמן ריצה
תהי M מ"ט דטרמיניסטית אשר עוצרת על כל קלט. **הזמן הריצה** או **הסיבוכיות זמן** של M היא פונקציה $f:\mathbb{N}\to\mathbb{N}$, כאשר $f(n)$ המספר צעדי חישוב המקסימלי ש- M מבצעת על קלט w של אורך n.

אם $f(n)$ זמן הריצה של M, אומרים כי M רץ בזמן $f(n)$ וש- M היא $f(n)$ זמן מכונת טיורינג

הגדרה 23: מחלקה של סיבוכיות זמן
המחלקת הסיבוכיות זמן מסומנת $\text{TIME}\left(t(n)\right)$ ומוגדרת להיות אוסף של כל השפות אשר ניתנות להכרעה על ידי מכונת טיורינג בזמן $O\left(t(n)\right)$.

משפט 19:
הגדרת זמן הריצה שנתנו היא תלויה במודל של מכונת הטיורינג שאיתו אנחנו עובדים.

משפט 20:
תהי $t:\mathbb{N}\to\mathbb{R}^+$ פונקציה $t(n)$.
אם מתקיים
$$t(n)\geqslant n$$
אז לכל מכונת טיורינג $O(t(n))$ רב-סרטי קיימת מ"ט $O(t^2(n))$ עם סרט אחד.

הגדרה 24: זמן הריצה של מ"ט לא דטרמיניסטית
תהי N מכונת טיורינג לא דטרמיניסטית.
הזמן הריצה של N מוגדרת להיות הפונקציה $f:\mathbb{N}\to\mathbb{N}$ כאשר $f(n)$ הוא המספר הצעדים המקסימלי אשר N מתוך כל הענפים של החישוב שלה על קלט של אורך n.

משפט 21:
תהי $t(n)$ פונקציה המקיימת $t(n)\geqslant n$. כל מ"ט $O(t(n))$ לא דטרמיניסטית N סרט אחד, שקולה למכונת טיורינג $2^{O(t(n))}$ דטרמיניסטית סרט אחד.

הגדרה 25: מכונת טיורינג פולינומית
מכונת טיורינג M תיקרא **פולינומית** או **יעילה** אם קיים $c\in\mathbb{N}$ כך ש- M פועלת בסיבוכיות זמן ריצה $O(n^c)$.

הגדרה 26: המחלקה P
המחלקה P היא אוסף השפות שקיימת מכונת טיורינג פולינומיאלית M המכריעה אותן. כלומר:
$$P=\bigcup_k \mathsf{TIME}\left(n^k\right) \ .$$

הגדרה 27: אלגוריתם אימות
אלגוריתם אימות של שפה A הוא אלגוריתם V כך ש-:
$$A=\left\{w \;\middle|\; \text{מקבל } V \text{ } \langle w,c\rangle \text{ על פי } c\right\}$$
במילים, **אלגוריתם אימות** הוא אלגוריתם V אשר מאמת כי הקלט w שייך לשפה A על פי התנאי c, שנקרא **אישור** (certification).

אנחנו מגדירים את זמן הריצה של V על פי האורך של w. לכן **אלגוריתם אימות זמן-פולינומיאלי** רץ בזמן פולינומיאלי $O\left(n^k\right)$ כאשר n האורך של w.

הגדרה 28: מחלקת הסיבוכיות NP
- המחלקה NP היא מחלקת השפות שניתן לאמתן באמצעות אלגוריתם זמן-פולינומיאלי.

הגדרה חלופית למחלקה NP הינה:
- המחלקה NP היא מחלקת השפות שניתן להכרעה באמצעות מ"ט אי-דטרמיניסטית זמן-פולינומיאלית.

למטה במשפט 22.

משפט 22: $A \in NP$ אם"ם A ניתנת לאימות ע"י N_{TM}
שפה A כלשהי שייכת למחלקה NP אם ורק אם A ניתנת להכרעה על ידי מכונות טיורינג אי-דטרמיניסטית זמן-פולינומיאלית.

הגדרה 29: פונקיצה הניתנת לחישוב זמן-פולינומיאלי
פונקציה $f : \Sigma^* \to \Sigma^*$ ניתנת לחישוב זמן-פולינומיאלי אם קיימת מ"ט זמן-פולינומיאלית M, עבורה על הקלט w, M עוצרת עם $f(w)$ על הסרט שלה.

הגדרה 30: פונקציה שניתנת לרדוקציה זמן-פולינומיאלית
השפה A ניתנת לרדוקציה זמן-פולינומיאלית לשפה B, שנסמן $A \leqslant_P B$, אם קיימת פונקציה שנתנת לחישוב זמן-פולינומיאלית $f : \Sigma^* \to \Sigma^*$ כך שלכל

$$w \in A \Leftrightarrow f(w) \in B \ .$$

הפונקציה f נקראת **הרדוקציה זמן-פולינומיאלית** של A ל- B.

משפט 23: אם $A \leqslant_P B$ ו- $B \in P$ אז $A \in P$
אם $A \leqslant_P B$ ו- $B \in P$ אז $A \in P$.

משפט 24: 3-SAT ניתנת לרדוקציה זמן-פולינומיאלית ל- CLIQUE
בהביית 3-SAT ניתנת לרדוקציה זמן-פולינומיאלית לבעיית CLIQUE:

$$3SAT \leqslant_p CLIQUE \ .$$

מסקנה 1: $3SAT \in P \quad \Rightarrow \quad CLIQUE \in P$
לפי משפט 23 ומשפט 24:

אם $CLIQUE \in P$ אז $3SAT \in P$.

הגדרה 31: NP-שלמות
שפה B היא **NP- שלמה** או **שלמה ב- NP** (NP-complete) אם היא מקיימת את השני התנאים הבאים:
1) $B \in NP$ וגם
2) $A \leqslant_p B$ עבור כל $A \in NP$.

במילים פשוטות: כל A ב- NP ניתנת לרדוקציה זמן-פולינומיאלית ל- B.

הגדרה 32: NP קשה
אם שפה B מקיימת את תכונה 2) אולם לא בהכרח את תכונה 1) בהגדרה 31
אז אומרים כי B **NP- קשה** או **קשה ב- NP** (NP-hard).

משפט 25:
אם B NP- שלמה ו- $B \in P$ אז $P = NP$.

משפט 26: אסוציאטיביות של NP שלמות
אם השני תנאים הבאים מתקיימים:
1) B היא שפה NP- שלמה.
2) קיימת $C \in NP$ עבורה $B \leqslant_p C$.
אז C שפה NP- שלמה.

משפט 27: משפט קוק לוין
הבעיית SAT היא NP - שלמה.

משפט 28: 3-SAT היא NP שלמה.
3-SAT היא NP שלמה.

6 נוסחאות נוספות

הגדרה 33: הבעיית הספיקות SAT

$$SAT = \{\langle\phi\rangle \mid \phi \text{ היא נוסחה בוליאנית ספיקה}\}$$

במילים, בעיית SAT שואלת את השאלה: בהינתן נוסחה שמכילה רק קשרים $\wedge$, $\vee$ ו- $\neg$ ("גם", "או" ו"לא"), האם קיימת השמה של ערכי אמת למשתנים כך שהנוסחה ϕ תקבל ערך אמת?
אם קיימת השמה כזו אז נאמר כי הנוסחה ϕ ספיקה.

הגדרה 34: הבעיית 3-SAT

$$3SAT = \{\langle\phi\rangle \mid \phi \text{ היא נוסחת בוליאנית בצורה 3CNF ספיקה.}\}$$

במילים, $3SAT$ היא הבעיית SAT שמוגדר בהגדרה 33 במקרה הנוסחה שהנוסחה היא בצורה 3CNF.
דוגמה של נוסחה בצורה 3CNF היא:

$$(x_1 \vee \bar{x}_1 \vee \bar{x}_2) \wedge (x_3 \vee x_2 \vee x_4) \wedge (\bar{x}_1 \vee \bar{x}_3 \vee \bar{x}_4)$$

הגדרה 35: הביית PATH
בהינתן גרף מכוון $G = (V, E)$.
הבעיית PATH שואלת את השאלה הבאה: בהינתן גרף מכוון $G = (V, E)$, וקדקודים s ו- t.
האם הגרף G מסלול בין קדקוד s לבין קדקוד t.

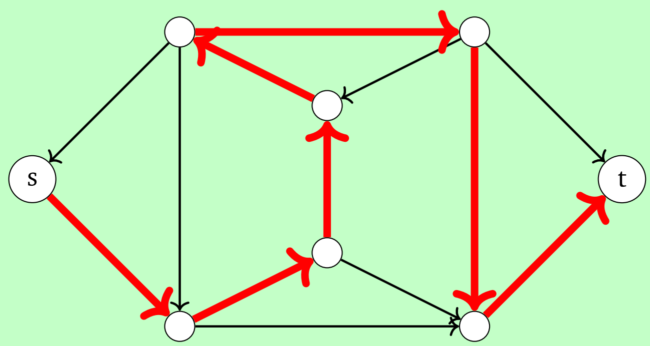
$$PATH = \{\langle G, s, t\rangle \mid G \text{ גרף מכוון שמכיל מסלול מכוון מ- } s \text{ ל- } t\} \ .$$

הגדרה 36: מסלול המילטוני
נתון גרף מכוון $G=(V,E)$.
מסלול המילטוני מקדקוד s לקדקוד t הוא מסלול אשר עובר דרך כל קדקוד בדיוק פעם אחת.

הגדרה 37: בעיית מסלול המילטוני HAMPATH
בהינתן גרף מכוון $G=(V,E)$ וקדקודים s ו- t.
בעיית המסלול ההמילטוני שואלת את השאלה: האם קיים מסלול המילטוני מקדקוד s לקדקוד t?

$$HAMPATH=\left\{\langle G,s,t\rangle \;\middle|\; \text{.}t \text{ ל- } s \text{ גרף מכוון המכיל מסלול המילטוני מ- } G\right\}$$

התרשים למטה מראה דוגמה של מסלול המילטוני בגרף מכוון.

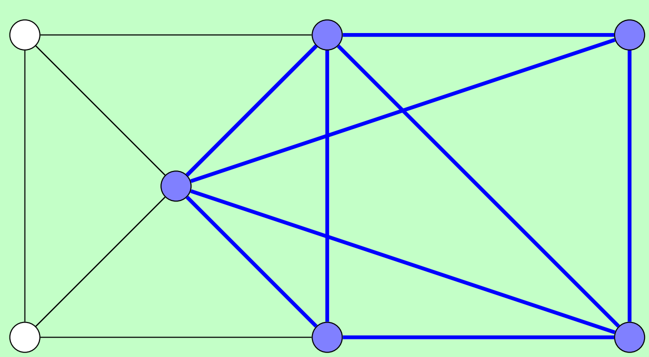


הגדרה 38:
בהינתן שלמים x,y.
הבעייה RELPRIME שואלת את השאלה: האם x,y זרים.

$$RELPRIME=\left\{\{x,y\}\in\mathbb{N} \;\middle|\; \text{gcd}(x,y)=1\right\}$$

הגדרה 39: קליקה
נתון גרף לא מכוון.
- קליקה בגרף לא מכוון הוא תת-גרף שבו כל זוג קדקודים קשורים על ידי קשת.
- k- קליקה היא קליקה שבו יש בדיוק k קדקודים.

התרשים למטה מראה דוגמה של 5- קליקה.



הגדרה 40: בעיית הקליקה

נתון גרף לא מכוון $G=(V,E)$. בעיית הליקה שואלת את השאלה:
האם הגרף G מכיל קליקה בגודל k.
בשפה פרומלית:

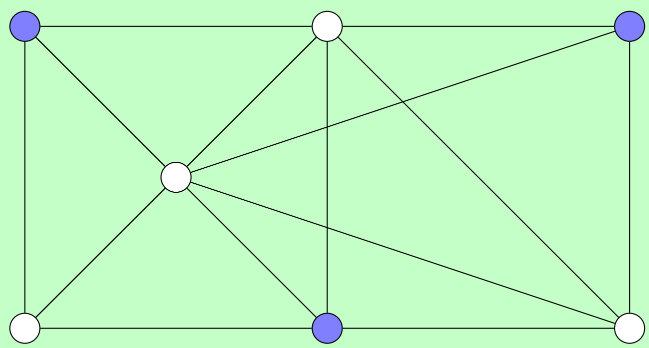
$$CLQ = \big\{\langle G,k\rangle \ \big|\ \text{גרף לא מכוון שמכיל קליקה בגודל } k \text{ לפחות.}\ G \big\}$$

הגדרה 41: קבוצה בלתי תלויה

נתון גרף לא מכוון $G=(V,E)$.
קבוצה בלתי תלויה ב- G היא תת-קבוצה של קדקודים $S\subseteq V$ כך שלכל שני קדקודים $u_1,u_2\in S$ מתקיים ש-

$$(u_1,u_2)\notin E\ .$$

התרשים למטה מראה דוגמה של גרף לא מכוון G שמכיל קבוצה בלתי תלויה בגודל 3.



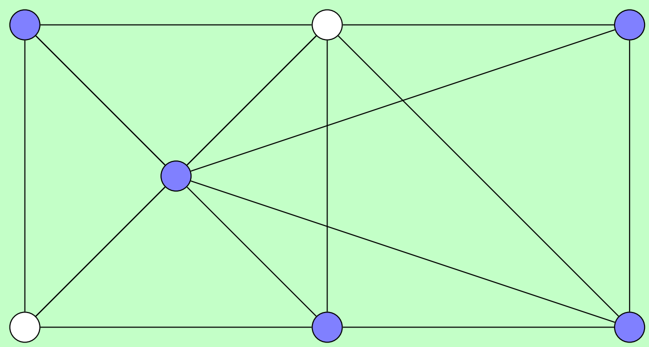
הגדרה 42: בעיית בקבוצה הבלתי תלוייה Independent Set (IS)

בהינתן גרף לא מכוון $G=(V,E)$ ומספר טבעי k.
הבעייה IS שואלת את השאלה: האם קיימת קבוצה בלתי תלוייה ב- G בגודל k לפחות.
בשפה פורמלית:

$$IS = \big\{\langle G,k\rangle \ \big|\ \text{מכיל קבוצה בלתי תלוייה בגודל } k \text{ לפחות.}\ G\big\}$$

הגדרה 43: כיסוי קדקודים

בהינתן גרף לא מכוון $G=(V,E)$.
כיסוי קדקודים ב- G הוא תת-קבוצה של קדקודים $C\subseteq V$ כך שלכל צלע $(u_1,u_2)\in E$ מתקיים:
$u_1\in C$ או $u_2\in C$.
הגרף למטה מכיל כיסוי קדקודים בגודל 5.



הגדרה 44: הבעיית כיסוי קדקודים (VC) Vertex Cover

בהינתן גרף לא מכוון $G = (V, E)$ ומספר טבעי k.

הבעיית כיסוי קדקודים שואלת את השאלה הבאה:

האם קיים כיסוי בקדקודים ב- G בגודל k?

בשפה פורמלית:

$$VC = \left\{ \langle G, k \rangle \;\middle|\; G \text{ מכיל כיסוי בקדקודים בגודל } k \right\} .$$

משפט 29: שפות NP- שלמות

SAT	NP- שלמה.	(משפט קוק לוין)
3SAT	NP- שלמה.	
HAMPATH	NP- שלמה.	
CLIQUE	NP- שלמה.	
INDEPENDENT-SET	NP- שלמה.	
VERTEX-COVER	NP- שלמה.	

חישוביות וסיבוכיות

מועד ב'

פתרון לדוגמא

ד"ר יוחאי טוויטו , ד"ר ירמיהו מילר .

סמסטר א, תשפ"ה'

מסמך זה כולל פתרון לדוגמא של המבחן. הפתרונות לשאלות הינן פתרונות לדוגמא. ניתן לפתור חלק בדרכים נוספות/אחרות, מלבד הדרך המוצעת בפתרון לדוגמא.

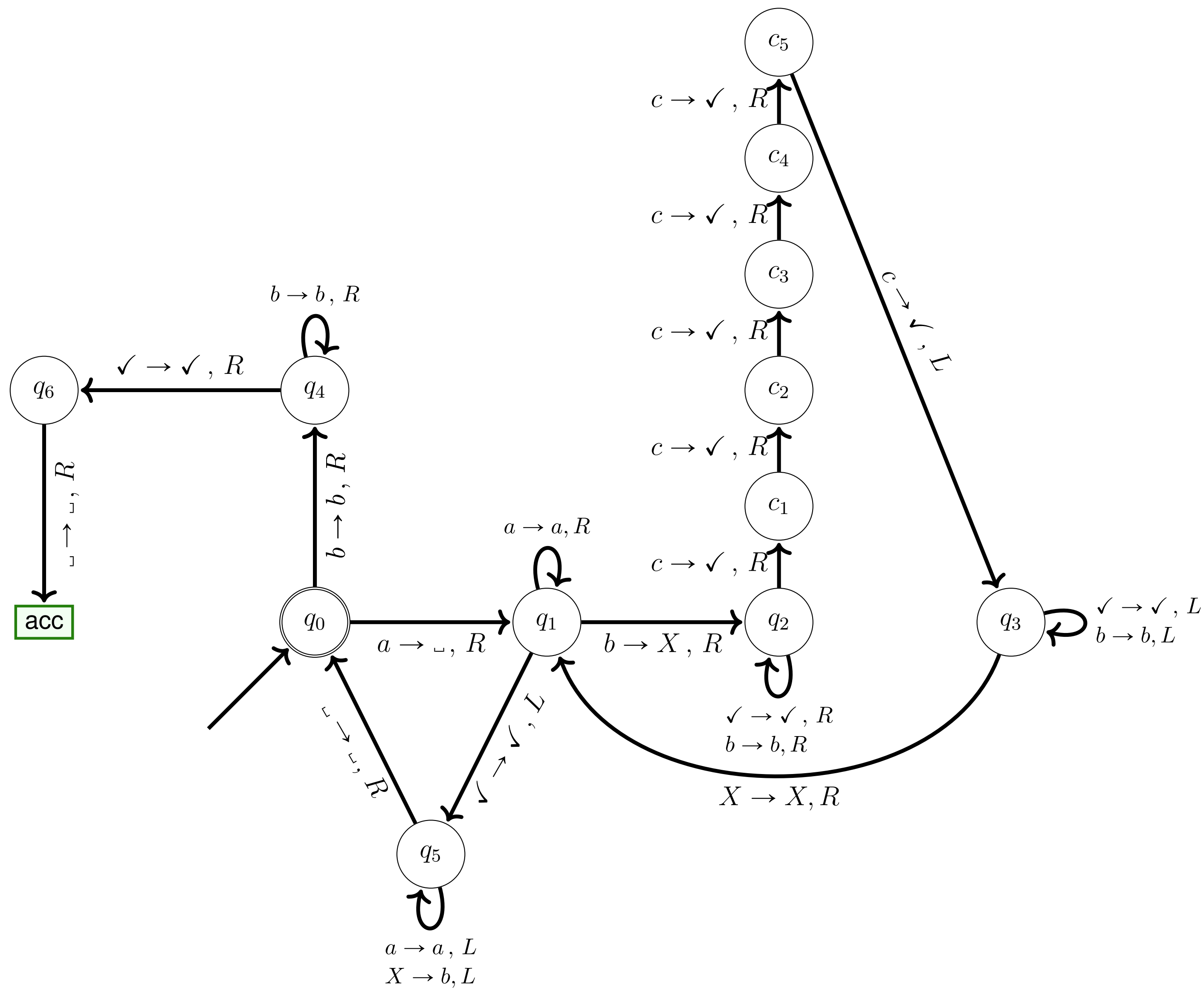
המכללה האקדמית להנדסה סמי שמעון
קמפוס באר שבע ביאליק פינת בזל 84100 | קמפוס אשדוד ז'בוטינסקי 84, 77245 | www.sce.ac.il | חייג: *

פתרונות

שאלה 1: מכונות טיורינג (20 נקודות)

סעיף א' (10 נקודות)

כל מעברים לא מופיעים בתרשים, עוברים למצב rej.



סעיף ב' (10 נקודות)

$$\sigma \in \{0,\ldots,9\}\ , \qquad \tau \in \{0,\ldots,9,*\}\ .$$

מצב	סימון בסרט	מצב חדש	כתיבה	תזוזה	תנאי
$X.*.*$	σ	$X.\sigma.*$	$\checkmark$	R	
$X.*.*$	$\checkmark$	$X.*.*$	$\circlearrowleft$	R	
$X.\sigma.*$	$0,1,\ldots,9,\checkmark$	$X.\sigma.*$	$\circlearrowleft$	R	
$X.\tau.*$	#	$Y.\tau.*$	$\circlearrowleft$	R	
$Y.\tau.*$	σ	$Y.\tau.\sigma$	$\checkmark$	R	
$Y.\tau.*$	$\checkmark$	$Y.\tau.*$	$\circlearrowleft$	R	
$Y.\tau.\sigma$	$0,1,\ldots,9,\checkmark$	$Y.\tau.\sigma$	$\circlearrowleft$	R	
$Y.\tau_1.\tau_2$	#	$Z.\tau_1.\tau_2$	$\circlearrowleft$	R	
$Z.\tau_1.\tau_2$	$\checkmark$	$Z.\tau_1.\tau_2$	$\circlearrowleft$	R	
$Z.\tau_1.\tau_2$	σ	back	$\checkmark$	L	$\tau_1,\tau_2 \neq \sigma \wedge \tau_1+\tau_2 \leqslant \sigma \wedge \tau_1,\tau_2 \neq *$
$Z**$	$\sqcup$	acc	$\circlearrowleft$	R	
back	$0,1,\ldots,9,\checkmark$	back	$\circlearrowleft$	L	
back	$\sqcup$	$X.*.*$	$\circlearrowleft$	R	

כל שאר המעברים עוברים ל rej.

שאלה 2: וריאציות על מכונות טיורינג (20 נקודות)

כיוון ראשון

פתרונות

תהי

$$M^O=\left(Q^O,\Sigma^O,\Gamma^O,\delta^O,q_0^O,\mathsf{acc}^O,\mathsf{rej}^O\right)\ ,$$

במודל O החד כיווני. נבנה מכונה

$$M^T=\left(Q^T,\Sigma^T,\Gamma^T,\delta^T,q_0^T,\mathsf{acc}^T,\mathsf{rej}^T\right)\ ,$$

שקולה במודל הדו כיווני T.

רכיבי המ"ט M^T זהים לאלו של המ"ט M^O, מלבד מהתכונה שהראש של M^O לא זז מעבר לקצה השמאולי של הקלט.

לכן כדי ש- M^T תהיה שקולה ל- M^O יש להוסיף מעברים לפונקצית המעברים של M^T כדי שהראש של M^T לא זז מעבר לקצה השמאולי של הקלט.

הרעיון הוא לסמן את המשבצת שמשמאול לתחילת הקלט עם סימן מיוחד \$, ואז להוסיף מעברים לפונקצית המעברים של M^T שמבטיחים שאם הראש נמצא למשבצת שמסומנת \$ אז הוא מיד חוזר ו- M^T חוזרת למצב ההתחתי של המ"ט M^O. זה מתבצע על ידי הוספת השורות האלו למטה לטבלת המעברים של M^T:

תנאי	תזוזה	כתיבה	מצב חדש	סימון	מצב
	L	$\circlearrowleft$	$q_\$$	σ	q_0^T
	R	$\$$	q_0^O	$\sqcup$	$q_\$$
$\forall q\in Q^O$	R	$\$$	q	$\$$	q

$$Q^T=Q^O\cup\{q_0^T,q_\$\}\ ,\qquad \Sigma^T=\Sigma^O\ ,\qquad \Gamma^T=\Gamma^O\cup\{\$\}\ ,\qquad \mathsf{acc}^T=\mathsf{acc}^O\ ,\qquad \mathsf{rej}^T=\mathsf{rej}^O\ .$$

כיוון שני

תהי

$$M^T=\left(Q^T,\Sigma^T,\Gamma^T,\delta^T,q_0^T,\mathsf{acc}^T,\mathsf{rej}^T\right)\ ,$$

במודל T הדו כיווני. נבנה

$$M^O=\left(Q^O,\Sigma^O,\Gamma^O,\delta^O,q_0^O,\mathsf{acc}^O,\mathsf{rej}^O\right)\ ,$$

במודל O החד כיווני.

נתאר סימולציה של הכונה החד-כיוונית במודל הדו-כיוונית.

הרעיון הוא לסמן קו על הסרט במשבת באמצע הקלט, ואז לקפל את הסרט בקו הזה. באופן הזה נקבל סרט עם קצה שמאולי ואינסופי ימינה. במשבצות של הסרט החדש המקופל יש שני תווים, אחד למעלה (U) ואחד למטה (D), מלבד מנקודת הקיפול שבו יש משבצת אחת שמסומנת \$.

באופן הזה אפשר לסמלץ את המכונה M^O במכונה M^T על ידי הוספת המעברים הבאים לטבלת המעברים של M^T. **לכל** $\tau,\sigma,\pi\in\Gamma^T$:

פתרונות

תנאי	תזוזה	כתיבה	מצב חדש	סימון	מצב
תזוזה שמאלה: $(q,\sigma) \xrightarrow{M^T} (p,\tau,L)$	L	π τ	$p.D$	π σ	$q.D$
	R	τ π	$p.U$	σ π	$q.U$
תזוזה שמאלה: $(q,\sqcup) \xrightarrow{M^T} (p,\tau,L)$	L	$\sqcup$ τ	$p.D$	$\sqcup$	$q.D$
	R	τ $\sqcup$	$p.U$	$\sqcup$	$q.U$
תזוזה ימינה: $(q,\sigma) \xrightarrow{M^T} (p,\tau,R)$	R	π τ	$p.D$	π σ	$q.D$
	L	τ π	$p.U$	σ π	$q.U$
תזוזה ימינה: $(q,\sqcup) \xrightarrow{M^T} (p,\tau,R)$	R	$\sqcup$ τ	$p.D$	$\sqcup$	$q.D$
	L	τ $\sqcup$	$p.U$	$\sqcup$	$q.U$
	R	$\circlearrowleft$	$q.U$	$\$$	$q.D$
	R	$\circlearrowleft$	$q.D$	$\$$	$q.U$
אתחול					
$\tau \in \Sigma \cup \{\sqcup\}$ $\sigma \in \Sigma$	R	$\$$	$q.\tau$	τ	q_0^O
	R	$\sqcup$ σ	$q.\tau$	τ	$q.\sigma$
	L	$\sqcup$ $\sqcup$	back	$\sqcup$	$q.\sqcup$
	L	$\circlearrowleft$	back	$\sqcup$ τ	back
	R	$\circlearrowleft$	$q_0^T.D$	$\$$	back
סיום					
			acc^O	הכל	acc$^T.D$
			acc^O	הכל	acc$^T.U$
			rej^O	הכל	rej$^T.D$
			rej^O	הכל	rej$^T.U$
כל השאר עוברים ל-rej					

$$\Gamma^O \supseteq \left(\Gamma^T \times \Gamma^T\right) \cup \{\$\} \ .$$

שאלה 3: התזה של צ'רץ'-טיורינג (20 נקודות)

סעיף א' (10 נקודות)

$$S \ \rightarrow \ \$Ca\# \ \rightarrow \ \$aaC\# \ \rightarrow \ \$aaE \ \rightarrow \ \$aEa \ \rightarrow \ \$Eaa \ \rightarrow \ aa$$

$$\begin{aligned} S \ &\rightarrow \ \$Ca\# \ \rightarrow \ \$aaC\# \ \rightarrow \ \$aaD\# \ \rightarrow \ \$aDa\# \ \rightarrow \ \$Daa\# \ \rightarrow \ \$Caa\# \\ &\rightarrow \ \$aaCa\# \ \rightarrow \ \$aaaaC\# \ \rightarrow \ \$aaaaE \ \rightarrow \ \$aaaEa \ \rightarrow \ \$aaEaa \ \rightarrow \ \$aEaaa \ \rightarrow \ \$Eaaaa \\ &\rightarrow \ aaaa \end{aligned}$$

באמצעות אינדוקציה על k ניתן להוכיח כי

$$L(G) = \left\{ w \in \Sigma^* \ \middle| \ w = \varepsilon \vee \left(w = a^{2^n} \ , \ n \in \mathbb{N} \right) \right\} \ .$$

סעיף ב' (10 נקודות)

$$S \ \rightarrow \ aBC \ \rightarrow \ abC \ \rightarrow \ abc$$

$$\begin{aligned} S \ &\rightarrow \ aSBC \ \rightarrow \ aaBCBC \ \rightarrow \ aaBHBC \ \rightarrow \ aaBBCC \ \rightarrow \ aabBCC \ \rightarrow \ aabbCC \\ &\rightarrow \ aabbcC \ \rightarrow \ aabbcc \ . \end{aligned}$$

אפשר להוכיח, ע"י אינדוקציה על n, כי

$$L(G) = \left\{ w \in \Sigma^* \ \middle| \ w = a^n b^n c^n \ , \ n \in \mathbb{N}^+ \right\} \ .$$

שאלה 4: אי כריעות (20 נקודות)

פתרונות

סעיף א' (10 נקודות)

נבנה מ"ט אי-דטרמיניסטית $M_{L_{\geqslant 3}}$ המכריעה את $L_{\geqslant 3}$.

התיאור הבא הוא תיאור של תוכנית אי-דטרמיניסטית של המכונת טיורינג $M_{L_{\geqslant 3}}$.

$M_{L_{\geqslant 3}} =$ על קלט x:

1. $M_{L_{\geqslant 3}}$ בודקת האם הקלט x הוא מכונת טיורינג.
   אם לא אז $M_{L_{\geqslant 3}}$ דוחה.
2. $M_{L_{\geqslant 3}}$ בוחרת באופן אי-דטרמיניטי 3 מילים w_1, w_2, w_3.
   - מריצה את M על w_1.
     * אם M דוחה $\Leftarrow$ $M_{L_{\geqslant 3}}$ דוחה.
   - מריצה את M על w_2.
     * אם M דוחה $\Leftarrow$ $M_{L_{\geqslant 3}}$ דוחה.
   - מריצה את M על w_3 ועונה כמוה.

<u>נכונות.</u>

$x \in L_{\geqslant 3} \Leftarrow x = \langle M \rangle$ ו- $|L(M)| \geqslant 3$.

$\Leftarrow$ $\exists$ 3 מילים w_1, w_2, w_3 המתקבלים ב- M.

$\Leftarrow$ $\exists$ ריצה של $M_{L_{\geqslant 3}}$ בה תבחר את w_1, w_2, w_3 ותריץ עליהם את M ותקבל

$\Leftarrow$ $M_{L_{\geqslant 3}}$ מקבלת את x.

$x \notin L_{\geqslant 3} \Leftarrow$ שני מקרים:

מצב 1. $x \neq \langle M \rangle \Leftarrow M_{L_{\geqslant 3}}$ דוחה את L.

מצב 2. $x = \langle M \rangle$ ו- $|L(M)| < 3$

$\Leftarrow$ לכל 3 מילים שונות w_1, w_2, w_3 לפחות אחת מהן לא מתקבלת ב- M.

$\Leftarrow$ בכל ריצה של $M_{L_{\geqslant 3}}$ בה היא תבחר 3 מילים w_1, w_2, w_3 השונות זו מזו, ולפחות אחת הריצות של M על מילים אלו תדחה או לא תעצור

$\Leftarrow$ בכל ריצה של $M_{L_{\geqslant 3}}$ על x, $M_{L_{\geqslant 3}}$ תדחה או לא תעצור

$\Leftarrow$ $M_{L_{\geqslant 3}}$ לא מקבלת את x.

סעיף ב' (10 נקודות)

נבנה רדוקציה מ- A_{TM}.

הפונקצית הרדוקציה היא:

$$f(x) = \begin{cases} \langle M' \rangle & x = \langle M, w \rangle \\ \langle M_{\varnothing} \rangle & x \neq \langle M, w \rangle \end{cases}$$

פתרונות

כאשר $M_\varnothing$ היא מ"ט הדוחה כל קלט ו- M' היא מ"ט שעל כל קלט x מריצה את M ועונה כמוה.

<u>אבחנה</u>

$$L(M') = \begin{cases} \Sigma^* & w \in L(M) \\ \varnothing & w \notin L(M) \end{cases}$$

<u>נכונות הרדוקציה</u>

נניח ש- $x \in A_{TM}$.

$\Leftarrow$ $x = \langle M, w\rangle$ ו- $w \in L(M)$.

$\Leftarrow$ $f(x) = \langle M'\rangle$.

$\Leftarrow$ $L(M') = \Sigma^*$.

$\Leftarrow$ $|L(M')| = \infty$.

$\Leftarrow$ $f(x) \in L_{\geqslant 3}$.

נניח ש- $x \notin A_{TM}$.
אז יש שני מקרים:

מצב 1: $x \neq \langle M, w\rangle$.

$\Leftarrow$ $f(x) = \langle M_\varnothing\rangle$ ו- $|L(M_\varnothing)| = 0$

$\Leftarrow$ $f(x) \notin L_{\geqslant 3}$.

מצב 2: $x = \langle M, w\rangle$ ו- $w \notin L(M)$.

$\Leftarrow$ $f(x) = \langle M'\rangle$

$\Leftarrow$ $L(M') = \varnothing$.

$\Leftarrow$ $|L(M')| = 0$.

$\Leftarrow$ $f(x) \notin L_{\geqslant 3}$.

שאלה 5: סיבוכיות זמן (20 נקודות)

סעיף א' (8 נקודות)

נבנה פונקצית הרדוקציה $f : \Sigma^* \to \Sigma^*$ שמוגדרת

$$f(\langle S, t\rangle) = \langle S'\rangle$$

כאשר $\langle S, t\rangle$ קלט של SubsetSum ו- $\langle S'\rangle$ קלט של Partition.

1) יהי $s = \sum\limits_{x \in S} x$.

2) נגדיר את הקבוצה החדשה S' על ידי הוספת האיבר $s-2t$ לקבוצה S:

$$S' = S \cup \{s-2t\} \ .$$

סעיף ב' (6 נקודות)

<u>כיוון $\Leftarrow$</u>

נניח ש- $\langle S, t\rangle \in$ SubsetSum.

$\Leftarrow$ קיימת תת-קבוצה $S \subseteq Y$ כך ש- $t = \sum\limits_{y \in Y} y$.

לכן:

$$\begin{aligned} \sum_{y \in (Y \cup \{s-2t\})} y &= |Y| + s - 2t \\ &= t + s - 2t \\ &= s - t \ . \end{aligned}$$

$$\begin{aligned} \sum_{y \in S' \backslash (Y \cup \{s-2t\})} y &= |S'| - (|Y| + s - 2t) \\ &= |S'| - |Y| - s + 2t \\ &= |S| + s - 2t - |Y| - s + 2t \\ &= |S| - |Y| \\ &= s - t \ . \end{aligned}$$

$\Leftarrow$ התת-קבוצה $Y \cup \{s-2t\}$ והתת-קבוצה $S' \backslash \big(Y \cup \{s-2t\}\big)$ מהוות חלקוה של הקבוצה S'.

$\Leftarrow$ Partition $\ni \langle S' \rangle$.

<u>כיוון $\Rightarrow$</u>

נניח ש- $\langle S' \rangle \in$ Partition.

$\Leftarrow$ קיימות תת-קבוצות $S'_1, S'_2 \subseteq S'$ כך שמתקיים

(1*) $$S'_1 \cup S'_2 = S'$$

-ו

(2*) $$\sum_{x \in S'_1} x = \sum_{x \in S'_2} x \ .$$

פתרונות

הקבוצה S קשור לקבוצה S' על ידי היחס $S' = S \cup \{s-2t\}$.
לכן

$$S_1' \cup S_2' = S \cup \{s-2t\} \qquad (3^*)$$

ללא הגבלת כלליות אנחנו נגדיר את התת-קבוצה $S_1 \subseteq S$ של הקבוצה S להיות

$$S_1 = S_1' \cup \{s-2t\} \ ,$$

ואנחנו נגדיר את התת-קבוצה $S_2 \subseteq S$ של הקבוצה S להיות

$$S_2 = S_2' \ .$$

מכאן מנובע מהמשוואה (3*) ש:

$$S_1 \cup S_2 = S_1' \cup S_2' + \{s-2t\} = S \cup \{s-2t\} \qquad \Rightarrow \qquad S_1 \cup S_2 = S \ . \qquad (4^*)$$

$\Leftarrow$ ניתן לרשום משוואה (2*) בצורה הבאה:

$$\sum_{x \in (S_1 \cup \{s-2t\})} x = \sum_{x \in S_2} x \ . \qquad (5^*)$$

ניתן לחלק את הסכום בצד השמאול של המשווה (5*) ולרשום אותה בצורה הבאה:

$$\sum_{x \in S_1} x + s - 2t = \sum_{x \in S_2} x \ . \qquad (6^*)$$

נוסיף את הסכום $\sum_{x \in S_1} x$ לשני האגפים של משוואה של (6*) ונקבל

$$\sum_{x \in S_1} x + \sum_{x \in S_1} x + s - 2t = \sum_{x \in S_2} x + \sum_{x \in S_1} x \ . \qquad (7^*)$$

הסכום בצד הימין של משוואה (7*) הוא הסכום $\sum_{x \in (S_1 \cup S_2)} x$.
לפי המשוואה (4*), $S_1 \cup S_2 = S$ לכן $\sum_{x \in (S_1 \cup S_2)} x = \sum_{x \in S} x$.
לכן הסכום בצד הימין של משוואה (7*) הוא הסכום של כל האיברים אשר בקבוצה S.
אנחנו מסמנים את הסכום הזה כ- $\sum_{x \in S} x = s$. לכן ניתן לרשום את משוואה (7*) בצורה הבאה:

$$\sum_{x \in S_1} x + \sum_{x \in S_1} x + s - 2t = s \ . \qquad (8^*)$$

אפשר לבטל s בצד שמאול ובצד ימין ולהעביר את ה- $2t$ לצד ימין ולקבל את המשוואה:

$$\sum_{x\in S_1} x + \sum_{x\in S_1} x = 2t \ , \tag{9*}$$

זאת אומרת

$$2\sum_{x\in S_1} x = 2t \qquad \Rightarrow \qquad \sum_{x\in S_1} x = t \ . \tag{10*}$$

$\Leftarrow$ קיימת תת קבוצה $S_1 \subseteq S$ של S שמקיימת את התנאי $\sum_{x\in S_1} x = t$.

$\Leftarrow$ SubsetSum $\in \langle S,t\rangle$.

סעיף ג' (6 נקודות)

הפונקצית הרדוקציה f, על קלט $\langle S,t\rangle$ מחזירה את הפלט $\langle S'\rangle$ כאשר $S' = S \cup \{s-2t\}$.

לכן הפונקציה מחשבת את הסכום s של כל האיברים שבקבוצה S ואז מחשבת את החיסור $s-2t$.

נסמן $n=|S|$ האורך של הקבוצה S.

אפשר לתאר את f בפסאודו-קוד באופן הבא:

שלב 1. הפונקציה f מאתחלת משתנה $s=0$.

שלב 2. הפונקציה נכנסת ללואה מעל כל האיברים שבקבוצה S ומחברת האיבר הנוכחי לערך של s כל איטרציה.

שלב 3. בסוף הפונקציה מחשבת את החיסור $s-2t$.

שלב 4. הפונקציה מחזירה את הקבוצה החדשה $S' = S \cup \{s-2t\}$.

- שלב 1 דורש צעד אחד. לכן הסיבוכיות של שלב 1 הוא $O(1)$.
- שלב 2 דורש n צעדים. לכן הסיבוכיות של שלב 2 הוא $O(n)$.
- שלב 3 דורש צעד אחד. לכן הסיבוכיות של שלב 3 הוא $O(1)$.
- שלב 4 דורש צעד אחד. לכן הסיבוכיות של שלב 4 הוא $O(1)$.

בסך הכל הסיבוכיות של הפונקציה f היא

$$O(1)+O(n)+O(1)+O(1)=O(n) \ .$$