

## תוכן העניינים

1	מכונות טיורינג	1
3	וריאציות של מכונות טיורינג	2
6	התזה של צ'רץ'-טיורינג	3
10	אי-כrüיעות	4
10	מחלקות החישוביות $R$ , $RE$ ו- $Co\ RE$ ותכונותן	5
11	רذוקציות	6
13	סיבוכיות	7
14	רذוקציה פולינומיאלית	8
14	NP שלמות	9
15	בעיית הספיקות ( $SAT$ )	
16	סיווג שפות ידיעות - סיבוכיות	
20	רذוקציות זמן פולינומיאליות	

## 1. מכונות טיורינג

### הגדרה 1: מכונת טיורינג

מכונת טיורינג (מ"ט) היא שביעה  $M$  כאשר:

$Q$	קבוצת מצבים סופית ולא ריקה
$\Sigma$	א"ב הקלט סופי
$\Gamma$	א"ב הסרט סופי
$\delta$	פונקציית המעברים
$q_0$	מצב התחלתי.
$q_{acc}$	מצב מקבל יחיד.
$q_{rej}$	מצב דוחה יחיד.

### הגדרה 2: קונפיגורציה

בහינתן מכונת טיורינג  $M$  ומילה  $w \in \Sigma^*$ . **קונפיגורציה** בritch של  $M$  על  $w$  היא שלושה  $(u, q, v)$  (או  $uqv$  לשם קיצור) כאשר:

- $\Sigma^* \in u$ : המילה מתחילת הסרט עד (לא כולל) התו שמתוחת לראש.
- $\Sigma^* \in v$ : המילה שמתוחילה מהຕן שמתוחת לראש ועד (לא כולל) ה-  $_u$  הראשון.

**הגדרה 3: גירה בצעד אחד**

תהי  $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{acc}}, q_{\text{rej}})$  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 כמפורטים ב-  $c_1$  עוברים ל-  $c_2$  בצעד בודד.

**הגדרה 4: גירה בכללי**

תהי  $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{acc}}, q_{\text{rej}})$  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 ניתן לעבור מ-  $c_1$  ל-  $c_2$  ב- 0 או יותר צעדים.

**הגדרה 5: קבלה ודחיה של מילה**

תהי  $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{acc}}, q_{\text{rej}})$  מכונת טיורינג, ו-  $w \in \Sigma^*$  מחרוזת. אומרים כי  $M$  **מקבלת את  $w$**  אם  $q_0 w \vdash_M^* u$  ואם  $w \in L$ . אומרים כי  $M$  **דוחה את  $w$**  אם  $q_0 w \vdash_M^* u$  ו-  $w \notin L$ . עבור  $u, v \in \Gamma^*$  כלשהם.

**הגדרה 6: הכרעה של שפה**

תהי  $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{acc}}, q_{\text{rej}})$  מכונת טיורינג, ו-  $L \subseteq \Sigma^*$  שפה. אומרים כי  $M$  **מכרעת את  $L$**  אם לכל  $w \in \Sigma^*$  מתקיים  $w \in L \iff M \text{ מקבלת את } w$ . אומרים כי  $M$  **דוחה את  $L$**  אם לכל  $w \in \Sigma^*$  מתקיים  $w \notin L \iff M \text{ דוחה את } w$ .

**הגדרה 7: קבלה של שפה**

תהי  $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{acc}}, q_{\text{rej}})$  מכונת טיורינג, ו-  $L \subseteq \Sigma^*$  שפה. אומרים כי  $M$  **מקבלת את  $L$**  אם לכל  $w \in \Sigma^*$  מתקיים  $w \in L \iff M \text{ מקבלת את } w$ . אומרים כי  $M$  **לא מקבלת את  $L$**  אם לכל  $w \in \Sigma^*$  מתקיים  $w \notin L \iff M \text{ לא מקבלת את } w$ . במקרה זה נכתב ש-  $L(M) = L$ .

**הגדרה 8: מכונת טיורינג שמחשבת פונקציה  $f$** 

תהי  $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{acc}}, q_{\text{rej}})$  מכונת טיורינג. אומרים כי  $M$  **מחשבת את  $f$**  אם  $f : \Sigma_1^* \rightarrow \Sigma_2^*$  ותהי  $\Sigma_2 \subset \Gamma$  ו-  $\Sigma = \Sigma_1$ . אומרים כי  $M$  **מחשבת פונקציה  $f$**  אם  $f : \Sigma_1^* \rightarrow \Sigma_2^*$  ותהי  $\Sigma_2 \subset \Gamma$  ו-  $\Sigma = \Sigma_1$ . אומרים כי  $M$  **מחשבת פונקציה  $f$**  אם  $f : \Sigma_1^* \rightarrow \Sigma_2^*$  ותהי  $\Sigma_2 \subset \Gamma$  ו-  $\Sigma = \Sigma_1$ .

## 2 וריאציות של מכונות טיורינג

### הגדרה 9: מודל חישוב

מודל חישובי = אוסף של מכונות שעבורם מוגדרים המושגים של הכרעה וקבלת של שפות.

### הגדרה 10: מודלים שקולים חישובי

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

- קיימת מכונה במודל  $A$  שמקரיעה את  $L$  אם ו רק קיימת מכונה כזו במודל  $B$ .
- קיימת מכונה במודל  $A$  שמקבלת את  $L$  אם ו רק קיימת מכונה כזו במודל  $B$ .

### הגדרה 11: מכונות שקולות חישובית

שתי מכונות הן שקולות חישובית אם הן מקבלות ודוחות בדיקת אותן המילים.

### משפט 1: מכונת טיורינג עם סרט ימינה בלבד

מודל מ"ט טם סרט אינסופי לכיוון אחד בלבד (מודל O) שקול למודל אינסופי בשני הכוונים (מודל T).  
כלומר, לכל שפה  $L$ :

- יש מ"ט מודול O שמקבלת את  $L$  אם ו רק יש מ"ט במודול T שמקבלת את  $L$ .
- יש מ"ט מודול O שמקריעת את  $L$  אם ו רק יש מ"ט במודול T שמקריעת את  $L$ .

### משפט 2: מכונת טיורינג מרובת סרטים

במכונות טיורינג מרובה סרטים:

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

בפרט, הראשים יכולים לזרז בכיוונים שוניםסרטים שונים.

- ישנו בקר מרכזי יחיד, שקובע את הפעולות בכל אחד מהסרטים, על סמך המידע שמתתקבל מכל הסרטים.

לכן, תוכן סרט אחד יכול להשפיע על הפעולות בשאר הסרטים.

- בתחילת החישוב, הקלט נמצא הסרט הראשון ושאר הסרטים ריקים.

### משפט 3: מ"ט מרובה סרטים שcolaה למ"ט עם סרט יחיד

לכל  $k$ , המודל של מ"ט עם  $k$  סרטים שcolaה למ"ט חישובי למודל של מ"ט עם סרט אחד.

**משפט 4: קבלה וחדיה של מילה ע"י מ"ט א-דטרמיניסטיבית**

עבור מ"ט לא דטרמיניסטיבית  $N$  ומילה  $w$ :

- $N$  מקבלת את  $w$  אם קיים חישוב של  $N$  על  $w$  שmagiu במצב מקבל.
- $N$  דוחה את  $w$  אם כל החישובים של  $N$  על  $w$  העוזרים במצב דוחה.

**משפט 5: קבלה וחדיה של שפה ע"י מ"ט א-דטרמיניסטיבית**

נתון מ"ט לא דטרמיניסטיבית  $N$  ושפה  $L$ :

- $N$  מכירעה את  $L$  אם  $N$  מקבלת את כל המילים ב-  $L$  ודוחה את כל המילים שאינם ב-  $L$ .
- $N$  מקבלת את  $L$  אם  $N$  מקבלת את כל המילים ב-  $L$  ולא מקבלת את כל המילים שאינם ב-  $L$ .

**משפט 6: מ"ט א-דטרמיניסטיבית שcola לה למ"ט דטרמיניסטיבית**

לכל מ"ט לא דטרמיניסטיבית קיימת מ"ט דטרמיניסטיביתcola.

**הגדרה 12: מכונת טיריניג א-דטרמיניסטיבית**

מכונת טיריניג א-דטרמיניסטיבית (מ"ט א"ד) היא שביעייה

$$M = (Q, \Sigma, \Gamma, q_0, q_{\text{acc}}, q_{\text{rej}})$$

כאשר  $Q, \Sigma, \Gamma, q_0, q_{\text{acc}}, q_{\text{rej}}$  מוגדרים כמו במ"ט דטרמיניסטי (ראו הגדרה 1).

$\Delta$  היא פונקציה המעבירים

$$\Delta : (Q \setminus \{q_{\text{acc}}, q_{\text{rej}}\}) \times \Gamma \rightarrow P(Q \times \Gamma \times \{L, R, S\}) .$$

$$\Delta(q, a) = \{(q_1, a, S), (q_2, b, L), \dots\} .$$

כלומר, לכל זוג  $q, \alpha \in Q, \alpha \in \Gamma$  יתכן מספר מעברים אפשריים, 0, 1 או יותר.

• קונפיגורציה של מ"ט א"ד זהה לקונפיגורציה של מ"ט דטרמיניסטיבית.

• לכל קונפיגורציה יתכן מספר קונפיגורציות עוקבות.

• לכל מילה  $\Sigma^* \in w$  יתכן מספר ריצות שונות:

◦ ריצות שmagiuות ל-  $q_{\text{acc}}$ .

◦ ריצות שmagiuות ל-  $q_{\text{rej}}$ .

◦ ריצות שלא עוזרות.

◦ ריצות שנתקעות.

**הגדרה 13: קבלה וחדיה של מילה ושפה של מכונת טיריניג א-דטרמיניסטיבית**

מילה  $\Sigma^* \in w$  מתתקבלת במ"ט א"ד  $M$  אם קיימת לפחות ריצה אחת שmagiu ל-  $q_{\text{acc}}$ . השפה של מ"ט א"ד  $M$  היא

$$L(M) = \{w \in \Sigma^* \mid \exists u, v \in \Gamma^* : q_0 w \vdash_* u q_{\text{acc}} v\}$$

כלומר:

◦  $w \in L(M)$  אם קיימת ריצה אחת שבה  $M$  מקבלת את  $w$ .

ו  $w \notin L(M)$  אם בכל ריצה של  $M$  על  $w$ ,  $M$  דוחה או לא עוצרת, או נתקעת.

#### הגדרה 14: מ"ט אי דטרמיניסטי המכريع שפה $L$

אומרים כי מ"ט אי דטרמיניסטי  $M$  מכיריע שפה  $L$  אם לכל  $w \in \Sigma^*$ :

- אם  $w \in L \Leftarrow w$  מקבלת את  $w$ .
- אם  $w \notin L \Leftarrow w$  דוחה את  $w$ .

#### הגדרה 15: מ"ט א"ד המקבלת שפה $L$

אומרים כי מ"ט א"ד דטרמיניסטי  $M$  מקבלת שפה  $L$  אם לכל  $w \in \Sigma^*$ :

- אם  $w \in L \Leftarrow w$  מקבלת את  $w$ .
- אם  $w \notin L \Leftarrow w$  דוחה את  $w$  או  $M$  לא עוצרת על  $w$ .

#### משפט 7: שקילות בין מ"ט א"ד למ"ט דטרמיניסטי ב- $RE$

לכל מ"ט א"ד  $N$  קיימת מ"ט דטרמיניסטי  $D$  כך ש-  
 $L(N) = L(D)$ .

כלומר לכל  $w \in \Sigma^*$ :

- אם  $N$  מקבלת את  $w$   $\Leftarrow D$  מקבלת את  $w$ .
- אם  $N$  לא מקבלת את  $w$   $\Leftarrow D$  לא מקבלת את  $w$ .

### 3 התזה של צ'רצ'-טיוורינג

শמות נרדפים לשפות כריעות ושפות קבילות

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

#### משפט 9: סגירות שפות קבילות

- איחוד
- חיתוך
- שרשור
- סגור קlien

#### משפט 8: סגירות שפות כריעות

השפות הכריעות סגורות תחת:

- איחוד
- חיתוך
- משלים
- שרשור
- סגור קlien

#### משפט 10: היחס בין הכרעה לקבלה

עבור כל שפה  $L$  התנאים הבאים מתקיימים.

- אם  $L$  הינה כרעה אז היא קבילה. כלומר:

$$L \in R \Rightarrow L \in RE.$$

- אם השפה  $L$  קבילה וגם והמשלים שלה  $\bar{L}$  קבילה אז  $L$  כרעה. כלומר:

$$L \in RE \wedge \bar{L} \in RE \Rightarrow L \in R.$$

#### הגדרה 16: שפת סימפל

##### משתנים

- טבעיים:  $i, j, k, \dots$   
מקבלים כערך מספר טبאי.
- מערכיים:  $C, B, A$  [...] בכל תא ערך מתוק א"ב  $\Gamma$  אין סופיים.
- אתחול: הקלט נמצא בתאים הראשונים של  $A$  [...].  
כל שאר המשתנים מאותחלים ל-0.

##### פעולות

- השמה בקבוע:  $i=3, B[i] = \#$
- השמה בין משתנים:  $i=k, A[k] = B[i]$
- פעולות חשבון:  $x = y + z, x = y - z, x = y \cdot z$

תנאים

- $B[i] == A[j]$  (מערכות).
- $x \geq y$  (משתנים טבעיות).

כל משתנה מופיע רק פעם אחת בכל פעולה או תנאי.

זרימה

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

```

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 17: קבלה ודחיה של מחuzeות 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 18: הכרעה וקבלת 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 ורקי המילים ב- L.

**משפט 11: שפת SIMPLE שקופה למוכנת טיריניג**

המודלים של מוכנת טיריניג ותוכניות SIMPLE שקופה.

**משפט 12: מ"ט ותוכניות מחשב**

מ"ט חזקה לפחות כמו תוכנית משחוב.

כל תוכנית מחשב ניתנת למימוש במ"ט.

לכן, כל שפה שהינה כריעה ע"י מחשב היא גם כריעה ע"י מ"ט.

וכמו כן, שפה שהינה קבילה ע"י מחשב היא גם קבילה ע"י מ"ט.

**הגדרה 19: דקדוקים כלליים**

בדקdock כללי, בצד שמאל של כלל יצירה יכולה להופיע מחרוזת (לא ריקה) כלשהי. פורמלית, כלל יצירה בדקדוק כללי הוא מהצורה

$$\gamma \rightarrow u$$

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

**משפט 13:**

תהי  $L$  שפה.  $L$  קבילה אם ו רק אם קיים דקדוק כללי  $G$  כך ש-  $L = L(G)$ .

מודל חישובי	דקdock	משפחת שפות
מוכנת טיריניג	כללי	קבילות
אוטומט מחסנית	חסר הקשר	חסירות הקשר
אוטומט סופי	רגולרי	רגולריות

**משפט 14:**

כל שפה חסרת הקשר אינה כריעה.

**משפט 15: התזה של צ'רצ' טיריניג**

התזה של צ'רצ' טיריניג מודל מ"ט מגלים את המושג האבסטרקטי של "אלגוריתם".  
כלומר, כל אלגוריתם שנitinן לתיאור כתהיליך מכניסטיubo:shvo:

- התהיליך מתבצע כסדרה של צעדים.
- כל צעד מצריך כמהות סופית של "עובדת".

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

**הגדרה 20: מודלים שקולים חישובית**

יהיו  $A$  ו-  $B$  מודלים חישוביים. אומרים כי  $A$  ו-  $B$  שקולים אם לכל שפה  $L$  מתקיימים:

- (1) קיימת מ"ט במודל  $A$  שמכריעה את  $L$  אם ורק קיימת מ"ט במודל  $B$  שמכריעת את  $L$ .
- (2) קיימת מ"ט במודל  $A$  שמקבלת את  $L$  אם ורק קיימת מ"ט במודל  $B$  שמקבלת את  $L$ .

**הגדרה 21: מכונת טירוג'ג מרובת סרטים**

מכונת טירוג'ג מרובה סרטים היא שבייעה:

$$M = (Q, \Sigma, \Gamma, \delta_k, q_0, q_{\text{acc}}, q_{\text{rej}})$$

כאשר  $Q, \Sigma, \Gamma, q_0, q_{\text{acc}}, q_{\text{rej}}$  מוגדרים כמו מ"ט עם סרט יחיד (ראו הגדרה 1).  
ההבדל היחידי בין מ"ט עם סרט יחיד לבין מטב"ס הוא הפונקציית המעברים. עבור מטמ"ס הפונקציה המעברים היא מצורמת הבא:

$$\delta_k : (Q \setminus \{q_{\text{acc}}, q_{\text{rej}}\}) \times \Gamma^k \rightarrow Q \times \{L, R, S\}^k$$

הkonfigורציה של מכונת טירוג'ג מרובה סרטים מסומנת  $(u_1q v_1, u_2q v_2, \dots, u_kq v_k)$ .

**משפט 16: שקולות בין מ"ט מרובה סרטים למ"ט עם סרט יחיד**

לכל מטמ"ס  $M$  קיימת מ"ט עם סרט יחיד  $M'$  השקולה לו  $M$ .

כלומר, לכל קלט  $w \in \Sigma^*$ :

- אם  $M$  מקבלת את  $w$   $\Leftarrow M'$  מקבלת את  $w$ .
- אם  $M$  דוחה את  $w$   $\Leftarrow M'$  דוחה את  $w$ .
- אם  $M$  לא עוצרת על  $w$   $\Leftarrow M'$  לא עוצרת על  $w$ .

## 4 אי-כריעות

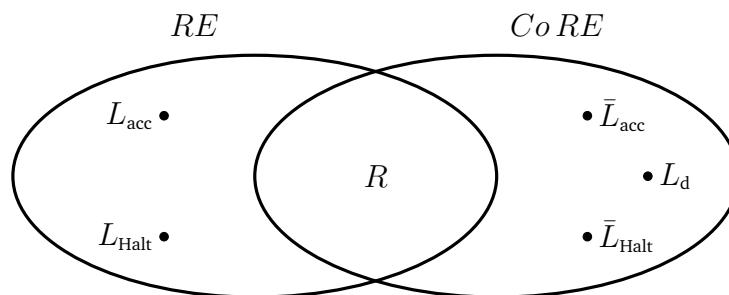
## משפט 17: סיווג שפות ידועות - חישוביות

$L_{\text{acc}} = \{\langle M, w \rangle \mid w \in L(M)\}$	$\in RE \setminus R$
$L_{\text{halt}} = \{\langle M, w \rangle \mid w \text{ עצרת על } M\}$	$\in RE \setminus R$
$L_M = \{\langle M \rangle \mid \langle M \rangle \text{ מקבלת את } M\}$	$\in RE \setminus R$
$L_d = \{\langle M \rangle \mid \langle M \rangle \notin L(M)\}$	$\in Co\,RE \setminus R$
$L_E = \{\langle M \rangle \mid L(M) = \emptyset\}$	$\in Co\,RE \setminus R$
$L_{EQ} = \{\langle M_1, M_2 \rangle \mid L(M_1) = L(M_2)\}$	$\notin RE \setminus R, \notin Co\,RE \setminus R$
$L_{REG} = \{\langle M \rangle \mid \text{רגולרית } L(M)\}$	$\notin RE \setminus R, \notin Co\,RE \setminus R$
$L_{NOTREG} = \{\langle M \rangle \mid \text{לא רגולרית } L(M)\}$	$\notin RE \setminus R, \notin Co\,RE \setminus R$

כריעה	קבילה	
✓	✗	$L_{\text{acc}}$
✗	✗	$\overline{L_{\text{acc}}}$
✗	✗	$L_d$
✓	✗	$L_{\text{Halt}}$
✗	✗	$\overline{L_{\text{Halt}}}$
✗	✗	$L_E$
✓	✗	$\overline{L_E}$
✗	✗	$L_{EQ}$
✗	✗	$\overline{L_{EQ}}$
✗	✗	$L_{\text{REG}}$
✗	✗	$L_{\text{NOTREG}}$

## משפט 18:

$$\begin{aligned} L_{\text{acc}} \in RE \setminus R &\Rightarrow \bar{L}_{\text{acc}} \notin RE, \\ L_{\text{halt}} \in RE \setminus R &\Rightarrow \bar{L}_{\text{halt}} \notin RE, \\ L_d \notin RE \setminus R. & \end{aligned}$$

5 המחלקות החישוביות  $R$ ,  $Co\,RE$  ו-  $RE$  ותכונותן

## הגדרה 22: כוכב קליני

בහינתן השפה  $L$ . השפה  $L^*$  מוגדרת:

$$L^* = \{\varepsilon\} \cup \{w = w_1 w_2 \cdots w_k \mid \forall 1 \leq i \leq k, w_i \in L\}$$

**הגדרה 23:**

- $.R = \{L \subseteq \Sigma^* \mid L \text{ מכיריה את } R\}$  • אוסף השפות הדירות מסומן  $R$  ומוגדר  
 $.RE = \{L \subseteq \Sigma^* \mid L \text{ מקבלת את } R\}$  • אוסף השפות הקבילות מסומן  $R$  ומוגדר  
 $.Co RE = \{L \subseteq \Sigma^* \mid \bar{L} \in RE\}$  • אוסף השפות שהמשלימה שלהן קבילה מסומן  $R$  ומוגדר

**משפט 19: סגירות של השפות הדירות והשפות הקבילות**

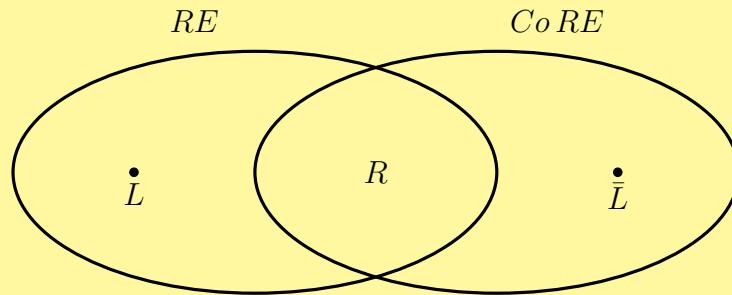
- 1) איחוד 2) חיתוך 3) שרשור 4) סגור קלין 5) משלימים.  
 • סגורה תחת:  
 1) איחוד 2) חיתוך 3) שרשור 4) סגור קלין.  
 • סגורה תחת:

**משפט 20: תכונות של השפות החישוביות**

1. אם  $L \in R$  וגם  $\bar{L} \in RE$  אז  $L \in RE$ .

2. אם  $(\bar{L} \in Co RE \setminus R)$  כי  $\bar{L} \notin RE$  אז  $L \in RE \setminus R$ .

3.  $RE \cap Co RE = R$ .

**הגדרה 24: מכונת טיורינג אוניברסלית**

מ"ט אוניברסלית  $U$  מקבלת כקלט זוג, קידוד של מ"ט  $\langle M \rangle$  וקידוד של מילה  $\langle w \rangle$ , וביצעת סימולציה של ריצה של  $M$  על  $w$  ועונה בהתאם.

$$L(U) = \{\langle M, w \rangle \mid w \in L(M)\} .$$

**6 רזוקציות****הגדרה 25: מ"ט המחשבת פונקציה**

בהתנן פונקציה  $\Sigma^* \rightarrow \Sigma^*$  :  $f$  אומרים כי מ"ט  $M$  מחשבת את  $f$  אם לכל  $x \in \Sigma^*$

- מגיעה  $-q_{acc}$  בסוף החישוב של  $f(x)$  וגם
- על סרט הפלט של  $M$  רשום  $f(x)$ .

**הגדרה 26: מ"ט המחשבת פונקציה**

בහינתן פונקציה  $\Sigma^* \rightarrow \Sigma^*$  אומרים כי  $f$  חסיבה אם קיימת מ"ט המחשבת את  $f$ .

**הגדרה 27: רדוקציה**

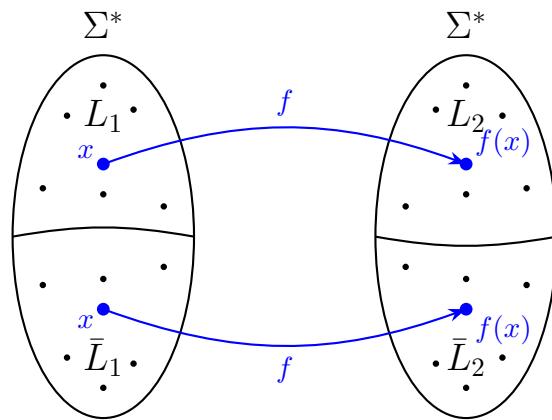
בහינתן שתי שפות  $L_1, L_2 \subseteq \Sigma^*$  אומרים כי  $L_1$  ניתנת לרדוקציה ל- $L_2$ , ומסמנים  $L_1 \leq L_2$ ,

אם קיימת פונקציה  $\Sigma^* \rightarrow \Sigma^*$  המכנית:

(1) חסיבה  $f$

(2) לכל  $x \in \Sigma^*$

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

**משפט 21: משפט הרדוקציה**

לכל שתי שפות  $L_1, L_2 \subseteq \Sigma^*$  איזה

$$L_1 \in R \iff L_2 \in R$$

$$L_1 \in RE \iff L_2 \in RE$$

$$L_1 \notin R \Rightarrow L_2 \notin R$$

$$L_1 \notin RE \Rightarrow L_2 \notin RE$$

**משפט 22: תכונות של רדוקציה**

- לכל שפה  $L$  מתקיים:  $L \leq L$
- אם  $L_1 \leq L_2$  אז  $L_1 \leq L_2$ .
- אם  $L_1 \leq L_2 \leq L_3$  אז  $L_1 \leq L_3$ .
- לכל  $L \in R$  ולכל  $L' \subseteq \Sigma^*$  מתקיים  $L \leq L'$ .

**משפט 23: משפט ריס**

עבור כל תכונה  $S$  של שפות שאינה טריואילית מתקיים:  $L_S \notin R$

- תכונה  $S$  לא טריואילית היא קבוצה של שפות ב  $RE$  כך ש  $S \neq \emptyset$  וגם  $S \neq RE$

$$.L_S = \{\langle M \rangle \mid L(M) = S\} \circ$$

## 7 סיבוכיות

### הגדירה 28: סיבוכיות זמן של מ"ט

סיבוכיות זמן של מכונת טיורינג (או אלגוריתם)  $M$  היא פונקציה  $f(|w|)$  שווה למספר צעדים לכל היותר ש-  $M$  מבצעת בחישוב של  $M$  על הקלט  $w$ .

### משפט 24: קשר בין סיבוכיות של מ"ט מרובת סרטים ומ"ט סרט יחיד

לכל מ"ט מרובה סרטים  $M$  הרצה בזמן  $f(n)$ , קיימת מ"ט סרט יחיד  $M'$  השköלה ל-  $M$  ורצה בזמן  $(f^2(n))$ .

### משפט 25: קשר בין סיבוכיות של מ"ט אי-דטרמיניסטי ומ"ט דטרמיניסטי

לכל מ"ט א"ד  $N$  הרצה בזמן  $f(n)$ , קיימת מ"ט דטרמיניסטי  $D$  השköלה ל-  $N$  ורצה בזמן  $2^{(f(n))}$ .

### הגדירה 29: אלגוריתם אimotoת

אלגוריתם אimotoת עבר בעה  $A$  הוא אלגוריתם  $V$  כך שלכל קלט  $\Sigma^* \in w$  מתקיים:  $w \in A$  אם ורק אם קיימת מילה  $y$  באורך פולינומיAli ב-  $|w|$  כך ש-  $V$  מקבל את הזוג  $(y, w)$ . כלומר:

- $V(w, y) = T \iff w \in A$
- $V(w, y) = F \iff w \notin A$

### הגדירה 30: המחלקות P ו- NP

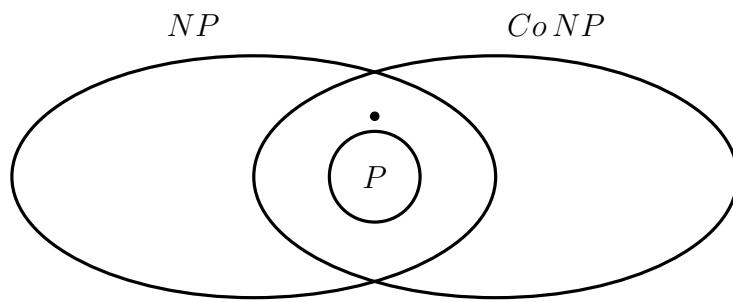
- $P$  = קבוצת כל השפות שיש להן מ"ט דטרמיניסטי המכריעה אותן בזמן פולינומי.
- $NP$  = קבוצת כל השפות שיש להן אלגוריתם אimotoת המאמת אותן בזמן פולינומי.

הגדרה שköלה:

- $NP$  = קבוצת כל השפות שיש להן מ"ט אי-דטרמיניסטי המכריעות אותן בזמן פולינומי.
- $CoNP = \{A \mid \bar{A} \in NP\}$
- $CoNP$  = קבוצת כל השפות שההמשלימה שליהן שייכת ל-  $NP$ .

### משפט 26: תכונות של P ו- NP

- $P \subseteq NP$
- סגורה תחת משלים: אם  $A \in P$  אז גם  $\bar{A} \in P$
- $P \subseteq NP \cap CoNP$



## 8 רדוקציה פולינומיאלית

### הגדרה 31: פונקציה פולינומיאלית

בහינתן פונקציה  $\Sigma^* \rightarrow \Sigma^*$ :  $f$ . אומרים כי  $f$  חסיבה בזמן פולינומיאלי אם קיים אלגוריתם (מ"ט דטרמיניסטי) המחשב את  $f$  בזמן פולינומיאלי.

### הגדרה 32: רדוקציה פולינומיאלית

בහינתן שתי בעיות  $A$  ו- $B$ . אומרים כי  $A$  ניתנת לרדוקציה פולינומיאלית ל- $B$ , ומסמנים  $A \leq_P B$ , אם קיימת פונקציה  $\Sigma^* \rightarrow \Sigma^*$ :  $f$  המקיים:

(1) חסיבה בזמן פולינומיאלי

(2) לכל  $w \in \Sigma^*$ :

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

### משפט 27: משפט הרדוקציה

לכל שתי בעיות  $A$  ו- $B$ , אם  $A \leq_P B$ , אז  $A \leq_P B$

$$A \in P \iff B \in P$$

$$A \in NP \iff B \in NP$$

$$A \notin P \Rightarrow B \notin P$$

$$A \notin NP \Rightarrow B \notin NP$$

## 9 NP שלמות

### הגדרה 33: NP - קשה (NP-hard)

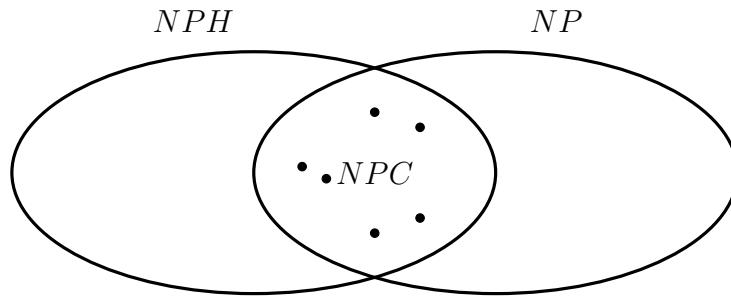
בעיה  $B$  נקראת  $NP$  קשה אם לכל בעיה  $A \in NP$  קיימת רדוקציה  $A \leq_P B$ .

**הגדרה 34:**  $NP$ -שלמה (NP-complete)

בעיה  $B$  נקראת  $NP$  שלמה אם

$$B \in NP \quad (1)$$

2) לכל בעיה  $A \in NP$  קיימת רדוקציה  $.A \leq_p B$



**משפט 28: תכונות של רדוקציה פולינומיאלית**

- אם קיימת שפה  $P = NP$   $B \in P$  ( $NP$  שלמה) וגם  $A$  אי-  $.P \leq_P B$   $A \in NPC$
- אם  $\bar{A} \leq_P \bar{B}$   $A \leq_P B$ .
- $.A \leq_p C \leq_p B$   $A \leq_p B$  וגם  $C$  אי-  $.A \leq_p B$
- $.A \leq_P B$  שאינה  $\emptyset, \Sigma^*, \Sigma^{**}$  מתקיים
- לכל  $P$   $B \in P$  ולכל  $A \in P$  מתקיים  $\emptyset, \Sigma^*, \Sigma^{**}$

**משפט 29: טרנזיטיביות של  $NP$ -שלמות**

תהי  $B$  בעיה  $-NP$ -שלמה. אז לכל בעיה  $C \in NP$ , אם  $B \leq_p C$  היא  $NP$  שלמה.

## 10 בעיית הספיקות (SAT)

**הגדרה 35: נוסחת CNF**

נוסחת  $CNF$ ,  $\phi$  היא נוסחה בוליאנית מעל  $n$  משתנים  $x_1, x_2, \dots, x_n$  המכילה  $m$  פסוקיות כאשר כל פסוקייה מכילה אוסף של ליטרלים  $(x_i \setminus \bar{x}_i)$  המוחברים ע"י  $OR$  ( $\vee$ ) בוליאני והפסוקיות מחוברות ע"י  $AND$  ( $\wedge$ ) בוליאני. לדוגמה:

$$\phi = \left( x_1 \vee \bar{x}_2 \vee x_4 \vee \bar{x}_7 \right) \wedge \left( x_3 \vee x_5 \vee \bar{x}_8 \right) \wedge \dots$$

**הגדרה 36: נוסחת 3CNF**

נוסחת  $3CNF$ ,  $\phi$  היא נוסחה  $CNF$  שבה בכל פסוקייה יש בדיק שולש ליטרלים. לדוגמה:

$$\phi = \left( x_1 \vee \bar{x}_2 \vee x_4 \right) \wedge \left( x_3 \vee x_5 \vee \bar{x}_8 \right) \wedge \dots$$

**הגדרה 37: נוסחת CNF ספיקה**

נוסחת  $CNF$ ,  $\phi$  היא ספיקה אם קיימת השמה למשתנים  $x_1, x_2, \dots, x_n$  ע"י  $T \setminus F$  כך ש-  $\phi$  מקבלת ערך  $T$ , כלומר בכל פסוקית ישנו לפחות ליטרל אחד שקיבל ערך  $T$ .

**הגדרה 38: בעיית SAT**

קלט: נוסחת  $CNF$ ,  $\phi$ .  
פלט: האם  $\phi$  ספיקה?

$$SAT = \{\langle \phi \rangle \mid \text{נוסחת } CNF \text{ ספיקה } \phi\}$$

**הגדרה 39: בעיית 3SAT**

קלט: נוסחת  $3CNF$ ,  $\phi$ .  
פלט: האם  $\phi$  ספיקה?

$$3SAT = \{\langle \phi \rangle \mid \text{נוסחת } 3CNF \text{ ספיקה } \phi\}$$

**משפט 30:**

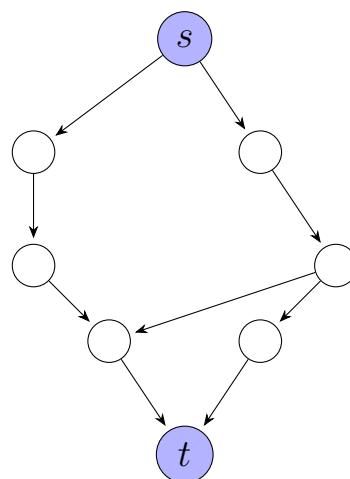
- $SAT \in NP$
- משפט קווקליון:  $SAT \in NPC$
- $3SAT \in NPC$
- $SAT \in P \Leftrightarrow P = NP$

**11 סיווג שפות ידיעות - סיבוכיות****הגדרה 40: בעיית מסלול PATH**

קלט: גרף מכובן  $G$  ושני קודקודים  $s$  ו-  $t$ .

פלט: האם  $G$  מכיל מסלול מקודקוד  $s$  לקודקוד  $t$ .

$$PATH = \{\langle G, s, t \rangle \mid \text{גרף מכובן המכיל מסלול מ- } s \text{ ל- } t \text{ }\}$$



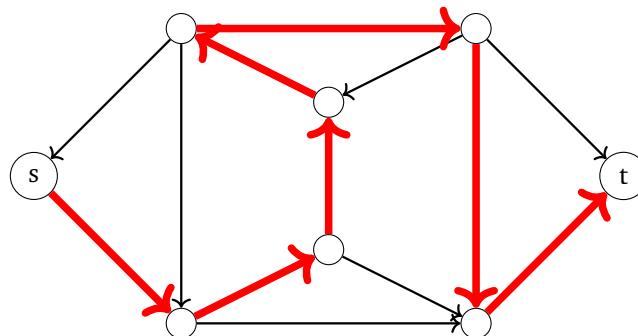
**הגדרה 41: בעית RELPRIME**

קלט: שני מספרים  $x$  ו-  $y$ .  
פלט: האם  $x$  ו-  $y$  זרים?

$$RELPRIME = \{\langle x, y \rangle \mid \gcd(x, y) = 1\} .$$

**הגדרה 42: מסלול המילטוני**

בහינתן גרף מכובן  $G = (V, E)$  ושני קודקודים  $s, t \in V$ . מסלול המילטוני מ-  $s$  ל-  $t$  הוא מסלול מ-  $s$  ל-  $t$  שעובר דרך כל קודקוד ב-  $G$  בדיקת פעם אחת.

**הגדרה 43: בעית מסלול המילטוני - HAMPATH**

קלט: גרף מכובן  $G = (V, E)$  ושני קודקודים  $s, t \in V$ .

פלט: האם  $G$  מכיל מסלול המילטוני מ-  $s$  ל-  $t$  ?

$$HAMPATH = \{\langle G, s, t \rangle \mid \text{G GRAPH מכובן המכיל מסלול המילטוני מ- } s \text{ ל- } t \text{ ?}\}$$

**הגדרה 44: מעגל המילטוני**

בහינתן גרף מכובן  $G = (V, E)$ .  
 מעגל המילטוני הוא מסלול מעגלי שעובר כל קודקוד ב-  $G$  בדיקת פעם אחת.

**הגדרה 45: בעית מעגל המילטוני - HAMCYCLE**

קלט: גרף מכובן  $G = (V, E)$ .

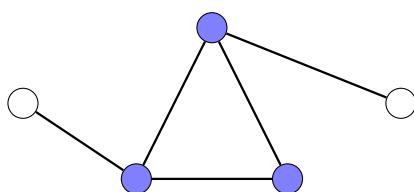
פלט: האם  $G$  מכיל מעגל המילטוני?

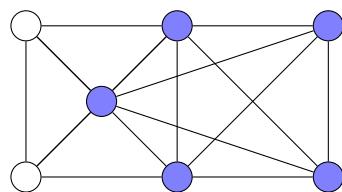
$$HAMCYCLE = \{\langle G \rangle \mid \text{G GRAPH מכובן המכיל מעגל המילטוני.}\}$$

**הגדרה 46: קליקה**

בහינתן גרף לא מכובן  $G = (V, E)$ . קליקה ב-  $G$  היא תת-קבוצה של קודקודים  $C \subseteq V$  כך שלכל שני קודקודים  $u, v \in C$  מתקיים  $(u, v) \in E$ .

קליקה בגודל 3:  $k = 3$ :





קליקה בגודל 5:  $k = 5$

#### הגדרה 47: בעיית הקליקה - CLIQUE

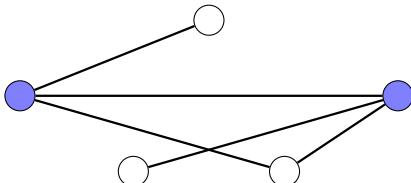
קלט: גרף לא מכוון  $G = (V, E)$  ומספר  $k$ .

פלט: האם  $G$  קליקה בגודל  $k$ ?

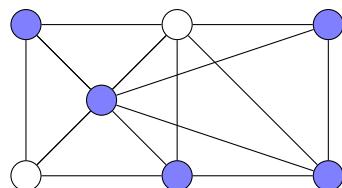
$$\text{CLIQUE} = \{\langle G, k \rangle \mid G \text{ גרף לא מכוון המכיל קליקה בגודל } k\}$$

#### הגדרה 48: כיסוי בקודקודים

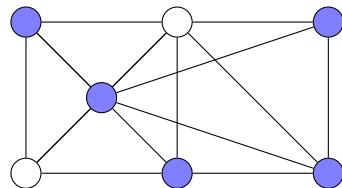
בاهינתן גרף לא מכוון  $G = (V, E)$ , כיסוי בקודקודים ב-  $G$  הוא תת-קבוצה של קודקודים  $C \subseteq V$  כך שלכל צלע  $v, u \in S$  מתקיים  $u \in C$  או  $v \in C$ .



כיסוי בקודקודים בגודל 2:  $k = 2$



כיסוי בקודקודים בגודל 3:  $k = 3$



כיסוי בקודקודים בגודל 4:  $k = 4$

#### הגדרה 49: בעיית VC

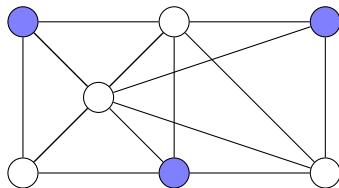
קלט: גרף לא מכוון  $G = (V, E)$  ומספר  $k$ .

פלט: האם קיימים כיסוי בקודקודים ב-  $G$  בגודל  $k$ ?

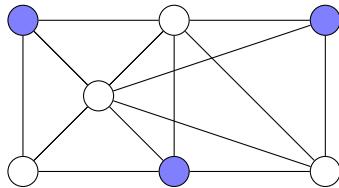
$$\text{VC} = \{\langle G, k \rangle \mid G \text{ גרף לא מכוון המכיל כיסוי בקודקודים בגודל } k\}$$

#### הגדרה 50: קבוצה בלתי תלואה

בاهינתן גרף לא מכוון  $G = (V, E)$ , קבוצה בלתי תלואה ב-  $G$  היא תת-קבוצה של קודקודים  $S \subseteq V$  כך שלכל שני קודקודים  $u, v \in S$  מתקיים  $(u, v) \notin E$ .



קובוצה בלתי תלויה בגודל 3 :  $k = 3$



קובוצה בלתי תלויה בגודל 3 :  $k = 3$

### הגדרה 51: בעיית IS

קלט: גרף לא מכוון  $G = (V, E)$  ומספר  $k$ .

פלט: האם קיימת קבוצה בלתי תלויה ב-  $G$  בגודל  $k$ ?

$$IS = \{ \langle G, k \rangle \mid G \text{ גראף לא מכוון המכיל קבוצה בלתי תלויה בגודל } k \}$$

### הגדרה 52: בעיית PARTITION

קלט: קבוצת מספרים שלמים  $.S = \{x_1, x_2, \dots, x_n\}$ .

פלט: האם קיימת תת-קובוצה  $Y \subseteq S$  כך ש-  $\sum_{y \in Y} y = \sum_{y \in S \setminus Y} y$  ?

$$PARTITION = \left\{ S \mid \sum_{y \in Y} y = \sum_{y \in S \setminus Y} y \text{ קבוצת שלמים, וקיימת תת-קובוצה } S \subseteq Y \text{ כך ש- } \right\}$$

### הגדרה 53: בעיית SubSetSum

קלט: קבוצת מספרים  $.S = \{x_1, x_2, \dots, x_n\}$  ומספר  $t$ .

פלט: האם קיימת תת-קובוצה של  $S$  שסכום איבריה שווה  $t$  ?

$$SubSetSum = \left\{ \langle S, t \rangle \mid \sum_{x \in Y} x = t \text{ קיימת } Y \subseteq S \text{ כך ש- } \right\}$$

**משפט 31:**

$PATH = \{ \langle G, s, t \rangle \mid t \text{-ל-} s \text{ גראף מכיוון המכיל מסלול מ- } G \}$	$\in P$
$RELPRIME = \{ \langle x, y \rangle \mid \gcd(x, y) = 1 \}$	$\in P$
$SAT = \{ \langle \phi \rangle \mid \phi \text{ היא נוסחת CNF ספייקה}$	$\in NP, \in NPC$
$3SAT = \{ \langle \phi \rangle \mid \phi \text{ היא נוסחת 3CNF ספייקה}$	$\in NP, \in NPC$
$IS = \{ \langle G, k \rangle \mid k \text{ גראף לא מכיוון המכיל קליקה בגודל } k \}$	$\in NP, \in NPC$
$CLIQUE = \{ \langle G, k \rangle \mid k \text{ גראף לא מכיוון המכיל קליקה בגודל } k \}$	$\in NP, \in NPC$
$VC = \{ \langle G, k \rangle \mid k \text{ גראף לא מכיוון המכיל כיסוי בקודקודים בגודל } k \}$	$\in NP, \in NPC$
$HAMPATH = \{ \langle G, s, t \rangle \mid t \text{-ל-} s \text{ גראף מכיוון המכיל מסלול המילטוני מ- } G \}$	$\in NP, \in NPC$
$HAMCYCLE = \{ \langle G \rangle \mid G \text{ גראף מכיוון המכיל מעגל המילטוני}$	$\in NP$
$SubSetSum = \left\{ \langle S, t \rangle \mid \sum_{x \in Y} x = t \text{ כך ש- } Y \subseteq S \text{ קיימת}\right\}$	$\in NP$
$\overline{HAMPATH}$	$\in CoNP$
$\overline{CLIQUE}$	$\in CoNP$

**משפט 32: בעיות פתוחות בתורת הסיבוכיות**

- $?P = NP$
- $?CoNP = NP$
- $?CoNP \cap NP = P$

**12 רזוקציות זמן פולינומיאליות****משפט 33: רזוקציות פולינומיאליות**

$SAT$	$\leq_P 3SAT$
$3SAT$	$\leq_P CLIQUE$
$CLIQUE$	$\leq_P IS$
$IS$	$\leq_P VC$
$SubSetSum$	$\leq_P PARTITION$
$HAMPATH$	$\leq_P HAMCYCLE$