

## תוכן העניינים

1	<b>מכונות טיורינג</b>
3	<b>וריאציות של מכונות טיורינג</b>
6	<b>התזה של צ'רצ'-טיורינג</b>
10	<b>אי-כrüיעות</b>
10	<b>מחלקות החישוביות <math>R</math>, <math>RE</math> ו- <math>Co\ RE</math> ותכונותן</b>
11	<b>רذוקציות</b>
13	<b>סיבוכיות</b>
14	<b>רذוקציה פולינומיאלית</b>
14	<b>NP שלמות</b>
15	<b>בעיית הספיקות (<math>SAT</math>)</b>
16	<b>סיווג שפות ידיעות - סיבוכיות</b>
20	<b>רذוקציות זמן פולינומיאליות</b>

## 1 מכונות טיורינג

### הגדרה 1: מכונות טיורינג

מכונת טיורינג (מ"ט) היא שביעה  $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{acc}, q_{rej})$  כאשר:

$\sqcup \notin \Sigma$	קבוצת מצבים סופית ולא ריקה
$\Sigma \cup \{\sqcup\} \subseteq \Gamma$	$Q$ א"ב הקלט סופי א"ב הסרט סופי
$\delta : (Q \setminus \{q_{rej}, q_{acc}\}) \times \Gamma \rightarrow Q \times \Gamma \times \{L, R\}$	פונקציית המעברים מצב התחלתי. מצב מקבל יחיד. מצב דוחה יחיד.
	$q_0$ $q_{acc}$ $q_{rej}$

### הגדרה 2: קונFIGורציה

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

- $\Gamma^* \in u$ : תוכן הסרט לפני הראש (מצד שמאל של הראש).
- $q \in Q$ : המצב הנוכחי של המכונת טיורינג.

- $\Gamma \in \sigma$ : תוכן הסרט במקומות של הראש, כלומר התו הנקרא במקומות הנוכחיים של הראש.
- $\Gamma^* \in \tau$ : תוכן הסרט אחורי הראש (מצד ימין של הראש).

### הגדרה 3: גירה בצעד אחד

תהי  $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{acc}, q_{rej})$  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 בסעיפים לעיל,  $c_1$  עוברם ל-  $c_2$  בצעד אחד בלבד.

### הגדרה 4: גירה בכללי

תהי  $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{acc}, q_{rej})$  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  $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{acc}, q_{rej})$  מכונת טיורינג, ו-  $w \in \Sigma^*$  מחרוזת. אומרים כי  $M$  **מקבלת** את  $w$  אם  $q_0 w \vdash_M^* u$  ואנו יכולים לעבור מ-  $u$  ל-  $v$  באמצעות סדרת הMOVES  $\sigma$ . אומרים כי  $M$  **דוחה** את  $w$  אם לא ניתן לעבור מ-  $u$  ל-  $v$  באמצעות סדרת הMOVES  $\sigma$ .

### הגדרה 6: הכרעה של שפה

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

### הגדרה 7: קבלה של שפה

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

במקרה זה נכתוב ש-  $L(M) = L$ .

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

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

- לכל  $^*\Sigma \in w$  מתקיים  $q_{\text{acc}}f(w) \vdash q_0w$ .

## 2 וריאציות של מכונות טיורינג

### הגדרה 9: מודל חישוב

מודל חישובי = אוסף של מכונות שעבורן מוגדרים המושגים של הכרעה ו渴בלה של שפות.

### הגדרה 10: מודלים שקולים חישובית

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

- קיימת מכונה במודל  $A$  שמקரעה את  $L$  אם וס"מ קיימת מכונה כזו במודל  $B$ .
- קיימת מכונה במודל  $A$  שמקבלת את  $L$  אם וס"מ קיימת מכונה כזו במודל  $B$ .

### הגדרה 11: מכונות שקולות חישובית

שתי מכונות הן שקולות חישובית אם הן מקבלות ודווחות בדיקת אותן המיללים.

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

מודל מכונת טיורינג עם סרט אינסופי לכיוון אחד בלבד (מודל 0) שקול למודל אינסופי בשני הכיוונים (מודל T).

כלומר, לכל שפה  $L$ :

- יש מכונת טיורינג ממודל 0 שמקבלת את  $L$  אם וס"מ יש מכונת טיורינג במודל T שמקבלת את  $L$ .
- יש מכונת טיורינג ממודל 0 שמקרעה את  $L$  אם וס"מ יש מכונת טיורינג במודל T שמקרעה את  $L$ .

### הגדרה 12: מכונת טיורינג מרובת סרטיים

מכונת טיורינג מרובה סרטיים היא שביעייה:

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

כאשר  $Q, \Sigma, \Gamma, q_0, q_{\text{acc}}, q_{\text{rej}}$  מוגדרים כמו מכונת טיורינג עם סרט יחיד (ראו הגדרה 1).

ההבדל היחיד בין מכונת טיורינג עם סרט יחיד לבין מכונת טיורינג מרובה סרטיים הוא הפונקציית המעברים.

עבור מטמ"ס הפונקציית המעברים היא מצורמת הבאה:

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

כאשר  $k$  הוא מספר טבעי השווה למספר הסרטיים של המכונה.

### משפט 2: תכונות של מכונת טיורינג מרובה סרטיים

במכונת טיורינג מרובה סרטיים:

- יתכנו מספר סרטיים.
- מספר הסרטיים סופי וקבוע מראש בזמן בניית המ"ט, ואינו תלוי בקלט או במהלך החישוב.
- לכל סרט יש ראש נפרד.

- הפעולות (תנועה וכתיבה) בכל סרט נעשית בנפרד. בפרט, הראשים יכולים לאוז בכיוונים שונים בסרטים שונים.
- ישנו בקר מרכז 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 לשאול חישובי למודל של מ"ט עם סרט אחד.

**הגדרה 13: מכונת טיורינג אי-דטרמיניסטיבית**

מכונת טיורינג אי-דטרמיניסטיבית (מ"ט א"ד) היא שבעייה

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

כאשר  $Q, \Sigma, \Gamma, q_0, q_{\text{acc}}, q_{\text{rej}}$  מוגדרים כמו במכונת טיורינג דטרמיניסטיבית (ראו הגדרה 1).  $\Delta$  היא פונקציה המעבירים

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

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

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

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

• לכל קונפיגורציה יתכן מספר קונפיגורציות עוקבות.

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

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

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

◦ ריצות שלא עוצרות.

**הגדרה 14: קבלה ודוחיה של מילה ע"י מ"ט אי-דטרמיניסטיבית**

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

•  $N$  מקבלת את  $w$  אם קיים חישוב של  $N$  על  $w$  שmagiu ל慈悲ן מקלט.

•  $N$  דוחה את  $w$  אם כל החישובים של  $N$  על  $w$  עוצרים במצב דוחה.

**הגדרה 15: קבלה ודוחיה של שפה ע"י מ"ט אי-דטרמיניסטיבית**

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

•  $N$  מכירעה את  $L$  אם  $N$  מקבלת את כל המילים ב-  $L$  ודוחה את כל המילים שאינן ב-  $L$ .

•  $N$  מקבלת את  $L$  אם  $N$  מקבלת את כל המילים ב-  $L$  ולא מקבלת את כל המילים שאינן ב-  $L$ .

**משפט 4: מ"ט אי-דטרמיניסטיבית שcolaה למ"ט דטרמיניסטיבית**

לכל מ"ט לא דטרמיניסטיבית קיימת מ"ט אי-דטרמיניסטיביתcolaה.

**הגדרה 16: שפה של מכונת טיורינג אי דטרמיניסטיבית**

השפה של מ"ט א"ד  $N$  היא

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

כלומר:

- אם  $w$  אם קיימת ריצה אחת שבה  $N$  מקבלת את  $w$ .
- אם  $w$  אם בכל ריצה של  $N$  על  $w$ ,  $N$  דוחה או לא עוצרת.

**הגדרה 17: מ"ט אי דטרמיניסטיבית המכירעה שפה  $L$** 

אומרים כי מ"ט אי דטרמיניסטיבית  $N$  מכירעה שפה  $L$  אם לכל  $w \in \Sigma^*$ :

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

**הגדרה 18: מ"ט א"ד המקבלת שפה  $L$** 

אומרים כי מ"ט אי דטרמיניסטיבית  $N$  מקבלת שפה  $L$  אם לכל  $w \in \Sigma^*$ :

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

**משפט 5: שיקולות בין מ"ט א"ד למ"ט דטרמיניסטיבית ב-  $RE$** 

לכל מ"ט א"ד  $N$  קיימת מ"ט דטרמיניסטיבית  $D$  כך ש-

$$L(N) = L(D).$$

כלומר לכל  $w \in \Sigma^*$ :

- אם  $N$  מקבלת את  $w$  קיבל את  $w$ .
- אם  $N$  לא מקבלת את  $w$  לא קיבל את  $w$ .

### 3 התזה של צ'רצ'-טיוורינג

שמות 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 7: סגירות שפות קבילות

- איחוד
- חיתוך
- שרשור
- סגור קlien

#### משפט 6: סגירות שפות כריעות

השפות הכריעות סגורות תחת:

- איחוד
- חיתוך
- משלים
- שרשור
- סגור קlien

#### משפט 8: היחס בין הכרעה לקבלה

עבור כל שפה  $L$  התנאים הבאים מתקיימים.

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

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

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

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

#### הגדרה 19: 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 20: קבלה ודחיה של מחזות 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 21: הקריאה וקבלת של שפות**

עבור שפה  $L$  ותוכנית  $P$  בשפת SIMPLE. נאמר כי

- $P$  מקריאה 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 9: שפת SIMPLE שקופה למכונית טיוריינג**

המודלים של מכונית טיוריינג ותוכניות SIMPLE שקופה.

**משפט 10: 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 22: 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  $(V \cup \Sigma)^*$ ,  $\gamma \in (V \cup \Sigma)^+$ ,  $u \in u$ .

**משפט 11:**

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

מודל חישובי	דקdock	משפחת שפות
מכונית טיוריינג	כללי	קבילות
אוטומט מחסנית	חסר הקשר	חסירות הקשר
אוטומט סופי	רגולרי	רגולריות

**משפט 12:**

כל שפה חסרת הקשר אינה כריעה.

**משפט 13: התזה של צ'רצ' טיוריינג**

התזה של צ'רצ' טיוריינג מודל מ"ט מגלים את המושג האבסטרקטי של "אלגוריתם".  
כלומר, כל אלגוריתם שנitinן לתיאור כתהיליך מכנייסטיubo: שבו:

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

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

**הגדרה 23: 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 24: מכונת טיריניג מרובת סרטים**

מכונת טיריניג מרובה סרטים היא שביעייה:

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

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 הבאה:

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

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

**משפט 14: שקולות בין מ"ט מרובה סרטים למ"ט עם סרט יחיד**

לכל מטמ"ס  $M$  קיימת מ"ט עם סרט יחיד  $M'$  השקול לה  $-M$ .

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

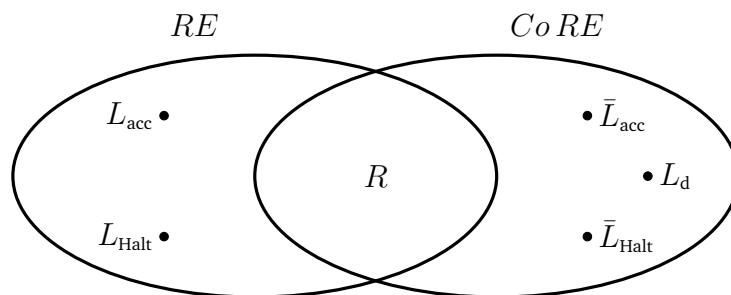
## משפט 15: סיווג שפות ידיעות - חישוביות

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

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

## משפט 16

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

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

## הגדרה 25: 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 26:**

$$\begin{aligned} R &= \{L \subseteq \Sigma^* \mid L \text{ מכיריה את } M\} \\ RE &= \{L \subseteq \Sigma^* \mid L \text{ מקבלת את } M\} \\ Co RE &= \{L \subseteq \Sigma^* \mid \bar{L} \in RE\} \end{aligned}$$

- אוסף השפות הדירות מסומן  $R$  ומוגדר
- אוסף השפות הקבילות מסומן  $RE$  ומוגדר
- אוסף השפות שהמשלימה שלהן קבילה מסומן  $Co RE$  ומוגדר

**משפט 17: סגירות של השפות הדירות והשפות הקבילות**

- (1) איחוד (2) חיתוך (3) שרשור (4) סגור קלין (5) משלים.  
 (1) איחוד (2) חיתוך (3) שרשור (4) סגור קלין.

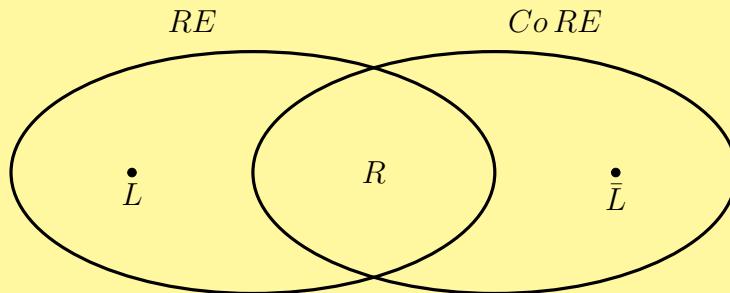
- סגירה תחת:  $R$
- סגירה תחת:  $RE$

**משפט 18: תכונות של השפות החישוביות**

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

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

$RE \cap Co RE = R$  .3

**הגדרה 27: 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 28: מ"ט המחשבת פונקציה**

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

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

**הגדרה 29: מ"ט המחשבת פונקציה**

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

**הגדרה 30: רדוקציה**

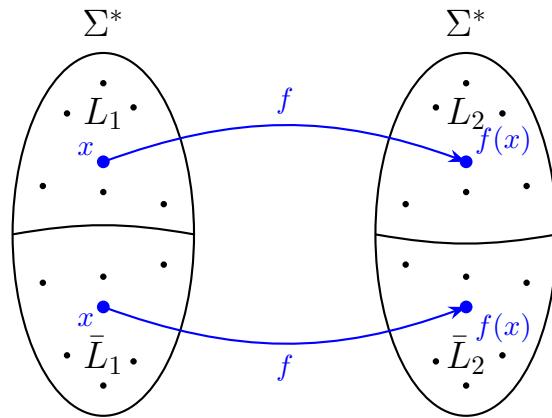
בහינתן שתי שפות  $\Sigma^*$  אומרים כי  $L_1, L_2 \subseteq \Sigma^*$  ניתנת לרדוקציה ל- $L_2$ , ומסמנים  $L_1 \leq L_2$ ,

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 19: משפט הרדוקציה**

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

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

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

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

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

**משפט 20: 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  $L' \not\in R$  מתקיים  $\emptyset \leq L' \leq L$ .

**משפט 21: משפט ריס**

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

- תכונה  $S$  לא טריויאלית 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 31: 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 22: קשר בין סיבוכיות של מ"ט מרובת סרטים ומ"ט סרט יחיד

לכל מ"ט מרובת סרטים  $M$  הרצה בזמן  $(n)^f$ , קיימת מ"ט סרט יחיד  $M'$  השකולה לו-  $M$  ורצה בזמן  $(O(n^2))$ .

### משפט 23: קשר בין סיבוכיות של מ"ט אי-דטרמיניסטי ומ"ט דטרמיניסטי

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

### הגדירה 32: אלגוריתם אימות

אלגוריתם אימות עברו בעיה  $A$  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:

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

### הגדירה 33: המחלקות P ו- NP

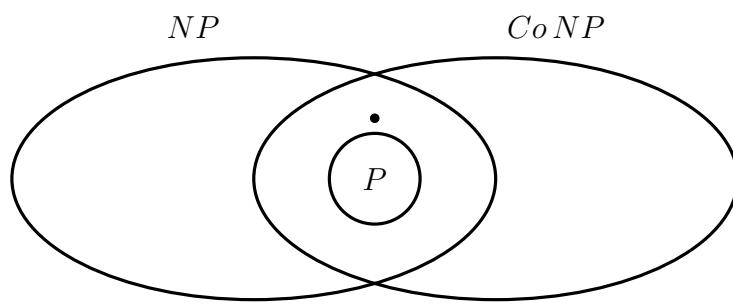
- $\bullet P$  = קבוצת כל השפות שיש להן מ"ט דטרמיניסטי המכריעה אותן בזמן פולינומי.
- $\bullet NP$  = קבוצת כל השפות שיש להן אלגוריתם אימות המאמת אותן בזמן פולינומי.

הגדרה שකולה:

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

### משפט 24: תכונות של P ו- NP

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



## 8 רדוקציה פולינומיאלית

### הגדרה 34: 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 35: 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 25: משפט הרדוקציה

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

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

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

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

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

## 9 NP שלמות

### הגדרה 36: $NP$ - קשה (NP-hard)

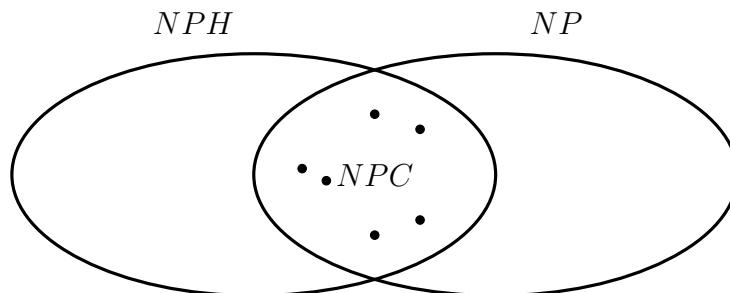
בעיה  $B$  נקראת  $NP$  קשה אם לכל בעיה  $A \in NP$  קיימת רדוקציה  $A \leq_P B$ .

**הגדרה 37:**  $NP$ -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 26:** תכונות של רדוקציה פולינומיאלית

- אם  $\bar{A} \leq_P \bar{B}$  אז  $A \leq_P B$ .
- אם  $A \leq_p C$  ו  $C \leq_p B$  אז  $A \leq_p B$ .

**משפט 27:** טרנזיטיביות של  $NP$ -שלמות

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

## 10 בעית הספיקות ( $SAT$ )

**הגדרה 38:** נוסחת  $CNF$

נוסחת  $CNF$ ,  $\phi$  היא נוסחה בוליאנית מעל  $n$  משתנים  $x_1, x_2, \dots, x_n$  המכילה  $m$  פסוקיות כasher כל פסוקייה מכילה אוסף של ליטרלים (OR) ( $\vee$ ) בוליאני והפסוקיות מחוברות ע"י (AND) 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 39:** 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 40: נוסחת CNF ספיקה**

נוסחת  $CNF$ ,  $\phi$  היא ספיקה אם קיימת השמה של המשתנים  $x_1, x_2, \dots, x_n$  כך ש-  $\phi$  מקבלת ערךאמת 1. ז"א בכל פסקית יש לפחות ליטרל אחד שמקבל את הערךאמת 1.

**הגדרה 41: בעיית SAT**

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

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

**הגדרה 42: בעיית 3SAT**

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

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

**משפט 28:**

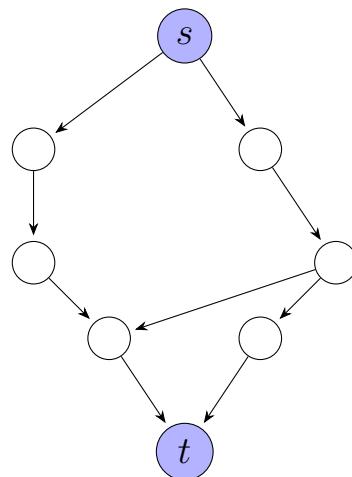
- $SAT \in NP$
- משפט קווקליון:  $SAT \in NPC$
- $3SAT \in NPC$
- $SAT \in P \Leftrightarrow P = NP$

**11 סיווג שפות ידיעות - סיבוכיות****הגדרה 43: בעיית מסלול PATH**

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

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

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

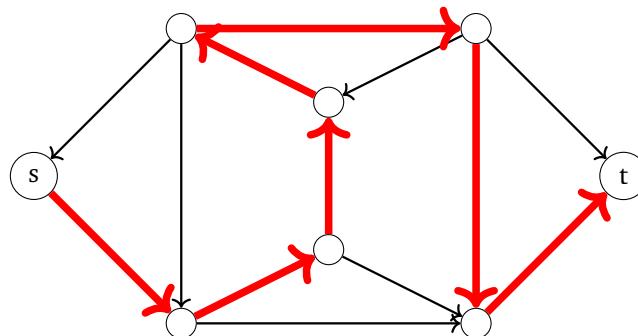


**הגדרה 44: בעיית RELPRIME**קלט: שני מספרים  $x$  ו-  $y$ .פלט: האם  $x$  ו-  $y$  זרים?

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

**הגדרה 45: 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 46: 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-  $t$  ?

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

**הגדרה 47: מעגל המילטוני**

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

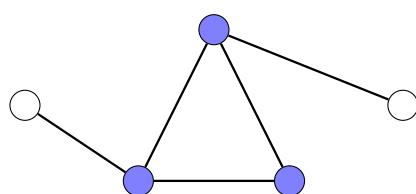
**הגדרה 48: בעית מעגל המילטוני - HAMCYCLE**קלט: גרף מכובן  $G = (V, E)$ .פלט: האם  $G$  מכיל מעגל המילטוני?

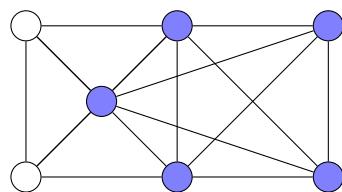
$$HAMCYCLE = \{\langle G \rangle \mid G \text{ גраф מכובן המכיל מעגל המילטוני.}\}$$

**הגדרה 49: 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:





קליקה בגודל 5:  $k = 5$

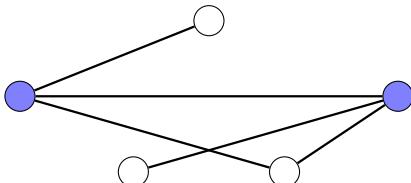
#### הגדרה 50: בעיית הקליקה - CLIQUE

קלט: גראף לא מכוון  $G = (V, E)$  ומספר  $k$ .  
פלט: האם  $G$  קליקה בגודל  $k$  לכל היותר?

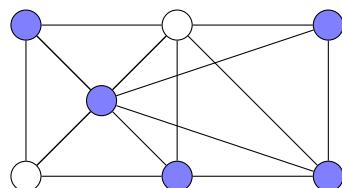
$$\text{CLIQUE} = \{\langle G, k \rangle \mid G \text{ גראף לא מכוון המכיל קליקה בגודל } k \text{ לכל היותר}\}$$

#### הגדרה 51: כיסוי בקודקודים

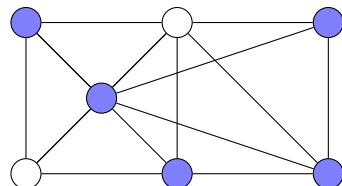
בاهינתן גראף לא מכוון  $G = (V, E)$ , כיסוי בקודקודים ב-  $G$  הוא תת-קובוצה של קודקודים  $C \subseteq V$  כך שלכל צלע  $v, u \in S$  מתקיים  $u \in C$  או  $v \in C$ .



כיסוי בקודקודים בגודל 2:  $k = 2$



כיסוי בקודקודים בגודל 5:  $k = 5$



כיסוי בקודקודים בגודל 5:  $k = 5$

#### הגדרה 52: בעית VC

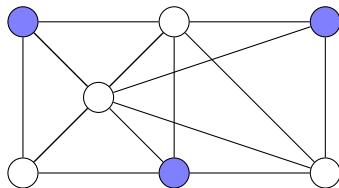
קלט: גראף לא מכוון  $G = (V, E)$  ומספר  $k$ .

פלט: האם קיים כיסוי בקודקודים ב-  $G$  בגודל  $k$  לכל היותר?

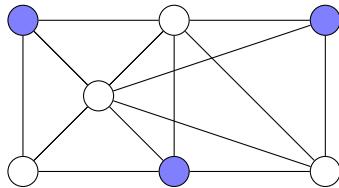
$$\text{VC} = \{\langle G, k \rangle \mid G \text{ גראף לא מכוון המכיל כיסוי בקודקודים בגודל } k \text{ לכל היותר}\}$$

#### הגדרה 53: קבוצה בלתי תלואה

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



קובוצה בלתי תלויה בגודל 3 :  $k = 3$



קובוצה בלתי תלויה בגודל 3 :  $k = 3$

#### הגדרה 54: בעיית IS

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

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

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

#### הגדרה 55: בעיית PARTITION

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

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

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

#### הגדרה 56: בעיית SubSetSum

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

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

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

**משפט 29:**

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

**משפט 30: בעיות פתוחות בתורת הסיבוכיות**

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

**12 רזוקציות זמן פולינומיאליות****משפט 31: רזוקציות פולינומיאליות**

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