<u>תזכורת:</u>
<u>הוכחת NP שלמות</u>

<u>הדרך הישירה:</u>
1. להוכיח שהשפה L היא ב NP.
2. להוכיח שלכל שפה אחרת $L' \in NP$ קיימת רדוקציה פולינומית $L' \le_p L$.

<u>הדרך העקיפה:</u>
1. להוכיח שהשפה L היא ב NP.
2. להוכיח עבור שפה L_2 שהיא NPC.
3. להראות רדוקציה פולינומית $L_2 \le_p L$

<u>בעיית החלוקה:</u>

$$PART = \left\{ x_1,\dots,x_n \mid \exists I : \sum_{i \notin I} x_i = \sum_{i \in I} x_i \right\} \in NPC.$$

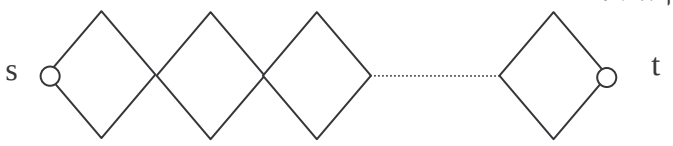
<u>בעיית המסלול הקצר ביותר עם אילוץ מחיר PATH</u>

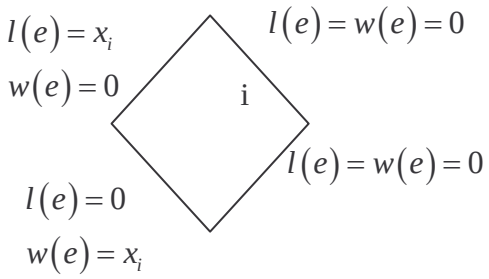
נתון:
1. גרף מכוון $G = (V,E)$
2. שני צמתים $s,t \in V$.
3. לכל קשת $e \in E$: $l(e)$ - אורך הקשת.
4. לכל קשת $e \in E$: $w(e)$ - מחיר הקשת.
5. W, L.

הבעיה: האם קיים מסלול מכוון A מ s אל t כך ש $\sum_{e \in A} w(e) \le W$ וגם $\sum_{e \in A} l(e) \le L$

טענה: $PATH \in NPC$.
הוכחה בדרך העקיפה:
1. $PATH \in NP$ (ננחש מסלול ונבדוק האם הוא מקיים את התנאים).
2. $PART \in NPC$ (ראינו בהרצאה הקודמת).
3. $PART \le_p PATH$.

נתון: $x_1,\dots,x_n$
נבנה את הגרף באופן הבא:





$$W = L = \frac{1}{2}\sum_{i=1}^{n} x_i$$

הרדוקציה היא פולינומית (מספר צמתי הגרף הוא $O(n)$ וכך גם מספר הקשתות).

<u>אבחנה:</u> כל מסלול מ s אל t בוחר בכל מעוין האם להשתמש בקשתות העליונות או התחתונות. ע"פ הבחירה האורך גדל ב x_i והמחיר לא משתנה, או להפך.

<u>תקפות:</u>

נניח שקיימת חלוקה של $x_1,...x_n$. כלומר קיימת קבוצה I כנדרש בהגדרה.

נראה כי קיים מסלול A מ s אל t כנדרש.

לכל $i \in I$, המסלול עובר בחלק העליון של המעוין ה i.

לכל $i \notin I$ המסלול עובר בחלק התחתון של המעוין ה i.

$$\sum_{e\in A} l(e) = \sum_{i\in I} x_i = \frac{1}{2}\sum_{i=1}^{n} x_i = L$$

$$\sum_{e\in A} w(e) = \sum_{i\notin I} x_i = \frac{1}{2}\sum_{i=1}^{n} x_i = W$$

הכיוון השני די ברור: בהינתן מסלול מ s אל t שעומד בדרישות נבנה חלוקה I באופן הבא:
אם המסלול עובר את המעוין ה i בחלקו העליון אז $i \in I$ ואחרת $i \notin I$.

בעיית SAT:

נתון פסוק CNF, φ והשאלה היא האם הוא ספיק. (ההגדרות בתרגול 10)

<u>אבחנה:</u> אם f פונקציה שהקלט שלה הוא n משתנים בוליאניים, אז קיים φ, פסוק CNF, עם לכל היותר 2^n פסוקיות, כל אחת מהן בגודל קטן או שווה ל n.

<u>"הוכחה":</u> לכל השמה x למשתנים,קיימת פסוקית C_x ש x מאפסת וכל השמה אחרת מספקת.

דוגמה: $x = 10011$. הפסוקית המתאימה תהיה $C_x = \overline{x}_1 \vee x_2 \vee x_3 \vee \overline{x}_4 \vee \overline{x}_5$.

$$\varphi = \bigwedge_{x: f(x)=0} C_x$$

<u>מסקנה:</u> אם $n = O(1)$ אז יש ל f פסוק CNF בגודל $O(1)$.

<u>משפט קוק SAT :COOK היא שפה NP-שלמה</u>

הוכחה: נראה שלכל שפה $L \in NP$ קיימת רדוקציה פולינומית $L \le_p SAT$.

הרדוקציה h_L: $w \in L \Leftrightarrow h_L(w) = \varphi \in SAT$

$L \in NP$, לכן קיימת מ"ט א"ד פולי' M_L שרצה זמן החסום ע"י פולינום p_L ו $L(M_L) = L$.

$w \in L \Leftrightarrow$ קיים מסלול מקבל של M_L על w.

$h_L(w) = \varphi \in SAT$ אם קיימת השמה מספקת לפסוק φ.

נראה התאמה דו כיוונית בין השמה למסלול:
ההשמה מספקת אם ורק אם המסלול המתאים לה הוא מסלול מקבל.

נסתכל על הקונפיגורציות של M_L:

טבלת חישוב של M_L על w:

$w = w_1 w_2 \ldots w_n$

כל כניסה בטבלה היא $a \in \Gamma \cup Q$

$t = p_L(|w|)$

נטבלה בגודל $(t+1)(t+1)$.

שורות קצרות נמלא ע"י b.

חישוב שקצר מ t - נשכפל את הקונפיגורציה הסופית.

<u>קבוצת המשתנים:</u>

$\{X_{i,j,a} \mid 0 \le i, j \le t \quad a \in \Gamma \cup Q\}$

$X_{i,j,a} = T$ אמ"מ במקום ה (i, j) של טבלת החישוב שנסתכל עליה מופיע הערך a.

<u>בניית הנוסחה:</u>

$\varphi = \varphi_{start} \wedge \varphi_{accept} \wedge \varphi_{compute} \wedge \varphi_{legal}$

נראה שכל אחת מתתי הנוסחאות היא נוסחת CNF וניתנת לחישוב פולינומי ב $|w|$.

כך נקבל ש φ הוא פסוק CNF הניתן לחישוב פולינומי.

φ_{start} - הקונפיגורציה התחילית של M_L על w.

φ_{accept} - קונפיגורציה מקבלת.

$\varphi_{compute}$ - לכל i ניתן לעבור מהקונפיגורציה C_i לקונפיגורציה C_{i+1}.

φ_{legal} - "תקינות ההשמה".

φ_{start}: משמעות: ערך האמת של φ_{start} יהיה T אם ורק אם השורה 0 של טבלת החישוב מתארת את הקונפיגורציה התחילית של M_L על w.

$$\varphi_{start} = x_{0,0,q_o} \wedge x_{0,1,w_1} \wedge x_{0,2,w_2} \wedge \ldots \wedge x_{0,n,w_n} \wedge x_{0,n+1,b} \wedge \ldots \wedge x_{0,t,b}$$

φ_{start} היא פסוק CNF כי היא אוסף של $t+1$ פסוקיות באורך 1 כל אחת.

היא ניתנת לחישוב פולינומי באורך המילה w.

φ_{accept}: ערך האמת שלה יהיה T אם ורק אם C_t היא קונפיגורציה מקבלת. $\varphi_{accept} = \bigvee_{0 \le j \le t} x_{t,j,q_A}$

זהו פסוק CNF המכיל פסוקית אחת בלבד.

φ_{legal}: ערך האמת שלה יהיה T אם ורק אם לכל כניסה (i,j) בטבלת החישוב, יש a יחיד כך ש $x_{i,j,a}=T$.

$$\varphi_{legal}=\bigwedge_{0\le i,j\le t}\left[\left(\underbrace{\bigvee\left(x_{i,j,a}\right)}_{a\in\Gamma\cup Q}\right)\wedge\left(\bigwedge_{a,b\in\Gamma\cup Q}\left(\left(\overline{x}_{i,j,a}\right)\vee\left(\overline{x}_{i,j,b}\right)\right)\right)\right]$$

$\varphi_{compute}$: בהנחה ש φ_{start} מתקיים:

ערך האמת של $\varphi_{compute}$ הוא T אם ורק אם כל שתי שורות עוקבות הן צעד חוקי של המכונה.

נסתכל על שתי קונפיגורציות עוקבות:

<u>אבחנה 1:</u> בין כל שתי קונפיגורציות עוקבות יש לכל היותר שלושה הבדלים.

<u>מסקנה:</u> טבלת החישוב היא חוקית אם ורק אם כל מלבן בגודל 3X2 הוא חוקי.

x	q	a
q'	x	b

$$\varphi_{compute}=\bigwedge_{0\le i,j}\varphi_{compute}^{\,i,j}$$

$\varphi_{compute}^{\,i,j}$ היא:

א. פונקציה שתלוי ב $O(1)$ משתנים: $x_{i',j',a'}:\begin{pmatrix} i'\in\{i,i+1\}\\ j'\in\{j,j+1,j+2\}\\ a'\in\Gamma\cup Q\end{pmatrix}$

ב. הפונקציה תלוי רק במכונה M_L (קבוע) ולא במילה w.

לכן ע"פ טענה שהוכחנו קודם, יש ל $\varphi_{compute}^{\,i,j}$ פסוק CNF מתאים בגודל $O(1)$ והוא עצמו לא תלוי במילה w. (הגודל בביטים הוא $O(\log|w|)$, האינדקסים i,j)

נותר להראות: h_L היא רדוקציה פולינומית תקפה.

$w\in L$ - לכן קיים חישוב מקבל של M_L על w.

נתבונן בחישוב הזה, ובפרט, כטבלת חישוב. מתוך טבלת החישוב נגדיר השמת אמת למשתנים.

$x_{i,j,a}=T$ אם במקום ה i,j בטבלת החישוב המובטחת כתוב a.

$x_{i,j,a}=T$ אם רשום שם משהו אחר.

השמה זו מספקת את כל אחת מ 4 תתי הנוסחאות ולכן גם את φ.

אם $\varphi\in SAT$ אז יש ל φ השמה המספקת אותה.

בפרט, ההשמה מספקת את φ_{legal} ולכל בכל כניסה i,j יש a יחיד כך ש $x_{i,j,a}=T$.

לכן מתוך ה a-ים הללו, נבנה טבלת בגודל $(t+1)(t+1)$.

ההשמה מספקת גם את $\varphi_{start},\varphi_{compute},\varphi_{accpect}$ ולכן החישוב הזה מתחיל מקונפיגורציה תחילית של M_L על w. מסתיים בקונפיגורציה מקבלת והוא חישוב חוקי. לכן $w\in L$.