4.6.2025 ***מודלים חישוביים***

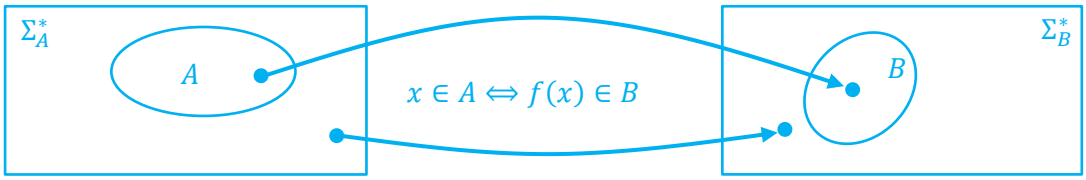
הרצאה 10: SAT היא NP-קשה

Based on previous iterations of this course, given by Nir Bitansky, Rotem Oshman, Iftach Haitner, and Omer Paneth.

מרצה: אורי שטמר

תזכורות:

- $\boldsymbol{P}$ = אוסף כל הבעיות שניתנות להכרעה בזמן פולינומי ע"י מ"ט דטרמיניסטית
- $\boldsymbol{NP}$ = אוסף כל הבעיות שניתנות לפתרון בזמן פולינומי ע"י מטל"ד
- **ראינו הגדרה אלטרנטיבית ל $\boldsymbol{NP}$ שאומרת:** $L \in NP$ אם"ם יש ל- L מוודא פולינומי
- **מוודא פולינומי עבור שפה $\boldsymbol{L}$:** מ"ט V המקיימת: **(א)** לכל $x \in L$ קיים $w \in \Sigma^*$ כך ש- $V(x,w)$ מקבל; **(ב)** לכל $x \notin L$ ולכל $w \in \Sigma^*$ מתקיים ש- $V(x,w)$ דוחה; **(ג)** זמן ריצת $V(x,w)$ פולינומי ב $|x|$ בלבד, מה שאומר שבה"כ נוכל להניח כי $|w|$ הוא פולינומי ב $|x|$
- **רדוקציה פולינומית:** זוהי רדוקציית מיפוי החשיבה בזמן פולינומי. בציור:



- **פסוק CNF:** הוא נוסחה מהצורה $\phi = (x_1 \vee \bar{x}_2 \vee x_3) \wedge (\bar{x}_3 \vee x_5 \vee x_6 \vee \bar{x}_7) \wedge (x_3 \vee \bar{x}_2)$
- **ראינו שפות:**

$$SAT = \{\phi : \text{ספיקה CNF היא נוסחת } \phi\}$$
$$CLIQUE = \{\langle G,k\rangle : \text{ גרף לא מכוון עם קליק בגודל } k\ G\}$$
$$IS = \{\langle G,k\rangle : \text{ גרף לא מכוון עם קב' ב"ת בגודל } k\ G\}$$

- **ראינו רדוקציות:** $SAT \leq_p 3SAT$ וגם $IS \leq_p CLIQUE$
- **NPC:** שפה L היא *NP*-קשה אם לכל $L' \in NP$ מתקיים $L' \leq_p L$.
  שפה L היא *NP*-שלמה אם היא *NP*-קשה וגם $L \in NP$.

<u>משפט (קוק-לוין):</u> SAT היא NP-קשה.

<u>הוכחה:</u>
תהי שפה $A \in NP$ ונראה $A \leq_p SAT$.

$A \in NP \Longleftarrow$ יש ל A מוודא פולינומי $V = (Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r)$.
כלומר מ"ט V כך ש:
(א) קיים פולינום p כך שלכל x, w זמן הריצה של $V(x,w)$ לכל היותר $p(|x|)$
(ב) כל $x \in L$ קיים w כך ש- $V(x,w) = 1$. בה"כ $|w| \leq p(|x|)$.
(ג) לכל $x \notin L$ ולכל w מתקיים $V(x,w) = 0$

<u>רעיון הרדוקציה:</u> נראה רדוקציה פולינומית f אשר בהינתן קלט x מחזירה פסוק $f(x) = \varphi_x$ עם התכונה הבאה:

תהיה "התאמה" בין הצבה מספקת ל φ_x לבין עד w כך ש- $V(x,w) = 1$

כלומר, נבנה את φ_x בצורה המאפשרת לנו לתרגם השמה מספקת ל φ_x לעד w המקיים $V(x,w) = 1$ וגם להיפך, כלומר מאפשרת לנו לתרגם עד w כך ש- $V(x,w) = 1$ להשמה מספקת עבור φ_x.

לכן נקבל ש-

$$x \in A \iff \text{קיים } w \text{ עבורו } V(x,w)=1 \iff \text{קיימת השמה המספקת את } \varphi_x \iff \varphi_x \in SAT$$

שימו לב: בזמן חישוב הרדוקציה, כאשר אנחנו מתרגמים את x ל- φ_x, אנחנו לא יודעים אם $x \in A$ או לא (ואנחנו לא יודעים אם קיים עד w מתאים או לא). לכן התיאור של הפסוק φ_x לא יכול להיות תלוי בשום w ספציפי. מה שכן יתקיים זה שכל השמה מספקת ל φ_x יהיה אפשר לתרגם לעד מתאים w. כלומר כל השמה מספקת ל φ_x "מקודדת" איזשהו עד w כך ש- $V(x,w)=1$.

יהיו x, w קלטים עבור V. נסמן $t = p(|x|) + 1$. נייצג חישוב של V על (x,w) ע"י טבלה:
(פורמלית צריך את ה *+1* הזה כדי שהאינדקסים בהמשך יהיו נכונים, אבל בוא נתעלם מזה...)

	$j=0$	$j=1$									$j=t$
$i=0$	#	q_0	x_1	x_2	$\cdots$	x_n	,	w_1	w_2	$\cdots$	w_ℓ
$i=1$	#	c_1									
$i=2$	#	c_2									
		$\vdots$									
$i=t$	#	c_t									

- השורה הראשונה בטבלה הזאת היא הקונפיגורציה ההתחלתית c_0 של V על x, w.
- השורה השניה היא הקונפ' c_1 ש V עוברת אליה בצעד אחד מ c_0, וכן הלאה.
- לכל הקונפיגורציות שלנו אנחנו מוסיפים # בצד שמאל.

<u>הנחה משפטת:</u> בלי הגבלת הכלליות אנחנו יכולים להניח שהמטריצה הזאת היא <u>ריבועית</u> בגודל $(t+1)\times(t+1)$.

איך אפשר להניח את זה?

- **לגבי הגובה:** אנחנו יודעים ש V מבצעת לכל היותר $t = p(|x|)$ צעדים. לשם פשטות נניח שיש בדיוק t צעדים. פורמלית, נניח בה"כ כי פונק' המעברים δ מוגדרת גם עבור מצב מקבל/דוחה באופן הבא:
$$\forall a \in \Gamma:\ \ \delta(q_a, a) = (q_a, a, R)\ \ ,\ \ \delta(q_r, a) = (q_r, a, R)$$
- **לגבי הרוחב:** המכונה מבצעת t צעדים ולכן הראש הקורא/כותב לעולם לא מגיע מעבר לתו ה t, כלומר לעולם לא מגיע מעבר לתו ה $\ell = t - n - 1$ של w (כי לפני w יש n תווים של x ועוד פסיק). לכן אפשר להניח ש- $|w| \leq \ell$. לשם פשטות נניח שמתקיים $|w| = \ell$ בדיוק (אחרת אפשר לרפד אותו בתו מיוחד ש V תתייחס אליו כמו ␣).

<u>הגדרה:</u>

$\Delta = \Gamma \cup Q \cup \{\#\}$ — התווים שיכולים להופיע בטבלה

נשים לב כי הגודל של Δ לא תלוי בגודל הקלט $n = |x|$. כלומר $|\Delta| = O(1)$.

<u>שימו לב:</u> בזמן חישוב הרדוקציה אנחנו יודעים את V (כי אנחנו מראים רדוקציה $SAT \leq_p A$ ו- V הוא המוודא הפולינומי של A) ואנחנו יודעים את x (הוא הקלט של הרדוקציה; אותו אנחנו אמורים לתרגם לפסוק CNF). אבל אנחנו לא יודעים את w.

לפסוק שנבנה φ תהיה את התכונה שכל הצבה המספקת אותו מתאימה לטבלה (t+1)x(t+1) כנ"ל כך שמתקיים: (א) השורה הראשונה שלה היא הקונפ' ההתחלתית של V על x ועל <u>איזשהו</u> w; (ב) כל שורה היא הקונפ' החוקית שעוברים אליה מהשורה הקודמת; (ג) הקונפיגורציה האחרונה היא קונפ' מקבלת.

משתנים:
לכל $0 \leq i, j \leq t$ יהיו משתנים שיקודדו את תוכן התו ה (i, j) בטבלה.
כיוון שישנם $|\Delta|$ משתנים אפשריים, לכל i, j ולכל $\sigma \in \Delta$ נגדיר משתנה $z_{i,j,\sigma}$
כלומר הגדרנו $O(t^2 \cdot |\Delta|) = O(t^2)$ משתנים.

(אינטואיציה: $z_{i,j,\sigma} = T$ אם"ם התו ה i, j בטבלה הוא σ)

הפסוק שנבנה $f(x) = \varphi_x$ יכיל 4 חלקים:
1. φ_{cell} – בכל מקום בטבלה רשום <u>בדיוק</u> תו אחד
2. φ_{init} – הקונפ' הראשונה היא קונפ' התחלתית של V על x, w עבור w <u>כלשהו</u> (בזמן בניית הרדוקציה אנחנו יודעים את x אבל לא יודעים את w)
3. φ_{accept} – החישוב מסתיים במצב מקבל, כלומר בקונפ' האחרונה המצב הוא q_a
4. φ_{move} – החישוב מתאר סדרה של קונפ' $c_0, c_1, \ldots, c_t$ כך ש- V עוברת בכל צעד מ c_i ל c_{i+1}

הערה: 1,2,3 לא תלויים בכלל בשפה A. רק 4 מתייחס למ"ט V.

תיאור φ_{cell}:

$$\varphi_{\text{cell}} = \bigwedge_{0 \le i,j \le t} \varphi_{\text{cell},i,j}$$

$$\varphi_{\text{cell},i,j} = \underbrace{\left(\bigvee_{\sigma \in \Delta} z_{i,j,\sigma}\right)}_{\text{רשום לפחות תו אחד}} \wedge \underbrace{\left(\bigwedge_{\substack{\sigma_1,\sigma_2 \in \Delta \\ \sigma_1 \neq \sigma_2}} \left(\overline{z_{i,j,\sigma_1}} \vee \overline{z_{i,j,\sigma_2}}\right)\right)}_{\text{לא רשומים שני תווים}}$$

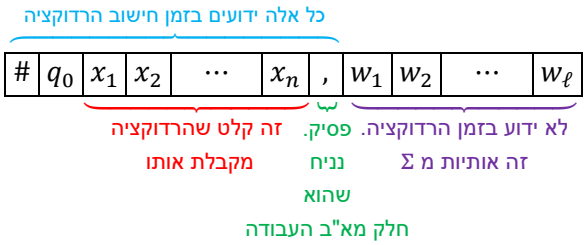
זהו פסוק CNF בגודל

$$O(\underbrace{t}_{\text{לכל } i} \cdot \underbrace{t}_{\text{לכל } j} \cdot \underbrace{|\Delta|^2}_{\text{קבוע}}) = O(t^2)$$

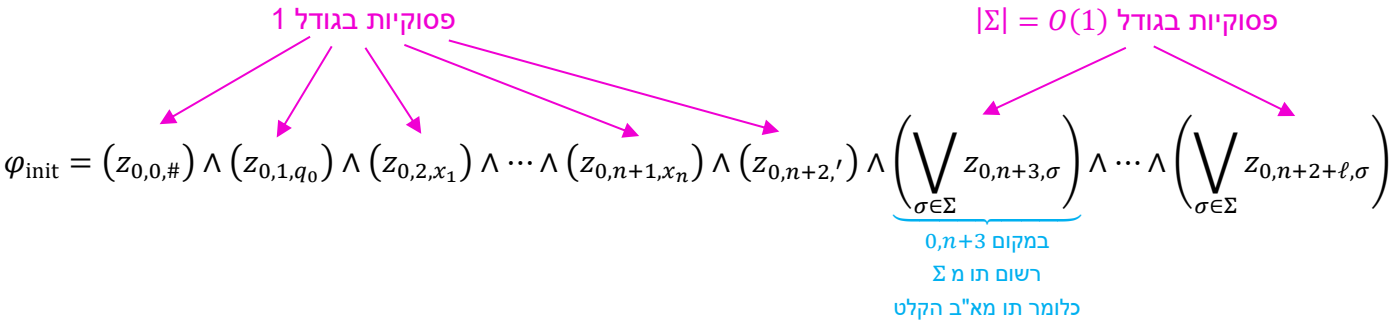
<u>טענה 1:</u> הצבה מספקת את φ_{cell} אם"ם היא מתאימה לטבלה בה בכל מקום רשום בדיוק תו אחד.

תיאור φ_{init}:

אנחנו רוצים לדרוש שהשורה הראשונה בטבלה מתאימה לקונפ' ההתחלתית של V על x ועל w כלשהו:



נגדיר:



זהו פסוק CNF בגודל $O(t)$.

<u>טענה 2:</u> הצבה מספקת את $\varphi_{\text{cell}} \wedge \varphi_{\text{init}}$ אם"ם היא מתאימה לטבלה בה בכל מקום רשום בדיוק תו אחד והשורה הראשונה מתאימה לקונפ' ההתחלתית של V על x ועל $w \in \Sigma^\ell$ כלשהו.

תיאור φ_{accept}:

אנחנו רוצים לדרוש שבקונפ' האחרונה המצב הוא q_a:

$$\varphi_{\text{accept}} = \underbrace{\left(\bigvee_{1 \le j \le t} z_{t,j,q_a} \right)}_{\text{כלומר לפחות אחד מהתווים בשורה האחרונה הוא } q_a}$$

φ_{accept} היא <u>פסוקית</u> בגודל $O(t)$.

<u>טענה 3:</u> הצבה מספקת את $\varphi_{\text{cell}} \wedge \varphi_{\text{accept}}$ אם"ם היא מתאימה לטבלה בה בכל מקום רשום בדיוק תו אחד ובשורה האחרונה מופיע המצב q_a.

החלק העיקרי של הרדוקציה – תיאור φ_{move}:

נגדיר

$$\varphi_{\text{move}} = \bigwedge_{0 \le i \le t} \varphi_{\text{move},i}$$

כאשר $\varphi_{\text{move},i}$ יקודד את הדרישה: אם ההצבה לשורה i מתאימה לקונפ' c_i אז ההצבה לשורה $i+1$ מתאימה לקונפ' c_{i+1} ש- V עוברת אליה בצעד אחד מ c_i.

<u>תזכורת:</u> אם V עוברת מ c_i ל c_{i+1} אז רוב התווים ב c_i, c_{i+1} יהיו זהים. רק התווים באזור הראש יכולים להשתנות. לדוגמה:

אם $\delta(q,a) = (q',b,R)$ אז

$\cdots$	q	a	$\cdots$
$\cdots$	b	q'	$\cdots$

אם $\delta(q,a) = (q',b,L)$ אז

$\cdots$	c	q	a	$\cdots$
$\cdots$	q'	c	b	$\cdots$

בכל מקרה, התו במקום ה $(i+1,j)$ נקבע מתוך התווים במקומות $(i,j+2),(i,j+1),(i,j),(i,\text{-}1)$. בציור:

$(i,\text{-}1)$	(i,j)	$(i,j+1)$	$(i,j+2)$
	$(i+1,j)$		

אם התווים במקומות $(i,j+1),(i,j),(i,\text{-}1)$ לא מכילים את המצב, אז התו במקום $(i+1,j)$ שווה לתו במקום (i,j). אחרת הוא יכול להשתנות (לפי פונק' המעברים), אבל בכל מקרה תלוי רק במקומות $(i,j+2),(i,j+1),(i,j),(i,\text{-}1)$.

<u>הגדרה:</u> חמישיית תווים $(\sigma_1,\sigma_2,\sigma_3,\sigma_4,\sigma_5)$ היא <u>חמישייה חוקית</u> אם כאשר במקומות $(i,j),(i,j+1),(i,j+2),(i,j-1)$ רשומים $\sigma_1,\sigma_2,\sigma_3,\sigma_4$ בהתאמה אז במקום $(i+1,j)$ צריכים לרשום σ_5.

נתחיל מלכתוב את φ_{move} בצורה לא תקינה (לא בפורמט CNF):

$$\varphi_{\text{move},i} = \bigwedge_{0\le j\le t} \varphi_{\text{move},i,j}$$

$$\varphi_{\text{move},i,j} = \bigwedge_{\substack{(\sigma_1,\sigma_2,\sigma_3,\sigma_4,\sigma_5)\\ \text{היישימח תיקוח}}} \left[\left(z_{i,j-1,\sigma_1} \wedge z_{i,j,\sigma_2} \wedge z_{i,j+1,\sigma_3} \wedge z_{i,j+2,\sigma_4} \right) \longrightarrow z_{i+1,j,\sigma_5} \right]$$

איך אנחנו יכולים לתרגם דרישת "אם אז" כזאת לפסוק CNF?
בצורת CNF הפסוק $A \longrightarrow B$ שקול ל $\overline{A} \vee B$
מדוע? כאשר הפסוק $\overline{A} \vee B$ מסתפק אנחנו יודעים:

- אם $A = T$ אז גם $B = T$
- אם $A = F$ אז B יכול להיות או T או F.

נקבל

$$\varphi_{\text{move},i,j} = \bigwedge_{\substack{(\sigma_1,\sigma_2,\sigma_3,\sigma_4,\sigma_5)\\ \text{היישימח תיקוח}}} \left(\overline{z_{i,j-1,\sigma_1}} \vee \overline{z_{i,j,\sigma_2}} \vee \overline{z_{i,j+1,\sigma_3}} \vee \overline{z_{i,j+2,\sigma_4}} \vee z_{i+1,j,\sigma_5} \right)$$

<u>טענה 4:</u> תהי y הצבה למשתני φ_x המתאימה לְקונפ' c_i. ההצבה הזאת מספקת את $\varphi_{\text{cell}} \wedge \varphi_{\text{move},i}$ אם"ם היא מתאימה לְקונפ' c_{i+1} ש- V עוברת אליה בצעד אחד מ c_i.

<u>הוכחת טענה 4:</u>
נראה רק את אחד הכיוונים, הכיוון השני דומה: נניח כי ההצבה מספקת את $\varphi_{\text{cell}} \wedge \varphi_{\text{move},i}$ ונראה שהיא מתאימה לקונפ' c_{i+1} ש- V עוברת אליה בצעד אחד מ c_i.
לכל j נסתכל על התווים $\sigma_1,\sigma_2,\sigma_3,\sigma_4$ שרשומים במקומות $j-1,\dots,j+2$ בקונפ' ה i בהתאמה.
אנחנו מניחים שההצבה מתאימה לקונפ c_i ולכן $z_{i,j-1,\sigma_1} = z_{i,j,\sigma_2} = z_{i,j+1,\sigma_3} = z_{i,j+2,\sigma_4} = T$.
בנוסף, אנחנו מניחים שההצבה מספקת את $\varphi_{\text{move},i}$ ולכן על פי הגרירה נקבל $z_{i+1,j,\sigma_5} = T$ עבור התו המתאים ב c_{i+1}.
מכיוון שההצבה מספקת את φ_{cell} אז זהו התו היחיד עבור המקום ה $(i+1,j)$ שמקבל ערך T.
כלומר בכל מקום ב c_{i+1} רשום התו הנכון.

מה הגודל של φ_{move}?

$$|\varphi_{\text{move}}| = t^2 \cdot |\varphi_{\text{move},i,j}| = t^2 \cdot O(\Delta^4) = t^2 \cdot O(1)$$

לכל תו אחד שמתאים לה — לכל רביעייה יש לנו

Δ הוא קבוע

לכן

$$|\varphi_{\text{move}}| = O(t^2)$$

<u>מסקנה 5:</u> הצבה מספקת את $\varphi_{\text{cell}} \wedge \varphi_{\text{init}} \wedge \varphi_{\text{move}}$ אם"ם **(א)** היא מתאימה לטבלה בה בכל מקום רשום בדיוק תו אחד; וגם **(ב)** השורה הראשונה מתאימה לְקונפ' ההתחלתית c_0 של V על x ועל $w \in \Sigma^{\ell}$ כלשהו; וגם **(ג)** לכל $i \in [t-1]$, השורה ה $i+1$ מתאימה לְקונפ' c_{i+1} ש- V עוברת אליה בצעד אחד מ c_i.

הוכחת מסקנה 5 היא באינדוקציה: בסיס טענה 2 (לגבי φ_{init}) וצעד טענה 4 (לגבי $\varphi_{\text{move},i}$)

<u>בסך הכל:</u> הצבה מספקת את $f(x) = \varphi_x = \varphi_{\text{cell}} \wedge \varphi_{\text{init}} \wedge \varphi_{\text{accept}} \wedge \varphi_{\text{move}}$ אם"ם ההצבה מתאימה לחישוב <u>מקבל</u> של V על x ועל איזשהו w, מה שאפשרי אם"ם $x \in A$.

אורך הפסוק הוא פולינומי, $|\varphi_x| = O(t^2)$, והתיאור של φ_x מראה איך לבנות אותו בזמן פולינומי.

מ.ש.ל. (משפט קוק-לוין)

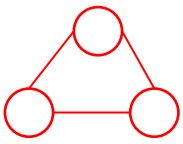
איפה אנחנו עומדים? ראינו ש SAT היא NP-קשה. כבר ראינו רדוקציה מ SAT ל 3SAT מה שמוכיח שגם 3SAT היא NP-קשה. עכשיו נראה רדוקציות נוספות

<u>טענה:</u> $3SAT \leq_p IS$

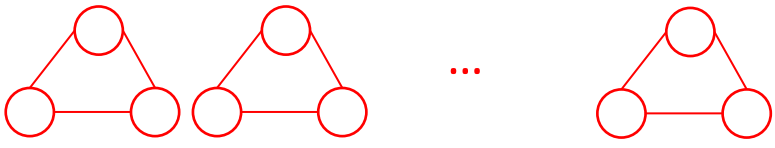
<u>מסקנה:</u> $IS, CLIQUE \in NPC$ (זכרו כי בשיעור שעבר ראינו ש- $IS \leq_p CLIQUE$)

<u>הוכחת הטענה:</u>

<u>הרעיון:</u> נסתכל על גרפים מהצורה



בגרף כזה 1 הוא גודל מקסימלי של קבוצה בלתי תלויה. עכשיו נסתכל על:



אם יש m משולשים אז יש קבוצה ב"ת בגודל m. אין קבוצה ב"ת בגודל $m+1$. כל קבוצה ב"ת בגודל m תכיל בדיוק צומת אחד מכל משולש.

תיאור הרדוקציה מ- *3SAT* ל- *IS*:

<u>קלט:</u> φ = פסוק *3CNF*. נניח כי $\varphi = \bigwedge_{i=1}^{m} c_i$ כאשר $c_i = (\ell_{i,1} \vee \ell_{i,2} \vee \ell_{i,3})$.

נבנה גרף $G = (V, E)$ עם $3m$ צמתים:

$$V = \{v_{1,1}, v_{1,2}, v_{1,3}, v_{2,1}, v_{2,2}, v_{2,3}, \dots, v_{m,1}, v_{m,2}, v_{m,3}\}$$

וקשתות $E = E_1 \cup E_2$ כאשר

קשתות משולשים

$$E_1 = \{(v_{i,1}, v_{i,2}), (v_{i,1}, v_{i,3}), (v_{i,2}, v_{i,3}) : 1 \le i \le m\}$$

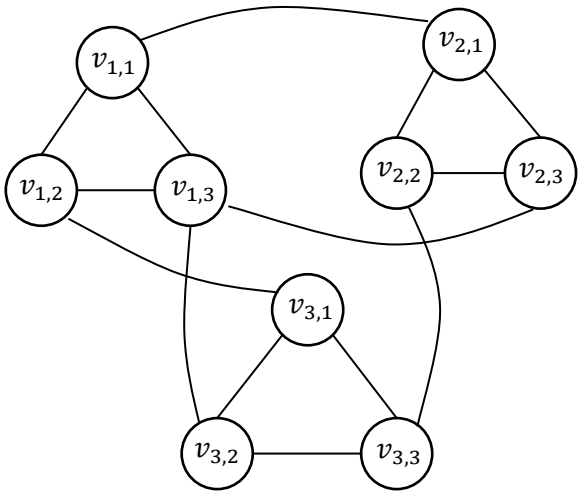
קשתות עקביות

$$E_2 = \left\{ (v_{i_1,j_1}, v_{i_2,j_2}) : \begin{array}{c} \text{קיים משתנה } x_k \text{ כך ש} \\ \ell_{i_1,j_1} = x_k \\ \text{וגם } \ell_{i_2,j_2} = \overline{x}_k \end{array} \right\}$$

ופלט הרדוקציה יהיה $f(\varphi) = (G, m)$

דוגמה: עבור קלט $\varphi = (\underbrace{x_1}_{\text{מתאים } v_{1,1} \text{ ל}} \vee x_2 \vee \overline{x_3}) \wedge (\underbrace{\overline{x_1}}_{\text{מתאים } v_{2,1} \text{ ל}} \vee x_4 \vee x_3) \wedge (\overline{x_2} \vee x_3 \vee \underbrace{\overline{x_4}}_{\text{מתאים } v_{3,3} \text{ ל}})$

נחזיר $f(\varphi) = (G, 3)$ עבור הגרף



מתיאור הרדוקציה ניתן לבנות אותה בצורה יעילה.

(צריך לעבור על כל הפסוק ולבנות את המשולשים, ואח"כ לכל x_i לעבור על הפסוק ולראות איפה הוא מופיע פעם כ x_i ופעם כ $\overline{x}_i$ ולהוסיף קשתות במידת הצורך)

נכונות הרדוקציה:

<u>כיוון 1: נניח כי $\varphi \in 3SAT$.</u>
לכן קיימת הצבה המספקת את φ, כלומר בכל פסוקית c_i קיים לפחות ליטרל אחד ℓ_{i,j_i} שמסתפק.
נגדיר קבוצה:

$$I = \{v_{i,j_i} : 1 \le i \le m\}$$

זאת קבוצה בגודל m. נראה שהיא ב"ת:

- בחרנו צומת אחד מכל משולש ולכן אין קשתות משולש בין 2 צמתים בקבוצה.
- מכיוון שכל ליטרל ℓ_{i,j_i} מסתפק לא יתכן ש- $\ell_{i,j_i} = x_k$ וגם $\ell_{i',j_{i'}} = \overline{x}_k$ ולכן אין בין הצמתים קשתות עקביות.

כלומר I היא קבוצה ב"ת בגודל m בגרף G ולכן $f(\varphi) = (G, m) \in IS$.

<u>כיוון 2: נניח $f(\varphi) = (G, m) \in IS$</u>
כלומר קיימת קבוצה ב"ת I בגרף G בגודל m.
I מכילה לכל היותר צומת אחד מכל משולש ולכן מכילה <u>בדיוק</u> צומת אחד מכל משולש (מכיוון שיש m משולשים).

נגדיר הצבה ל- φ ונוכיח שהיא מספקת:

- לכל $v_{i,j} \in I$: אם $\ell_{i,j} = x_k$ אז נגדיר $x_k = T$
  אם $\ell_{i,j} = \overline{x}_k$ אז נגדיר $x_k = F$
- אם x_k לא קיבל ערך אזי בצורה שרירותית נגדיר $x_k = T$.

ההצבה הזאת מוגדרת הייטב, כלומר לא ייתכן שהצבנו $x_k = T$ וגם $x_k = F$, כי אחרת הייתה קשת בין שני הצמתים שגרמו להצבות האלה בסתירה לכך ש- I קבוצה ב"ת.

ההצבה הנ"ל מספקת כל פסוקית: לכל i קיים j כך ש- $v_{i,j} \in I$, כלומר הליטרל $\ell_{i,j}$ מופוע ב- c_i ומסתפק בהצבה.

כלומר ההצבה מספקת כל פסוקית c_i ולכן מספקת את $\varphi = \bigwedge_{i=1}^{m} c_i$ ולכן $\varphi \in SAT$.

בעיית ***Subset Sum (SUSU)***

הקלט הוא אוסף של מספרים $a_1, a_2, \dots, a_k \in \mathbb{N}$ ומספר נוסף $t \in \mathbb{N}$. השאלה היא האם יש תת קבוצה של ה-a_i-ים שסכומה הוא בדיוק t. פורמלית,

$$\text{SubsetSum} = \left\{ (A,t) \ : \begin{array}{c} t \in \mathbb{N} \text{ and } A \subseteq \mathbb{N} \text{ is a multiset} \\ \text{such that } \exists B \subseteq A \text{ satisfying} \\ \sum_{a \in B} a = t \end{array} \right\}$$

דוגמאות:

$$(\{2,3,7\},5) \in \text{SubsetSum}$$

$$(\{2,3,3,7\},9) \in \text{SubsetSum}$$

$$(\{2,3,7\},6) \notin \text{SubsetSum}$$

הבעיה בבירור ב- NP (העד הוא הקבוצה B...)
נראה שהיא גם NP-קשה בעזרת רדוקציה מ 3SAT.

<u>טענה:</u> $3SAT \leq_p Subsetsum$

<u>הוכחה:</u>
נראה הרדוקציה f אשר בהינתן קלט φ שהוא פסוק 3CNF מחזירה קלט עבור SUSU כלומר מחזירה קבוצה A ומספר t.

נניח כי ל φ יש n משתנים $x_1, \dots, x_n$ ויש m פסוקיות $c_1, \dots, c_m$.

נבנה מולטיסט A המכילה $2n+2m$ מספרים בבסיס עשרוני (כ"א עם $n+m$ ספרות) באופן הבא:

- לכל ליטרל $z \in \{x_i, \overline{x_i}\}$ נגדיר מספר u_z כך שכל הספרות שלו הם 0 פרט ל:
  - הספרה ה- i היא 1
  - לכל פסוקית c_j אשר הליטרל z מופיע בה, הספרה ה- $(n+j)$ היא 1
- לכל פסוקית c_j נגדיר v_j כך שהספרה ה $(n+j)$ היא 1 ושאר הספרות 0
- נגדיר $A = \{u_{x_1}, u_{\overline{x_1}}, \dots, u_{x_n}, u_{\overline{x_n}}, v_1, v_1, v_2, v_2, \dots, v_m, v_m\}$

נגדיר t כך ש- n הספרות הראשונות הן 1 ו- m הספרות האחרונות הן 3

פלט הרדוקציה: $f(\varphi) = (A, t)$

לדוגמה, עבור $\varphi = (x_1 \vee \overline{x_2} \vee x_3) \wedge (x_2 \vee \overline{x_3} \vee x_4)$
הרדוקציה שלנו תחזיר A עם 8 מספרים ומספר נוסף t המוגדרים באופן הבא:

	1	**2**	**3**	**4**	**5**	**6**
u_{x_1}	1	0	0	0	1	0
$u_{\overline{x_1}}$	1	0	0	0	0	0
u_{x_2}	0	1	0	0	0	1
$u_{\overline{x_2}}$	0	1	0	0	1	0
u_{x_3}	0	0	1	0	1	0
$u_{\overline{x_3}}$	0	0	1	0	0	1
u_{x_4}	0	0	0	1	0	1
$u_{\overline{x_4}}$	0	0	0	1	0	0
v_1	0	0	0	0	1	0
v_1	0	0	0	0	1	0
v_2	0	0	0	0	0	1
v_2	0	0	0	0	0	1
t	1	1	1	1	3	3

<u>הוכחת נכונות:</u>

<u>כיוון ראשון:</u>

נניח ש- φ ספיק. ניקח השמה מספקת ל $x_1, \dots, x_n$ ונבנה ממנה תת-קבוצה B שתפתור את SUSU:

- לכל ליטרל z, נוסיף את u_z ל- B אם"ם z מסתפק.
- לכל פסוקית c_j, נסמן ב $1 \le s_j \le 3$ את מספר הליטרלים שמסתפקים ב- c_j. זהו מספר בין 1 ל 3 כי יש לפחות ליטרל אחד מסופק (כי ההשמה מספקת) ויש לכל היותר 3 כי יש 3 ליטרלים בפסוקית.
- נוסיף $0 \le 3 - s_j \le 2$ עותקים של v_j ל- B.

מהבניה נובע ש- $t = \sum_{a \in B} a$.

- עבור כל אחת מ n העמודות הראשונות לקחנו בדיוק ליטרל אחד ולכן סכום כל עמודה כזאת הוא 1. עבור כל אחת מ m העמודות האחרונות, השלמנו את הסכום ל 3 בעזרת המשתנים v_j, v_j'

<u>כיוון שני:</u>

נניח קיימת $B \subseteq A$ שסכומה הוא $t = 1^n 3^m$. נגדיר השמה המספקת את φ באופן הבא: לכל $i \in [n]$ נגדיר $x_i = T$ אם"ם $u_{x_i} \in B$.

מדוע זאת השמה מספקת?

- לכל $i \in [n]$, מכיוון שהספרה ה- i בסכום של B היא 1, בדיוק אחד מהשניים נכון: או $u_{x_i} \in B$ או $u_{\overline{x_i}} \in B$. לכן, ההשמה שהגדרנו מקיימת:
  - אם $u_{x_i} \in B$ אז $x_i = T$
  - אם $u_{\overline{x_i}} \in B$ אז $u_{x_i} \notin B$ ולכן $x_i = F$

- במילים אחרות, אם $u_z \in B$ אז הליטרל z מסתפק בהשמה שהגדרנו

- לכל $1 \le i \le m$ המספר v_i מופיע לכל היותר פעמיים ב- B ותורם לכל היותר 2 לסכום העמודה. לכן קיים $u_z \in B$ המקיים $u_z[n+i] = 1$. כלומר ליטרל z השייך לפסוקית c_i ומסתפק בהשמה שלנו.

- כלומר ההשמה שהגדרנו מספקת כל c_i ולכן מספקת את φ.

<u>הערה:</u> איך שהגדרנו את המספרים שלנו, בכל עמודה יכולים להיות לכל היותר 5 אחדים. לכן, מכיוון שאנחנו עובדים בבסיס עשרוני, לא יכול להתקיים carry.

<u>הערה:</u> הראינו ש SUSU היא NP-קשה כאשר המספרים מקודדים בבסיס עשרוני. זה נשאר נכון גם כאשר המספרים מקודדים בבינארי (חשבו מדוע). אבל אם המספרים מקודדים באונרי אז זה כבר לא נכון ואפשר לפתור את הבעיה בזמן פולינומי (לא נראה את זה בקורס שלנו; זה אלג' פשוט בעזרת תכנון דינמי).