רדוקציות מאאגניבות [SAT ל-IS]

נראה:

$$SAT \le_p IS$$

$$\cancel{VC \le_p Subset\ Sum}$$

$$\cancel{Subset\ Sum \le_p Knapsack}$$

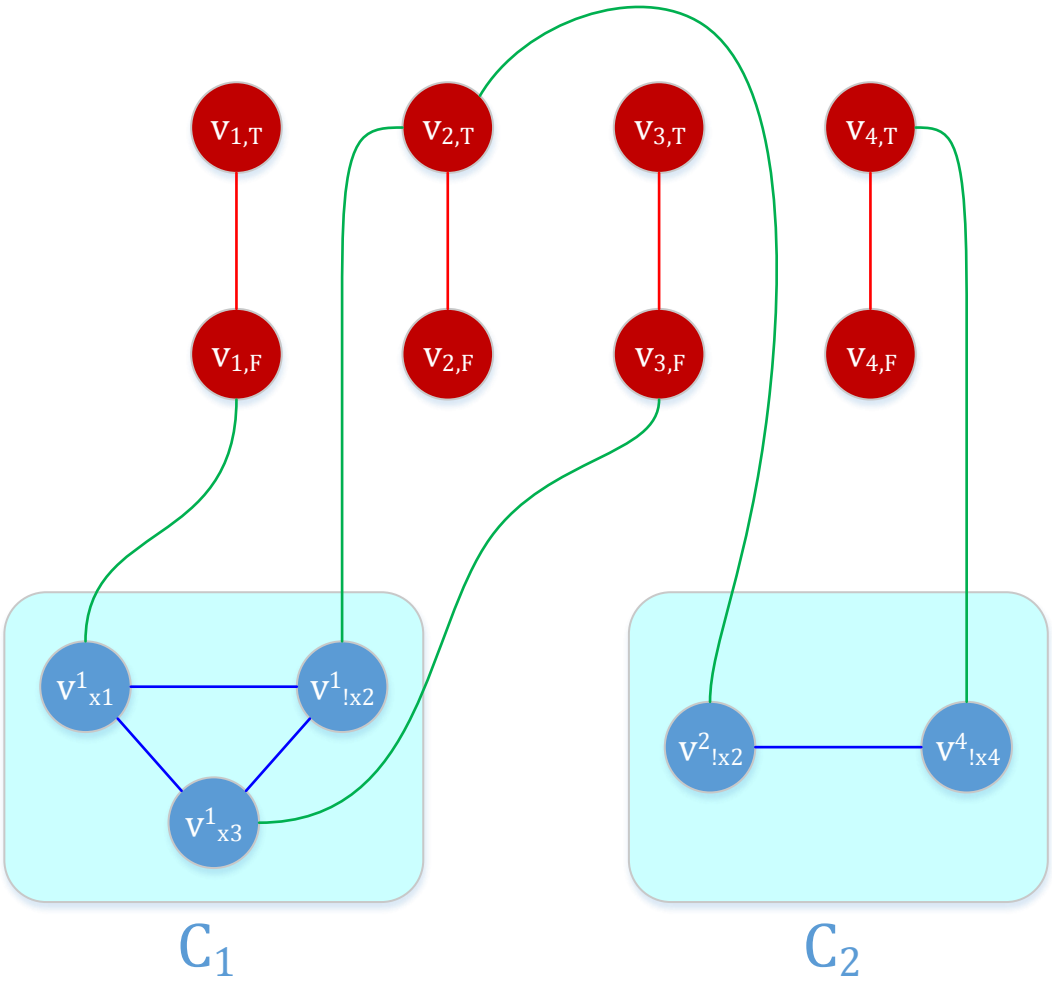
$$\cancel{SAT \le_p 3SAT}$$

[את שלושת הרדוקציות האחרונות לא נספיק להראות, אז פשוט תאמינו לנו שהן מתקיימות.]

כפי שהתחלנו להסביר בשיעור הקודם, אנו רוצים להראות רדוקציה מ-SAT ל-IS, ולשם כך בהינתן נוסחה עבור SAT נייצר עבורה גרף מתאים – למשל עבור הנוסחה:

$$\varphi = \underbrace{\left(x_1 \vee \neg x_2 \vee x_3\right)}_{C_1} \wedge \underbrace{\left(\neg x_2 \vee \neg x_4\right)}_{C_2}$$

נבנה את הגרף:



[להוסיף הסבר]

נשים לב שאם יש n משתנים ו- m פסוקיות, אז אנו מעוניינים למצוא קבוצה בלתי תלויה בגודל $k=n+m$ [[יש לבחור השמה לכל משתנה (= n קדקודים) ולפחות ליטרל אחד בכל פסוקית שיקבל ערך $\mathcal{T}$ (= m קדקודים, כי גם הגבלנו את הגרף כך שגם ייבחר **לכל היותר** ליטרל אחד).]]

הרדוקציה הפורמלית

<u>נגדיר את הגרף</u>:

קדקודים:

$$V_{C_j}=\left\{v_{l_i}^j \middle| l_i\in C_j\right\} \qquad V_{x_i}=\left\{v_{i,\mathcal{T}},v_{i,\mathcal{F}}\right\}$$

$$V_\varphi=\bigcup_{\substack{x_i \text{ is a}\\ \text{variable}\\ \text{in } \varphi}} V_{x_i}\cup\bigcup_{\substack{C_j \text{ is a}\\ \text{clause}\\ \text{in } \varphi}} V_{C_j}$$

קשתות:

$$E_{assign}=\left\{\left(v_{i,\mathcal{T}},v_{i,\mathcal{F}}\right)\middle| x_i \text{ is a variable in } \varphi\right\}$$

$$E_{choose}=\left\{\left(v_{l_{i'}}^j,v_{l_i}^j\right)\middle|\begin{array}{c}C_j \text{ is a clause in } \varphi\\ l_i,l_{i'}\in C_j\\ l_i\neq l_{i'}\end{array}\right\}$$

$$E_{SAT}=\left\{\left(v_{x_i}^j,v_{i,\mathcal{F}}\right)\middle| x_i\in C_j\right\}\cup\left\{\left(v_{\neg x_i}^j,v_{i,\mathcal{T}}\right)\middle|\neg x_i\in C_j\right\}$$

השמה **שלא** מספקת את הליטרל

הוכחת נכונות הרדוקציה

טענה 1 [קיום השמה מספקת]

קיימת השמה מספקת ל- φ אם"ם קיימת קבוצה בלתי תלויה $U\subseteq V_\varphi$ כך ש:

(1) לכל משתנה x_i: $\left|U\cap V_{x_i}\right|=1$ [[כלומר או שמשתמשים ב- $x_{i,\mathcal{T}}$ או שב- $x_{i,\mathcal{F}}$ (רק אחד)]]

(2) לכל פסוקית C_j: $\left|U\cap V_{C_j}\right|=1$ [[כלומר משתמשים רק בקדקוד המתאים לליטרל אחד]]

<u>הוכחה</u>:

נשים לב: כל השמה למשתנים $\{x_i\}$ שקולה לקבוצה שמקיימת את תנאי (1).

צ"ל: כל השמה (באופן שקול, בחירה של U מקיימת את (1)) היא מספקת $\Leftrightarrow$ ניתן להרחיב את U לקבוצה בלתי תלויה שמקיימת את (2).

הערה: כל U שמקיימת את (1) וְ-(2) לא מכילה קשתות מסוג E_{assign}, E_{choose}.

נוכיח:
קיימת קב"ת U שמקיימת את (1) ואת (2)
$\Leftrightarrow$ קיימת U שמקיימת את (1) ואת (2) כך שלכל קשת $(u,v) \in E_{SAT}$ מתקיים $u \notin U$ או $v \notin U$ [[צריך שלא תהיה אף קשת מהגרף, אבל לפי ההערה אנו כבר יודעים שאין קשתות מתוך E_{assign}, E_{choose}, לכן נשאר רק לוודא שאין קשתות מ- E_{SAT}]]
$\Leftrightarrow$ קיימת U כנ"ל כך שלכל פסוקית C_j, אם $l_i \in C_j$ נבחר (כלומר אם $v_{l_i}^j \in U$) אזי U **לא** **מכילה** את קדקוד ההשמה $l_i \leftarrow \mathcal{F}$
$\Leftrightarrow$ קיימת U כנ"ל כך שלכל ליטרל l_i שנבחר U מכילה את ההשמה $l_i \leftarrow \mathcal{T}$ (עקב (1))
$\Leftrightarrow$ קיימת U כנ"ל כך שההשמה המוגדרת ע"י U מספקת כל ליטרל שנבחר עבור פסוקית (ולכל פסוקית בחרנו ליטרל כזה)
$\Leftrightarrow$ קיימת השמה ל- $\{x_i\}$ שמספקת ליטרל כלשהו בכל פסוקית $C_j \in \varphi$
$\Leftrightarrow$ קיימת השמה שמספקת כל פסוקית
$\Leftrightarrow$ קיימת השמה שמספקת את φ.

□

טענה 2 [גודל קב"ת]
כל קב"ת U בגודל $n+m \le$ (מספר המשתנים $= n$, מספר הפסוקיות $= m$) מקיימת את (1) וְ-(2).

<u>הוכחה</u>:
כל קב"ת מכילה לכל היותר קדקוד אחד בכל V_{x_i} (אחרת היא תכיל קשת ב- E_{assign}).
כל קב"ת מכילה לכל היותר קדקוד אחד בכל V_{C_j} (אחרת היא תכיל קשת ב- E_{choose}).

כל הקבוצות V_{x_i}, V_{C_j} יחד מהוות חלוקה של V_φ לתת-קבוצות (זרות), לכן כל קבוצה U שמכילה קדקוד אחד לכל היותר בתת-קבוצה של החלוקה **ומקיימת** $|U| =$ מס' תתי-הקבוצות בחלוקה – חייבת להכיל **בדיוק** קדקוד אחד בכל קבוצה, דהיינו לקיים את (1) ואת (2).

□

משפט [נכונות הרדוקציה]

$$(V_\varphi, E_\varphi, n+m) \in IS \Leftrightarrow \varphi \in SAT$$

<u>הוכחה</u>:

"$\Leftarrow$" זה טענה 1.
"$\Rightarrow$" – לפי טענה 2, אם קיימת $U \subseteq V$ בלתי תלויה בגודל $n+m \le$ אזי היא מקיימת את (1) ואת (2), ואז לפי טענה 1 יש השמה מספקת ל- φ.

□

משפט קוק-לוין (Cook-Levin)

לכל שפה $A \in NP$ יש קדוקציה $A \leq_p SAT$.

אנו נתחיל מבעיית חימום לפני שניגש להראות את הוכחת המשפט הגדול.

חימום: IS ל-SAT

נראה:

$$IS \leq_p SAT$$

מופע ל-IS: גרף $G=(V,E)$ ומספר k.

בעיה: האם קיימת קב"ת בגודל $k \leq$ ב-G?

<u>המטרה</u>: למצוא פסוק φ כך שקיימת קב"ת בגודל $k \leq$ ב-G $\Leftrightarrow \varphi$ ספיק.

למשל, ננסה לקודד את התנאי: "לכל קשת $(u,v) \in E$ מתקיים $u \notin U$ או $v \notin U$".

נגדיר משתנים w_u לכל $u \in V$.

משמעות השמה ל-$\{w_u\}$:

$$w_u = \begin{cases} \mathcal{T}, & u \in U \\ \mathcal{F}, & u \notin U \end{cases}$$

התנאי "$u \notin U$ או $v \notin U$" שקול לפסוקית:

$$C_{(u,v)} = (\neg w_u \vee \neg w_v)$$

<u>נשים לב</u>: השמה תספק את $C_{(u,v)} \Leftrightarrow U$ שמתאימה להשמה מקיימת $u \notin U$ או $v \notin U$.

נגדיר את הנוסחה להיות:

$$\varphi_{IS} = \bigwedge_{(u,v) \in E} C_{(u,v)}$$

טענה [השמה מספקת אם"ם קבוצה בלתי תלויה]

השמה תספק את $\varphi_{IS} \Leftrightarrow$ הקבוצה המתאימה היא קב"ת ב-G.

מה שכבר אמרנו מוכיח את זה.
כעת נשאר לנו לטפל בעניין גודל הקבוצה.

<u>דוגמה</u>: נקודד את התנאי $|U| \geq 1$:

$$\bigvee_{u\in V} w_u$$

<u>דוגמה</u>: נקודד את התנאי $|U|\geq 2$:

$$\bigvee_{\substack{u,v\in V\\ u\neq v}} \left(w_u \wedge w_v\right)$$

באופן כללי, ע"מ ליצור פסוקיות שתדרושנה $|U|\geq k$ נצטרך פסוקית לכל אפשרות בחירה של k קדקודים – ועבור k מספיק גדול, ערך זה הינו בסדר גודל אקספוננציאלי.
בנוסף, פסוקיות אלה לא מהצורה שאנו רוצים (פסוקיות OR שביניהן יש AND).
לכן דרך זו לרדוקציה לא טובה לנו.

רעיון חלופי לרדוקציה הדומה למשפט

(נניח ש- $V=\{1,\dots,|V|\}$)

<u>$\text{Verify}(U,k)$:</u>

- $Count \leftarrow 0$
- עבור $t=1,\dots,|V|$ בצע:
  - אם $t\in U$ אז $Count \leftarrow Count+1$
- $Accept \leftarrow (Count\geq k)$

נגדיר מערך:

$$A[j]=\begin{cases}\mathcal{T}, & Count\geq j\\ \mathcal{F}, & Count<j\end{cases}$$

לכן לפני הלולאה (סוף איטרציה 0) המערך יראה כך:

	0	1	2					$\lvert V\rvert$
A:	$\mathcal{T}$	$\mathcal{F}$	$\mathcal{F}$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\mathcal{F}$

ובאופן כללי, בנקודת זמן כלשהי, הוא נראה כך:

	0	1		$Count$				$\lvert V\rvert$
A:	$\mathcal{T}$	$\mathcal{T}$	$\cdots$	$\mathcal{T}$	$\mathcal{F}$	$\mathcal{F}$	$\cdots$	$\mathcal{F}$

<u>המטרה</u>: לקודד קיצת אלגוריתם.

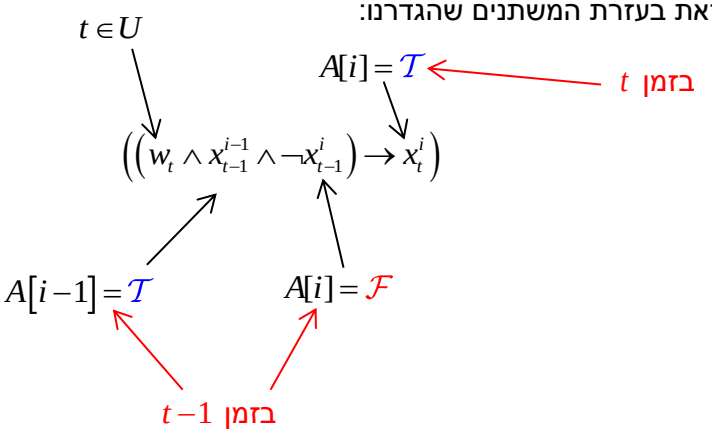
נגדיר משתנים x_t^i.
משמעות ההשמה:

ערכו של $A[i]$ בסוף איטרציה $x_t^i = t$

מעבר מנקודת זמן אחת לנקודה הבאה:

[ציור]

אם נכתוב זאת בעזרת המשתנים שהגדרנו:



ניזכר מלוגיקה שהגרירה $A \rightarrow B$ שקולה לפסוק $\neg A \vee B$, לכן הנ"ל שקול לפסוקית הבאה:

$$\left(\neg\left(w_t \wedge x_{t-1}^{i-1} \wedge \neg x_{t-1}^{i}\right) \vee x_t^i\right)$$

ולפי חוקי דה-מורגן, הנ"ל זהה לפסוקית:

$$\left(\neg w_t \vee \neg x_{t-1}^{i-1} \vee x_{t-1}^{i} \vee x_t^i\right)$$

קורסי בחירה באלגוריתמים

- אלגוריתמים 2 ($\frac{1}{2}$ עדן, $\frac{1}{2}$ עופר ניימן):
  - כפל מטריצות [אלגוריתמים יותר יעילים מ- $O(n^3)$ לחישוב כפל מטריצות]
  - שידוכים בגרפים כלליים
  - בדיקת ראשוניות
  - קריפטוגרפיה [הצפנה מבלי היכולת להעביר סוד מתואם מראש]
  - חישוב קוונטי
- אלגוריתמי קירוב (רק עדן):
  - התמודדות עם בעיות NP-קשות
  - לדוגמה, בכיסוי צמתים: למצוא VC בגודל OPT – זה קשה.
    אבל יודעים למצוא VC בגודל $OPT \le k \le 2OPT$ בזמן סביר.
    עם זאת, למצוא VC בגודל $OPT \le k \le 1.36 \cdot OPT$ זו גם בעיה NP-קשה.
    לא ידוע מה קורה עבור מספרים בין 1.36 ל- 2.
  - דוגמה נוספת – בעיית Knapsack:
    למצוא KS עם ערך OPT – קשה.
    למצוא פתרון עם ערך $1.9999 \cdot OPT$ – קל.
    אפילו עם ערך $\left(1-\frac{1}{n^{100}}\right)$ ניתן למצוא פתרון בזמן $poly(n)$.

אם אתם מרגישים בסדר עם החומר (בגדול עוקבים אחרי מה שקורה בכיתה, ומצליחים להסתדר עם שיעורי הבית בצורה סבירה) – מומלץ לקחת אחד מהם (או את שניהם).
[בקורסים של עדן יש רק מבחן בית (כלומר אין מבחן סופי, אלא רק עבודה ביתי עם משקל גדול יותר).]