פרק ד

עד עתה הדגש שלנו היה על חישוביות, והשאלה העקרית בה דנו היתה "בהנתן שפה L, האם ניתן להכריע/לקבל אותה במודל החישובי שלנו?". בפרט, פירשנו חישוב יעיל כחישוב שניתן לבצע במודל שלנו.

בפרק הזה אנו נדון בסיבוכיות, מושג המעדן בצורה ניכרת את מושג החישוביות.

פורמלית, נגיד כי החישוב הוא יעיל אם הוא מתבצע בזמן פולינומיאלי באורך הקלט. המודל שלנו נשאר מ"ט, אבל כיוון שמ"ט יכולה לבצע כל דבר שיכולה לעשות תוכנית ב C עם [illegible] ריבועי לכל היותר (בזמן החישוב), מ"ט שקולה לתוכניות ב C מבחינת יעילות. כך, נשתמש במה שנוח לנו.

הגדרה חשובה, המבטאת דוגמט ה CS Theory of מה ניתן לחשב

נמשיך עם ההגדרות. התוכנית (דט' T) תקרא יעילה אם קיים פולינום $p(x)$ כך שזמן ריצה של T על קלט w הוא לכל היותר $p(|w|)$.

שפה L (= בעיה L) ניתנת לפתרון יעיל אם קיימת תוכנית דט' יעילה המכריעה אותה.

המחלקה של כל השפות (= בעיות) הניתנות לפתרון יעיל נקראת P.

שוב, לפי הקונצנזוס, P: אלה כל השפות/בעיות שאנו באמת יכולים להתמודד איתם

מחלקה אחרת, בעלת עניין רב, היא מחלקת

NP. זאת מחלקת השפות/בעיות, שעבורם קיימת תוכנית לא דט' המקבלת (לא מכריעה!) אותם בזמן פולינומיאלי באורך הקלט.

דרך שקולה (נסו להבין מדוע) לאפיין NP היא:

$L=\{w\}_{w\in\Sigma^*} \in NP \Leftrightarrow$

אם $w\in L$ ק"מ מחרוזת $g(w)$ שאורכה פולינומיאלי ב-$|w|$, כך שהשפה

$$L' = \{w\square g(w) \mid w\in L\}$$

שייכת ל-P.

(בפרט, זה אומר שעבור $w\notin L$ אין $g(w)$ כזאת).

כך, לדוגמא, כך נראות הבעיות הטיפוסיות בשתי המחלקות:

P	NP	
האם גרף מכיל זיווג בגודל $\geq k$?	האם גרף מכיל קליקה בגודל $\geq k$?	ניחוש: דוגמת קודקודים המהווה קליקה כזאת
האם G 2-צביע?	האם G 3-צביע?	ניחוש: 3-צביעה חוקית
האם G מכיל מעגל אוילר?	האם G מכיל מעגל המילטוני?	ניחוש: מעגל כזה
האם מספר n הנתון בקידוד בינארי הוא ריבוע מלא?	האם מספר n (בבינארי) הינו פריק?	ניחוש: m_1,m_2 כך ש: $n=m_1\cdot m_2$
האם בהינתן קבוצת מספרים, יש ביניהם אחד השווה לסכום כל האחרים?	האם בהינתן קבוצת מספרים, יש בה תת-קבוצה המסתכמת ל-0?	ניחוש: תת-קבוצה כזאת

החשיבות של המחלקה NP נובעת מהעובדה שהמון בעיות תאורטיות ומעשיות משתייכות אליה. הבעיה העיקרית בתאוריה (ואולי לא בתאוריה) של מדעי המחשב - והמדע בכלל, היא השאלה

$$P \overset{?}{=} NP$$

מתדיינים, כמובן, $NP \supseteq P$

עבור הבעיות המצוינות ברשימה שלנו לא ידוע שום אלגוריתם פולינומיאלי, והשאלה שייכותם ל-P פתוחה לחלוטין. כמו למשל הבעיה הרביעית, אשר אחרי 30 שנות מחקר, התגלתה כבעיה פתירה בזמן פולינומיאלי.

<u>שים לב</u>: כיוון מ"ט/תוכניות מקבלת, אך לא מכריעה, המשלים של בעיה ב-NP באופן טיפוסי לא חייבת להיות שייכת ל-NP. כך, מחלקת הגרפים, הלא ניתנים ל-3-צביעה, איננה (כנראה) שייכת ל-NP.

בפרק הזה נדון בעיקר במבנה של מחלקה NP, מנקודת מבט של השאלה $NP \overset{?}{=} P$. לצורך זה נגדיר יחס $A \geq_p B$ בין שפות, שהמשמעות העיקרית שלו (בהקשר זה, לפחות) היא: אם $A \in P$, אז גם $B \in P$.

<u>הגדרה</u>: תהיינה $A \subseteq \Sigma_1^*$, $B \subseteq \Sigma_2^*$.
אנו נגיד כי $A \geq_p B$ אם ד"מ $\varphi: \Sigma_2^* \to \Sigma_1^*$ כך ש:

- φ ניתנת לחישוב יעיל (כ"א פולינומיאלי);
- אם $w \in B$, אז $\varphi(w) \in A$;
- אם $w \notin B$, אז $\varphi(w) \notin A$

$\Leftrightarrow$ אם $\varphi(w) \in A$ אז $w \in B$.

נראה כי: $A \geq_p B$, $B \geq_p C$ $\Downarrow$ $A \geq_p C$

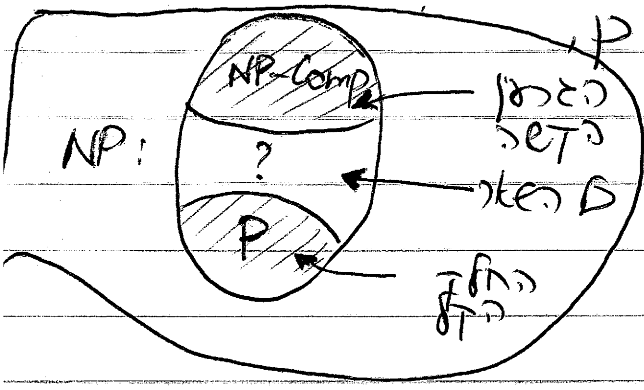
57

אם מתבונן במחלקה NP תחת הסדר $\leq_p$, מתגלה עובדה מפתיעה הבאה: קיימת בעיה מסוימת בNP (שמה SAT; נפרט בהמשך) כך שעבור כל בעיה אחרת $X \in NP$ מתקיים $X \leq_p SAT$. בפרט, כדי להכריע האם $NP=P$, מספיק להכריע האם $SAT \in P$.

הדבר המפתיע הבא הוא כי קיימות המון בעיות מעניינות תאורטית ומעשית $X \in NP$, כך ש $SAT \leq_p X$! בפרט, כל הבעיות המופיעות בעמוד 55 תחת NP הן כאלה! (פרט, כמובן לבעיה הרביעית).

מחלקת כל הבעיות $X \in NP$ כך ש $SAT \leq_p X$, נקראות NP-Complete. תחת היחס $\leq_p$, כל אחת מהבעיות הנ"ל קשה לפחות כמו כל בעיה אחרת בNP, וכל שתי בעיות ב NP-Complete שקולות זו לזו (מדוע?).

התמונה של NP, היא, אם כן,



החשיבות של החלוקה הזאת היא כזאת:

נניח כי קיבלנו בעיה B,
והצלחנו להוכיח כי היא שייכת לNP. ניסינו למצוא אלגוריתם יעיל בשבילה (כ"א לדעת האם $B \in P$) ולא הצלחנו. אם נצליח להראות כי B היא NP-שלמה, זה יתן לנו הוכחה די' (מסוג) של B, ויברור כי אין, כפי הידוע למצוא כיום, אלגוריתם פולינומיאלי לB.

הגדרה: SAT היא אוסף כל הנוסחאות הבוליאניות (בלי כמתים!) הספיקות.

* **משפט Cook - Levin**

עבור כל שפה $L \in NP$, $L \leq_p SAT$.

הוכחה: כיוון ש $L \in NP$, ק"מ מ"ט T כך אשר מקבלת את השפה $L' = \{w \square g(w) \mid w \in L\}$ בזמן poly(|w|)

נניח כי ל T (בה"כ) יש תכונות הבאות:

⊛ $\phi = Q_T \cap \Gamma_T$; ⊛ $\square \notin \Sigma_T$; ⊛ אם T מגיע למצב מקבל, היא חוזרת לתחילת הסרט, ושם עוצרת.
⊛ $g(w) \in \Gamma_T^*$

עבור $w \in L$ נגדיר טבלה בגודל $poly(|w|) \times poly(|w|)$ אשר השורה ה-i שלה מתארת את מצב הסרט בזמן i:

q_0	w_1	w_2	...	w_n	$\square$	x_1	...	x_m	$\flat$	$\flat$	..	$\flat$
u_0	q_1	w_2	...			=						$\flat$
u_0	u_1	q_2	...			=						$\flat$
⋮												
q_A	...											$\flat$
q_A												$\flat$

w ; $g(w)$; $0 \rightarrow$; מצב מקבל ועוצר

משבצת מוסגרת: מיקום/מצב הראש

⊛ **אבחנה א**: $w \in L \Leftrightarrow$ ק"מ ניחוש $g(w)$ מתאים $\Leftrightarrow$ ק"מ טבלה חוקית עבור w, T.

T: מכונה

מהי טבלה חוקית? נגדיר את הדבר במלים, עבור w, T ואז נתרגם את זה לנוסחא בוליאנית.

* φ_{start} :

$$\varphi_{start} = X_{00q_0} \wedge X_{01w_1} \wedge \dots \wedge X_{0nw_n} \wedge X_{0(n+1)\square} \bigwedge_{i=n+2}^{poly(|w|)} \left(\bigvee_{\sigma\in\Gamma_T} X_{0i\sigma} \right)$$

* $\varphi_{defined}$:

$$\varphi_{defined} = \bigwedge_{0\le i,j\le poly(|w|)} \left[\left(\bigvee_{\sigma\in Q_T\cup\Gamma_T} X_{ij\sigma} \right) \wedge \left(\bigwedge_{\sigma\ne\tau} X_{ij\sigma} \to \overline{X_{ij\tau}} \right) \right]$$

* φ_{accept} :

$$\varphi_{accept} = X_{poly(|w|),0,q_A}$$

* φ_{legal} :

$$\bigwedge_{i=1}^{poly(|w|)} \bigwedge_{j=0}^{poly(|w|)} \left(\left(X_{i-1,j-1,\sigma_1} \wedge X_{i-1,j,\sigma_2} \wedge X_{i-1,j+1,\sigma_3} \right) \to X_{ij\,f(\sigma_1,\sigma_2,\sigma_3)} \right)$$

מוגדר ע"י T.

סה"כ, רדוקצי' בניה

$$W \xrightarrow[\text{תאור של T}]{\text{מבצע את}} \varphi_W = \varphi_{start} \wedge \varphi_{defined} \wedge \varphi_{accept} \wedge \varphi_{legal}$$

* הבניה פולינומיאלית – $O(poly^2(|w|))$.
* אם $w\in L$, φ_w ספיקה. פשוט נבחר כשמה אמיתית של חישוב $T(w)$; אם במקום i,j מופיע σ, נשים $X_{ij\sigma}\leftarrow T$; כל השאר יקבלו F.
* אם $w\notin L$, אין חישוב חוקי (כי אין נתיב טוב) לכן שום השמה לא חוקית. אחרת, לו φ היתה ספיקה, היינו מקבלים סתירה. ☐

① תנאי start :

השורה הראשונה נראית כך: (צעד 0)

$$\boxed{q_0 w_1 \dots w_n \square \dots\dots}$$

צד עם Q_T

② תנאי accept :

השורה האחרונה מתחילה ב- q_A.

③ תנאי defined :

בכל משבצת של הטבלה עומד סימן אחד ויחיד $\in Q_T \cup \Gamma_T$.

④ תנאי legal :

החישוב אכן T-חוקי. תנאי ה-T-חוקיות אפשר לנסח באופן לוקלי: הכרחי ומספיק כי מצב המשבצת ה-j בשורה ה-(i+1)-ית נקבע לחלוטין ע"י מצב המשבצות j-1, j, j+1 בשורה ה-i-ית:

$$\begin{array}{l|c|c|c|l}
 & & j & & \\
i \rightarrow & \sigma_1 & \sigma_2 & \sigma_3 & \in Q \cup \Gamma \\
i+1 \rightarrow & & f(\sigma_1,\sigma_2,\sigma_3) & & \in Q \cup \Gamma
\end{array}$$

נקבע לחלוטין ע"י התיאור של T.

נסח את זה בנוסחה בוליאנית, המוגדרת ע"י T ו- w :

⊛ המשתנים שלנו : $\{X_{ij\sigma}\}_{\substack{0 \le i,j \le poly(|w|) \\ \sigma \in Q \cup \Gamma}}$

המשמעות של משתנה $X_{ij\sigma}$:

$X_{ij\sigma} = true \iff$ במשבצת i,j של הטבלה עומד σ

84

* בהינתן גרף G, האם G 3-צביע?

<u>טענה</u>: בעית 3-צביעות היא NP-קשה.

<u>הוכחה</u>: נראה

3-צביעות $\leq_P$ SAT.

תהי φ נוסחת תחשיב פסוקים: נבנה גרף G_φ כך ש-G_φ 3-צביע אמ"מ φ ספיקה.

* שלב ראשון:

$\varphi \longrightarrow$ (I) הצגה עצית

* שלב שני:

... $\longrightarrow$ (II) הצגה עצית שדלה אשר משתמשת בפעולות ∨ ו-¬ בלבד.

* שלב שלישי:

נצא מהצגה (II) ונבנה גרף G_φ. נשים לב שאפשר להציג את (II) באופן הבא:

st. line. prog.

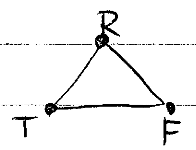
* מתחילים מה משתנים

$x_1, \ldots, x_n$

בכל שלב מוסיפים נוסחה φ_i חדשה אשר מהווה ∨ או ¬ של הנוסחאות הקודמות.

$x_1 .. x_n, \varphi_{n+1} \ldots$

$\varphi_{last} = \varphi$



בניה: נגדיר תחילה משולש ונסמן באופן סימבולי את קדקודיו ב- T, F ו- R.

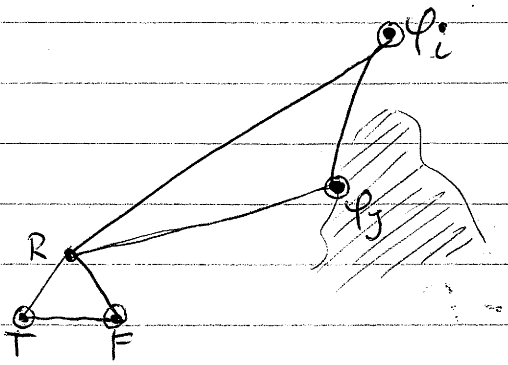
בהמשך הקדקודים יקראו <u>כחול</u> אם יש צלע בינו ובין הקדקוד המסומן R.

* נבנה קודקוד כחול לכל נוסחה φ_i. בהתחלה - קודקוד (כחול) לכל משתנה x_i.

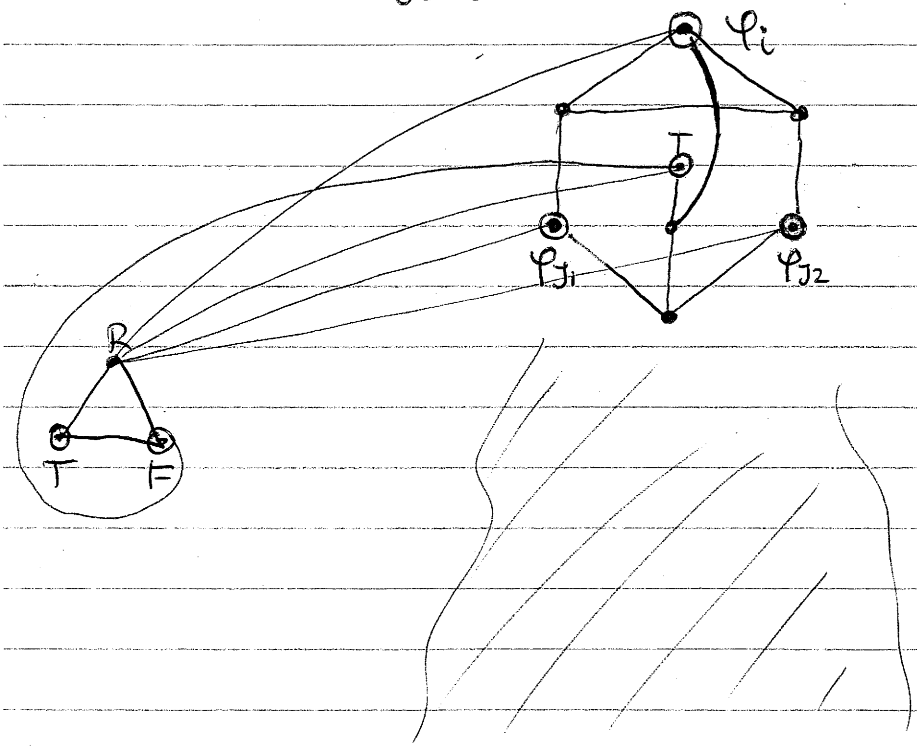
⊕ שלב i- $(n<i)$:

אם $\varphi_i = \neg\varphi_j$ עבור $j<i$,

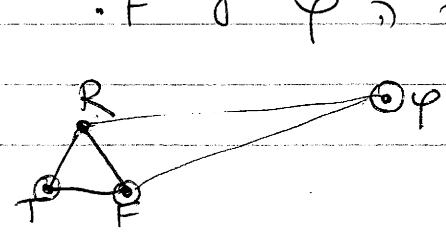
⊙ כחול



אם $\varphi_i = \varphi_{j_1} \vee \varphi_{j_2}$ עבור $j_1, j_2 < i$, נעשה כך:



⊕ בסוף: נחבר את הקודקוד ה φ ל F:

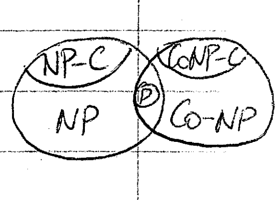


הגדרה: שפה S נקראת NP-Comp אם: S∈NP ולכל L∈NP מתקיים $S \underset{p}{\geq} L$.

משפט Cook-Levin טוען כי SAT הינו NP-Comp. אולם, כפי שנראה, הוא לא יחיד. לדוגמא, אם מתקיים $S \underset{p}{\geq} SAT$, ברור כי S הינו NP-C.

$\underset{p}{\geq}$ טרנזיטיבי

השפות ה-NP-שלמות מהוות את הגרעין הקשה של NP. כיוון שכולן שקולות זו לזו עד כדי רדוקציות פולינומיאליות, אם מצליחים להוכיח כי S NP-שלמה, זה אומר שאיש בעולם לא ידע (נכון להיום) לפתור את S באופן יעיל.



בחלק הנותר של הקורס נעסוק בדוגמאות חשובות של שפות NP-שלמות.

(3SAT)

מספר המשתנים בפסוק

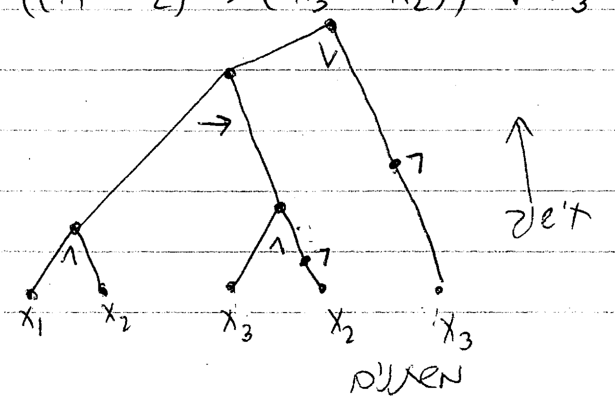
משפט * 3-CNF-SAT הינו NP שלם.

הוכחה: נראה כי $3SAT \underset{p}{\geq} SAT$. (כל פסוק מכיל 3 משתנים/שלילתם)

תהי φ נוסחא בוליאנית (נניח מסודר בסוגריים). אפשר להציג את φ כתבנית של חישוב של עץ בינארי כדלהלן:

באופן יעיל!

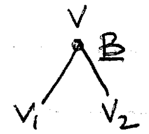
$$((x_1 \wedge x_2) \rightarrow (x_3 \wedge \neg x_2)) \vee \neg x_3$$



עץ חישוב בינארי, עלים - משתנים, צמתים - מסומנים בפעולות בוליאניות.

$x_{v_1} \Leftrightarrow v_1$

לכל צומת v נגדיר x_v:

 $\rightarrow \quad \underbrace{\left(\left(x_{v_1} \ \underline{B} \ x_{v_2}\right) \leftrightarrow x_v\right)}_{f_v}$;

$\varphi \rightarrow \bigwedge_v f_v \wedge x_{root}$ $\quad$ $O(|\varphi|)$

ברור כי φ ספיקה אם"ם $\bigwedge_v f_v \wedge x_{root}$ ספיקה.
מספיק להראות שכל f_v ניתן לכתוב בצורה של 3CNF. לכל B אחד מ $\{\neg, \rightarrow, \wedge, \vee\}$.
נכונה, לדוגמא, עבור $\neg$ ועבור $\vee$.

$$\neg x_1 \leftrightarrow x_2 \Leftrightarrow (\neg x_1 \rightarrow x_2) \wedge (x_2 \rightarrow \neg x_1)$$
$$\Leftrightarrow (x_1 \vee x_2) \wedge (\neg x_2 \vee \neg x_1).$$

$$(x_1 \vee x_2) \Leftrightarrow x_3 \Leftrightarrow (\neg(x_1 \vee x_2) \vee x_3) \wedge (\neg x_3 \vee x_1 \vee x_2)$$
$$\Leftrightarrow ((\neg x_1 \wedge \neg x_2) \vee x_3) \wedge \ldots \Leftrightarrow (\neg x_1 \vee x_3) \wedge (\neg x_2 \vee x_3) \wedge \ldots$$

הגודל הסופי: $O(|\varphi|)$. מש"ל

דוגמאות של בעיות NP-שלמות על גרפים!

בעיה ה **Ind. Set**:

בהינתן זוג $\langle G,K \rangle$ (גרף ומספר טבעי), האם קיימת ב G קבוצה ב"ת בגודל $\geq K$?

טענה: $\text{Ind Set} \in \text{NP-Comp.}$

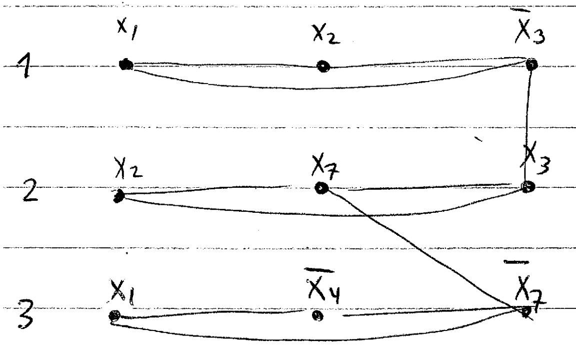
הוכחה: נראה כי

$$\text{Ind Set} \geq_p \text{3-SAT}.$$

$$\varphi = \underset{1}{(x_1 \vee x_2 \vee \overline{x_3})} \wedge \underset{2}{(x_2 \vee x_7 \vee x_3)} \wedge \underset{3}{(x_1 \vee \neg x_4 \vee \neg x_7)}$$

n פסוקים

$G_\varphi \quad |G_\varphi| = 3n$



קודקודים:
בכל פסוק תהיה 3 קודקודים (שורה)!

צלעות:
- שלושת הקודקודים השייכים לאותו פסוק תמיד מחוברים זה לזה.
- קודקוד המתאים ל x_i תמיד יהיה מחובר לכל הקודקודים המתאימים ל $\overline{x_i}$.

טענה: φ ספיק $\Leftrightarrow$ G_φ מכיל קבוצה ב"ת בגודל $\geq n$.

(למשתנה קודקודים) מספר הצלעות / 3

הוכחה: $\Leftarrow$ נתבונן בהשמה מספקת של φ. נסמן את כל הקודקודים להם ההשמה שלהם נותנת true. בכל שורה חייב להיות קודקוד כזה; נבחר באופן שרירותי קודקוד אחד כזה עבור כל שורה. סה"כ נבחרו n קודקודים. הם בלתי תלויים. ✓

⇐ נניח כי φ מכיל קבוצה בת"ל S בגודל $\geq m$. בהכרח, $m=|S|$; מכילה קודקוד אחד בדיוק בכל שורה. נגדיר השמה (חלקית) ל-φ, אשר משייכת ערך true לקודקודים שנבחרו.

לדוגמה, אם $\bar{x}_i$ אז ... $x_i \to 0$.

אזי, ההשמה הנ"ל מוגדרת היטב ומספקת את φ.
מ.ש.ל.

---

vertex cover

* בעיית ה-Dominating Set:
בהינתן גרף G ומספר k, האם G מכיל קבוצת קודקודים S בגודל $\leq k$ אשר לכל קודקוד ב-V יש שכן ב-S?

<u>טענה</u>: Dominating Set $\in$ NP-complete.

<u>הוכחה</u>:
Dom. Set $\geq_p$ Ind. Set

G מכיל Dom.set בגודל $\leq k$ אמ"מ G מכיל Ind.Set בגודל $\geq n-k$.
מ.ש.ל.

---

* בעיית ה-CLIQUE:
בהינתן גרף G ומספר k, האם G מכיל קליקה (צ"ל קבוצת קודקודים שכל שניים מהם שכנים) בגודל $\geq k$?

<u>טענה</u>: CLIQUE $\in$ NP-Complete.

הוכחה: CLIQUE $\geq_p$ Ind. Set

G מכיל קליקה בגודל $\geq k$ $\Leftrightarrow$ $\bar{G}$ מכיל Ind.set בגודל $\geq k$.

מ.ש.ל.