<u>תזכורת:</u>

$P=\{L \mid L=L(M)$ כך ש M פולינומית **<u>דטרמיניסטית</u>** מ"ט קיימת$\}$

$NP=\{L \mid L=L(M)$ כך ש M פולינומית **<u>אי-דטרמיניסטית</u>** מ"ט קיימת$\}$

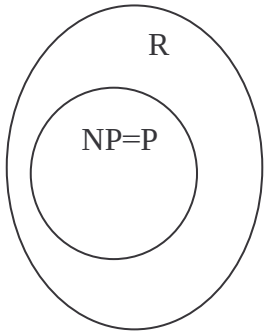
לא ידוע האם $P=NP$ - השאלה הפתוחה המרכזית במדעי המחשב.

<u>הגדרה:</u> שפה L נקראת NP-שלמה אם:

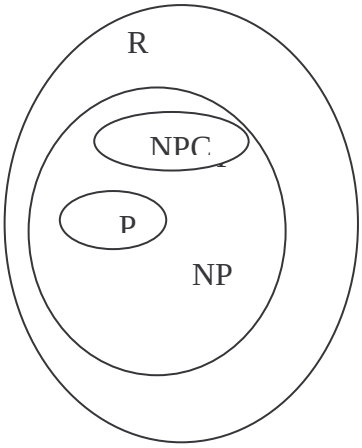
א. $L \in NP$

ב. לכל שפה $L' \in NP$ מתקיים: $L' \le_P L$

אם NP=P



אם $NP \neq P$



הוכחת NP-שלמות:

א. ישירה.

ב. עקיפה: אם $L \in NP$ וגם $L_2 \in NPC$ וגם $L_2 \le_P L$ אז $L \in NPC$.

ראינו בתרגול 10 ש $SAT \in NPC$ ולכן $3SAT \in NPC$.

נראה שגם השפה $VC \in NPC$ ולכן גם השפות $HS, SC, 01IP$ הן NP-שלמות (ראינו בהרצאה הקודמת).

SAT:

בהינתן פסוק CNF, φ, הוא שייך ל SAT אם הוא ספיק. (ההגדרות לפסוקים בתרגול 10)

VC:

בהינתן גרף $G=(V,E)$ ומספר k, הוא שייך ל VC אם קיים כיסוי בצמתים B בגודל k של הגרף.

משפט: $VC \in NPC$.

ידוע ש $VC \in NP$ (ראינו בהרצאה הקודמת)

ידוע ש $3SAT \in NPC$ (נוכיח אי שם בעתיד הרחוק)

צ"ל: $3SAT \le_P VC$.

כלומר, להראות שקיימת רדוקציה f פולינומית שמתאימה לכל פסוק $3CNF$, φ, זוג (G,k) באופן שמתקיים $\varphi \in 3SAT \Leftrightarrow (G,k) \in VC$ (*)

נתון φ המורכב מ n משתנים ו m פסוקיות. נבנה (G,k) מתאים:

G:

א. n זוגות של צמתים שנקרא להם "צמתי ליטרלים" ונסמן אותם כליטרלים:
$x_1,\overline{x}_1,x_2,\overline{x}_2,...,x_n,\overline{x}_n$ כאשר יש קשת בין x_i ל $\overline{x}_i$ עבור כל i.

ב. לכל פסוקית ב φ נתאים משולש שצמתיו מסומנים בליטרלים המתאימים ולצמתים הללו נקרא "צמתי פסוקיות". לכל מופע של ליטרל בפסוקית, יש צומת נפרד.
לכן מספר הצמתים הכולל הוא בדיוק $|V|=2n+3m$

ג. לכל צומת פסוקית (מסעיף ב') המסומנת בליטרל l נוסיף קשת המחברת אותו לצומת הליטרל (מסעיף א') המסומן באותו l. לכן מספר הקשתות הכולל הוא: $|E|=n+3m+3m=n+6m$

נבחר $k=n+2m$.
בשביל לכסות כל אחת מהקשתות המחברות בין צמתי ליטרלים, צריך n צמתים.
בשביל לכסות את כל המשולשים מסעיף ב', צריך $2m$ צמתים.

טענה: לא צריך צמתים נוספים אם ורק אם הפסוק ספיק.

נוכיח שקיבלנו רדוקציה פולינומית:
<u>פולינומית</u>: בזמן $poly(n,m)$ קל להמיר את φ לגרף G. נשים לב ש $|\varphi|\geq n,m$.

<u>תקפות:</u>
א. נניח שהפסוק φ הוא ב $3SAT$ ונוכיח ש $(G,k)\in VC$.
$\varphi\in 3SAT$ ולכן הוא ספיק, כלומר יש השמה אמת למשתנים שמספקת את φ.
נוכיח שקיים כיסוי בגודל k בגרף.

<u>נתאר את הכיסוי B:</u>
א. מכל זוג צמתי ליטרלים, $x_i,\overline{x}_i$ נבחר את זה שמקבל ערך אמת T. עד כה n צמתים.
ב. בכל פסוקית קיים ליטרל שקיבל ערך אמת T בהשמה. את שני האחרים נכניס לכיסוי. $2m$ צמתים.
סה"כ $|B|=n+2m=k$.
נוכיח ש B הוא כיסוי מתאים.
קשתות בין צמתים ליטרלים - מכוסות, ע"פ סעיף א' בבניית הכיסוי.
קשתות המרכיבות את המשולשים - מכוסות, ע"פ סעיף ב' בבניית הכיסוי.
קשתות בין צמתי פסוקיות לבין צמתי ליטרלים: אם צומת הפסוקית המסומן ב l אינה בכיסוי אז על פי הבניה (סעיף ב') l מקבל ערך אמת T בהשמה, ולכן צומת הליטרל l כן נמצא בכיסוי (סעיף א'). לכן הקשת מכוסה.
אם צומת הפסוקית המסומן ב l כן בכיסוי, אז בוודאי שהקשת מכוסה.

ב. נניח ש $(G,k)\in VC$ ונראה שהפסוק φ הוא ב $3SAT$. נראה השמת אמת:
נתון לנו כיסוי B בגודל k.
כל כיסוי מכיל לפחות n צמתי ליטרלים ולפחות $2m$ צמתי פסוקיות.
לכל כל כיסוי בגודל k מכיל בדיוק n צמתי ליטרלים ובדיוק $2m$ צמתי פסוקיות.
לכן מהבניה, נובע שכל כיסוי בגודל k משתמש בדיוק בצומת ליטרל אחד בכל זוג $x_i,\overline{x}_i$ ובדיוק 2 צמתים בכל משולש.

נתאר את השמת האמת:
לכל זוג $x_i,\overline{x}_i$ ניתן ערך אמת T לליטרל שבכיסוי (יש בדיוק אחד כזה ולכן ההשמה מוגדרת היטב)

מספיק להוכיח שלכל פסוקית C_j יש ליטרל שמקבל ערך אמת T. (כי הפסוק φ הוא פסוק CNF).
נתבונן בליטרל l בפסוקית שאינו בכיסוי. (יש אחד כזה כי הראנו שבדיוק 2 מהליטרלים כן בכיסוי).
הקשת המחברת בינו לבין צומת הליטרל מכוסה ע"י B ולכן צומת הליטר הוא בכיסוי ולכן ערך האמת של l הוא T ולכן ערך האמת של הפסוקית C_j הוא T.

<u>משפט:</u>
א. קיימת שפה $L \in R \setminus P$
ב. קיימת שפה $L \in R \setminus NP$
הוכחה:
א. הוכחה באמצעות לכסון: נבנה מ"ט U כך שהשפה שלה $L = L(U)$ היא ב R ושונה מכל שפה המתקבלת ע"י מ"ט פולינומית.

U על קלט x:
* נתייחס לקלט באופן הבא: $x = 1^k 0 \langle M \rangle$
(נשים לב ש $\langle M \rangle$ מופיע באינסוף x-ים: $(10\langle M \rangle, 110\langle M \rangle, 1110\langle M \rangle, \ldots)$
* נריץ את M על x. (ע"י מ"ט אוניברסאלית) למשך לכל היותר 2^k צעדים.
אם M עוצרת על x תוך 2^k צעדים אז אם היא מקבלת אז נדחה ואם היא דוחה אז נקבל.
אם M לא עוצרת אז U עוצרת ו... (מקבלת או לא???)

- מהבניה U עוצרת תמיד ולכן $L = L(U) \in R$.
- נניח בשלילה שקיימת מ"ט M פולינומית המקבלת את L, עם פולינום $p(n)$. יהיה k מספיק גדול כך ש $2^k \geq p\left(k+1+\left|\langle M \rangle\right|\right)$.
נתבונן בריצת U על הקלט $x = 1^k 0 \langle M \rangle$.
זמן הריצה של M על x קטן מ $2^k \geq p\left(k+1+\left|\langle M \rangle\right|\right)$ ולכן בסימולציה M עוצרת או דוחה, ההפך ממנה, ולכן השפות שלהן שונות ומכיוון ש $L = L(U)$ נקבל ש $L(M) \neq L$ בסתירה.

ב. אם $L \in NP$ אז קיימת מ"ט א"ד M הרצה זמן n^c ומקבלת את L.
$NP \subseteq R$ ולכן קיימת מ"ט דטרמיניסטית M' הרצה זמן 2^{n^c} עבור L.
נבנה את U באותה צורה עם חסם 2^{2^k} על הזמן.

<u>דוגמאות לשפות NP שלמות (בעיות חלוקה ואריזה):</u>
<u>בעיית החלוקה - PART</u>
קלט: $X_1, .., X_n$ שלמים אי שליליים.
האם ניתן לחלק את המספרים לשתי קבוצות שסכומן זהה?
זאת אומרת, האם קיימת $I \subseteq \{1, \ldots, n\}$ כך ש $\sum_{i \in I} x_i = \sum_{i \notin I} x_i = \frac{1}{2} \sum_{i \in \{1,..,n\}} X_i$?

<u>בעיית האריזה החד מימדית</u> $BIN-PACKING$:
נתונים: גודל תא B ואיברים בגדלים $X_1,...,X_n$ ומספר k.
האם ניתנת לארוז את האיברים ל k תאים באופן חוקי, כלומר בכל תא סכום הגדלים קטן או שווה ל B.

טענה: $BP \in NPC$:
$BP \in NP$ (ננחש לכל איבר באיזה מ k התאים הוא נארז ונבדוק חוקיות)
נראה: $PART \le_P BP$

הרדוקציה:

$$X_1,...,X_n \to \begin{pmatrix} B=\frac{1}{2}\sum X_i \\ k=2 \\ X_1,...,X_n \end{pmatrix}$$

דוגמה: בעיית תרמיל הגב: $KNABSACK$:
נתונים: B גודל התרמיל.
$X_1,...,X_n$ הגדלים של הפריטים.
$C_1,...,C_n$ התועלת של כל פריט.
k תועלת מבוקשת.
האם ניתן לארוז לתרמיל פריטים שגודלם ב B והתועלת שלהם היא לפחות k.

טענה: $KNABSACK \in NPC$
$KNABSACK \in NP$ - (פשוט ננחש איזה פריטים להכניס ונבדוק חוקיות).
$PART \le_P KNABSACK$
הרדוקציה:

$$X_1,...,X_n \to \begin{pmatrix} B=\frac{1}{2}\sum X_i \\ k=\frac{1}{2}\sum X_i \\ X_1,...,X_n \\ \forall i: C_i = X_i \end{pmatrix}$$

אם $X_1,...,X_n \in PART$ אז קיימת $I \subseteq \{1,...,n\}$ כך ש $\sum_{i\in I} x_i = \sum_{i\notin I} x_i = \frac{1}{2}\sum_{i\in\{1,..,n\}} X_i$.
נבחר את האיברים ב I לתוך התרמיל.
נקבל: $\sum_{i\in I} x_i = \sum_{i\in I} C_i = \frac{1}{2}\sum_{i\in\{1,..,n\}} X_i = k = B$
אם $f(X_1,...,X_n) \in KN...$:
תהי I קבוצת הפריטי בתרמיל.
לפי קריטריון הגודל: $\sum_{i\in I} x_i \le B = \frac{1}{2}\sum_{i\in\{1,..,n\}} X_i$.

לפי קריטריון התועלת: $\sum_{i\in I} C_i = \sum_{i\in I} X_i \geq k = \frac{1}{2}\sum_{i\in\{1,..,n\}} X_i$.

לכן $\sum_{i\in I} X_i = \frac{1}{2}\sum_{i\in\{1,..,n\}} X_i$ ולכן I הוא פתרון לבעיית החלוקה.