

ההיררכיה הפולינומית

$$\begin{aligned}
 x \in L &\Leftrightarrow \exists \underbrace{w}_{\substack{\text{באורך} \\ \text{פולינומי}}} . \underbrace{M(x, w)}_{\substack{\text{מכונת טיורינג} \\ \text{דטרמיניסטית פולינומית}}} = 1 & \Sigma_1 = \text{NP} \quad \text{מחלקת כל השפות } L \text{ עבורן} \\
 x \in L &\Leftrightarrow \forall \underbrace{w}_{\substack{\text{באורך} \\ \text{פולינומי}}} . \underbrace{M(x, w)}_{\substack{\text{מכונת טיורינג} \\ \text{דטרמיניסטית פולינומית}}} = 1 & \Pi_1 = \text{coNP} \quad \text{מחלקת כל השפות } L \text{ עבורן} \\
 x \in L &\Leftrightarrow \exists w_1 . \forall w_2 . M(x, w_1, w_2) = 1 & \Sigma_2 \quad \text{מחלקת כל השפות } L \text{ עבורן} \\
 x \in L &\Leftrightarrow \forall w_1 . \exists w_2 . M(x, w_1, w_2) = 1 & \Pi_2 \quad \text{כנ"ל, אבל}
 \end{aligned}$$

באותו אופן, מגדירים את Σ_i ו- Π_i .

דוגמאות:

$$\begin{aligned}
 1. \quad \text{Max-Clique} &= \left\{ \langle G, k \rangle \mid \begin{array}{l} \text{גודל הקליק המקסימלי} \\ \text{ב- } G \text{ הוא בדיוק } k \end{array} \right\} : \text{Max-Clique} \in \Sigma_2 \\
 &\quad \exists \underbrace{S_1}_{\substack{\text{קליק} \\ \text{בגודל } k}} . \forall \underbrace{S_2}_{\substack{\text{בדקת ש- } S_1 \text{ קליק} \\ \text{בגודל } k \text{ אינו קליק} \\ \text{בגודל } k+1}} . M(x, S_1, S_2) = 1 & \text{הסבר:} \\
 2. \quad \text{Min-DNF} &= \left\{ \langle \varphi \rangle \mid \begin{array}{l} \text{אין נוסחה } \varphi' \\ \text{שקולה קטנה יותר} \end{array} \right\} : \text{Min-DNF} \in \Pi_2 \\
 &\quad \forall \underbrace{\varphi'}_{\substack{\text{פסוק} \\ \text{השמה } \varphi, \\ \text{ואם כן תבדוק שאכן } x \text{ שונה בין } \varphi' \text{ ל- } \varphi}} . \exists \underbrace{x}_{\substack{\text{תבדוק ש- } \varphi' \text{ קטנה יותר מ- } \varphi, \\ \text{ואם כן תבדוק שאכן } x \text{ שונה בין } \varphi' \text{ ל- } \varphi}} . M(\varphi, \varphi', x) = 1 & \text{הסבר:} \\
 &\quad \text{הערה: כנראה ששפה זו היא } \Pi_2 \text{-שלמה.}
 \end{aligned}$$

טענות:

$$\begin{aligned}
 &\Sigma_i \subseteq \Pi_{i+1} \\
 &\Pi_i \subseteq \Sigma_{i+1} \\
 &\text{BPP} \subseteq \Sigma_2 \cap \Pi_2
 \end{aligned}$$

$$\text{הגדרה: } \text{PH} = \bigcup_i \Sigma_i$$

PCP

הגדרה: $\text{PCP}(r, q)$ - אוסף השפות L עבורן קיימת מערכת הוכחה כך ש:

- אם $x \in L$, המוודא (הסתברותי) מקבל בהסתברות 1.
 - אם $x \notin L$, המוודא (הסתברותי) מקבל בהסתברות לכל היותר $\frac{1}{2}$.
- המוודא לא מטיל יותר מ- $O(r)$ מטבעות, ולא מבצע יותר מ- $O(q)$ שאילתות להוכחה. אורך ההוכחה חסום על ידי $O(q) \cdot 2^{O(r)}$.

המטרה: להוכיח כי $\text{NP} \subseteq \text{PCP}(\text{Poly}(n), 1)$.

רעיון: **QuadEq** (בעיה NP-קשה).

איך נבנה פרוטוקול הוכחה?

נקרה להשמה מספקת u (באורך n).

מחשב את $u \otimes u$ - מטריצה או וקטור בגודל n^2 שמכילה את כל הזוגות $u_i \cdot u_j$.

נכתוב את קידוד *Hadamard* ל- u ו- $u \otimes u$.

$$f(x_1, \dots, x_k) = \sum_{i=1}^k a_i x_i$$

עבור וקטור a באורך k , ניתן להגדיר פונקציה ליניארית

הקידוד - הצבת כל הערכים האפשריים בתוך הפונקציה f (פעם אחת u מהווה את המקדמים, ובפעם השנייה $u \otimes u$).

הבודקים - בודקים בעזרת "מבחן לינאריות" שאכן הצבנו את הקידוד של u ו- $u \otimes u$.

בודקים שהווקטור האחד הוא אכן טנזור של הווקטור השני.

לוקחים סכום מקרי של המשוואות הנתונות, ובודקים בקידוד של $u \otimes u$ האם באמת הפתרון חוקי.