נושא 3 - היררכיה פולינומית

א) המחלקה Σ_i^P

לכל $i\in\mathbb{N}$ נגדיר את Σ_i^P להיות אוסף השפות L, שקיימת עבורן מ"ט דטרמיניסטית ופולינומית M ופולינום $p(\cdot)$ כך שלכל $x\in\{0,1\}^*$ מתקיים:

$$x\in L \iff \exists u_1\in\{0,1\}^{p(|x|)}\ \forall u_2\in\{0,1\}^{p(|x|)} \dots Q_i u_i\in\{0,1\}^{p(|x|)}\ M(x,u_1,u_2,\dots,u_i)=1$$

כאשר Q_i היא כמת $\forall$ אם i זוגי ו-$\exists$ אם i אי-זוגי.

כלומר Σ_i^P זהו אוסף כל השפות שיש להן מ"ט דטרמיניסטית המכריעה אותן באמצעות שימוש ב-i עדים כאשר הכמת על כל עד הוא $\exists$ ו-$\forall$ לסירוגין.

ב) המחלקה Σ_2^P

לפי ההגדרה מסעיף קודם, Σ_2^P היא אוסף כל השפות L שקיימת להן מ"ט דטרמיניסטית ופולינומית M ופולינום $p(\cdot)$ כך שלכל $x\in\{0,1\}^*$ מתקיים:

$$x\in L \iff \exists u_1\in\{0,1\}^{p(|x|)}\ \forall u_2\in\{0,1\}^{p(|x|)}\ M(x,u_1,u_2)=1$$

דוגמאות לשפות ב-Σ_2^P:

(1) $ExactIndset=\{\langle G,K\rangle \mid$ גרף לא מכוון שיש בו קבוצה בת"ל בגודל K אך אין בו קבוצה כזו בגודל $K+1$ $G\}\in\Sigma_2^P$.

הוכחה: נגדיר מ"ט דטרמיניסטית M שעל הקלט $\langle G,K\rangle,u_1,u_2$ תבדוק:

- תבדוק ש-u_1 וקטור בינארי באורך $|V(G)|$ שבו K אחדות, ועבור לכל שני אינדקסים i,j שערכם 1, M עובדת שאין צלע בין v_i ל-v_j. אם לא מתקיים תחזיר 0.
- תבדוק ש-u_2 אינה מכילה $K+1$ אחדות או שקיימים שני אינדקסים i,j שערכם 1 כך שיש צלע בין v_i ל-v_j. אם לא מתקיים תחזיר 0, אחרת תחזיר 1.

הוכחת נכונות: מאוד קל להוכיח ש-M פולינומית ושתנאי ה-$\Leftarrow$ מתקיים.

(2) $MIN\text{-}EQ\text{-}DNF=\{\langle\varphi,K\rangle \mid$ קיימת נוסחת DNF ψ בגודל קטן שווה K והיא שקולה לנוסחת DNF $\varphi\}\in\Sigma_2^P$

הוכחה: נגדיר מ"ט דטרמיניסטית M שעל הקלט $\langle\varphi,K\rangle,u_1,u_2$ תבדוק:

- תבדוק ש-u_1 מייצגת נוסחת DNF ψ באורך קטן שווה K, אם לא מתקיים תחזיר 0.
- תבדוק ש-u_2 מייצגת השמה חוקית z עבור ψ ו-φ ואכן מתקיים $\varphi(z)\equiv\psi(z)$. אם מתקיים תחזיר 1.

הערה - $MIN\text{-}EQ\text{-}DNF\in\Sigma_2^P\text{-}COMPLETE$, זהו משפט Umans.

משפט: $NP, coNP\subseteq\Sigma_2^P$.

הוכחה: שכן ל-NP מספיק העד הראשון ויכול להתעלם מהשני, בפרט $NP=\Sigma_1^P$, ואילו ל-$coNP$ מספיק העד השני ויכול להתעלם מהראשון.

(22)

ג) המחלקה Π_i^P

מחלקה זו ניתן להגדיר בשני דרכים:

(1) לכל $0<i\in\mathbb{N}$ נגדיר את Π_i^P להיות אוסף השפות L, שקיימת עבורן מ"ט דטרמיניסטית ופולינומית M ופולינום $p(\cdot)$ כך שלכל $x\in\{0,1\}^*$ מתקיים:

$$x\in L \iff \forall u_1\in\{0,1\}^{p(|x|)}\ \exists u_2\in\{0,1\}^{p(|x|)} \dots Q_i u_i\in\{0,1\}^{p(|x|)}\ M(x,u_1,u_2,\dots,u_i)=1$$

כאשר Q_i הוא $\exists$ אם i זוגי ו-$\forall$ אם i אי-זוגי. כלומר בעצם שינוי סדר הכמתים ב-Σ_i^P.

(2) נגדיר $\Pi_i^P=\{L \mid \overline{L}\in\Sigma_i^P\}$.

ג) המחלקה Π_2^P

לפי ההגדרה מעלה קודם, Π_2^P היא אוסף כל השפות L שקיימת להן מ"ט דטרמיניסטית ופולינומית M ופולינום $p(\cdot)$ כך שלכל $x\in\{0,1\}^*$ מתקיים: $x\in L \iff \forall u_1\in\{0,1\}^{p(|x|)}\ \exists u_2\in\{0,1\}^{p(|x|)}\ M(x,u_1,u_2)=1$

דוגמאות לשפות ב-Π_2^P: $\text{Exact Indset}\in\Pi_2^P$, $\overline{\text{MIN-EQ-DNF}}\in\Pi_2^P$

משפט: $NP, coNP\subseteq\Pi_2^P$.

הוכחה: לכל $L\in coNP$ מספיק הצד הראשון כדי לבנות מ"ט מוודאת כמו שנדרש, בפרט מתקיים $coNP=\Pi_1^P$.

כנ"ל, לכל $L\in NP$ מספיק הצד השני לבנות מכונה מוודאת שיכולה להתעלם מהצד הראשון.

ה) המחלקה PH (Polynomial Hierarchy)

נגדיר את המחלקה PH כך: $PH=\bigcup_{i=1}^{\infty}\Sigma_i^P=\bigcup_{i=1}^{\infty}\Pi_i^P$

אבחנות:

- $\Sigma_i^P\subseteq\Pi_{i+1}^P$ - אבחנה זו נכונה שכן לכל $L\in\Sigma_i^P$ ניתן לבנות מ"ט הרצויה ל-Π_{i+1}^P שמתעלמת מ-u_1.
- $\Pi_i^P\subseteq\Sigma_{i+1}^P$ - אותו הסדר כמו אבחנה קודמת.
- $\Sigma_i^P\subsetneq\Sigma_{i+1}^P$ - לא מוכח אך כזו האמונה הרווחת.

ו) קריסת ההיררכיה הפולינומית

הגדרה: נאמר ש-PH קורסת ל-i אם מתקיים $PH=\Sigma_i^P$, כלומר יש איזשהו $0<i\in\mathbb{N}$

המקיים $\Sigma_i^P=\bigcup_{j\geq i}\Sigma_j^P$ שכן ברור שמתקיים: $\bigcup_{j=1}^{i}\Sigma_j^P\subseteq\Sigma_i^P$.

משפטים:

(1) לכל $0<i\in\mathbb{N}$ אם מתקיים $\Sigma_i^P=\Pi_i^P$ אזי PH קורסת ל-i. [צ] יוכח בשאלה 4 ושאלה 1

(2) אם $P=NP$ אזי $PH=P$.

הוכחה: אם $P=NP$. אזי - $NP=coNP$, ואז לפי משפט (1) PH קורסת ל-1 כלומר $PH=NP=coNP$, ולפי ההנחה (נתון) $PH=P$.

בס"ד

ג) שלמות עבור הרמה ה-i ב-PH

נגדיר שפה לכל רמה i ב-PH שהיא שלמה עבור אותה רמה

$\Sigma_i SAT = \{\psi = \exists u_1 \forall u_2 \dots Q u_i\, \varphi(u_1,\dots,u_i) \mid$ ל-ψ יש השמה מספקת, $u_1,\dots,u_i$ וקטורים בוליאנים, φ נוסחת CNF ללא כמתים. Q_i היא $\exists$ עבור i אי-זוגי ו-$\forall$ עבור i זוגי $\} \in \Sigma_i^P$-COMPLETE

הוכחת הטענה במטלה 4 שאלה 2.2.

משפטים:

(1) אם ק"מת שפה L שהיא שלמה ב-PH אזי קיים $0<i\in\mathbb{N}$ כך ש-PH קורסת ל-i. כלומר $PH=\Sigma_i^P$.

הוכחה: אם L שלמה ב-PH, אזי בהכרח $L\in PH$ ואזי $L=\Sigma_i^P$ עבור i כלשהו. כעת לכל $L'\in PH$ מתקיים $L'\le_p L$ ולכן $L'\in\Sigma_i^P$. ומכאן $PH=\Sigma_i^P$.

(2) אם $PH=PSPACE$ אזי קיים $0<i\in\mathbb{N}$ כך ש-PH קורסת לרמה i.

הוכחה: כיוון ש-$PH=PSPACE$ ו-TQBF שלמה ב-PSPACE, אזי TQBF גם שלמה ב-PH ולכן לפי (1) הטענה מתקיימת.

(3) לכל $0<i\in\mathbb{N}$ מתקיים: $\Sigma_i^P = NP^{\Sigma_i SAT}$. $NP^{\Sigma_i SAT}$ היא NP עם אורקל לשפה $\Sigma_i SAT$.