תורת הסיבוכיות - תרגול 5
ההיררכייה הפולינומית

ההירכייה הפולינומית - הגדרה והגדרה אלטרנטיבית

נחזור בזריזות על ההגדרות. כזכור, ההיררכייה הפולינומית הוגדרה באופן רקורסיבי, עם הבסיס $\Delta_0^p = \Sigma_0^p = \Pi_0^p = \mathrm{P}$ וצעד הבניה:

$$\begin{aligned}\Delta_{n+1}^p &= \mathrm{P}^{\Sigma_n^p}\\ \Sigma_{n+1}^p &= \mathrm{NP}^{\Sigma_n^p}\\ \Pi_{n+1}^p &= \mathrm{coNP}^{\Sigma_n^p}\end{aligned}$$

ולבסוף ההיררכייה הפולינומית כולה מוגדרת באמצעות $\mathrm{PH} = \bigcup_{n=0}^{\infty} \Sigma_n^p$.

נשים לב לכך שאפשר גם להגדיר $\Sigma_{n+1}^p = \mathrm{NP}^{\Pi_n^p}$ והדבר יקל עלינו בהוכחות בהמשך (זאת מכיוון שאם $L \in \Sigma_n^p$ אז $\overline{L} \in \Pi_n^p$ עם אותה מכונת אוב אי דטרמיניסטית, ואוב ל־$\overline{L}$ מאפשר לסמלץ אוב ל־L על ידי שאילת שאלות ולקיחת התשובה ההפוכה).

מבחינה היסטורית ההיררכייה הפולינומית הוגדרה כאנלוגיה בעלת זמן חישוב יעיל להיררכייה דומה שסיווגה שפות בלוגיקה - ההיררכייה האריתמטית. הניסוח המקובל להיררכייה האריתמטית הוא באמצעות כמתים, וניסוח דומה קיים גם עבור ההיררכייה הפולינומית. כשם שההגדרה באמצעות מכונות אוב מכלילה במובן מסויים את הגדרת NP ו־coNP באמצעות מכונות אי דטרמיניסטיות, ההגדרה באמצעות כמתים מכלילה את הגדרת NP ו־coNP באמצעות יחסים.

בהינתן פסוק $\varphi(x,y)$ בלוגיקה מסדר ראשון ("תחשיב היחסים") עם משתנים חופשיים x,y ופולינום $p(n)$, נשתמש בסימון $\exists_p y(\varphi(x,y))$ בתור קיצור של $\exists y(|y| \le p(|x|) \wedge \varphi(x,y))$. כלומר, זהו כמת "קיים" אשר הטווח שלו מוגבל לערכים פולינומיים ב־x. בדומה נגדיר את $\forall_p$: $\forall_p y(\varphi(x,y))$ יהיה קיצור של $\forall y(|y| \le p(|x|) \Rightarrow \varphi(x,y))$, כלומר הדרישה היא ש־$\varphi(x,y)$ יתקיים לכל הערכים של y שגודלם חסום על ידי $p(|x|)$.

אם C היא מחלקת שפות, נגדיר מחלקה $\exists\mathrm{C}$ באופן הבא: $L \in \exists\mathrm{C}$ אם ורק אם קיימת $L' \in \mathrm{C}$ ופולינום $p(n)$ כך ש־$L = \{x | \exists_p y : (x,y) \in L'\}$.

בדומה נגדיר את $\forall\mathrm{C}$: $L \in \forall\mathrm{C}$ אם ורק אם קיימת $L' \in \mathrm{C}$ ופולינום $p(n)$ כך ש־$L = \{x | \forall_p y : (x,y) \in L'\}$.

נשתמש בסימון $\exists\neg$ כאלטרנטיבה ל־$\forall$ ובסימון $\forall\neg$ כאלטרנטיבה ל־$\exists$.

כמו כן בהינתן מחלקת שפות C נסמן $\mathrm{coC} = \left\{\overline{L} | L \in \mathrm{C}\right\}$.

שתי אבחנות בסיסיות שיסייעו לנו בהבנת הסימון החדש:

1. $\mathrm{NP} = \exists\mathrm{P}$.
2. לכל $Q_1, \ldots, Q_k \in \{\forall, \exists\}$ מתקיים $\mathrm{co}[Q_1 \ldots Q_k \mathrm{C}] = \neg Q_1 \ldots \neg Q_k [\mathrm{coC}]$.

באמצעות הסימונים שהצגנו קל לתת הגדרה אלטרנטיבית להיררכייה הפולינומית:

$$\begin{aligned}\Sigma_k^p &= \underbrace{\exists\forall\exists\ldots Q}_{k}\mathrm{P}\\ \Pi_k^p &= \underbrace{\forall\exists\forall\ldots Q}_{k}\mathrm{P}\end{aligned}$$

קל לראות כי $\Pi_k^p = \mathrm{co}\Sigma_k^p$ על פי הגדרה זו.

ניתן גם לתת הגדרה אינדוקטיבית:

$$\Sigma_{k+1}^{p} = \exists\Pi_{k}^{p}$$
$$\Pi_{k+1}^{p} = \forall\Sigma_{k}^{p}$$

וניתן גם לתת הגדרה "מפורשת":

$L\in\Sigma_k^p$ אם ורק אם קיימת $L'\in\mathrm{P}$ ופולינום $p(n)$ כך ש־$L=\{x|\exists_p y_1\forall_p y_2\dots Q_p y_k:(x,y_1,\dots,y_k)\in L'\}$.

$L\in\Pi_k^p$ אם ורק אם קיימת $L'\in\mathrm{P}$ ופולינום $p(n)$ כך ש־$L=\{x|\forall_p y_1\exists_p y_2\dots Q_p y_k:(x,y_1,\dots,y_k)\in L'\}$.

שימו לב שכל הכמתים כאן חסומים על ידי אותו פולינום $p(n)$; זהו תרגיל נחמד להוכיח כי זה לא מגביל את הכלליות של ההגדרה (שבה לכל כמת יש פולינום משל עצמו).

הוכחת האפיון האלטרנטיבי

גם בהגדרה עם מכונות אוב וגם בהגדרה עם כמתים, $\Sigma_0^p=\Pi_0^p=\mathrm{P}$. על מנת להראות כי ההגדרות שקולות נותר להוכיח באינדוקציה שלכל k מתקיים ש־$\exists\Pi_k^p=\mathrm{NP}^{\Pi_k^p}$ (כלומר, ששתי ההגדרות עבור Σ_{k+1}^p מזדהות). אם נוכיח זאת אז ינבע מייד גם שהמחלקות המשלימות שוות, כלומר $\forall\Sigma_k^p=\mathrm{coNP}^{\Sigma_k^p}$ (ולכן שתי ההגדרות עבור Π_{k+1}^p מזדהות).

ראשית נוכיח ש־$\exists\Pi_k^p\subseteq\mathrm{NP}^{\Pi_k^p}$. יהי $L\in\exists\Pi_k^p$, אז על פי הגדרה קיימים $L'\in\Pi_k^p$ ופולינום $p(n)$ כך ש־$L=\{x|\exists_p y:(x,y)\in L'\}$.

נותר כעת להוכיח את הכיוון השני, $\exists\Pi_k^p\supseteq\mathrm{NP}^{\Pi_k^p}$ שהוא מורכב משמעותית יותר. הרעיון הבסיסי זהה לזה שבהוכחת שני האפיונים של NP; נגדיר יחס שבו לכל x מתאים y ש"מתאר" את הריצה של מכונת NP עם אוב לשפה ב־Π_k^p. עם זאת, היכולת של המכונה לפנות לאוב תצריך מהיחס שלנו להכיל פרטי מידע נוספים שלא היו בהוכחה ההיא.

תהא אם כן $L\in\mathrm{NP}^{\Pi_k^p}$. פירוש הדבר הוא שקיימת מכונת טיורינג אי דטרמיניסטית M עם אוב לשפה $A\in\Pi_k^p$ כך ש־$L\left(M^A\right)=L$.

נגדיר שפה L' בתור שפת הזוגות (x,y) כך ש־M^A מקבלת את x בריצה שפרטיה מתוארים על ידי y (נסביר את המשמעות המדויקת של כך בהמשך) ונראה שיש פולינום $p(n)$ כך ש־$|y|\le p(|x|)$ תמיד. אם נצליח להגדיר את L' באופן הזה כך ש־$L'\in\Pi_k^p$, סיימנו.

על פי הנחת האינדוקציה, כדי להראות כי $L'\in\Pi_k^p$ מספיק להראות כי $L'\in\mathrm{coNP}^{\Sigma_{k-1}^p}$. כלומר, אנו רוצים להראות שקיימת מכונת טיורינג אי דטרמיניסטית M', עם אוב לשפה $A'\in\Sigma_{k-1}^p$, כך שעל קלט (x,y) שבו y **לא** מתאר ריצה מקבלת של M על x, למכונה M' קיים מסלול שבו היא עוצרת ודוחה, וכמו כן אם (x,y) כן מתאר ריצה מקבלת של M אז M' אינה דוחה.

לצורך כך, y כולל שלושה מרכיבים:

1. תיאור הבחירות האי־דטרמיניסטיות של M במהלך החישוב שלה על x.
2. תיאור התשובות של האוב ל־A על השאלות של M לאוב במהלך הריצה.
3. עבור כל תשובת "לא", הוכחה לכך שתשובת ה"לא" נכונה (נסביר את משמעותה המדוייקת בהמשך).

ברור כי בעזרת 1 ו־2 ניתן לבדוק דטרמיניסטית האם M בריצתה על x אכן עוצרת ומקבלת, ואם זה לא קרה, לדחות. נותר אם כן להבין כיצד ניתן לזהות שאחת מהתשובות בסעיף 2 היא שקרית ולדחות גם במקרה זה.

כזכור, $A\in\Pi_k^p$, כלומר $A=\forall A'$ עם פולינום חוסם $q(n)$ כך ש־$A'\in\Sigma_{k-1}^p$. אם כן, A' תהיה שפת האוב האוב של המכונה M'.

כעת, אם y כולל את הטענה ש־$w\in A$ למרות שבפועל $w\notin A$ קל להפריך זאת מייד: המכונה שלנו תנחש s כך ש־$|s|\le q(|w|)$, תבדוק האם $(w,s)\in A'$ בעזרת האוב, ואם התשובה שלילית ־ תדחה מייד (שכן **לכל** $|s|\le q(|w|)$ חייב להתקיים $(w,s)\in A'$ ־ זו משמעות $A=\forall A'$). אם כן, במקרה זה קיים ל־M' מסלול חישוב דוחה.

המקרה השני הוא המסובך יותר. אם y כולל את הטענה ש־$w\notin A$ אך בפועל $w\in A$, כיצד נפריך את הטענה? לצורך כך אנו דורשים כי y יכיל, בנוסף לטענה ש־$w\notin A$, גם "הוכחה" לכך ־ s כך שמתקיים $(w,s)\notin A'$ ו־$|s|\le q(|w|)$. אם כן, המכונה שלנו יכולה לבדוק, עבור זוג (w,s) הנתון ב־y, האם אכן $(w,s)\notin A'$ ו־$|s|\le q(|w|)$. אם y שיקר ובפועל $w\in A$ אז מובטח לנו שיתקיים $(w,s)\in A'$ ושוב נתפוס את y בשקר ונדחה כנדרש.

בבירור M' פולינומית. גם אורך y הוא תמיד פולינומי ב־x שכן תיאור (1) הוא פולינומי ב־x שהרי M פולינומית; תיאור (2) הוא פולינומי ב־x שכן M שואלת רק מספר פולינומי של שאלות ולכל אחת מהן התשובה היא ביט בודד, ותיאור (3) הוא פולינומי כי יש מספר פולינומי של "הוכחות", ואורך כל הוכחה הוא חסום על ידי $q(|w|)$, ו־$|w|$ עצמו חסום על ידי זמן הריצה של M. מכל אלו אנו מסיקים כי קיים פולינום $p(n)$ כך ש־$|y|\le p(|x|)$ לכל $(x,y)\in L'$, כנדרש.

Σ_n^p ו-Π_n^p-שלמות

כהרגלנו עם מחלקות סיבוכיות חדשות אנו מחפשים בעיות שהן שלמות במחלקת סיבוכיות זו (במקרה זה, ביחס למחלקה P). השפות שנציג מהוות גשר בין השפה ה-NP-שלמה SAT ובין השפה ה-PSPACE-שלמה TQBF.

נשתמש ב-$\varphi(u_1, u_2, \ldots, u_n)$ לסימון פסוק (לא בהכרח CNF) כאשר $u_1, \ldots, u_n$ מייצגים לא משתנים בודדים אלא סדרות של משתנים. נגדיר:

$$\begin{aligned}\Sigma_n\mathrm{SAT} &= \{\exists u_1 \forall u_2 \ldots Q u_n \varphi(u_1, \ldots, u_n) \,|\, \exists u_1 \forall u_2 \ldots Q u_n \varphi(u_1, \ldots, u_n) = 1\} \\ \Pi_n\mathrm{SAT} &= \{\forall u_1 \exists u_2 \ldots Q u_n \varphi(u_1, \ldots, u_n) \,|\, \forall u_1 \exists u_2 \ldots Q u_n \varphi(u_1, \ldots, u_n) = 0\}\end{aligned}$$

במילים - אלו הם פסוקי QBF אמיתיים לוגית שבהם אנו מגבילים את מספר האלטרנציות בין הכמתים של קיים ולכל.

בבירור $\mathrm{SAT} = \Sigma_1\mathrm{SAT}$ ו-$\overline{\mathrm{SAT}} = \Pi_1\mathrm{SAT}$ (כאן SAT היא שפת הפסוקים הספיקים, לא רק פסוקי ה-CNF הספיקים). כמו כן ניתן לחשוב אינטואיטיבית על TQBF כעל "$\Sigma_\infty\mathrm{SAT}$" או "$\Pi_\infty\mathrm{SAT}$" - כלומר, מספר האלטרנציות **אינו חסום** (אך כמובן שלכל פסוק ספציפי ב-TQBF הוא סופי שכן הפסוק כולו סופי).

נעבור להוכחה כי בעיות אלו הן שלמות, ונסתפק בבעיות ה-Σ_n^p-שלמות. קל לראות באמצעות האפיון האלטרנטיבי ש-$\Sigma_n\mathrm{SAT} \in \Sigma_n^p$ - פשוט נגדיר $L' = \{(\varphi, u_1, \ldots, u_n) \,|\, \varphi(u_1, \ldots, u_n) = 1\}$

וכעת $\Sigma_n\mathrm{SAT} = \{x | \exists y_1 \forall y_2 \ldots Q y_k : (x, y_1, \ldots, y_k) \in L'\}$, מה שמראה שייכות ל-$\Sigma_n^p$ על פי ההגדרה ה"מפורשת" שהצגנו קודם.

כעת נראה כי השפה היא Σ_n^p-קשה, ונצטרך לבצע חלוקה למקרים.

נניח כי n הוא אי זוגי. תהא $L \in \Sigma_n^p$, אז קיים פולינום $p(n)$ ושפה $L' \in \mathrm{P}$ כך ש-$L = \{x | \exists_p y_1 \forall_p y_2 \ldots \exists_p y_n : (x, y_1, \ldots, y_n) \in L'\}$.

תהא M' המכונה עבור L'. אז מתוך $\langle M' \rangle$ ו-x ניתן לבנות, באותה טכניקה של משפט קוק, פסוק $\varphi_{M,x}(Y_1, \ldots, Y_n, Z)$ שמבצע סימולציה של ריצת M על $(x, y_1, \ldots, y_n)$, כאשר x מקודד בתוך $\varphi_{M,x}$ ואילו לכל i, Y_i היא קבוצת משתנים שמתארת את המחרוזת y_i (אשר אורכה חסום על ידי $p(|x|)$ כך שניתן פשוט לכלול ב-Y_i משתנים המתארים כל ביט של y_i) ו-Z היא קבוצת משתני העזר של הפסוק.

נשים לב כי $\varphi_{M,x}(Y_1, \ldots, Y_n, Z) \in \Sigma_n\mathrm{SAT}$ שכן ניתן "לאחד" את Y_n ו-Z אל תוך u_n (כי כל שנדרש ממשתני העזר Z הוא שקיימת השמה כלשהי עבורם שמספקת את הפסוק). דהיינו, $u_i = Y_i$ לכל $1 \le i < n$ ו-$u_n = Y_n Z$.

הנקודה המהותית כאן היא שאמנם קבוצות המשתנים שלנו הן גדולות בהרבה בגודלן מ-n, אבל מספר **האלטרנציות** הנדרש לנו אינו גדול יותר.

אם n הוא זוגי, קיימת שפה $L' \in \mathrm{P}$ ופולינום $p(n)$ כך ש-$L = \{x | \exists_p y_1 \forall_p y_2 \ldots \forall_p y_n : (x, y_1, \ldots, y_n) \in L'\}$. גם כאן נבנה פסוק $\varphi_{M,x}(Y_1, \ldots, Y_n, Z)$ שמבצע סימולציה של ריצת M' על $(x, y_1, \ldots, y_n)$, אך הפעם עלינו לבנות את הפסוק באופן כזה שהשמה למשתני העזר Z שאיננה חוקית דווקא **מספקת** את הפסוק (ולכן השאלה האם $\exists Y_1 \ldots \forall Y_n, Z \varphi_{M,x}(Y_1, \ldots, Y_n, Z) = \mathrm{T}$ תלויה באופן התנהגות M' על השמה שבה ה-Z-ים אכן מתארים ריצה חוקית של M').