תורת החישוביות – תרגול מס' 10
השפה SAT ווריאציות עליה

המחלקות P ו־NP – תזכורת

P היא מחלקת השפות שיש מכונות טיורינג דטרמיניסטיות בעלות זמן ריצה פולינומי (או בקיצור – "מכונות פולינומיות") שמקבלות אותן.

NP היא מחלקת השפות שיש מכונות טיורינג **אי דטרמיניסטיות** פולינומיות שמקבלות אותן.

ל־NP יש אפיון נוסף שנזכיר כעת. יחס $R \subseteq \Sigma^* \times \Sigma^*$ הוא:

- חסום פולינומית אם קיים פולינום $p(n)$ כך שלכל $(x,y) \in R$ מתקיים $|y| \le p(|x|)$ (הגודל של y מוגבל להיות פולינומי בגודל של x).
- ניתן לזיהוי פולינומי אם השפה $L = \{(x,y) \mid (x,y) \in R\}$ מקיימת $L \in \mathrm{P}$ (בהינתן זוג x,y ניתן לבדוק דטרמיניסטית בזמן פולינומי ב־x אם הם ביחס R או לא).

בהינתן יחס R ניתן להגדיר באמצעותו שפה באופן הבא: $L = \{x | \exists y : (x,y) \in R\}$. דהיינו, L כוללת את כל ה־x־ים שיש עבורם y **כלשהו** כך שהזוג x,y נמצא ביחס R.

לעתים עוזר לחשוב על y כעל "הוכחה לשייכות x לשפה L". ההוכחה היא קצרה יחסית (R חסום פולינומית) וניתן לבדוק בקלות יחסית אם y אכן מוכיח ש־x שייך לשפה (R ניתן לזיהוי פולינומי).

משפט: $L \in \mathrm{NP}$ אם ורק אם קיים R שהוא חסום פולינומית וניתן לזיהוי פולינומי כך ש־$L = \{x | \exists y : (x,y) \in R\}$.

השפה SAT

בתחשיב הפסוקים משתמשים ב**משתנים** $x_1, x_2, \ldots$ שיכולים לקבל ערכי אמת ושקר ־ T ו־F (או 1 ו־0). **שלילה** של משתנה x מסומנת ב־$\overline{x}$.
ליטרל u הוא משתנה או שלילתו של משתנה.

פסוקית CNF היא ביטוי מהצורה $C = (u_1 \vee u_2 \vee \ldots \vee u_k)$ כאשר $u_1, \ldots, u_k$ הם ליטרלים.

פסוק CNF הוא ביטוי מהצורה $C_1 \wedge C_2 \wedge \ldots \wedge C_t$ כאשר $C_1, \ldots, C_t$ הן פסוקיות CNF.

השמה לפסוק CNF היא פונקציה שמתאימה לכל משתנה ערך T או F. ברגע שבו נקבעת השמה למשתנים, נקבע באופן חד משמעי ערך האמת של הפסוק כולו ($\overline{x}$ מקבל ערך הפוך מ־x; פסוקית מקבלת ערך T אם אחד מהליטרלים שמופיעים בה מקבל ערך T; פסוק מקבל ערך T רק אם כל הפסוקיות שלו מקבלות ערך T).

פסוק CNF הוא **ספיק** אם קיימת השמה שנותנת לו ערך T.

SAT היא שפת כל פסוקי ה־CNF הספיקים.

אם יש לנו פסוק CNF שבו כל פסוקית מכילה **בדיוק** k ליטרלים, אומרים שזהו פסוק $k - \mathrm{CNF}$. השפה $k - \mathrm{SAT}$ היא אוסף פסוקי ה־$k - \mathrm{CNF}$ הספיקים. בתרגול זה נתעניין במיוחד בשפות 3SAT ו־2SAT.

3SAT

שייכות ל־NP: הגדרה באמצעות מ"ט א"ד

ראשית נרצה לראות כי $3\mathrm{SAT} \in \mathrm{NP}$. מכונה אי־דטרמיניסטית עבור 3SAT פועלת כך: בהינתן פסוק φ המכונה בודקת אם זהו פסוק 3CNF ואחרת היא דוחה מייד. אם הפסוק חוקי, המכונה מנחשת השמה τ ומחשבת את $\tau\left(\varphi\right)$ (ערך האמת שההשמה τ נותנת ל־φ). אם הערך הוא T, המכונה מקבלת, ואחרת היא דוחה.

ניחוש τ דורש זמן פולינומי שכן τ היא מחרוזת בת n ביטים (כאשר n הוא מספר המשתנים בפסוק) ו־$n \le |\varphi|$. גם חישוב $\tau\left(\varphi\right)$ דורש זמן פולינומי (כל פסוקית יש לבדוק רק פעם אחת). לכן המכונה פולינומית.

אם φ ספיק אז קיימת τ שמספקת אותו, ולכן במסלול החישוב שבו המכונה מנחשת את τ היא תקבל, ומכאן שהמכונה מקבלת את φ.

אם φ אינו ספיק אז לכל τ יתקיים $\tau\left(\varphi\right)=\mathrm{F}$ ולכן המכונה תדחה בכל מסלול חישוב ולכן היא תדחה את φ.

שייכות ל־NP: הגדרה באמצעות יחס

נרצה כעת להראות כי $3\mathrm{SAT} \in \mathrm{NP}$ באמצעות ההגדרה האלטרנטיבית. עלינו להציג יחס R שהוא חסום פולינומית, ניתן לזיהוי פולינומי ומגדיר את 3SAT.

נגדיר אם כן את היחס $R=\{(\varphi,\tau)\mid$ פסוק 3CNF φ ו־τ השמה שמספקת אותו$\}$.

היחס חסום פולינומית כי כפי שכבר הערנו, $|\tau| \le |\varphi|$.

היחס ניתן לזיהוי פולינומי כי כפי שכבר הערנו, בהינתן τ קל לחשב את $\tau\left(\varphi\right)$ (יש גם לוודא כי φ הוא פסוק 3CNF).

היחס בבירור מגדיר את 3SAT.

$\mathbf{SAT} \le_p \mathbf{3SAT}$

נראה כעת רדוקציה פולינומית מ־SAT אל 3SAT. יחד עם מה שכבר ראינו, זה מוכיח כי 3SAT היא NP־שלמה.

מספיק להראות איך לתרגם פסוקית אחת $C=\left(u_1 \vee u_2 \vee \ldots \vee u_n\right)$ לפסוק 3CNF; עבור פסוק כללי אפשר להפעיל את התהליך על כל פסוקית לחוד.

אם $C=\left(u_1\right)$ אז מתרגמים אותה לפסוקית $\left(u_1 \vee u_1 \vee u_1\right)$.

אם $C=\left(u_1 \vee u_2\right)$ אז מתרגמים אותה לפסוקית $\left(u_1 \vee u_1 \vee u_2\right)$

אם $C=\left(u_1 \vee u_2 \vee u_3\right)$ משאירים אותה כמות שהיא.

עד כה היה קל לראות שכל השמה שמספקת את הפסוקית המקורית, מספקת גם את החדשה ולהפך.

עבור פסוקית $C=\left(u_1 \vee u_2 \vee \ldots \vee u_n\right)$ כך ש־$n \ge 4$ הפתרון מורכב יותר ודורש שימוש במשתני עזר שנסמן כ־$y_1, y_2, \ldots, y_{n-3}$.

נחליף את הפסוק בסדרת הפסוקיות הבאה:

$$\left(u_1 \vee u_2 \vee y_1\right) \wedge \left(\overline{y_1} \vee u_3 \vee y_2\right) \wedge \ldots \wedge \left(\overline{y_{n-3}} \vee u_{n-1} \vee u_n\right)$$

אם בהשמה כלשהי C מסתפק אז קיים u_k שמקבל T. נגדיר השמה שמספקת את סדרת הפסוקיות החדשה שלנו: למשתנים המקוריים יושמו אותם ערכים כמו בהשמה המקורית, ואילו ל־y_i־ים יושמו ערכים באופן הבא: $y_i=\mathrm{T}$ לכל $i \le k-2$, ו־$y_i=\mathrm{F}$ לאחרים. השמה זו לכל ה־y_i־ים מספקת את כל הפסוקיות למעט $\left(\overline{y_{k-2}} \vee u_k \vee y_{k-1}\right)$, ופסוקית זו מסתפקת שכן u_k מקבל ערך T. הראינו כי אם C היה ספיק, כך גם הפסוקית החדשה, ועם "אותה השמה" (פרט לכך שמשתני העזר החדשים מקבלים ערכים שלא נכללו בהשמה המקורית).

בכיוון השני, אם יש השמה שמספקת את הפסוק החדש, אז נראה כי אותה השמה כשהיא מצומצמת למשתנים שב־C מספקת את C. אם לא, אז בהכרח כל ה־u_k־ים מקבלים F. כעת נראה באינדוקציה כי כל ה־y_i־ים מקבלים את הערך T: הבסיס ברור שכן בפסוקית $\left(u_1 \vee u_2 \vee y_1\right)$ אם y_1 לא יקבל T הפסוקית לא תסתפק. כעת נתבונן בפסוקית $\left(\overline{y_{i-1}} \vee u_{i+1} \vee y_i\right)$. $\overline{y_{i-1}}$ מקבל F על פי הנחת האינדוקציה (כי y_i קיבל T) ו־u_{i+1} מקבל F על פי ההנחה ש־C לא הסתפק; בהכרח y_i מקבל T. אולם כעת נקבל כי y_{n-2} מקבל T ולכן הפסוקית $\left(\overline{y_{n-2}} \vee u_{n-1} \vee u_n\right)$ אינה מסתפקת – סתירה.

2SAT

בניגוד ל־3SAT שהיא NP־שלמה, השפה 2SAT שייכת ל־P. נתאר כאן אלגוריתם שמכריע, בהינתן פסוק 2CNF, האם הוא ספיק או לא.

הרעיון הבסיסי הוא שניתן לחשוב על פסוקית מהצורה $(\overline{x} \vee y)$ כפסוקית מהצורה $(x \Rightarrow y)$, וגם כפסוקית מהצורה $(\overline{y} \Rightarrow \overline{x})$. מכאן שניתן לבנות עבור פסוק 2CNF φ את "גרף הגרירות" שלו שצמתיו הם הליטרלים של הפסוק (כלומר, x ו־$\overline{x}$ לכל משתנה x שמופיע בפסוק), והפסוקית $(\alpha \vee \beta)$ מייצרת את הקשתות $\overline{\alpha} \to \beta$ ו־$\overline{\beta} \to \alpha$. הרעיון הוא שאם $\beta \to \alpha$ אז מתן ערך T ל־α מאלץ אותנו לתת ערך T גם ל־β.

שימו לב לסימטריה של הגרף: אם יש קשת $\beta \to \alpha$ אז יש גם קשת $\overline{\alpha} \to \overline{\beta}$. מכאן שאם יש מסלול $\beta \rightsquigarrow \alpha$ יש מסלול $\overline{\alpha} \rightsquigarrow \overline{\beta}$.

כעת ניתן לנסח קריטריון תורת־גרפי לספיקות φ: φ **אינו ספיק** אם ורק אם קיים משתנה x כך שיש מסלול מ־x אל $\overline{x}$ ומסלול מ־$\overline{x}$ אל x (כלומר, x ו־$\overline{x}$ נמצאים על מעגל מכוון). ברור כי קיום זוג מסלולים שכזה מבטיח שהפסוק אינו ספיק. בכיוון השני, המטרה היא לבצע השמה של ערכי אמת לצמתי הגרף כך שאם $u \to v$ אז לא ייתכן ש־v קיבל T ואילו u קיבל F. אם כן, לכל צומת α כך שאין מסלול מ־α אל $\overline{\alpha}$ נבצע השמה של ערכי T ל־α ולכל הצמתים הישיגים ממנו, ו־F לשלילתם. השיטה הזו עשויה להיתקל בשתי בעיות: ניתקל בבעיה אם יש β כך ש־$\beta, \overline{\beta}$ שניהם ישיגים מ־α, אבל בשל הסימטריה של הגרף זה אומר ש־$\overline{\alpha}$ ישיג מ־$\overline{\beta}$ ולכן $\overline{\alpha}$ ישיג מ־α והנחנו שזה לא קורה. כמו כן עשויה להיות בעיה אם יהיה צומת β שאנו רוצים לתת לו ערך T אבל כבר קיבל קודם ערך F; אבל אם זה קרה, זה בהכרח קרה כאשר ב־$\overline{\beta}$ הושם T ואז גם ב־$\overline{\alpha}$ היה צריך להיות מוצב T (כי אם $\alpha \rightsquigarrow \beta$ אז $\overline{\beta} \rightsquigarrow \overline{\alpha}$).

אם כן, אלגוריתם ההשמה שהגדרנו אכן עובד. קל לראות שההשמה הזו אכן מספקת את φ.

כעת כל שנותר לעשות כדי לבדוק האם φ ספיק או שאינו ספיק הוא לבנות את הגרף המתאים ולבצע DFS מכל צומת. אם נמצא זוג צמתים $x, \overline{x}$ שיש מסלול מכל אחד מהם אל השני, לדחות; ואחרת לקבל. ביצוע DFS־ים שכאלו הוא כמובן פולינומי, ומכאן ש־$2\text{SAT} \in \text{P}$.