

חישוב לא יוניפורמי

מודל יוניפורמי(עסקנו קודם) הוא מודל בו קיימת הנחה שישנו אלגוריתם אחד לכל אורך קלט.

- היום:**
- 2 מודלים לא יוניפורמיים: אלגוריתם שונה לכל אורך קלט.
 - חישוב לא יוניפורמי נלמד כנסיון נוסף להבין את שאלת P מול NP .
 - להוכיח שקילות בין המודלים.
 - נסיק מסקנות לגבי שאלת P מול NP .

מודל לא יוניפורמי ראשון - מודל מעגלים

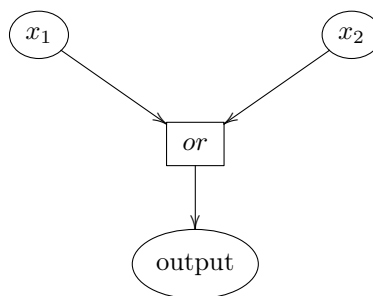
הגדרה - מעגל בוליאני

גרף מכוון בעל שלושה סוגי קודקודים:

- קלט - קשתות יוצאות
- שער - קשתות נכנסות/יוצאות
- פלט - קשת אחת שנכנסת

דוגמא

מעגל שמחשב or של שני משתנים:



מעגל מסויים יכול לטפל באורך קלט מסויים, ולכן נעסוק במשפחות של מעגלים. במשפחה של מעגלים, יש מעגל לכל אורך קלט.

הגדרה

נאמר שמשפחה של מעגלים $\{C_n\}_{n=1}^{\infty}$ מחשבת פונקציה $f : \{0, 1\}^* \rightarrow \{0, 1\}$ אם לכל קלט $x \in \{0, 1\}^*$ מתקיים

$$f(x) = 1 \iff C_{|x|}(x) = 1$$

גודל של מעגל - אמת מידה של הסיבוכיות שלו. גודל המעגל C מסומן ב- $|C|$, מייצג את מספר הקשתות במעגל.

הערה

בהינתן מעגל $C_{|x|}$ וקלט x נוכל לחשב את $C(x)$ בזמן שתלוי פולינומית ב- $|C|$.

הגדרה

קבוצה $A \subseteq \{0, 1\}^*$ ניתנת להכרעה ע"י משפחת מעגלים בגודל פולינומי אם קיימת משפחה של מעגלים $\{C_n\}_{n=1}^{\infty}$ כך שלכל קלט $x \in \{0, 1\}^*$ ופולינום $P(\cdot)$ כך שלכל קלט $x \in \{0, 1\}^*$, $x \in A \iff C_{|x|}(x) = 1$ וכן $|C_{|x|}| \leq P(|x|)$.

מודל לא יוניפורמי שני - מכונת טיורינג שמקבלת עצה

הגדרה

נאמר שפונקציה $f : \{0, 1\}^* \rightarrow \{0, 1\}$ שייכת למחלקה P/l עבור פונקציה $l : \mathbb{N} \rightarrow \mathbb{N}$ אם קיימת מ"ט A פולינומית וסדרה אינסופית של מחרוזות עצה $\{a_n\}_{n=1}^{\infty}$ כך שמתקיימים התנאים הבאים:

$$1. \text{ לכל } x \in \{0, 1\}^* \text{, } A(a_{|x|}, x) = f(x)$$

$$2. \text{ לכל } n \in \mathbb{N} \text{, } |a_n| = l(n)$$

הגדרה

$$P/poly = \bigcup_{\substack{p = p(n) \\ \text{polynomial}}} P/p$$

$P/poly$ - בעיות הכרעה הניתנות להיות מוכרעות ע"י מ"ט הרצה בזמן פולינומי ומקבלת עצה בעלת אורך פולינומי באורך הקלט.

נשים

לא להתבלבל בין העצה של $P/poly$ לבין העד של NP .

ננסה להבין את הכוח הטמון בעצה

תהי $f: \mathbb{N} \rightarrow \{0, 1\}$ פונקציה לא כריעה כלשהי (ראינו בחישוביות שפונקציות כאלו קיימות). נגדיר $f': \{0, 1\}^* \rightarrow \{0, 1\}$ ע"י $f'(|x|) := f(|x|)$. נשים לב שאם f אינה כריעה אזי גם f' אינה כריעה. לכן, ע"פ הנחתנו, f' אינה כריעה. אבל $f' \in P/1$ כי $f \notin P$. f' אינה ב- P . ע"פ הגדרת f' , $f'(x_1) = f'(x_2)$ (נותן ערך זהה) לכל $x_1, x_2 \in \{0, 1\}^*$ המקיימים $|x_1| = |x_2|$. לכן נגדיר את מכונת הטיורינג שמכריעה את f' ומשתמשת בעצה באורך 1 להיות מכונה המחזירה את ערך העצה $f'(|x|) = a_{|x|}$.

מסקנה

$$P = P/0 \subsetneq P/1 \subseteq P/poly$$

שקילות בין המודלים

טענה

קבוצה A שייכת ל- $P/poly$ \iff קיימת משפחת מעגלים פולינומית המכריעה את A .

הוכחה

\implies נניח שקיימת משפחת מעגלים $\{C_n\}_{n=1}^\infty$ פולינומית שמכריעה את A . נראה ש $A \in P/poly$:

נבנה מ"ט M המקבלת קלט $x \in \{0, 1\}^*$ ועצה שהינה מעגל $C_{|x|}$. $M(x, C_{|x|})$ - מכונת הטיורינג M מריצה את המעגל $C_{|x|}$ (שהתקבל כעצה) עם הקלט x ומחזירה את התשובה.

מכיוון שמשפחת המעגלים חסומה פולינומית, אזי העצה חסומה פולינומית ב- $|x|$. מכריעה את A אזי אם M מכריעה את A ולכן $A \in P/poly$.

\impliedby נניח כי $A \in P/poly$, כלומר קיימת מ"ט המקבלת עבור קלט x עצה בגודל חסום ע"י $P(|x|)$ עבור פולינום $P(\cdot)$ ומכריעה את A , כלומר מחזירה 1 אם $x \in A$:

$$x \in A \iff M(x, a_{|x|}) = 1$$

המכונה M ניתנת להמרה לסדרת מעגלים $\{C_n\}_{n=1}^\infty$ המכריעה את A , והיא חסומה פולינומית באופן הבא: עבור זוג של קלט x ועצה $a_{|x|}$ קיים מעגל $C_{|x|}^*$.

בוליאני המקבל כקלט את x ו $a_{|x|}$ שמחזיר ערך הזהה ל $M(x, a_{|x|})$ וגודלו חסום פולינומית בזמן הריצה של M . כלומר חסום פולינומית ע"י $P(|x|)$ עבור פולינום $P(\cdot)$ כלשהו.

נבנה כעת מעגל $C_{|x|}$ המקבל כקלט את x בלבד כך שמתקיים $C_{|x|}(x) = C_{|x|}^*(x, a_{|x|})$. נעשה זאת ע"י שנקבע במעגל $C_{|x|}^*$ את המשתנים המתאימים לעצה לקבל את ערך העצה המתאים ל $|x|$ ואח"כ נפשט לוגית את המעגל כך שמתקבל מעגל התלוי במשתני x בלבד, $C_{|x|}$ הרצוי.

אם $P = NP$ אזי מתקיים $NP \subseteq P/poly$.

משפט

אם $NP \subseteq P/poly$ אזי $PH = \Sigma_2$.

הוכחה

נראה שאם $NP \subseteq P/poly$, $\Pi_2 \subseteq \Sigma_2$ (ע"פ משפט שראינו בשיעור שעבר אזי $PH = \Sigma_2$).
 תהי $A \in \Pi_2$ ונניח $NP \subseteq P/poly$. נראה $A \in \Sigma_2$.
 $\Pi_2 \subseteq \Sigma_2 \iff A \in \Sigma_2$ נראה $A \in \Sigma_2$.
 $A \in \Pi_2$, ז"א קיים פולינום $P(\cdot)$ ומוודא V כך שלכל x

$$\forall y \exists z |y|, |z| < P(|x|), V(x, y, z) = 1 \iff x \in A$$

נגדיר B באופן הבא:

$$(x, y) \in B \iff \exists z |z| \leq P'(|(x, y)|), V'((x, y), 2) = 1$$

$$V'((x, y), 2) = V'(x, y, z)$$

$$P'(|(x, y)|) = P'(|x| + P(|x|)) = P'(|x|) + P'P(|x|)$$

ולכן $B \in NP$, ועל פי הנחתנו $NP \subseteq P/poly$ ולכן $B \in P/poly$

$$\forall y |y| < P(|x|), (x, y) \in B \iff x \in A$$

$$\exists \text{circle } C_x \forall y V'(C_x, y, x) \iff x \in A???$$

$$C_x = (C_1^x, \dots, C_{P(|x|)}^x)$$

$f(x, y) \in B \iff (x, y) \in B$ כלומר - SAT ל B קיימת רדוקציית קארפ מ SAT ל B .
 $|f(x, y)| \leq P(|x|)$, SAT

מההנחה $NP \subseteq P/poly$ מסיקים שקיימת סדרת מעגלים $\{C_n\}_{n=1}^\infty$ המכריעים את SAT . לכל x נקבע $C_x := (C_1, \dots, C_{P(|x|)})$ כאשר C_i הוא מעגל המכריע את SAT עבור קלט באורך i .

נראה כעת את תיאור V' :

1. חשב $\varphi = f(x, y)$

2. בדוק בעזרת C_x האם $\varphi \in SAT$, אם לא דחה.

3. אם כן, בצע רדוקציה עצמית ומוצא השמה מספקת ל φ .

4. אם ההשמה שמצאנו מספקת אכן את φ קבל, אחרת דחה.

כעת ברור: אם $\exists y (x, y) \notin B$ אזי V' ידחה, ולכן

$$\exists C_x \forall y V(C_x, x, y) = 1 \iff \forall y (x, y) \in B \iff x \in A$$

ולכן

$$\exists C_x \forall y V'(x, x, y) = 1 \iff x \in A$$

$$\implies A \in \Sigma_2$$

■