יעילות

הגדרה

- תהי M מ"ט (דט') ו־x מחרוזת. נסמן $\text{steps}\left(M,x\right)$ את מספר הצעדים ש־M מבצחת בחישוב על x.(אם $M\uparrow x$ אזי $\text{steps}\left(M,x\right)=\infty$)
- תהי M מ"ט(דט')ו־$f:\mathbb{N}\rightarrow\mathbb{N}$. נאמר כי M פועלת בסיבוכיות זמן f אם לכל x $\text{steps}\left(M,k\right)\leq f\left(\left|x\right|\right)$.
- תהי L שפה, $f:\mathbb{N}\rightarrow\mathbb{N}$. נאמר כי L בעלת סיבוכיות(זמן) f אם קיימת מ"ט M שמכריעה את L, ו־M פועלת בסיבוכיות זמן f.

עבור $f:\mathbb{N}\rightarrow\mathbb{N}$, נסמן $\text{TIME}\left(f\right)$ כאוסף כל השפות L בעלות סיבוכיות זמן $O\left(f\right)$ בפרט אם $g\leq f$(כלומכ לכל n $g\left(n\right)\leq f\left(n\right)$) אזי $\text{TIME}\left(g\right)\subseteq\text{TIME}\left(f\right)$

טענה

תהי L שפה בעלת סיבוכיות זמן f במודל TM_{k}(כלומר מ"ט עם k סרטים). אזי L בעלת סיבוכיות זמן $O\left(f^{2}\right)$ במודל מ"ט עם סרט בודד.

רעיון בהוכחה

אם החישוב של המכונה עם k סרטים לוקח $f\left(n\right)$ צעדים, אזי החישוב של המכונה עם סרט בודד לוקח $f\left(n\right)\cdot2\cdot2\cdot f\left(n\right)=f^{2}\left(n\right)$(המרחק המקסימלי בין שני ראשים הוא $2f\left(n\right)$, בכל צעד יש 2 סריקות, ויש $f\left(n\right)$ צעדים).

נסמן

$$P=\bigcup_{k=1}^{\infty}\text{TIME}\left(n^{k}\right)$$

=אוסף השפות בעלות סיבוכיות זמן פולינומית=אוסף השפות הניתנות להכרעה בזמן פולינומי.

הגדרה

תהי N מ"ט ל"ד, x מחרוזת.

- נסמן $\text{steps}\left(N,x\right)$ את מספר הצעדים המקסימלי שN עושה בחישוב כלשהו על x.
- עבור מ"ט ל"ד N ופונקציה $f:\mathbb{N}\to\mathbb{N}$. נאמר כי N פועלת בסיבוכיות זמן f אם לכל x, $\text{steps}\left(N,x\right)\leq f\left(\left|x\right|\right)$.
- עבור שפה L ופונקציה f, נאמר כי L בעלת סיבוכיות ל"ד f אם קיימת מ"ט ל"ד N שמכריעה את L ופועלת בסיבוכיות זמן f.
- נסמן $\text{NTIME}\left(f\right)$ את קבוצת השפות בעלות סיבוכיות ל"ד $O\left(f\right)$

נניח L בעלת סיבוכיות זמן ל"ד f. מה ניתן להגיד על הסיבוכיות הדט' של L?
אם רוצים לעבור על כל מסלול, ונניח שבכל צעד יש רק 2 אפשרויות, אז סה"כ יש $2^{f(n)}$ מסלולים.

נסמן

$$NP=\bigcup_{k=1}^{\infty}\text{NTIME}\left(n^{k}\right)$$

שאלה

$$\boxed{P\overset{?}{=}NP}$$

זוהי שאלה מהותית - האם קיימות בעיות שניתן לפתור בNP אבל לא בP?

$\mathbf{NP'}$

לפעמים יש בעיות שקשה למצוא את התשובה, אבל קל לבדוק את התשובה. למשל - האם יש בגרף מעגל המילטוני(כלומר מעגל שעובר בכל קודקוד פעם אחת בלבד)? קשה לבדוק את זה, אבל אם מישהו נותן לנו מעגל המילטוני - אפשר לבדוק בזמן לינארי שהתשובה נכונה.

הגדרה

תהי L שפה. נאמר כי $L\in NP'$ אם קיים אלגוריתם A וקבועים b,c,d כך שמתקיים:

1. לכל (x,y), $A\left(x,y\right)$ מבצע לכל היותר $O\left(\left|x,y\right|^{d}\right)$ צעדים.
2. לכל $x\in L$, קיים y, $\left|y\right|\leq\left|x\right|^{b}+c$ כך ש$A\left(x,y\right)=1$.

3. לכל $x \notin L$, לכל y $A(x,y)=0$.

במילים פשוט - $L \in NP'$ אם הבדיקה היא פולינומית - לאו דווקא המציאה.

דוגמה

$HAM \subseteq \{G\}$ כך שבG מעגל המילטוני. $HAM \in$

עוד דוגמה

נותנים לנו נוסחא בצורת CNF - לדוגמה $(x_1 \vee \neg x_2 \vee x_3) \wedge (\neg x_1 \vee \neg x_2) \wedge (x_1 \vee x_3)$.
האם הנוסחא ספיקה? כלומר האם יש הצבה מספקת?
במקרה הזה יש: לדוגמה

$$x_1 = T$$

$$x_2 = F$$

$$x_3 = T$$

דוגמה לנוסחא שאין לה הצבה מספקת: $(x_1) \wedge (\neg x_2)$

הגדרה: $SAT \subseteq \{\psi\}$ כך שψ בצורת CNF והיא ספיקה.

$$SAT \in NP'$$

טענה

$$NP' = NP$$

הוכחה

$\subseteq$ תהי $L \in NP'$, נראה ש$L \in NP$. קיימים A, b, c, d ע"פ ההגדרה של NP'.
נבנה אלגוריתם ל"ד B שמכריע את L בסיבוכיות זמן פולינומית:

$B(x)$:
1. בחר באופן ל"ד y כך ש$|y| \leq |x|^b + c$.
2. הרץ $A(x,y)$ והחזר את התשובה המתקבלת.

מתקיים:
- אם $x \in L$ קיים y ($|y| \leq |x|^b + c$) כך ש$A(x,y)=1$. בחירה של y זה תיתן $B(x)=1$.

- אם $x \notin L$ אזי לכל $A(x,y)=0$
  ⇐ כל חישוב של $B(x)=0$

סיבוכיות: $O\left(|x|^b + c + (|x|+|y|)^d\right) = O\left(|x|^b + c + \left(|x| + |x|^b + c\right)^d\right) =$
$O\left(|x|^{bd}\right)$ - קיבלנו פולינום ב$|x|$.

$\supseteq$ נניח $L \in NP$, נראה $L \in NP'$. כלומר קיים אלגוריתם ל"ד B שפועל בסיבוכיות זמן $O\left(|x|^k\right)$ ומכריע את L. נבנה $A(x,y)$ וb,c,d כהגדרת NP':

$A(x,y)$ (x - קלט, y - רשימת בחירות ל"ד)

1. הרץ $B(x)$ ובכל צעד קבע את החישוב הל"ד ע"פ המחרוזת y, והחזר את התשובה המתקבלת.

מתקיימים:
- אם $x \in L$ אזי קיים חישוב של $B(x)$ שמחזיר 1, ומספר הצעדים של החישוב $|x|^k$. נבחר את y להיות סדרת הבחירות הל"ד בחישוב הנ"ל. $|x|^k \ge |y|$, ועבור הy הנ"ל $A(x,y)=1$.
- אם $x \notin L$ אזי לכל סדרת בחירות ל"ד $B(x) = 0$ (ע"פ הגדרת הכרעה ל"ד).

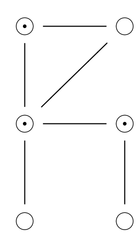
סיבוכיות הזמן של A לינארית (כי y באורך החישוב). ■

מסקנה

ניתן להגדיר את בעיית $P \stackrel{?}{=} NP$ בתור - האם כל בעיה שאפשר <u>לבדוק</u> בזמן פולינומי, אפשר גם <u>למצוא</u> בזמן פולינומי?

דוגמה - כיסוי קודקודים Vertex Cover

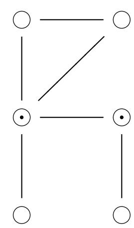
מהו כיסוי קודקודים מינימלי של גרף? כלומר בחירה מינימלית של קודקודים כך שכל הקשתות יגעו באחד הקודקודים הנבחרים?



קלט: (G,n), וצריך לבדוק אם יש ניתן לכסות את הגרף עם n קודקודים. הבעיה בNP' ולכן בNP, שכן בהינתן כיסוי, ניתן לבדוק אם כל הקשתות נכללות בו, ואם מספר הקודקודים קטן או שווה לn, בזמן פולינומי. נסמן: VC

דוגמה נוספת - קבוצה שלטת Dominating Set

קבוצת קודקודים בגרף שכל קודקוד אחר הוא בקבוצה או שכן של אחד הקודקודים בקבוצה.

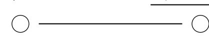
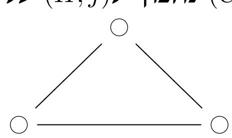


נסמן: DS

טענה

אם $Ds \in P$ אזי גם $VC \in P$. כלומר אם ישנו אלגוריתם פולינומי להכריע את DS אזי ישנו גם אלגוריתם פולינומי להכריע את VC.

הוכחה

נבנה רדוקציה פולינומית מVC לDS. את (G,k) נהפוך ל(H,j) על ידי כך שנהפוך כל קשת למשולש:  יהפוך ל  . כדי לבחור את כל הקודקודים, צריך לבחור אחד מהקודקודים במשולש - אבל אין טעם לבחור את האמצעי, כי תמיד אפשר לבחור במקומו את אחד האחרים, ולכן תמיד נבחר את הקשת במרכז.

מתקיים

אם $(H,j) \in VC$ אזי תהי A קבוצת הקודקודים שמכסה את כל קשתות H. $|A| \leq j$. אזי אותה קבוצת קודקודים גם שולטת על כל קודקודי G, כי עבור הקודקודים השונים כל קודקוד שכן של צלע כלשהי(מניחים שאין קודקודים מבודדים) וכמו כן כל קודקוד חדש שכן לשני צדי הקשת המתאימה ולכן נשלט ע"י הקודקוד שמכסה את הקשת. $\Leftarrow (G,k) \in DS$

ומצד שני

נניח $(G,k) \in DS$. תהי A קבוצת הקודקודים בG, $|A| \geq k$, וA שולטת בG. אזי נבנה מA קבוצה A' כך שבA' יש רק קודקודים מH, $|A| = |A'|$, על ידי כך שכל קודקוד של A שאינו מH נחליף באחד משני השכנים שלו. אזי A' קבוצה שלטת בG, כי כל קודקוד שנשלט בA ע"י קודקוד מH ממשיך להיות נשלט גם בA'. קודקוד שנשלט ע"י קודקוד שאינו מH, נשלט במקור ע"י קודקוד חדש אבל עתה נשלט ע"י השכן שנבחר(וע"פ בנייה). בפרט, A' שולט על כל הקודקודים החדשים.

כל קודקוד כנ"ל שכן רק לשני קודקודים שבצידי הקשת המתאימה $\Leftarrow$ הקודקוד ששולט על הקודקוד החדש גם מכסה את הקשת $\Leftarrow$ A' כיסוי קודקודים.