

17.3.09

סיכום - שיעור 3

אבטור: עמיתים עמיתים של הקורס מאז הקורס
 קובץ: 15 בלוג, יום שני

צמח עמיתים

1. Independent Set: היתוך של G ומסלול A , האם יש G

קבוצה בלתי פתוחה A . שייך NP - P . (אילו NP - P)

2. HAMPATH: היתוך של G , האם יש מסלול שמתחיל בנקודה

בדיוק כפי שצוה. שייך NP - P . (אם NP - P)

3. Linear Programming: היתוך של n משוואות

$$\begin{cases} 2x - 3y + 5z \geq 7 \\ 4x + 2y - z \leq 10 \\ \dots \end{cases}$$

האם יש למעשה פתרון בממשיים? (למשל, $\log m \cdot m$)

האם B הוא המסלול הארוך ביותר בקבוצה. המסלול P במסלול

למסלול הארוך ביותר (1971).

4. Integer Programming: צורת מסלול הקובעת, אך שאלה האם יש פתרון

בממשיים? המסלול שייך NP - P (צריך להחליט האם המסלול P הוא

צריך להחליט האם יש המסלול הארוך ביותר. האם יש NP - P

NP - P).

5. Graph Isomorphism: היתוך של G_1, G_2 , האם הם

איזומורפיים, כלומר האם הם אותו מסלול שייך NP - P (צריך להחליט האם המסלול P הוא

המסלול NP (נוצח במאמצים במחשבים האמיתיים של הקורסאים)

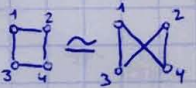
G_1 (אם G_2). כל אלה פתוחים האם בדיק P (אם האם הוא NP - P)

אם האמת P היא P (כי יש כזה היום אלגוריתם למערכת לסיבות).

6. Compositeness: האם מסלול N ניתן הוא פריק (כלומר, לא ראשוני)?

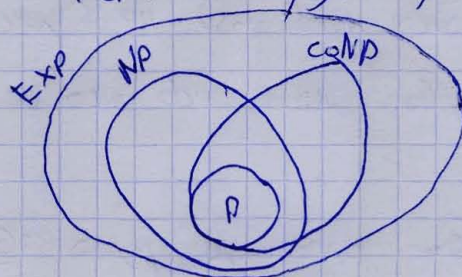
צריך לשקלל כי אולי הקבוצה היא $\log N$ ולא N . הן אלו P הבעיה

NP - P . ב-2002 הוכחו כי היא P . (Agarwal Kayana Saxena)



7. Primality: בתוך מספר N , האם הוא ראשוני? בעיה ב-P (כי הולכת לה ב-P), אך לא ידוע ש"גיה ~~היא~~ ב-P. היע
 ב-NP בזכות Pratt ב-1975. (האזינו לא הסתכן).
 גבא! ראשוני אזר ולתת! 1,133,836,730,401

8. Factoring: בתוך מספר N ומספר A , האם יש מחלק
 ראשוני במרום בין 2 ל- A ? הבעיה נקראת שבתוך A יש
 פצצה כי מוכח שיש מחלק ראשוני קטן יותר מ- $\sqrt{N}$. נכלול
 תחום בינוי של מחלק ראשוני A ב- A בלתי תלוי ב- A , מחלקים
 אחרים A ב- A ומשלים קטנה בלתי תלוי ב- A מחלק
 (בס. נתיב). הבעיה ב-NP (המחלק יתקן בלתי תלוי מחלק הראשוני
 שיתן מ- A . לא ידוע אלא מחלק שיתן ראשוני כי אולי לא ראשוני אלא
 ש או מחלק ראשוני במרום בין 2 ל- A). הבעיה היא ש- $NP \neq coNP$.
 המושג ידוע כיום לראשונה ש- A וייתכן ש- NP מספר בין 2 ל- A .
 מכיוון שהבעיה שיתן $NP \neq coNP$, לא מאמינים שהיא NP -שלמה
 כי אם $NP = coNP$. הבעיה היא בהכרח ש- A מוכח בהכרח RSA
 ומאמינים שהיא קשה למכין (לא ב-P).



למאנים שכן נראה כי אולי נון של הקבוצה, אך ייתכן של אחר
 מהחברים ב- P .

$$EXP := \bigcup_{c \geq 1} DTIME(2^{cn})$$

$$P \subseteq NP \subseteq EXP$$

לסמן

בוכחה: $P \subseteq NP$: אולי לומר בלתי ב-P. (נראה שהיא ב-P ב-NP.
 מכיוון ש- $P \subseteq NP$, יש אמצעי מ שמתחיל ב- P סוף תהליך.
 האמצעים המוכחים שיתן מוכח, ונראה ש- A ב- P ונתיב
 אחר המוכח

$NP \subseteq EXP$: גרסא שבה $L \in NP$. לפי האזרה, קיים אלגוריתם גנרלי מ שהזכר

פונקציונלי, ופונקציון q שמיצב את המידע. נניח שאנחנו מ' מנסים

את $M(x, w)$ על q $2^{|x|}$, מס' w ומקבל גנרלי מנסים

את מהירות קריאה. קל לראות כי מ' מנסה את L

הוא בזמן אקספוננציאלי, ולכן $L \in EXP$

הוכחה חלופית ל-NP

נניח גנרלי מ' אלגוריתם לא דטרמיניסטי. זהו אלגוריתם וואל אם היכול לנסות

"כניס" אל דטרמיניסטי" שאומר לנו להחליט לפי גנרלי מנסים מהי התוצאה.

האלגוריתם מקבל את x ופונקציון q שמיצב את המידע. מקבל

מחר אלגוריתם לא דטרמיניסטי, הוא בזמן $T(n)$ על q היכול לנסות

מס' w בזמן $T(n)$.

הוכחה נניח שבה L ש"כ L - $NTIME(T(n))$ קיים גנרלי מ

אלגוריתם לא דטרמיניסטי שהזכר בזמן $T(n)$.

$$NP = \bigcup_{c=1}^{\infty} NTIME(n^c)$$

הוכחה $NP \subseteq \bigcup_{c=1}^{\infty} NTIME(n^c)$: גרסא L שבה $L \in NP$. לפי האזרה, קיים

אלגוריתם ~~מנסה~~ מנסים ופונקציון q שמיצב את המידע.

הוא. נניח אלגוריתם לא דטרמיניסטי:

```

bool w[p(x)];
for i=1 to p(x)
  non-det-choice {
    w[i]=0
  } or {
    w[i]=1
  }
return M(x, w)

```

קל לראות שזוהי התוצאה פונקציונלית.

והאלגוריתם מנסה נניח את L .

הקטן L של כל c $\bigcup_{c \geq 1} \text{NTIME}(n^c) \subseteq \text{NP}$ או לא?

מ שר בשטן יט עבד גשמו סכס. נמנן אסורין מוונג י' מ שר
בשטן סוף ואלא ונקט ער קאט יט. י' מ גרף אט מ סורה סתרי.
סורה ונעטרי בער אל מנר יחילט מר לעמל קב צולן לו צרמניס י' י'
אמ י' ס צול מרקא, י' ער שטאל אט היינטיג נקט. אט אין ס צול
נקט אט אין ער שיצורס י' מ מוונג.

NP - פונקציונליות

הערה רצוק'י (karp) בולגריה נמסר A לסבר B היל
+ שנתן כחשוד במס בולגריה קן עכס x.

$$x \in A \iff f(x) \in B$$

$$A \leq_p B \quad \text{no} \quad \exists f, g \text{ s.t. } W, P \text{ etc}$$

$A \in_p C$	של	$B \in_p C$	פולי	$A \in_p B$	פולי	1	<u>דיוק</u>
אם P (עבור) $A \in P$	של	$B \in P$	פולי	$A \in_p B$	פולי	2	
(הוכחה) $A \in NP$	של	$B \in NP$	פולי	$A \in_p B$	פולי	3	
(Code) $A \in NP$	של	$B \in NP$	פולי	$A \in_p B$	פולי		

$B \leq_p A$ $\Rightarrow$ $B \in NP$ $\wedge$ $x \in NP$ $\Rightarrow A$ $\Rightarrow$ yes

NP - NP PC1 NP - 2 A's PC NP A NP

כש' 18/7 ה'תש"ס נפטר מן העולם קק-177.