תרגול 1

יום רביעי 02 מרץ 2016 12:07

רדוקציה עצמית

מחלקת סיבוכיות -

קבוצה של בעיות חישוביות בעלות סיבוכיות משאבים(זמן, מקום וכו') דומה.

- ניתן לדבר על סוגים שונים של בעיות ואופן הגדרתן.
- דוגמא קלאסית על בעיה היא SAT העוסקת בסיפוקיות של נוסחאות בוליאניות
- פעמים רבות נדבר על המקרה הפרטי שהנוסחה נתונה בפורמט CNF:
  $\phi = (x_{11} \vee x_{12} \vee \cdots \vee x_{1n}) \wedge (x_{21} \vee \cdots \vee x_{2n}) \wedge \cdots \wedge (x_{m1} \vee x_{m2} \vee \cdots \vee x_{mn})$
- ניתן לשאול אל השאלות הבאות:
  - האם קיימת השמת אמת המספקת את ϕ?
  - מהי השמת האמת המספקת את ϕ ? (או שנחזיר " ⊥ " אם לא קיימת השמה שמספקת את הנוסחא)

ההבדל שבין 2 השאלות הללו מוביל ל-2 צורות אופייניות להצגת בעיה נתונה:

- בעיית ההכרעה - המטרה היא לקבוע האם קיים פתרון לבעיה נתונה או לא. (התשובה היא בוליאנית: 1- קיים, 0- לא קיים)
- בעיית חיפוש/אופטימיזציה- המטרה היא מציאת פתרון/פתרון אופטימלי לבעיה נתונה או להחזיר שלא קיים פתרון כזה(נחזיר "⊥" במצב שאין פתרון)

- ברור שבהינתן אלגוריתם הפותר את בעיית החיפוש/אופטימיזציה ניתן להשתמש בו כדי לפתור את בעיית ההכרעה, אם מצאנו פתרון נחזיר 1 אחרת נחזיר 0.
  הכיוון השני לא ברור באותה מידה, כדי לטפל בו ניזכר במושג הרדוקציה.

- רדוקצית טיורינג פולינומית(רדוקצית קוק) - נתונות 2 בעיות חישוביות L_1 ו- L_2, נאמר ש- $L_2 \leq_T^P L_1$ אם בהינתן "קופסא שחורה" A(אלגוריתם, בהמשך נקרא לזה גישת אורקל ל- A) הפותרת את הבעיה L_1 , ניתן ליצור אלגוריתם פולינומי M(עד כדי זמן הריצה של A) הפותר את L_2 ומשתמש ב"קופסא השחורה" A לכל היותר מספר פולינומי של פעמים.

- רדוקציה עצמית - היא רדוקציית טיורינג פולינומית מבעיית החיפוש/אופטימיזציה לבעיית ההכרעה.
  כלומר, בהינתן אלגוריתם A המחזיר האם קיים או לא קיים פתרון לבעיה הנתונה, ניתן ליצור אלגוריתם M המוצא את הפתרון תוך שימוש ב-A בזמן פולינומי(עד כדי זמן הריצה של A)

דוגמאות:

- בעיית SAT- נניח שקיים אלגוריתם שבהינתן נוסחא ϕ מחזיר האם קיימת השמת אמת המספקת את הנוסחא או לא.
  ניצור אלגוריתם M שבהינתן נוסחא פולינומית בפורמט CNF מוצא השמת אמת המספקת אותה או מחזיר "⊥ " (לא קיימת השמה כזו).
  אלגוריתם M המקבל נוסחא בוליאנית ϕ (בפורמט CNF):
  אם $A(\phi) = 0$ החזר " ⊥ "
  עבור i מ-1 עד n:
  הצב $x_i = T$ וצמצם את ϕ ל- ϕ_T
  אם $A(\phi_T) = 1$
  המשך עם ϕ_T בתור ϕ
  אחרת
  הצב $x_i = F$ צמצם את ϕ ל- ϕ_F
  המשך עם ϕ_F בתור ϕ
  החזר את כל ההצבות שהמשכנו איתן.

דוגמת הרצה-

נתונה הנוסחא הבאה:

$\phi = (x_1 \vee \neg x_2 \vee x_3) \wedge (\neg x_1 \vee x_2 \vee x_3) \wedge (\neg x_1 \vee \neg x_2 \vee \neg x_3)$

הקריאה $A(\phi)$ מחזירה 1

באיטרציה הראשונה בלולאה באלגוריתם M נציב $x_1 = T$ ונקבל $\phi_T = (x_2 \vee x_3) \wedge (\neg x_2 \vee \neg x_3)$

נריץ $A(\phi_T)$ ונקבל 1

לכן באיטרציה השניה נציב $x_2 = T$ ונקבל $\phi_T = \neg x_3$

נריץ $A(\phi_T)$ ונקבל 1

ולכן באיטרציה השלישית נציב $x_3 = T$ ונקבל $\phi_T = F$ נריץ $A(\phi_T)$ ונקבל 0. לכן נציב $x_3 = F$ ונקבל $\phi_F = T$ ובכך נסיים.

השמת האמת שתוחזר: $x_1 = T, x_2 = T, x_3 = F$

תרגול 2

יום ראשון 24 אפריל 2016 15:20

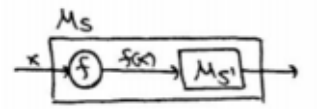
רדוקציות, P, PN, PF, PC, רדוקציות-

- יחס חסום פולינומית - יחס $R \subseteq \{0,1\}^* \times \{0,1\}^*$ נקרא יחס חסום פולינומית אם קיים פולינום $P(\cdot)$ כך שלכל $(x,y) \in R$ מתקיים $|y| \le p(|x|)$
- המחלקה PF - $R \in PF$ אם:
  1) R הוא יחס חסום פולינומית.
  2) קיים אלגוריתם פולינומי דטרמניסטי כך שבהינתן x הוא מוצא y כך ש- $(x,y) \in R$ או מחזיר שלא קיים y שכזה.
- המחלקה PC- $R \in PC$ אם:
  1) R הוא יחס חסום פולינומית
  2) קיים אלגוריתם פולינומי דטרמניסטי שמחזיר 1 אם $x \in S$ ו- 0 אחרת.
- המחלקה P- תהיי $S \subseteq \{0,1\}^*$ בעיית הכרעה/שפה.
  $S \in P$ אם קיים אלגוריתם פולינומי דטרמניסטי שמחזיר 1 אם $x \in S$ ו-0 אחרת.
- המחלקה NP- תהיי $S \subseteq \{0,1\}^*$ בעיית הכרעה/שפה.
  $S \in NP$ אם קיימת מערכת הוכחה מסוג NP ל- S , כלומר, $S \in NP$ אם קיימים פולינום $P(\cdot)$ ומוודא v פולינומי דטרמנסטי המקיימים:
  1) שלמות- אם $x \in S$ אז קיים "עד" y כך שמתקיים $|y| \le p(|x|)$ ו- $v(x,y) = 1$.
  2) נאותות- אם $x \notin S$ אז לכל y $v(x,y) = 0$

רדוקציית many-to-one(רדוקציית קארפ)-

תהיינה S ו'S בעיות הכרעה, נאמר שקיימת רדוקציית קארפ מS ל'S(מסומן ע"י $S \le_M^P S'$) אם קיימת פונקציה f הניתנת לחישוב בזמן פולינומי כך ש- $f(x) \in S' \Leftrightarrow x \in S$ כלומר בהינתן מופע x של הבעיה S, ניתן ליצור בזמן פולינומי מופע $f(x)$ של 'S כך ש $f(x) \in S' \Leftrightarrow x \in S$.

נשים לב שאם $S \le_M^P S'$, אז בהינתן אלגוריתם $M_{S'}$ על הפלט שהתקבל מ-f ומחזיר את תשובה של $M_{S'}$.



NP-hardness- תהי S בעיית הכרעה.

S היא NP-hard/ NP קשה. אם: $\forall S' \in NP : S' \le_M^P S$

NP-Completeness - תהי S בעיית הכרעה. S היא NP/ NPC- שלמה אם:

1) $S \in NP$
2) S היא NP- קשה.

- משפט קוק- לוין - $SAT \in NPC$
- $co - NP = \{S | \bar{S} \in NP\}$ - השפות שהמשלימים שלהם ב- NP

תרגיל - נניח ש $P \neq NP$. קבעו עבור כל אחת מהטענות הבאות האם היא נכונה או לא נכונה או תלויה בשאלה פתוחה.

א) תהי $S \in NPC$ ותהי S' בעיית הכרעה כך ש- $S \subseteq S'$ אז $S' \in NPC$.
פתרון: לא נכון, תהי $S = SAT$ ו- S' קבוצת כל הנוסחאות בפורמט CNF. קל לראות ש- $S = SAT \subseteq S'$
אבל $SAT \in NPC$ ו- $S' \in P$ ומכיוון ש- $P \neq NP$ בהכרח $S \notin NPC$.

ב) המחלקה NPC סגורה תחת איחוד, כלומר $S_1,S_2 \in NPC \Rightarrow S_1 \cup S_2 \in NPC$.
פתרון- לא נכון, תהיינה $S_1 = \{(\phi,k) | \phi \in SAT \vee k \text{ is even}\}$
$S_2 = \{(\phi,k) | \phi \in SAT \vee k \text{ is odd}\}$
קל לראות ש- $S_1,S_2 \in NPC$, אבל:
$S_1 \cup S_2 = \{(\phi,k) | \phi \in SAT \vee k \in \mathbb{Z}\}$
ברור ש - $S_1 \cup S_2 \in P$ ולכן מכאן $S_1 \cup S_2 \notin NPC$

ג) תהי השפה $BIG_{CLIQUE} = \{G | G -$ מכיל קליקה בגודל $n - 4$ כאשר n מספר הקודקודים ב $\}$
טענה: $BIG - CLIQUE \in NPC$
פתרון: לא נכון, ישנן $\binom{n}{n-4} = O(n^2)$ אפשרויות לבחור קבוצה של $n - 4$ קודקדים.
ניתן לבדוק עבור כל אפשרות האם קבוצת הקודקודים שנבחרו מהווה קליקה בזמן $O(n^2)$ אם באחת הבדיקות מצאנו קליקה נחזיר 1, אחרת נחזיר 0. כלומר ישנו אלגוריתם פולינומי המכריע את $BIG - CLIQUE$.
כלומר: $BIG - CLIQUE \in P \Rightarrow^{P \neq NP} BIG - CLIQUE \notin NPC$

תרגול 4

יום רביעי 30 מרץ 2016 11:04

דוגמא קונקרטית ליחס שאינו ניתן לרדוקציה עצמית
נגדיר יחס- $R = \{(N,(n_1,n_2))|N = n_1 * n_2 ,n_1,n_2 \in \mathbb{N},1 < n_1,n_2 < N\}$
בעיית ההכרעה של יחס זה: (S_R) ניתנת לפיתרון בזמן פולינומי(זוהי בעיית ה-PRIMES שיש לה מבחן ראשוניות AKS שפותר אותה בזמן פולינומי)
לעומת זאת בעיית החיפוש שהיא בעיה של פירוק לשני גורמים לא טריוואלי משערים שהיא בעיה קשה שלא ניתנת לפתרון בזמן פולינומי(בעיית ה-Integer-Factory)
(שייך לNP וגם לco-NP)

שקילות ההגדרות של NP
ראינו שתי הגדרות של המחלקה NP.
הגדרה 1(באמצעות מ"ט ל"ד):
תהי $S \subseteq \{0,1\}^*$ בעיית הכרעה/שפה. $S \in NP$ אם קיימת מ"ט ל"ד פולינומית המכריעה את S
הגדרה 2(באמצעות מערכת הוכחה):
$S \subseteq \{0,1\}^*$ בעיית הכרעה/שפה. $S \in NP$ אם קיימת מערכת הוכחה מסוג NP ל-S. כלומר קיימים פולינום P ואלגו' מוודא פולינומי דט' v כך שמתקיים:

1. שלמות: אם $x \in S$ אז קיים y כך ש $|y| \le p^{(|x|)}$ ו$v(x,y) = 1$
2. נאותות: אם $x \notin S$ אז לכל y מתקיים $v(x,y) = 0$

הוכחה:(סקיצה)
כיוון ראשון:
נניח של-S יש מערכת הוכחה מסוג NP ניצור מ"ט ל"ד פולינומית M שמכריעה את S באופן הבא:
בהנתן קלט x, M תנחש $y \in \{0,1\}^{p(|x|)}$ באופן ל"ד תריץ את v על (x,y) ותחזיר את מה שv מחזיר.
קל לראות שעבור $x \in S$ קיים מסלול מקבל ב-M ואילו עבור $x \notin S$ לא קיים מסלול שכזה.

כיוון שני:
נניח שקיימת מ"ט ל"ד פולינומית M שמכריעה את S. ניתן ליצור מ"ט דט' 'M שמקבלת (x,y) ופועלת באופן הבא:
M מבצעת את הצעד ה-i-י הל"ד שלה 'M מסתכלת ב-y בבלוק ה-i-י שלו (ולפי הקידוד שנקבע מראש) ופועלת על פי מה שמופיע בו. באופן דט' (הבלוק הזה קובע לאיזה מצב לעבור, מה לשים בסרט ולהיכן להזיז את הראש הקורא) בסופו של דבר 'M מחזירה את מה שמחזירה את מה ש-M מחזירה בסיום הסימולציה.
קל לראות שעבור $x \in S$ קיים מסלול מקבל של המכונה הל"ד M שאורכו פולינומי. ולכן קיים y שמהווה "מדריך" למסלול הזה ומאפשר ל-M' להחזיר ועבור (x,y).
לעומת זאת אם $x \notin S$ לא קיים אף y שמהווה "מדריך" למסלול מקבל במכונה הל"ד(כיוון שאין עבור $x \notin S$) ולכן תמיד המוודא יחזיר 0.

ההיררכיה הפולינומית
הגדרות:

1. $S \in \Sigma_k$ אא"מ קיימים פולינום p ואלג' מוודא פולינומי דט' v כך ש:

$$x \in S \Leftrightarrow \exists y_1 \in \{0,1\}^{p(|x|)} \forall y_2 \in \{0,1\}^{p(|x|)} \exists y_3 \in \{0,1\}^{p(|x|)} \dots Q y_k \in \{0,1\}^{p(|x|)}$$

$$s.t. \quad v(x,y_1,y_2 \dots y_k) = 1 \qquad Q = \begin{cases} \exists & \text{k אי זוגי} \\ \forall & \text{k זוגי} \end{cases}$$

דוג'
Min-Vertex-Cover מכילה את כל הזוגות ,(G,k) כך שכיסוי הקודקודים המינילמי ל-G גודלו בדיוק k
טענה: $Min - Vertex - Cover \in \Sigma_2$
הוכחה: $(G,k) \in MVC \Leftrightarrow \exists S \subseteq v(G), \forall S \in V(G)\ s.t.\ \ v\big((G,k),S,S'\big) = 1$
כאשר v מקבל כקלט זוג (G,k) ותת קבוצה של קודקודים S ו- S' ומחזיר 1 אם מתקיימים התנאים הבאים. ו-0 אם אחרת:

1. $|S| = k$
2. S מהווה כיסוי קודקים חוקי ל-G (כלומר לכל קשת בE(G) יש קודקוד בקבוצה)
3. S' לא כיסוי קודקדים חוקי של G או ש $|S'| \ge k$

קל לראות שהמוודא V רץ בזמן פולינומי ומקיים את התנאים של Σ_2 ולכן
$Min - Vertex - Cover \in \Sigma_2$

תרגול 5

יום רביעי 06 אפריל 2016 11:01

ההיררכיה הפולינומית

הגדרות:

1. $S \in \Sigma_k$ אא"מ קיימים פולינום p ואלג' מוודא פולינומי דט' v כך ש:

$$x \in S \Leftrightarrow \exists y_1 \in \{0,1\}^{p(|x|)} \forall y_2 \in \{0,1\}^{p(|x|)} \exists y_3 \in \{0,1\}^{p(|x|)} \dots Q y_k \in \{0,1\}^{p(|x|)}$$
$$s.t. \quad v(x,y_1,y_2 \dots y_k) = 1 \qquad Q = \begin{cases} \exists & \text{k אי זוגי} \\ \forall & \text{k זוגי} \end{cases}$$

2. $S \in \pi_k$ אא"מ קיימים פולינום $p()$ ומוודא פולינומי דט' v כך שמתקיים:

$$x \in S \Leftrightarrow \forall y_1 \in \{0,1\}^{p(|x|)} \forall y_2 \in \{0,1\}^{p(|x|)} \exists y_3 \in \{0,1\}^{p(|x|)} \dots Q' y_k \in \{0,1\}^{p(|x|)}$$
$$s.t. \quad v(x,y_1,y_2 \dots y_k) = 1 \qquad Q' = \begin{cases} \forall & \text{k אי זוגי} \\ \exists & \text{k זוגי} \end{cases}$$

הגדרה 1:

$$PH = \bigcup_{k=0}^{\infty} \Sigma_k$$

הגדרה 2: (באמצעות מ"ט עם גישת אורקל)

תהי $f: \{0,1\}^* \to \{0,1\}^*$

פונקצית אורקל. מ"ט M עם גישת אורקל ל-f (סימון M^f) . היא מ"ט שיש לה סרט נוסף המכונה "סרט אורקל," כאשר M יכולה לכתוב מחרוזת z על סרט האורקל, ולקבל עליו חזרה בצעד אחד את הערך של $f(z)$. פעולה זו נקראת "שאילתא" ומבוצעת בעצד אחד מרגע הפעלת השאילתא ועד חזרת התשובה.

עבור שפה/בעיית הכרעה A. מ"ט עם גישת אורקל ל-A (סימון: M^A) היא מ"ט שיכולה לכתוב על סרט האורקל שלה מחרוזת a ולקבל חזרה תשובה האם $a \in A$ או לא(פונ' בולינאנית)

- המחלקה של בעיית המוכרעות ע"י מ"ט הפולי' דט' עם גישת אורקל לפונ' f מכונה P^f ובאופן דומה המחלקה של הבעיות המוכרעות ע"י מ"ט פולי' ל"ד עם גישת אורקל לפונ' f היא NP^f.
- כמו כן, מוגדר עבור מחלקת בעיות הכרעה C:

$$P^C = \bigcup_{f \in C} P^f \,, NP^C = \bigcup_{f \in C} NP^f$$

הקשר בין הגדרה 1 ל2-

$\Sigma_{k+1} = NP^{\Sigma_k}$ לכל $k \geq 0$

סימונים ותכונות:

3. $\pi_k = co\Sigma_k$
4. $\Delta_{k+1} = P^{\Sigma_k}$
5. $\Sigma_k \subseteq \Sigma_{k+1}$ ו- $\pi_k \subseteq \pi_{k+1}$
6. $\pi_k \subseteq \Sigma_{k+1}$ ו- $\Sigma_k \subseteq \pi_{k+1}$
7. $\pi_k \subseteq \Sigma_k \Rightarrow \Sigma_k = \Sigma_{k+1}$ (עבור $k \geq 1$)
8. $\Sigma_k = \Sigma_{k+1} \Rightarrow PH = \Sigma_k$

תרגיל-

הוכיחו באמצעות הגדרה 2:

1. $\Delta_k \subseteq \pi_k \cap \Sigma_k$

פתרון: נראה $\Delta_k \subseteq \Sigma_k$. $\Delta_k = P^{\Sigma_{k-1}}$ ו- $\Sigma_k = NP^{\Sigma_{k-1}}$

תהיי $S \in \Delta_k$, כלומר קיימת מ"ט פולי' דט' עם גישת אורקל לשפה כ- Σ_{k-1} שמכריעה את S, לכן קיימת מ"ט ל"ד פולי' עם גישת אורקל לשפה ב- Σ_{k-1} המכריעה את S (אותה המכונה)

ולכן $S \in \Sigma_k = NP^{\Sigma_{k-1}}$. נראה ש $\Delta_k \subseteq \pi_k$. תהי $S \in \Delta_k$ אזי גם $\bar{S} \in \Delta_k$ (ניתן להשתמש באותה מ"ט ולהפוך את התשובה) $\Leftarrow$ $\bar{S} \in \Sigma_k$ ולכן $S \in \pi_k$.

2. $\Sigma_k \subseteq \pi_{k+1}$

נראה ש $\Sigma_k \subseteq \Delta_{k+1}$ ומכאן נסיק את מה שצריך לפי סעיף 1. תהיי $S \in \Sigma_k$ נוכיח ש $S \in \Delta_{k+1} = P^{\Sigma_k}$.

נבנה מ"ט פולי' עם גישת אורקל לS- שמכריעה S באופן הבא: בהינתן קלט x המכונה תשאל את האורקל שלה עם המחרוזת x ותחזיר את תשובתו.

3. $\pi_k \subseteq \Sigma_{k+1}$

נוכיח $\pi_k \subseteq \Delta_{k+1}$ ומכאן לפי סעיף 1. נובעת הטענה תהיי $S \in \pi_k$

נוכיח $S \in \Delta_{k+1}$. מכך ש $S \in \pi_k$ נובע ש $\bar{S} \in \Sigma_k$. ניתן לבנות מ"ט עם גישת אורקל ל- $\bar{S}$ שמכריעה את S באופן הבא: בהינתן קלט x המכונה תשאל את האורקל עם המחרוזת x ותחזיר תשובה הפוכה לזו של האורקל.

תרגול 6

יום רביעי 13 אפריל 2016 10:40

ההיררכיה הפולינומית

תרגיל 1)
MIN-CNF מכילה את כל הנוסחאות הבוליאניות בצורת CNF שאין נוסחה אחרת קצרה יותר השקולה להן.

טענה: $MIN-CNF \in \pi_2$
באמצעות הגדרה 1:
$\phi \in MIN-CNF \Leftrightarrow \forall \phi' \ \exists v \quad s.t\ v(\phi,\phi',v)=1$
כאשר המוודא מקבל נוסחה ϕ , נוסחה ϕ' והשמת אמת v, ומחזיר 1 אם מתקיימים התנאים הבאים(0 אחרת):
1. ϕ בפורמט CNF
2. ϕ' לא בפורמט CNF או (ϕ' בפורמט CNF וגם אם $|\phi'| < |\phi|$ אז $\phi(v) \neq \phi'(v)$)

קל לראות שכל הבדיקות של המוודא מתבצעות בזמן פולינומי. אם $\phi \in \mathrm{MIN-CNF}$ אז היא בפורמט תקין, וכל נוסחה אחרת שהיא בפורמט התקין וקצרה ממנה תהיה השמת אמת שהן לא יהיו שקולות עבורה.
לעומת זאת, אם $\phi \notin MIN-CNF$ אז או שהיא לא בפורמט התקין(ולכן תמיד נחזיר 0) או שתהיה נוסחה תקינה כלשהי קצרה מ-ϕ כך שלכל השמת אמת v היא תהיה שקולה ל-ϕ (ולכן תמיד נחזיר 0).

באמצעות הגדרה 2:
ראשית נגדיר שפה $NOT-EQUE$ המכילה את כל זוגות הנוסחאות הבוליאנית (ϕ_1,ϕ_2) שאינן שקולות זו לזו.
קל לראות ש $NOT-EQUE \in NP$, העד יהיה השמת אמת עבורה הנוסחאות לא שקולות.
כעת, נראה ש $\overline{\mathrm{MIN-CNF}} \in \Sigma_2 = NP^{NP}$ כאשר $\overline{MIN-CNF}$ מכילה את כל הנוסחאות הבוליאניות שאינן בפורמט CNF או שקיימת נוסחה בפורמט CNF קצרה יותר השקולה להן.
נראה מ"ט (אלגו') ל"ד פולי' עם גישת אורקל ל- NOT-EQUE שפותר את הבעיה.
בהינתן נוסחה ϕ :
- אם ϕ אינה בפורמט CNF- החזר 1.
- ננחש באופן ל"ד נוסחה ϕ' בפורמט CNF הקצרה מ- ϕ
- אם $(\phi,\phi') \in NOT-EQUE$ (שאילתא לאורקל) - החזר 0.
- החזר 1.

אפשר לראות שהאלגו' מתבצע בזמן פולינומי ל"ד.
נכונות(סקיצה כיוון 1):
אם ϕ בצורת CNF ושייכת ל- MIN-CNF בהכרח קיימת נוסחה ϕ' בפורמט CNF קצרה יותר השקולה לה, לכן קיים ניחוש שעבורו השאילתא לאורקל תחזיר 0 ולכן יוחזר 1.

בהרצאה הוכח באמצעות גדרה 1 שלכל $k \geq 1$ אם $\pi_k = \Sigma_k$ אז $\Sigma_{k+1} = \Sigma_k$
נוכיח מקרה פרטי של טענה זו באמצעות הגדרה 2.
תרגיל: הוכיחו באמצעות הגדרה 2 שאם $co-NP = NP$ אז $NP = NP^{NP}$
הוכחה:
כיוון אחד ברור תמיד $NP \subseteq NP^{NP}$ נוכיח ש $NP^{NP} \subseteq NP$.
תהיי $S \in NP^{NP}$ לכן קיימת מ"ט ל"ד פולי M^A עם גישת אורקל ל-A ששייכת לNP המכריעה את S.
המכונה M^A היא מהצורה הבאה:

בצע...
בצע...
נחש...
.
.
.
אם $x \in A$ אז (השאילתא לאורקל)
בצע..
נחש..
.
.
אחרת
בצע..
נחש..

.
.
.
.
.

מכיוון ש-A שייכת ל-NP קיימת מ"ט ל"ד פולינומית M_A שמכריעה את A כמו כן, מכיוון ש- $co-NP=NP$ אז $\bar{A} \in NP$ ולכן קיימת מ"ט ל"ד פולינומית $M_{\bar{A}}$ שמכריעה את $\bar{A}$.
ניצור מ"ט ל"ד פולינומית M שמכריעה את S באופן הבא:

בהינתן קלט x, המכונה M תסמלץ את הריצה של M^A על הקלט x,
כאשר M^A מבצעת שאילתת אורקל עם מחרוזת y המכונה M תריץ במקום זאת את המכונה M_{A} על המחרוזת y.
אם קיבלנו 1 אז M תבצע את מה ש-M^A מבצעת בהינתן תשובה חיובית מהאורקל.
אם קיבלנו 0 אז נריץ את $M_{\bar{A}}$ עם y.
אם $M_{\bar{A}}$ החזירה 1 נבצע את מה ש-M^A מבצעת בהינתן תשובה שלילית מהאורקל.
אם שתי המכונות החזירו 0, נחזיר 0 מיד.

תרגול 7

יום רביעי 04 מאי 2016 11:00

$P_{/poly}$

$P_{/poly}$ היא מחלקה של שפות/ בעיות הכרעה המתקבלות ע"י מעגלים לוגיים בגודל פולינומי.

מה ההבדל בין אלגו' רגיל למעגל לוגי?

קלט לאלגוריתם יכול להיות מכל אורך שהוא.

ולכן אחיד לכל אורכי הקלט. לעומת זאת, מעגל הוא קבוע לאורך קלט מסויים. ולכן צריך לבנות מעגל שונה לכל אורך קלט.

חישוב זה נקרא חישוב לא יוניפורמי.

הגדרה 1: $L \in P/poly$ אם קיימת סדרה אינסופית של מעגלים לוגיים $\{C_n\}_{n\in\mathbb{N}}$. כך שלכל n, יש ל- n C_n קודקודי קלט וקיים פולינום $p(\cdot)$ כך ש $|C_n| \le p(n)$ (הגודל של מעגל לוגי הוא מספר הקשתות במעגל)

ולכל $x \in \{0,1\}^n$ מתקיים $C_n(x) = \begin{cases} 1 & x \in L \\ 0 & x \notin L \end{cases}$

הגדרה 2: $L \in P/poly$ אם קיימת מ"ט הרצה בזמן פולינומי M, בעלת שני סרטי קלט, פולינום $p(\cdot)$, וסדרה אינסופית $\{a_n\}_{n\in\mathbb{N}}$ של מחרוזת יעוץ כך שלכל n $|a_n| \le p(n)$ ולכל $x \in \{0,1\}^n$ מתקיים: $M(x,a_n)$

$= \begin{cases} 1 & x \in L \\ 0 & x \notin L \end{cases}$

משפט 1: $P \subseteq P/poly$ (אפשר לתת עצה ריקה)

משפט 2: $NP \nsubseteq P/poly \Rightarrow P \neq NP$

משפט 3: המחלקה $P/poly$ מכילה שפות לא כריעות (ולכן $P/poly \nsubseteq NP$)

משפט 4: אם $PH = \Sigma_2 \Leftarrow NP \subseteq P/poly$

תרגיל:

נגדיר מחלקה $P/2^n$ באופן דומה להגדרת $P/poly$, כך שבמחלקה זו מחרוזות הייעוץ יכולות להיות אקספוננצאליות בגודל הקלט. הוכיחו שכל שפה L שייכת למחלקה זו.

פתרון:

תהי שפה L. לכל n נגדיר את a_n להיות המחרוזת שבאינדקס ה- i שלה מופיע 1, אם המחרוזת הבינארית באורך n שמייצגת i שייכת ל-L ו-0 אחרת .

קל לראות שלכל n $|a_n| = 2^n$ כמו כן, ניתן ליצור מכניזם M שבהינתן קלט x באורך n ומחרוזת הייעוץ a_n המכונה תסתכל באינדקס i במחרוזת a_n כאשר i הוא הערך המספרי של הקלט הבינארי x, ותחזיר ערך הביט שמופיע באינדקס הזה. קל לראות שמכונה זו מחזירה תשובה נכונה לכל x בהינתן מחרוזות הייעוץ המתאימה.

תרגיל:

נגדיר את המחלקה P/log בדומה למחלקה $P/poly$ פרט לעובדה שאורך מחרוזות הייעוץ לוגריתמי באורך הקלט.

הוכיחו $NP = P \Leftarrow NP \subseteq P/\log$

פתרון:

עבור כל $a_n \in \{0,1\}^{\log n}$

רדוקציה עצמית

$M(\phi',a_n)$

בודקים את ההשמה.

- צריך לוודא שהאורך ישאר באותו גודל בשביל הרדוקציה העצמית ולכן צריך לרפד.

**********להמשיך**********

תרגול 3

יום שישי 06 מאי 2016 12:14

שאלות דודי

יום שני 09 מאי 2016 23:51

- היררכיה פולינומית
- אורקל
- רדוקציות
- חסום פולינומית
- יחס שאינו ניתן לרדוקציה עצמית

תרגיל 2

יום שלישי 17 מאי 2016 11:46

רויטל שיפמן
203438973
89-225-02

1. הוכיחו שהבעיות הבאות הן NP-שלמות:

א. [10 נק'] נתון אוסף C של תתי-קבוצות של קבוצה סופית S. נדרש להכריע האם ניתן לחלק את הקבוצה S לשתי תתי-קבוצות S_1 ו-S_2 כך שאף תת-קבוצה ב-C לא מוכלת בשלמותה ב-S_1 או ב-S_2.

1)

א) נוכיח שהשפה A1 ב- NPC

נראה שהיא NP-

תהיי S קבוצה סופית

נקבל את הקלט - אוסף C של תתי קבוצות של S

ונקבל עד - S_1,S_2 כך ש $S_1 \cup S_2 = S$ וגם $S_1 \cap S_2 = \emptyset$

עבור כל קבוצה נבדוק האם קיים לפחות איבר אחד בS_1 ואיבר אחד בS_2

אם כן אז זה בשפה.

נראה שהיא NPC-

נעשה רדוקציה מ SAT כך ש

$(\psi) \in SAT \Leftrightarrow f(C) \in A1$

הרעיון:

הבניה:

האיברים יהיו כל הליטרלים שנמצאים בפסוקיות(אם קיים בשתי פסוקיות x_1 נוסיף רק פעם אחת). וגם נוסיף איבר x_k כלשהו.

כל פסוקית בSAT תהיה קבוצה $X \in C$

ולכל קבוצה X נוסיף את האיבר x_k.

הקבוצות S_1,S_2 הן בעצם S_1 - הליטרלים עם השמה של True וS_2 - הליטרלים עם השמה של False

הוכחות נכונות:

$(\psi) \in SAT \Rightarrow f(S,C) \in A1$: אם ψ שייך לSAT אזי לכל פסוקית יהיה לפחות איבר אחד שנמצא בS_1 (כי יש לפחות איבר אחד שהוא True בכל פסוקית ולכן גם בכל $X \in C$.) ואת האיבר x_k נשים בS_2 ומכיוון שהוא נמצא בכל X אזי בכל קבוצה $X \in C$ קיים לפחות $x_1 \in S_1$ ו$x_2 \in S_2$ ולכן $f(C) \in A1$

$(\psi) \in SAT \Leftarrow f(C) \in A1$ אם קיימות S_1,S_2 שמקיימות את הדרישה אזי קיימת הצבה מספקת של SAT כי באחת הקבוצות יהיה בהכרח איברים מכל הפסוקיות מתוך ההגדרה.

2. [15 נק'] הראו רדוקציה עצמית מפורשת מגרסת האופטימיצה של כל אחת מהבעיות בשאלה הקודמת לגרסת ההכרעה שלהן.

2) תהי M מכונה המכריעה את A1. נבנה מכונה F1 פולינומית עם גישת אורקל שבהינתן (S,C) מחזירה את החלוקה S_1,S_2 שמקיימת את השפה A1 אם קיים ו⊥ אם לא קיים.

$F1(S,C)$

1. אם $M(S,C) = 0$ נחזיר ⊥
2. נבחר x_1 כלשהו ונכניס אותו לS_1 ו$S_2 = \emptyset$
3. לכל $x \in S \backslash x_1$:
   - 3.1 אם $M(S,C \cup \{\{x_1,x\}\}) = 1$ אז
     - 3.1.1 נוסיף את $\{x_1,x\}$ לC וגם נכניס את x לS_2
   - 3.2 אחרת נוסיף את x לS_1
4. נחזיר את S_1,S_2

F1 פולינומית חוץ מהשיאלתא של M. אנו רצים סה"כ לולאה פעם אחת.

3. [12 נק'] תהיינה S_1 ו-S_2 בעיות הכרעה, כך ש-$S_1,S_2 \in NP \cap coNP$.
נגדיר: $S_1 ** S_2 = \{x \mid x \text{ is in exactly one of } S_1,S_2\}$. הוכיחו או הפריכו $S_1 ** S_2 \in NP \cap coNP$.

הוכחה:
מכיוון שזה בNP קיימת מכונה שמכריעה כנ"ל coNP

צ"ל $S_1 ** S_2 \in NP \cap coNP$
ידוע כי $S_1,S_2 \in NP \cap coNP$ ולכן קיימת מכונה Ms1 שמכריעה את S_1 וגם קיימת מכונה כלשהי Ms2 שמכריעה את S_2 וגם קיימת מכונה Ms12 שמכריעה את המשלים של S_1 וקיימת Ms22 שמכריעה את המשלים של S_2 . כולן פולינומיות ל"ד
נראה $S_1 ** S_2 \in NP$:
נבנה מכונה M(x) פולינומית ל"ד שמכריעה את $S_1 ** S_2$
1) נריץ את Ms1(x) ו- Ms22(x)
   1.1 אם שניהם החזירו 1 נחזיר 1.
2) נריץ את Ms2(x) ו- Ms12(x)
   2.1 אם שניהם החזירו 1 נחזיר 1.
3) החזר 0
קל לראות שהאלגוריתם פולינומי ל"ד כיוון ש כל המכונות פולינומיות ל"ד.
ולכן $S_1 ** S_2 \in NP \cap coNP$ מש"ל.

4. [20 נק'] בעיית הכרעה תיקרא **בעיה אונארית** אם כל מחרוזת השייכת לה היא מהצורה 1^k (המחרוזת של k אחדות) עבור k>0 כלשהו. הוכיחו כי אם קיימת בעיה אונארית שהיא NP-Complete אזי P=NP.

<u>הוכחה</u>: תהא $NPC \ni L \subseteq \{1\}^*$, ולכן $SAT \leq_p L$. תהא f הרדוקציה שלכל φ מחזירה $f(\varphi) = 1^i$ כאשר $i \leq p(n)$ כאשר p פולינום ו-n מספר משתני הנוסחה φ / אורך φ. נראה אלגי ל-SAT הרץ בזמן פולי' ומכך נסיק $P = NP$. נשתמש במערך A שכל ערכיו מאותחלים ל-$unknown$. נגדיר את $SAT(\varphi(x_1, \dots, x_n), A)$:

- אם $n = 0$ החזר את φ (t או f).
- אם $A\left[\underset{=i}{|f(\varphi)|}\right] \neq unknown$, החזר את $A[|f(\varphi)|]$.
- אם $SAT(\varphi(t, x_2, \dots, x_n), A)$ או $SAT(\varphi(f, x_2, \dots, x_n), A)$ נשים t ב-$A[|f(\varphi)|]$ ונחזיר t, אחרת נשים f ונחזיר f.

הרעיון: עבור קלט בגודל n יתכנו 2^n קלטים אפשריים, אך f ממפה אותם לקבוצה קטנה יחסית – בגודל $p(n)$ (כי לכל $x \in L$ i היחיד באורך i הוא 1^i ואין עוד קלטים אחרים אפשריים באורך i). לכן שמירת הערכים ב-A תחסוך בדיקות בהמשך = תחסוך התפצלויות בעץ האלגי הנאיבי.
נכונות: נובעת מכך ש-$\varphi(x_1, \dots, x_n)$ ספיקה אמ"מ $\varphi(t/f, x_2, \dots, x_n)$ ספיקה. זמן ריצה: בכל שלב נבחר צומת שמתאים לקריאה רקורסיבית בעץ הרקורסיה (לא עלה) ונסיר אותו ואת המסלול המוביל אליו מהשורש: $O(n)$ צמתים. נעשה זאת עד שהעץ יתרוקן. כל קריאה רקורסיבית כזו הנמצאת בתחתית המסלול מתאימה לערך שונה מהמערך A, ולכן לכל היותר יוסרו $p(n)$ מסלולים. סה"כ: $O(n \cdot p(n))$. בכל קריאה כזו מפעילים את f ולכן סה"כ $O(p^2(n) \cdot n)$.

5. [15 נק'] נגדיר את המחלקה PH* באופן הבא:

$$\Sigma_1^* = NP$$
$$\Pi_1^* = coNP$$
$$\Sigma_{k+1}^* = NP^{\Pi_k^*}$$
$$\Pi_{k+1}^* = co\Sigma_{k+1}^*$$
$$PH^* = \bigcup_{k=1}^{\infty} \Sigma_k^*$$

הוכיחו או הפריכו PH=PH*.

5) כדי להוכיח $PH^* = PH$ נוכיח ש $\Sigma_k^* = \Sigma_k$ לכל k.
כי $(\Sigma_0 \leq \Sigma_1)$ $PH^* \cup_{k=1}^{\infty} \Sigma_k^* = \cup_{k=0}^{\infty} \Sigma_k = PH$
הוכחה: בהרצאה הוכחנו $NP^{\Sigma_k} = NP^{\pi_k}$

נשתמש בזה כדי להוכיח באינדוקציה את הטענה.
עבור $k = 1$ $\Sigma_1^* = NP = \Sigma_1$
נניח נכונות עבור $x < k$ נוכיח עבור k.
$\Sigma_{k+1}^* = NP^{\pi_k^*} = NP^{co\Sigma_k^*} =$ אינדוקציה $= \mathrm{NP}^{\mathrm{co}\Sigma_k}$ (ט.ע) $= \mathrm{NP}^{\pi_k} = \mathrm{NP}^{\Sigma_k} = \Sigma_{k+1}$
הוכחנו נכונות המשפט לכל $k > 0$ $\Sigma_k = \Sigma_k^*$
ומכאן $PH^* = PH$
מש"ל.

6. [18 נק'] מחלקה C נקראת *סגורה למשלים* אם לכל שפה L מתקיים $L \in C \Rightarrow \bar{L} \in C$.
מחלקה C נקראת *סגורה לכוכב* אם לכל שפה L מתקיים $L \in C \Rightarrow L^* \in C$.

<u>תזכורת</u>: L^* היא קבוצת כל המילים שהן שרשור של מספר כלשהו של מילים מ-L (כולל את המילה הריקה שהיא שרשור של אפס מילים).

עבור המחלקות P^{SAT} ו-NP^{SAT} הוכיחו או הפריכו את סגירותן למשלים ולכוכב (אין להוכיח טענות המבוססות על השערות שלא הוכחו – כדוגמת NP=P).

P^{SAT} סגורה למשלים.
תהי $S \in P^{SAT}$ אזי קיימת מכונה פולינומית דטרמניסטית M עם גישת אורקל לSAT שמכריעה את S.
נבנה מכונה M1 שמכריעה את S משלים.
$M1(x)$
1. נריץ את M(x)
2. אם M(x)=1 נחזיר 0 אחרת נחזיר 1.

קל לראות שזה פולינומי.

P^{SAT} סגורה לכוכב
תהי $L \in P^{SAT}$ אזי קיימת מכונה פולינומית דטרמניסטית M עם גישת אורקל לSAT שמכריעה את L.
נגדיר תוכנית $c(S,i,j)$ שמחזירה את המילה שיש בS בין האינדקס ה- i לאינדקס ה- j .
נבנה מכונה M2 שמכריעה את L^*
1. נגדיר מערך A בגודל $n + 1$
2. $B[0] \leftarrow true$
3. עבור כל i בין 1 לn
   3.1 $B[i] \leftarrow false$
   3.2 עבור כל j בין 0 ל-i
      3.2.1 אם $B[j] = true$ וגם $M(c(S,i,j)) = 1$
         3.2.1.1 $B[i] \leftarrow true$
4. נחזיר את $B[n]$

זה תכנות דינאמי והסיבוכיות זמן ריצה $O(n^3 p(x))$ ($p(x)$ זה זמן הריצה של M) וזה פולינומי.

NP^{SAT} סגורה לכוכב.
תהיי $S \in NP^{SAT}$ אזי קיים מוודא V_s פולינומי עם גישת אורקל לSAT כך ש:
$x \in S \Leftrightarrow \exists y: V_s(x,y) = 1$
נבנה מוודא S^* פולינומי עם גישת אורקל לSAT כך ש:
$x \in S^* \Leftrightarrow \exists y: V_{s^*}(x,y) = 1$
נשתמש בפונ' c שהגדרנו בטענה הקודמת.
$S^*(x)$
1. אם y לא מהצורה $y = (i_1,y_1), \dots ,(i_k,y_k),(|x|,y_{k+1})$ נדחה.
2. נסמן - $i \leftarrow 0, j \leftarrow i_k, k \leftarrow 1$
3. כל זמן ש $k \le K + 1$
   3.1 נריץ $V_s(c(x,i,j))$ אם דחה אז נדחה.
   3.2 $k \leftarrow k + 1$

3.3 $i \leftarrow j$
3.4 $j \leftarrow i_k$
4. נאשר.

$\mathrm{NP}^{\mathrm{SAT}}$ סגור למשלים $\Leftrightarrow PH = \Sigma_2$

$\underline{\Rightarrow}$

יהי $S \in NP^{SAT}$ אז לפי טענת עזר $S \in NP^{NP} = \Sigma_2$ ולכן $S \in \Pi_3$ ומתקיים (בגלל ש$PH = \Sigma_2$) $\Pi_3 = \Pi_2$ ולכן $S \in \Pi_2 = co\Sigma_2$ ולכן $\bar{S} \in \Sigma_2$

$\underline{\Leftarrow}$

$NP^{SAT} = NP^{NP} = \Sigma_2$ סגורה למשלים אז

$$\Sigma_2 = \Pi_2$$

$\underline{\subseteq}$

תהי $S \in \Sigma_2$ משמע $\bar{S} \in \Sigma_2$ ולכן $S \in \Pi_2$

$\underline{\supseteq}$

תהי $S \in \Pi_2$ משמע $\bar{S} \in \Sigma_2$ ולכן $S \in \Sigma_2$

מכאן PH קורסת לΣ_2 (לפי טענה מההרצאה) ולכן $PH = \Sigma_2$

תרגול 8

יום רביעי 18 מאי 2016 13:03

$P/poly$
שפה S תקרא דלילה אם קיים פולינום $p(.)$ כך שלכל $n \geq 0$ מתקיים $|S \cap \{0,1\}^n|$
$\leq p(n)$
הוכיחו $NP \subseteq P/poly$ אמ"מ לכל $L \in NP$ קיימת רדוקצית קוק מ- L לשפה דלילה.

הוכחה: מספיק להוכיח $SAT \in P/poly$
אמ"מ קיימת רדו' קוק מ-SAT לשפה דלילה.

$\Leftarrow$ נניח ש- $SAT \in P/poly$ כלומר קיימת סדרה של מחרוזות ייעוץ $\{a_n\}_{n\in N}$
וקיים פולינום $q(.)$ וקיימת מ"ט פולי' דט' M כן שלכל $|a_n| \leq q(n)^n$
ולכל $x \in \{0,1\}^n$ מתקיים

$$M(x,a_n) = \begin{cases} 1 & x \in SAT \\ 0 & x \notin SAT \end{cases}$$

נגדיר $S_i^n = 0^{i-1}\,10^{q(n)-i}$ כמו כן נגדיר :
לכל $n \geq 0$
$S = \{1^n 0 S_i^n | 1$ הוא a_n – ב i – ה כך שהביט $n \geq 0$ לכל$\}$
$a_n = 01011$

1110010000

1110000100
1110000010
קל לראות ש-S היא שפה דלילה, שכן מתקיים
$|S \cap \{0,1\}^{n+1+q(n)}| \leq |a_n| \leq q(n)$

כעת ניצור רדוקצית קוק מ- SAT לS. לשם כך ניצור מ"ט פולי דט' M^S (עם גישת אורקל ל-S) שמכריעה את SAT באופן הבא:
בהינתן קלט x באורך n:
1) צור את a_n ע"י $q(n)$ שאילתות האורקל הבאות:
$1^n 0 S_{q(n)}^n, \dots, 1^n 0 S_2^n, 1^n 0 S_1^n$
(אם האורקל החזיר 1 עבור שאילתא $1^n 0 S_i^n$ סימן שהביט ה-i הוא 1 ב-a_n אחרת ערכו של ביט זה הוא 0)
2) הרץ את $M(x,a_n)$ והחזר את תשובתה.

המכונה M^s מכריעה את SAT בזמן פולינומי כיוון שהיא מבצעת מס' פולי' של שאילתות אורקל, ויתר הפעולות שהיא מבצעת מתבצעות אף הן בזמן פולינומי.
לכן קיימת רדו' קוק מ-SAT ל-S

$\Rightarrow$ קיימת רדו' קוק מ-SAT לשפה דלילה S . לפיכך, קיימת מ"ט דט' פולי' M^s שמכריעה את SAT כאשר S שפה דלילה.
תהי $t(.)$ פונ' פולי' שחוסמת את זמן הריצה של M^s . ולכן האורך של שאילתא שM^s-מבצעת על קלט באורך n הוא לכל היותר $t(n)$
נבנה את a_n כך שתהיה שרשור של כל המחרוזות ב-S עד לאורך $t(n)$. מכיוון שS-דלילה קיים פולי- $p(.)$ כך שלכל n $|S \cap \{0,1\}^n| \leq p(n)$ ולכן, אורך המחרוזת באורך i ב-S הוא לכל היותר $i * p(i)$ ולכן מתקיים
$|a_n| \leq \Sigma_{i=0}^{t(n)} i * p(i) \leq t^2(n) * p(t(n))$
ולכן האורך של a_n פולי' בn.- ניתן ליצור מ"ט פולי' דט' M שבהינתן נוסחה ϕ באורך n

ועצה a_n תפעל באופן הבא:
M תסמלץ את M^S. כאשר M^s מבצעת שאילתת אורקל עם מחרוזת y כלשהי, M תסרוק את a_n ובמידה ו-y נמצאת בa_n הדבר שקול לתשובה חיובית של האורקל. אחרת הדבר שקול לתשובה שלילית של האורקל.

האלגו/המכו' M רצה בזמן פולי' כיוון ש-M^s רצה בזמן פולי' והאורך של a_n הוא גם חסום פולי' לכן קיבלנו ש- $SAT \in P/poly$

תרגול 9

יום רביעי 25 מאי 2016 12:53

סיבוכיות מקום

קריאה	בלבד	דו	כיווני				קלט

קריאה	בלבד	חד כיווני offline	דו כיווני online				ניחוש

קריאה	כתיבה	דו-כיווני				עבודה

כתיבה	בלבד	חד-כיווני				פלט

משפט: תהיי $S: N \to N$ פונ' , כאשר $S(n) \geq \log n$ מתקיים:
$NSPACE_{online}(S(n)) = NSPACE_{offline}(\Theta(\log S(n))$

(⇒)

	.	מקום:	כמות
1.	מיקום ראש קורא בסרט הקלט.	$\log n$	n
2.	תוכן סרט העבודה	$S(n)$	$2^{O(S(n))}$
3.	מיקום ראש קורא בסרט העבודה	$\log S(n)$	$S(n)$
4.	מצב המכונה	$O(1)$	$\lvert S_{m_{off}}\rvert$

$S(n)$	$2^{O(S(n))} = h * 2^{O(S(n))} * S(n) * \lvert S_{m_{off}}\rvert$

Offline
ניחוש

c_1	c_2	c_3	....	c_m

כל בלוק הוא $O(S(n))$

$c_2 = abc$
$c_3 = acd$

$c_i(CWG_1, CWG_2, \dots) \leq \#conf(M,x)$

$c'_l(CWG'_1, CWG'_2, \dots)$

$$\sum_{i=1}^{\#conf(m,x)} \#conf(m,x)^i \leq \cancel{\#conf(m,x)} * \#conf(m,x)^{\#conf(m,x)+1} \leq 2^{2^{O(S(n))}}|\Gamma|$$

Online - ניחוש

b_1	b_2	b_3	...	b_m

תרגול 10

יום רביעי 01 יוני 2016 11:02

סיבוכיות מקום:

משפטים שונים בנושא מקום:

1. $DTIME(S(n)) \subseteq DSPASE(S(n)) \subseteq NSPACE(S(n)) \subseteq DTIME(n * 2^{O(S(n))})$
2. $NL \subseteq DSPACE(\log^2 n)$ ובאופן כללי
$NSPACE(S(n)) \subseteq DSPACE(S(n^2))$
3. $NL = coNL$ ובאופן כללי
$NSPACE(S(n)) = coNSPACE(S(n))$
4. $PH \subseteq SPSACE = NPSACE \subseteq EXP$

משפט היררכיית המקום:
תהיי פונ' $G: N \to N$ $G(n) \geq \log n$ כך ש $G(n)$ היא $Space - constructible$ ותהיי $g(n)$ כך ש $g(n) = o(G(n))$
ומתקיים ש $SPACE(g(n))$ מוכל ממש ב-$SPACE(G(n))$

הוכחה:
מספיק להראות שקיימת שפה L כך ש $L \in SPACE(G(n))$ אבל $L \notin SPACE(g(n))$
נגדיר את השפה L ע"י מכונה M_L המכריעה אותה תוך שימוש ב- $O(G(n))$ מקום.
M_L תפעל באופן הבא:
בהינתן קלט $w =< M,y >$ כך ש $|w| = n$
1. הרץ את M לw למשך לכל היותר $2^{G(n)}$ צעדים עם לכל היותר $G(n)$ מקום.
2. אם $M(w)$ מקבלת במסגרת מגבלות הזמן והמקום של צעד 1- דחה. אחרת קבל.

נבחר k גדול מספיק כך שיתקיימו התנאים הבאים:
1. $g(k) < G(k)$
2. M'_L (מכונה שמכריעה את L ב$g(n)$ מקום) מבצעת פחות מ$2^{G(k)}$ צעדים על קלטים מאורך k
$DSPASE(g(n)) \subseteq DTIME(\cancel{n} * 2^{O(G(n))})$
3. הסימולציה של M'_L על הקלטים באורך k יכולה להתבצע תוך שימוש ב- $G(k)$ מקום.
$w =< M'_L, 1^k >$
**********יש המשך אצל יצחק**********

טענה: $SPACE(n) \neq P$
הוכחה: נניח בשלילה ש $SPACE(n) = P$
תהי $L \in SPACE(n^2)$ שפה. אזי קיימת מ"ט M_L שמכריעה את L בסיבוכיות מקום $O(n^2)$
נגדיר $M_{L'}$ שמכריעה L' בסיבוכיות מקום $O(n)$ באופן הבא:
1. בהינתן קלט y נבדוק שהוא מהצורה $x01^{|x|^2}$ עבור x כלשהו. אם לא- נדחה.
2. המכונה תריץ את M_L על x ותחזיר את תשובתה.
את בדיקה 1 ניתן לבצע בסיבוכיות מקום $O(n)$ כמו כן צעד 2 ניתן לבצע בסיבוכיות מקום $O(|x|^2) = O(|y|)$,
כיוון ש $|y| = |x| + 1 + |x|^2$
קיבלנו ש, $L' \in SPACE(n)$ לפי הנחת השלילה. $L' \in P$ לפיכך, קיימת מכונת טיורינג $M^*_{L'}$ שמכריעה את L'
בסיבוכיות זמן $O(n^c)$ עבור קבוע $c > 0$ כלשהו.
נבנה מ"ט M^*_L שמכריעה L באופן הבא:
1. בהינתן קלט x המכונה תיצור $y = x01^{|x|^2}$
2. המכונה תריץ את $M^*_{L'}$ על y ותחזיר את תשובתה.
את צעד 1 ניתן לבצע ב-$O(|y|) = O(|x|^2)$ זמן.
ואת צעד 2 ניתן לבצע ב- $O(|y|^c) = O(|x|^{2c})$
קיבלנו שניתן להכריע את L בסיבוכיות זמן פולי'. ולכן $L \in P$, לפי ההנחה $L \in SPACE(n)$
קיבלנו שכל שפה L ב- $SPACE(n^2)$ שייכת ל- $SPACE(n)$ בסתירה למשפט ההיררכיית המקום.

תרגיל 4

יום שני 06 יוני 2016 20:50

1)

1. [20 נק'] הראו שקיימת שפה כריעה L כך ש-$L \in P/poly$ אבל $L \notin P$.

5. [13 נק'] הוכיחו שהבעיה הבאה NL-שלמה:

קלט: גרף מכוון G עם n קדקודים, ולכל קשת משקל חיובי. הנחה: משקל כל קשת חסום על ידי פולינומית במספר הקדקודים.

שאלה: האם הגרף מקיים את אי שוויון המשולש? (כלומר האם לכל קשת מכוונת (x, y) משקל הקשת קטן-שווה ממשקל כל מסלול מכוון בגרף מ-x ל-y).

נקרא לבעיה E. נוכיח כי E היא NL שלמה.
לפי משפט שלמדנו בהרצאה $NL = co - NL$ אז נראה כי co-E היא co-NL.
(co-E - האם קיימת לפחות קשת אחת שמשקל הקשת(x,y) גדול ממשקל מסלול מכוון בגרף מ-x ל-y)

6. בהינתן גרף מכוון G, M_G היא מכונת טיורינג שמקבלת כקלט שמות של שני קדקודים u, v ב-G (בקידוד בינרי) ומחזירה 1 אם יש ביניהם קשת ב-G ו-0 אחרת.
נניח ש-M_G דטרמיניסטית ורצה במקום n^2 (שימו לב, n הוא אורך השמות של הקדקודים ולא גודל הגרף G).

נגדיר את הבעיה L באופן הבא:
קלט: זוג x ו-y בגרף G, וקידוד של המכונה $<M_G>$.
שאלה: האם יש ב-G מסלול מ-x ל-y.

א. [5 נק'] הראו ש-L שייכת למחלקה PSPACE.

ב. [10 נק'] הראו ש-L קשה עבור המחלקה PSPACE.

תרגול 11

יום רביעי 15 יוני 2016 11:00

אלגוריתמים הסתברותיים:
מ"ט הסתברותית M היא:

1. מ"ט ל"ד המחליטה על המעברים שלה בהתאם לתוצאות הטלת מטבע אחיד.
2. מ"ט דטרמינסטית שמקבלת קלט נוסף r(המתקבל על סרט מיוחד - סרט הרנדומיות) שהוא סדרת הטלות מטבע אקראיות שמתפלגות באופן אחיד.

המחלקה RP(אלגו' שטועים בכיוון אחד)
$L \in RP$ אם קיימת מ"ט הסתברותית M בעל סיבוכיות זמן ריצה פולינומית כך שמתקיים:
$x \in L \Rightarrow \Pr_r[M(x,r) = 1] \geq \frac{1}{2}$
$x \notin L \Rightarrow \Pr_r[M(x,r) = 0] = 1$
הערות:

1. $P \subseteq RP \subseteq NP$
2. ניתן לשנות את הקבוע $\frac{1}{2}$ לכל מספר בין $\frac{1}{p(|x|)}$ ל- $1 - \frac{1}{2^{p(|x|)}}$ עבור פולי' $p(.)$ כלשהו ע"י אמפליפיקציה.
3. המחלקה $coRP$
$L \in RP$ אם קיימת מ"ט הסתברותית M הרצה בזמן פולינומי ומתקיים:
$x \in L \Rightarrow \Pr_r[M(x,r) = 1] = 1$
$x \notin L \Rightarrow \Pr_r[M(x,r) = 0] \geq \frac{1}{2}$

המחלקה BPP:
נגדיר את הפונ' האופיינית לשפה L:

$$\chi_L(x) = \begin{cases} 1 & x \in L \\ 0 & x \notin L \end{cases}$$

$L \in BPP$ אם קיימת מ"ט הסתברותית M שרצה בזמן פולינומי ומתקיים:
$P_r[M(x,r) = \chi_L(x)] \geq \frac{2}{3}$
הערות:

1. $RP \subseteq BPP$
2. היחס בין NP ו-BPP לא ידוע.
3. ניתן להקטין את ההסתברות לטעות ל- $1 - \frac{1}{2^{p(n)}}$
עבור פולי' $p(.)$ כלשהו ע"י הרצות חוזרות ובחירת רוב.
4. $BPP = coBPP$
5. $BPP \subseteq p/poly$ וגם $BPP \subseteq \Sigma_2 \cap \pi_2$

דוג' לאלגו' הסתברותי- וידוא מכפלת מטריצות:
נתונה השפה הבאה:
$MAT - VERIFY = \{(A,B,C) | A \times B = C$ ומתקיים $n \times n$: {A,B ו – C הן מטריצות בגודל
ניתן להכריע שייכות לשפה זו בפשטות ע"י אלגו שרץ בזמן $O(n^3)$
נראה אלגו' הסתברותי שרץ בזמן $O(n^2)$ ומקיים את התנאים של $coRP$
האלגו' M פועל באופן הבא:
בהינתן מטריצות C,B,A:

1. צור וקטור בינארי r באורך n באופן רנדומי(מתקבל על סרט ברנדומיות)
2. חשב $P = A * (Br) - Cr$
3. אם P הוא וקטור האפס נחזיר 1 אחרת נחזיר 0.
עבור $(A,B,C) \in MAT - VERIFY$ מתקיים:
$p = A * (Br) - Cr = (AB)r - Cr = (AB - C)r = 0$
כלומר $P_r[M(x,r) = 1] = 1$ עבור כל $x \in MAT - VERIFY$

עבור $(A,B,C) \notin MAT-VERIFY$:

נגדיר: $D = A * B - C = (d_{ij})$

$p = D\mathrm{r} = (AB - c)r = A(Br) - Cr = (p_1, p_2, \dots, p_n)^T$

מכיוון $A * B \neq C$ הרי שקיים אלמנט ב-D שאינו אפס. נניח ש $d_{ij} \neq 0$ (עבור i ו-j מסוימים)

ע"פ הגדרת מכפלת מטריצות מתקיים:

$p_i = \Sigma_{k=1}^{n} d_{ik} * r_k = d_{i1} * r_1 + d_{i2} * r_1 + \dots + d_{ij} * r_j + \dots + d_{in} * r_n = y + d_{ij} * r_j$

עבור y קבוע כלשהו.

לפי נוסחת $Bayes$ מתקיים.

$P_r[p_i = 0] = P_r[p_i = 0 | y = 0] * P_r[y = 0] + P_r[p_i = 0 | y \neq 0] * P_r[y \neq 0]$

מתקיים:

$P_r[p_i = 0 | y = 0] = P_r[r_j = 0] = \frac{1}{2}$

$P_r[p_i = 0 | y \neq 0] = P_r[r_j = 1 \cap d_{ij} = -y] \leq P_r[r_i = 1] = \frac{1}{2}$

להמשיך.. מלא נוסחאות

תרגול 12

יום רביעי 15 יוני 2016 18:02

אלגו הסתבורתיים:
תרגיל:
הוכיחו שאם $NP \subseteq BPP$ אז $NP = RP$
פיתרון:
על מנת להראות ש- $NP = RP$ צ"ל $RP \subseteq NP$ וגם $NP \subseteq RP$.
החלק הראשון $RP \subseteq NP$ נכון תמיד כפי שהוכח בהרצאה.
נראה כי $NP \subseteq RP$
מספיק להראות לשם כך ששפה שהיא NP-שלמה נמצאת ב-RP נראה זאת עבור SAT.

מהנתון ש $NP \subseteq BPP$ נובע ש $SAT \in BPP$ ולכן קיימת מ"ט הסתברותית 'M הרצה בזמן פולינומי ומכריעה את SAT כך שמתקיים לכל x:
$P_r[M'(x,r) = \chi_{SAT}(x)] \geq \frac{2}{3}$
ע"י מס' פולי' של הרצות חוזרות של 'M ובחירה לפי רוב ניתן לקבל מ"ט הסתברותית M שרצה בזמן פולי ומכריעה את SAT כך שלכל x מתקיים:
$P_r[M(x,r) = \chi_{SAT}(x)] \geq 1 - \frac{1}{4n}$
כעת נראה מ"ט הסתברותית M^* המכריעה את SAT בדרישות ההסתברות של RP.
בהינתן קלט x ומחרוזת רנדומית $r = (r_1,r_2, \dots ,r_{n+1})$ המכונה M^* תפעל באופן הבא:

1. בדוק האם $M(x,r_1) = 0$ אם כן החזר 0
2. אחרת,
   2.1 עבור כל משתנה v_i בנוסחא x:
   a. הצב 0 במשתנה v_i בנוסחא x וצמצם אותה ל-x_0
   b. אם $M(x_0,r_{i+1}) = 1$ המשך עם x_0
   c. אחרת, הצב 1 במשתנה v_i בנוסחא x וצמצם אותה ל x_1, המשך עם x_1.
   2.2 הצב את השמת האמת שהתקבלה מהשלב הקודם בנוסחה המקורית x אם הנוסחא מסופקת החזר 1 אחרת החזר 0.

אם $x \notin SAT$ אז מכיוון שבכל מקרה M^* בודקת את השמת האמת שהתקבלה מהרדוקציה העצמית, הרי שבהכרח נחזיר 0 כיוון שלא ניתן לספק את x.
אם $x \in SAT$ אם בכל $n + 1$ ההרצות של M הוחזרה התשובה הנכונה, נקבל השמת אמת שמספקת את x ולכן בשלב 2.2 נחזיר 1.
לכן ההסתברות ש- M^* תחזיר תשובה שגויה במקרה זה היא לכל היותר ההסתברות ש-M תטעה באחת מ-$n + 1$ ההרצות שלה ב-M^*.
ההסתברות לטעות של M בהרצה בודדת היא לכל היותר $\frac{1}{4n}$ לכן ההסתברות שנטעה באחת מ$n + 1$ ההרצות של M במסגרת M^* היא לכל היותר $\frac{n+1}{4n} \leq \frac{1}{2}$ לפי חסם האיחוד.
לכן קיבלנו שעבור $x \in SAT$ מתקיים:
$P_r[M^*(x,r) = 1] \geq \frac{1}{2}$
ועבור $x \notin SAT$ $P_r[M^*(x,r) = 0] = 1$
$NP \subseteq \mathrm{RP} \Leftarrow SAT \in RP \Leftarrow$
■
לפי רוב ניתן לקבל מ"ט הסתברותית M שרצה בזמן פולי' ומכריעה את SAT כך שלכל x מתקיים
$P_r[M(x,r) = \chi_{SAT}(x)] \geq 1 - \frac{1}{4n}$

תרגיל:
המחלקה ZPP:
הגדרה 1:
$L \in ZPP$ אם קיימת מ"ט הסתברותית M הרצה בזמן פולי' כל שמתקיים:

$\forall x \quad P_r[M(x,r) = '\perp'] \leq \frac{1}{2}$
$\forall x \quad P_r[M(x,r) = \chi_L(x) \; or \; M(x,r) = '\perp'] = 1$

הגדרה 2:
$L \in ZPP$ אם קיימת מ"ט הסתברותית M שמחזירה תמיד תשובה נכונה(0 או 1) ותוחלת זמן הריצה שלה פולינומית.
הגדרה 3:
$ZPP = RP \cap coRP$
משפט: כל ההגדרות הנ"ל שקולות.

שקילות הגדרות 1 ו-2:
$(2 \Leftarrow 1)$
תהיי $L \in ZPP$ לפי הגדרה 1. כלומר קיימת מ"ט הסתברותית M שמקיימת את ההסתברות של הגדרה 1.
ניצור מ"ט הסתברותית M' שתריץ את המכונה M שוב ושוב עד לקבלת תשובה החלטית ונחזיר אותה.
נניח שהפולינום $p(.)$ חוסם את זמן הריצה של M.
מס' הפעמים שיש להריץ את M עד לקבלת תשובה הוא משתנה גאומטרי שהפרמטר p שלו גדול שווה חצי,
לכן תוחלת מס' ההרצות היא 2 (שזה $\frac{1}{p}$) לכל היותר.
מכאן נקבל שתוחלת זמן הריצה של M' היא $2p(.)$ כנדרש.

$(1 \Leftarrow 2)$
תהיי $L \in ZPP$ לפי הגדרה 2. כלומר קיימת מ"ט הסתברותית M שמכריעה את L בתוחלת זמן ריצה פולינומית. נניח שהפולינום $p(.)$ חוסם את תוחלת זמן הריצה של M.
ניצור מ"ט הסתברותית M' שמריצה את M למשך $2p(n)$ צעדים על קלט באורך n. במידה והתקבלה תשובה סופית מ-M במהלך $2p(n)$ צעדים אלה נחזיר אותה, אחרת נחזיר ' ⊥ '
ברור שמתקיים:
$\forall x: P_r[M'(x,r) = \chi_L(x) \; or \; M(x,r) = '\perp'] = 1$
$\forall x: P_r\left[M'(x,r) = '^{\perp}'\right] = P_r[\text{M(x,r) לא עוצרת לאחר 2p(n) צעדים}]$
אם נגדיר מ"מ x להיות מס' הצעדים ש-M רצה אז
$= P_r[x \geq 2p(n)] \leq \left(\text{אי שיוויון מרקוב}\right) \frac{E[x]}{2p(n)} = \frac{p(n)}{2p(n)} = \frac{1}{2}$
$(1 \Leftarrow 3)$
תהיי $L \in RP \cap coRP$ כלומר קיימת מ"ט הסתברותית M שמכריעה את L ותוחלת זמן ריצה פולינומית. נניח שהפולינום $p(.)$ חוסם את תוחלת זמן הריצה של M.
ניצור מ"ט הסתברותית M' שמכריעה את M למשך $2p(n)$ צעדים על קלט באורך

נהיה לי בלאגן.. יצחק לא ברור מה הוא עשה פה :)

המחלקה MA מוגדרת באופן אנאלוגי ל-NP כאשר המוודא הוא מ"ט הסתברותית(פולינומית).
נגדיר את המחלקה $MA_{\frac{2}{3},\frac{1}{3}}$ להיות המחלקה שמכילה את השפה L כך שקיימת מ"ט פולי' הסתברותית M שמקיימת:
$x \in L \Rightarrow \exists y Pr_r[M(x,y,r) = 1 \geq \frac{2}{3}$
$x \notin L \Rightarrow \forall y \Pr[M(x,y,r) = 1] \leq \frac{1}{3}$
באופן דומה נגדיר את $MA_{1,\frac{1}{3}}$ להיות המחלקה שמכילה את השפות כך שקיימת מ"ט הסתברותית פולינומית M מקיימת:
$x \in L \Rightarrow \exists y Pr_r[M(x,y,r) = 1 = 1$
$x \notin L \Rightarrow \forall y \Pr[M(x,y,r) = 1] \leq \frac{1}{3}$

תרגול 13

יום רביעי 22 יוני 2016 10:58

תרגול אחרון

אלגוריתמים הסתברותיים

המחלקה MA מוגדרת באופן אנאלוגי למחלקה NP כאשר המוודא הוא מ"ט הסתברותית.
נגדיר את המחלקה $MA_{\frac{2}{3},\frac{1}{3}}$ להיות המחלקה שמכילה את השפות c כך שקיימת מ"ט הסתברותית M שמכריעה את L, כך שמתקיים:

$$x \in L \Rightarrow \exists y \Pr(M(x,y,r) = 1) \geq \frac{2}{3}$$

$$x \notin L \Rightarrow \forall y \Pr[M(x,y,r) = 1] \leq \frac{1}{3}$$

באופן דומה נגדיר את $MA_{1,\frac{1}{3}}$ להיות המחלקה שמכילה את השפות L כך שקיימת מ"ט הסתברותית פולינומית M שמכריעה את L כך שמתקיים:

$$x \in L \Rightarrow \exists y Pr_r[M(x,y,r) = 1] = 1$$

$$x \notin L \Rightarrow \forall y \Pr[M(x,y,r) = 1] \leq \frac{1}{3}$$

הוכיח $MA_{\frac{2}{3},\frac{1}{3}} = MA_{1,\frac{1}{3}}$

פיתרון:

כיוון אחד ברור נראה כי אם $L \in MA_{\frac{2}{3},\frac{1}{3}}$ אז $L \in MA_{1,\frac{1}{3}}$

בגלל ש $L \in MA_{\frac{2}{3},\frac{1}{3}}$ אז מתקיים מוודא פולינומי הסתברותי שמקיים:

$$x \in L \Rightarrow \exists y \Pr(v(x,y,r) = 1) \geq \frac{2}{3}$$

$$x \notin L \Rightarrow \forall y \Pr[v(x,y,r) = 1] \leq \frac{1}{3}$$

ע"י הרצות חוזרות של המוודא v ובחירה עפ"י רוב ניתן ליצור מוודא v^* שמשתמש במס' פולי של ביטים רנדומיים והסתברות השגיאה שלו לא עולה על $\frac{1}{2^n}$

בדומה להוכחה מההרצאה ש $BPP \subseteq \Sigma_2$ נשתמש ב"שיטה הסתברותית" להוכחת הטענה.
באופן ספציפי, ניתן להראות ש $x \in L$ אז קיימות $ploy(n) = k$ מחרוזות $r_1, r_2, \dots, r_k$ באורך פולי' m(קטן מ-k) כך ש:

$$\forall r_0 \; \exists i \in \{1,2,\dots,k\} s.t \; v^*(x,y,r_0 \oplus r_i) = 1$$

כדי להראות זאת מספיק להראות שמתקיים:

$$\Pr\left(\forall r_0 \left(V_{i=1}^{k} v^*(x,y,r_0 \oplus r_i) = 1\right)\right) > \frac{1}{2}$$ (r הוא שרשור של $r_0, \dots, r_k$)

כדי להראות זאת, נתבונן במאורע המשלים:

$$\Pr\left(\exists r_0 \left(V_{i=1}^{k} v^*(x,y,r_0 \oplus r_i) = 0\right)\right) \leq \left(\text{לפי חסם האיחוד}\right) \Sigma_{r_0 \in \{0,1\}^m} \Pr\left(\left(V_{i=1}^{k} v^*(x,y,r_0 \oplus r_i)\right)\right)$$

$$= \Sigma_{r_0 \in \{0,1\}^m} \Pr\left(\left(\wedge_{i=1}^{k} \left(v^*(x,y,r_0 \oplus r_i) = 0\right)\right)\right) = 0$$

$$= \left(\text{כל המאורעות שעושים בניהן וגם הם בת}\right) = \Sigma_{r_0 \in \{0,1\}^m} \Pi_{i=1}^{k} \Pr\left(\left(V_{i=1}^{k} v^*(x,y,r_0 \oplus r_i)\right)\right)$$

$$= 0 \leq \Sigma_{r_0 \in \{1,0\}^m} \Pi_{i=1}^{k} \frac{1}{2^n} = \Sigma_{r_0 \in \{0,1\}^m} = 2^m * \frac{1}{2^{kn}} < \frac{1}{2^n}$$

לכן ניתן ליצור מוודא v' שכאשר הוא מקבל $x, y' (= y|r_1|r_2| \dots |r_k), r_0$ הוא יריץ את v^* על $x,y,r_0 \oplus r_i$ כל פעם עבור r_i שונה. במידה ובאחת ההרצות הוחזר 1 נחזיר 1 אחרת נחזיר 0.
לפי מה שהוכחנו המוודא החדש עבור $x \in L$ תמיד יהיה צודק כיוון שיהיה r_i שיקיים $v^*(x,y,r_0 \oplus r_i) = 1$

לעומת זאת, אם $x \notin L$ אז מתקיים:

$$\Pr[v^*(x,y,r_0 \oplus r_i) = 1] \leq \frac{1}{2^n}$$

לכן ההסתברות ש-v' יחזיר 1 עבור $x \notin L$ היא:

$$\Pr\left(v^*(x,y,r_0 \oplus r_i) = 1 \; for \; some \; i\right) \leq k * \frac{1}{2^n} \leq \frac{1}{3}$$

תרגיל:
הוכיחו $P^{\#p} \subseteq PSPACE$

תרגיל 6

רויטל שיפמן
203438973

יום חמישי 30 יוני 2016 12:16

5. [15 נק'] הוכיחו כי לכל שפה S∈PP קיימת רדקוציית-קוק לפונקציה f∈#P ולהיפך.

רדוקציה מPP ל#P:
תהי $L \in PP$ ו M_L' מכונה שמכריעה את L בPP
נגדיר את היחס $R_L = \{(x,r)|M(x,r) = 1\}$ $(|r| \le p(x))$
$f_{R_L}(x) > \frac{1}{2} * 2^{|p(|x|)|} \Leftrightarrow x \in L$

רדוקציה מ$\#P$ לPP
נתבונן על היחס $R \in PC$ שמונה את f והשפה $S_f = \{(x,N)|f(x) \ge N\}$
$p(.)$ פולינום שמציין את הפתרונות עבור R $((x,y) \in R \Rightarrow (|y| = p(|x|))$
נחשב אלגו' A כך שבהינתן קלט (x,N) בהסתברות חצי בוחר $y \in \{0,1\}^{p(|x|)}$ בהתפלגות אחידה ומחזיר 1 אמ"מ $(x,y) \in R$ אחרת מחזיר 1 בהסתברות $\frac{2^{p(|x|)}-N+0.5}{2^{p(|x|)}}$
$A((x,N),r)$:

1. אם $r_0 = 1$ (ההסתברות היא חצי)
   א) נבחר $y \in \{0,1\}^{P(|x|)}$ שרירותי
   ב) אם $(x,y) \in R$ נחזיר 1 אחרת 0
2. אם $r_0 = 0$
   א) מחזיר 1 בהסתברות $\frac{2^{p(|x|)}-N+0.5}{2^{p(|x|)}}$

מתקיים $P_r[A(x) = 1] > \frac{1}{2} \Leftrightarrow (x,N) \in S_f$
$P_r[A(x) = 1] = \frac{1}{2} + \frac{1}{2}[\,(f_R(x) - N + 0.5)/2]$
$f_R(x) - N > 0$
אם $f_R(x) > N$ אזי $(x,N) \in S_f$
אחרת $f_R(x) < N$ ולכן $f_R(x) - N < 0 \Leftarrow$

$P_r[A((x,N),r) = 1] > \frac{1}{2} \Leftrightarrow (x,N) \in S_f$
ולכן $S_R \in PP$

נראה רדוקציה מf_R לS_p
נבנה אלגו' A שמחשב את f_R עם גישת אורקל לS_{f1} ונבצע חיפוש בינארי בטווח $0 - 2^{p(|x|)}$
מס' הצעדים הוא $\log 2^{p(|x|)}$ ולכן הוא פולינומי כנדרש.

ומכאן שיש את הרדוקציות הנדרשות.
משל.

6. [15 נק'] הראו כי אם לכל f∈#P קיימת מכונת טיורינג הסתברותית פולינומית M כך ש

$Pr_r\,[f(x) / 5 \le M(x,r) \le 5 \cdot f(x)] \ge 1-1/(3|x|)$.

אזי $PH = NP^{RP}$

אם קיימת מכונה M כזאת אזי $NP \subseteq BPP$ נראה:
תהי $L \in NP$ נוכיח ש$L \in BPP$
מכיוון ש$L \in NP$ אזי קיימים פולינום $P(\cdot)$ ומוודא v פולינומי דטרמנסטי המקיימים:

- אם $x \in L$ אז קיים "עד" y כך שמתקיים $|y| \le p_L(|x|)$ ו- $v(x,y) = 1$.
- אז $x \notin L$ אז לכל y $v(x,y) = 0$

נסמן $R_L = \{(x,y)|v(x,y) = 1, |y| < P_L(|x|)\}$ ולכן $R_L \in PC$
ומכאן $f_{R_L} \in \#P$ לפי ההנחה קיימת מכונה הסתברותית פולינומית M_L כך ש

$$P_{r_1}\left[\frac{f_{R_L}(x)}{5} \le M_L(x,r) \le 5 * f_{R_L}(x)\right] \ge 1 - \frac{1}{3} \ge \frac{2}{3}$$

נבנה אותה:
$M(x,r)$:
נחזיר האם $M_L(x,r) = 0$

נשים לב שההסתברויות תואמות לדרישות שלנו

$$x \in L \Rightarrow P_r[M(x,r) = 1] = P_r[M(x,r) \ne 0] \ge 1 - \frac{1}{3} \ge \frac{2}{3}$$

$$x \notin L \Rightarrow P_r[M(x,r) = 0] = P_r[M(x,r) = 0] \ge 1 - \frac{1}{3} \ge \frac{2}{3}$$

ולכן $L \in BPP$ ומכאן הראינו ש $NP \subseteq BPP$

אנו יודעים כי $RP \subseteq BPP$
הוכחנו בהרצאה $RP \subseteq NP$
בתרגול הוכחנו ש אם $NP \subseteq BPP$ אזי $NP = RP$
ולכן $NP^{NP} = NP^{RP}$
ומכאן $NP^{NP} = PH = NP^{RP}$
משל

תרגול 9

יום חמישי 14 יולי 2016 21:44

סיבוכיות מקום

קריאה	בלבד	דו	כיווני				קלט

קריאה	בלבד	חד כיווני offline	דו כיווני online				ניחוש

קריאה	כתיבה	דו-כיווני				עבודה

כתיבה	בלבד	חד-כיווני				פלט

משפט: תהיי $S: N \to N$ פונ' , כאשר $S(n) \geq \log n$ מתקיים:
$NSPACE_{online}\big(S(n)\big) = NSPACE_{offline}(\Theta(\log S(n))$

(⇒)

מקום:

1.	מיקום ראש קורא בסרט הקלט.	$\log n$
2.	תוכן סרט העבודה	$S(n)$
3.	מיקום ראש קורא בסרט העבודה	$\log S(n)$
4.	מצב המכונה	$O(1)$

$S(n)$

סיכום

יום שישי 08 יולי 2016 13:57

P - אוסף השפות שקיימת מ"ט דטרמיניסטית שמכריעה אותן.
NP - אוסף השפות קיימת מ"ט ל"ד שמכריעה אותן.

- יחס חסום פולינומית - יחס $R \subseteq \{0,1\}^* \times \{0,1\}^*$ נקרא יחס חסום פולינומית אם קיים פולינום $P(\cdot)$ כך שלכל $(x,y) \in R$ מתקיים $|y| \leq p(|x|)$
- המחלקה PF - $R \in PF$ אם:
  1) R הוא יחס חסום פולינומית.
  2) קיים אלגוריתם פולינומי דטרמניסטי כך שבהינתן x הוא מוצא y כך ש- $(x,y) \in R$ או מחזיר שלא קיים y שכזה.
- המחלקה PC- $R \in PC$ אם:
  1) R הוא יחס חסום פולינומית
  2) קיים אלגוריתם פולינומי דטרמניסטי שמחזיר 1 אם $x \in S$ ו- 0 אחרת.
- המחלקה P- תהיי $S \subseteq \{0,1\}^*$ בעיית הכרעה/שפה.
  $S \in P$ אם קיים אלגוריתם פולינומי דטרמניסטי שמחזיר 1 אם $x \in S$ ו-0 אחרת.
- המחלקה NP- תהיי $S \subseteq \{0,1\}^*$ בעיית הכרעה/שפה.
  $S \in NP$ אם קיימת מערכת הוכחה מסוג NP ל- S , כלומר, $S \in NP$ אם קיימים פולינום $P(\cdot)$ ומוודא v פולינומי דטרמנסטי המקיימים:
  1) שלמות- אם $x \in S$ אז קיים "עד" y כך שמתקיים $|y| \leq p(|x|)$ ו- $v(x,y) = 1$.
  2) נאותות- אם $x \notin S$ אז לכל y $v(x,y) = 0$

בעיית חיפוש ניתנת להתאמה ליחס $R \subseteq \{0,1\}^* \times \{0,1\}^*$, כאשר $R = \{(x,y) \mid (x,y) \in R\}$. בעיית החיפוש שמתאימה ליחס R היא הבעיה שבהינתן x יש למצוא y כך ש-$(x,y) \in R$, ואם אין y כזה יש להחזיר $\perp$'.

הגדרה 1.1 יחס חיפוש ייקרא **חסום פולינומיאלית** אם קיים פולינום p כך שעבור כל $(x,y) \in R$ מתקיים

$$|y| \leq p(|x|)$$

הגדרה 1.2 מחלקת בעיות החיפוש הניתנות לפתרון פולינומיאלי נקראית $\mathbf{PF}$[1], ומגדרת כך:

$$\mathbf{PF} = \{R \mid \exists A: \ A \text{ is polynomial, and } A(x) \text{ returns } y \text{ such that } (x,y) \in R \text{ or } \perp \text{ if no such } y \text{ exists}\}$$

ומוגדר גם אוסף הפתרונות האפשריים עבור x,

$$R(x) = \{y \mid (x,y) \in R\}$$

הגדרה 1.3 המחלקה $\mathbf{PC}$[2] מוגדרת כך:

$$\mathbf{PC} = \{R \mid R \text{ is polynomial bounded}, \exists A \text{ polynomial}, \ A(x,y) \text{ returns } 1 \iff (x,y) \in R\}$$

$PC \subseteq PF$ זוהי שאלה פתוחה ששקולה ל $NP \subseteq P$
$PF \nsubseteq PC$

- נוכיח ע"י שפה לא כריעה איחוד של שפה של כל המילים שנגמרות ב1 קל למצוא מילה בשפה(1) ולכן היא בPF אבל אם אפשר להכריע אז אפשר להכריע שפה שאינה ניתנת להכרעה.

$PC \subseteq PF \Leftrightarrow NP \subseteq P(NP = P)$

- נראה גרירה דו כיוונית ונבנה יחס כך שיקיים את את ההכלות הדרושות. כדי להראות את ההכלה בPF עשינו רדוקציה עצמית.

רדוקציות:

רדוקציה של בעיה B לבעיה A היא אלגוריתם הפותר את בעיה B ע"י שימוש באלגוריתם בפותר את בעיה A. נשים לב כי בהוכחה של **משפט 1.7**, עשינו רדוקציה מ-R ל-S'_R, כאשר R היא בעיית החיפוש ו-S'_R היא בעיית הכרעה.

הגדרה 2.1 רדוקציית קוק מבעייה B לבעיה A מתוארת כמכונת טיורינג פולינומיאלית עם *גישת אורקל* M^A, כאשר M^A פותרת את בעיה B תוך שימוש בשאילתות אורקל לבעיה A.

הגדרה 2.2 (רדוקציית Karp-קארפ) היא רדוקציה בין שתי בעיות הכרעה החשיבה בזמן פולינומיאלי, מקרה פרטי של רדוקציית קוק. כלומר, בהינתן שתי קבוצות $S_1, S_2 \subseteq \{0,1\}^*$, רדוקציית קארפ מ-$S_1$ ל-S_2 היא פונקציה $f: \{0,1\}^* \to \{0,1\}^*$ החשיבה בזמן פולינומיאלי כך ש-

$$x \in S_1 \iff f(x) \in S_2$$

(מקרה פרטי של רדוקצית קוק, זוהי הרדו' שהיינו עושים בחישוביות, יש קופסא שחורה)

הגדרה 2.4 עבור $R \subseteq \{0,1\}^* \times \{0,1\}^*$ נאמר כי R הוא בעל רדוקציה עצמית אם קיימת רדוקציה פולינומיאלית מ־R ל־S_R כאשר

$$S_R = \{x \mid \exists y: (x,y) \in R\}$$

(רדוקציה מבעיית הכרעה לבעיית חיפוש- אם אנו יודעים להכריע אנחנו יכולים למצוא ממש פיתרון)

NP שלמות:

הגדרה 3.1 עבור $S \subseteq \{0,1\}^*$, S תיקרא <u>NP-קשה</u> אם קיימת רדוקציה מכל $S' \in \mathrm{NP}$ ל-S.

הגדרה 3.2 $S \subseteq \{0,1\}^*$ תיקרא <u>NP-שלמה</u> אם S היא NP-קשה וכן $S \in \mathrm{NP}$.

הערה 3.3 למעשה NP-שלמות מוגדרת יחסית לרדוקציות קארפ[1]. כלומר, S היא NP-שלמה אם $S \in \mathrm{NP}$ וקיימת רדוקציית קארפ מכל $S' \in \mathrm{NP}$ ל-S.

טענה - קיימות שפות NP שלמות-

הוכחה דומה להוכחה בחישוביות ע"י השפה -

$$R_u = \left\{ \left(\left\langle M, x, 1^t \right\rangle, y \right) \mid M \text{ is a Turing machine, } M \text{ accepts } (x,y) \text{ within } t \text{ steps, and } |y| < t \right\}$$

רדוקציה עצמית:

טענה 3.6 כל יחס $R \in \mathrm{PC}$ שבעיית ההכרעה שלו S_R היא NP-שלמה הוא **בעל רדוקציה עצמית**. כלומר, קיימת רדוקציה מ-R ל-S_R.

- קיימת טרנזיטיביות רדוקציות.

משפט 3.7 (*Ladner*) אם $\mathrm{P} \neq \mathrm{NP}$ אזי קיימת קבוצה $A \in \mathrm{NP}$, $A \notin \mathrm{P}$ וכן $A \notin \mathrm{NPC}$. כלומר, A אינה NP-שלמה.

להשלים הוכחה

Co-NP:

הגדרה 4.1 המחלקה co-NP מוגדרת להיות:

$$\text{co-NP} = \{\{0,1\}^* \backslash L \mid L \in \mathrm{NP}\}$$

(המשלים של שפה בNP היא ב co-NP)

הגדרה שקולה לכך היא עבור יחס R שהינו ב-PC, אז בעיית ההכרעה שלו היא ב-NP:

$$L_R = \{x \mid \exists y : (x,y) \in R\} \in \mathrm{NP}$$

ועבור co-NP:

$$\{0,1\}^* \backslash L_R = \{x \mid \forall y : (x,y) \notin R\} \in \text{co-NP}$$

השערה 1. $\mathrm{P} \neq \mathrm{NP}$.

השערה 2. $\mathrm{NP} \neq \text{co-NP}$.

- אם $P \neq NP \cap coNP$ אזי קיים יחס בחיתוך שלא ניתן לרדוקציה עצמית.
- $NP \neq coNP \Rightarrow P \neq NP$

טענה 4.2 לא תמיד קיימת רדוקציית קארפ בין $L \in \mathrm{NP}$ ל-$\overline{L} \in \text{co-NP}$.

טענה 4.3 עבור $L \in \mathrm{NP}$ תמיד קיימת רדוקציית קוק מ-L ל-$\overline{L}$.

נשים לב כי ידוע ש־$\mathrm{P} \subseteq \mathrm{NP} \cap \text{co-NP}$.

השערה 3. $\mathrm{P} \subsetneq \mathrm{NP} \cap \text{co-NP}$.

טענה 4.4 אם $\mathrm{NP} \cap \text{co-NP}$ מכיל קבוצות שהן NP-קשות, אזי $\mathrm{NP} = \text{co-NP}$.

תזכורת. (מחישוביות) NP סגור לרדוקציות קארפ. כלומר, אם קיימת רדוקציית קארפ מ-L' ל-L וכן $L \in \mathrm{NP}$ אזי $L' \in \mathrm{NP}$.

NP אינו סגור (כנראה) לרדוקציית קוק. ז"א, אם קיימת רדוקציית קוק מ-L' ל-L וכן $L \in \mathrm{NP}$, אזי לא ניתן להסיק $L' \in \mathrm{NP}$.

ההיררכיה הפולינומית:

הגדרה 5.3 עבור $k \in \mathbb{N}$ נגדיר את Π_k להיות

$$\Pi_k = \{\{0,1\}^* \backslash L \mid L \in \Sigma_k\} = \mathrm{co} - \Sigma_k$$

ההיררכיה הפולינומית, המסומנת ב-PH היא מחלקה שמכלילה את NP ואת co-NP. נראה כי PH סגורה לרדוקציות קוק, וכי מתקיים $\mathrm{NP} = \mathrm{P} \iff \mathrm{PH} = \mathrm{P}$.

הגדרה 5.1 עבור $k \in \mathbb{N}$ נגדיר את המחלקה Σ_k באופן הבא. נאמר ש-$A \in \Sigma_k$ אם קיים מוודא פולינומי V ופולינום $P(\cdot)$ כך שלכל x מתקיים:

$$x \in A \iff \exists y_1 \forall y_2 \exists y_3 \dots Q_k y_k : |y_i| < P(|x|), V(x_1, y_1, y_2, \dots, y_k) = 1$$

כאשר $Q_k = \exists$ אם k אי-זוגי, ו־$Q_k = \forall$ אם k זוגי.

נשים לב למשל כי $\mathbf{NP} = \Sigma_1$, $\mathbf{P} = \Sigma_0$.

הגדרה 5.2 נגדיר את ההיררכיה הפולינומית $\mathbf{PH}$ ע"י

$$\mathbf{PH} = \bigcup_{k=0}^{\infty} \Sigma_k$$

נשים לב כי $\mathbf{PH}$ היא אכן היררכיה לפחות במובן חלש, כלומר $\Sigma_k \subseteq \Sigma_{k+1}$[1].

נשים לב כי $\Pi_0 = \mathbf{P}$, $\Pi_1 = \text{co-NP}$. כמו כן, נשים לב כי $A \in \Pi_k \iff$ קיים מוודא פולינומי V ופולינום $P(\cdot)$ כך ש-

$$x \in A \iff x \notin \overline{A} \iff \neg(\exists y_1 \forall y_2 \dots Q_k y_k, V(x, y_1, \dots, y_k) = 1) \iff$$
$$\iff \forall y_1 \exists y_2 \forall y_3 \dots Q_k y_k, V(x, y_1, \dots, y_n) = 0$$

כאשר $|y_i| < P(|x|)$. ולכן ניתן להגדיר את Π_k באופן דומה ל-Σ_k ע"י סדרת k כמתים שמתחילה בכמת $\forall$.

התכונות הבאות נובעות מההגדרה של Σ_k ו-Π_k,

1. $\Pi_k \subseteq \Pi_{k+1}$.
2. $\Pi_k \subseteq \Sigma_{k+1}$ - $A \in \Pi_k$, אז קיים $V, P(\cdot)$ כך ש־

$$x \in A \iff \forall y_1 \exists y_2 \dots Q_k y_k : |y_i| < P(|x|), V(x, y_1, \dots y_k) = 1$$

נגדיר $V'(x, y_1, \dots, y_{k+1}) = V(x, y_2, \dots, y_{k+1})$ ויתקיים:

$$\exists y_1 \forall y_2 \dots Q_{k+1} y_{k+1} : V(x, y_1, \dots, y_{k+1}) = 1 \iff x \in A$$

3. $\Sigma_k \subseteq \Pi_{k+1}$.

מטענות אלו, נובע שניתן להגדיר את ההיררכיה הפולינומית כך,

$$\mathbf{PH} = \bigcup_{k=0}^{\infty} \Pi_k$$

טענה 5.4 $S \in \Sigma_{k+1}$ אם ורק אם קיים פולינום $P(\cdot)$ וקבוצה $S' \in \Pi_k$ כך ש-

$$S = \{x \mid \exists y, y < P(|x|), (x, y) \in S'\}$$

טענה 5.5 עבור $k \geq 1$, אם $\Pi_k \subseteq \Sigma_k$ אזי $\Sigma_k = \Sigma_{k+1}$.

טענה 5.6 אם $\Sigma_{k+1} = \Sigma_k$ אזי $\mathbf{PH} = \Sigma_k$.

מסקנה 5.7 $\mathbf{P} = \mathbf{NP} \iff \mathbf{P} = \mathbf{PH}$.

הגדרה 5.8 עבור פונקציית אורקל $f : \{0,1\}^* \to \{0,1\}$ ומ"ט ל"ד פולינומית M וקלט x, נגדיר את $M^f(x) = 1$ אם קיים מסלול מקבל של x תוך אפשרות גישה לאורקל f.

המחלקה של הקבוצות המתקבלות ע"י מ"ט ל"ד פולינומית בעלת גישת אורקל ל־f מכונה $\mathbf{NP}^f$. עבור $\mathcal{C}$ מחלקה של בעיות הכרעה,

$$\mathbf{NP}^{\mathcal{C}} = \bigcup_{f \in \mathcal{C}} \mathbf{NP}^f$$

משפט 5.9 לכל $k \geq 0$, $\Sigma_{k+1} = \mathbf{NP}^{\Sigma_k}$.

$(NP^{\Pi_k} = NP^{\Sigma_k})$

טענה 5.10 תהי $S \in \mathbf{NP}$. תהי S' כך שקיימת רדוקציית קוק מ-S' ל-S. אזי, $S' \in \Sigma_2$.

נשים לב שמכאן נוכל להסיק בצורה דומה את סגירות $\mathbf{PH}$ לרדוקציות קוק, ע"י הוכחה הזהה לזו של טענה **5.10**.
חישוב לא יוניפורמי:

בחישוב יוניפרמי קיים אלגו' אחד.

הגדרה 6.1 מעגל הוא גרף מכוון, המכיל קודקודים משלושה סוגים,

1. קלט.
2. שער לוגי מהסוג $\mathrm{AND}, \mathrm{OR}, \mathrm{NOT}$.
3. פלט.

מעגל מסוים מתאים לאורך קלט מסויים ולכן נעסוק במשפחות של מעגלים.

הגדרה 6.2 נאמר כי משפחה של מעגלים ${C_n}^{\infty}{}_{n=1}$ מחשבת את הפונ' $f:\{0,1\}^* \to \{0,1\}$ אם לכל קלט x $C_{|x|}(x) = f(x)$

גודל של מעגל מוגדר להיות כמות הקשתות בו, ונסמן זאת ב-$|C|$

הגדרה 6.3 נאמר שקבוצה $A \subseteq \{0,1\}^*$ ניתנת לפתרון ע"י משפחת מעגלים $\{C_n\}_{n=1}^{\infty}$ בגודל פולינומי אם קיים פולינום $p(\cdot)$ כך ש-

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

וכן $\left|C_{|x|}\right| \leq p(|x|)$.

הגדרה 6.4 נאמר שפונקציה $f : \{0,1\}^* \to \{0,1\}$ שייכת למחלקה $\mathbf{P}/\ell$ עבור $\ell : \mathbb{N} \to \mathbb{N}$ אם קיים אלג' פולינומי[1] M וסדרר אינסופית של מחרוזות עצה $\{a_n\}_{n=1}^{\infty}$ כך שמתקיימים התנאים הבאים,

1. לכל $x \in \{0,1\}^*$, $A\left(a_{|x|}, x\right) = f(x)$.
2. לכל $n \in \mathbb{N}$, $|a_n| = \ell(n)$.

טענה 6.5 $\mathbf{P}/1$ מכילה שפות **שאינן כריעות**, ולכן $\mathbf{P} \subsetneq \mathbf{P}/1$.

הגדרה 6.6 נגדיר את המחלקה $\mathbf{P}/\mathbf{poly}$ להיות,

$$\mathbf{P}/\mathbf{poly} = \bigcup_{\text{polynomial } p(\cdot)} \mathbf{P}/p$$

משפט 6.7 קבוצה A שייכת ל־$\mathbf{P}/\mathbf{poly}$ $\iff$ A ניתנת לפתרון ע"י משפחת מעגלים בגודל פולינומי.

טענה 6.8 אם $\mathbf{NP} \subseteq \mathbf{P}/\mathbf{poly}$ אזי $\mathbf{PH} = \Sigma_2$.

סיבוכיות זיכרון:

- סרט קלט - לקריאה בלבד.
- סרט פלט - לכתיבה בלבד.
- סרט עבודה - סרט לקריאה וכתיבה, וסיבוכיות הזכרון נמדדת עפ"י השטח המנוצל בסרט זה.
- א"ב בינארי.

הגדרה 7.1 נאמר כי בעיה מסויימת שייכת למחלקה $\mathbf{DSPACE}(s(n))$ עבור s פונקציה כלשהי, אם בהינתן קלט לבעיה באורך n ניתן להכריע את הבעיה, ע"י שימוש במכונת טיורינג[1], וגישה ללכל היותר $s(n)$ תאים מוך סרט העבודה.

טענה 7.2 לכל פונקציה t, $\mathbf{DTIME}(t(n)) \subseteq \mathbf{DSPACE}(t(n))$.

טענה 7.3 מתקיים

$$\mathbf{DSPACE}(s(n)) \subseteq \mathbf{DTIME}\left(n \cdot 2^{\mathcal{O}(s(n))}\right)$$

הערה 7.4 נשים לב כי עבור $s(n) \geq \log n$, $\mathbf{DSPACE}(s(n)) \subseteq \mathbf{DTIME}\left(2^{\mathcal{O}(s(n))}\right)$.

כעת, נתרכז תחילה בבעיות הניתנות לחישוב בזכרון לוגריתמי.

הגדרה 7.5 נגדיר את המחלקה המתאימה

$$\mathbf{L} = \bigcup_{c} \mathbf{DSPACE}(\ell_c)$$

כאשר $\ell_c = c \log n$.

מסקנה 7.6 $\mathbf{L} \subseteq \mathbf{P}$.

1. מודל ה-On-line, כאשר למכונה יש מעברים שלא מוגדרים באופן יחיד, הבחירה איזה מעבר לבצע נעשית באופן אקראי בזמן הריצה. הקלט מתקבל $\iff$ יש מסלול מקבל.

1. מודל ה-On-line, כאשר למכונה יש מעברים שלא מוגדרים באופן יחיד, הבחירה איזה מעבר לבצע נעשית באופן אקראי בזמן הריצה. הקלט מתקבל $\iff$ יש מסלול מקבל.

2. מודל ה-Off-line, ובמקרה זה המכונה היא דטרמיניסטית אך היא מקבלת קלט עזר נוסף (עד). הקלט מתקבל $\iff$ יש עד שגורם למכונה לקבל.

הגדרה 7.7 נאמר שבעיה שייכת למחלקה $\mathbf{NSPACE}(s(n))$ עבור פונקציה s כלשהי, אם בהינתן קלט לבעיה באורך n ניתן להכריע את הבעיה ע"י מ"ט ל"ד במודל ה־On-line ע"י שימוש בזיכרון מתוך סרט העבודה החסום ע"י $s(n)$.

אבחנה. מתקיים[3]

$$\mathbf{DSPACE}(s(n)) \subseteq \mathbf{NSPACE}(s(n))$$
$$\mathbf{NTIME}(t(n)) \subseteq \mathbf{NSPACE}(t(n))$$

הגדרה 7.8 המחלקה הלא דטרמיניסטית המקבילה ל-$\mathbf{L}$ היא

$$\mathbf{NL} = \bigcup_c \mathbf{NSPACE}(\ell_c)$$

כאשר $\ell_c = c \log n$.

טענה 7.9 $\mathbf{L} \subseteq \mathbf{NL} \subseteq \mathbf{P}$.

הגדרה 7.10 עבור $A' \in \mathbf{NL}$ נאמר שקיימת רדוקציית log-space מ-A' ל-A אם בהינתן קלט x, קיימת פונקציה $f(x)$ החשיבה בזכרון לוגריתמי ב-$|x|$ כך שמתקיים

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

הגדרה 7.11 בעיה A הינה שלמה ב-$\mathbf{NL}$ אם מתקיימים שני התנאים הבאים.

1. $A \in \mathbf{NL}$.
2. לכל $A' \in \mathbf{NL}$, קיימת רדוקציית log-space מ-A' ל-A.

להלן תיאור של בעיה שלמה ב-$\mathbf{NL}$:

$$\text{St-conn} = \{(G, s, t) \mid G \text{ is a directed graph, there exists a path from } s \text{ to } t\}$$

משפט 7.14 (משפט Savitch) מתקיים כי

$$\mathbf{NL} \subseteq \mathbf{DSPACE}\left(\log^2 n\right)$$

כלומר, $\mathbf{NSPACE}(\log n) \subseteq \mathbf{DSPACE}\left(\log^2 n\right)$.

אנו מוכיחים אלגו' שרץ בסיבוכיות הנדרשת לSt-conn ובגלל שהיא שלמה זה יהיה נכון להכל.
אלגו רקורסיבי שמחלקים ל2 כל פעם.

משפט 7.15 (משפט Savitch המוכלל) עבור $s(n) \geq \log n$, מתקיים

$$\mathbf{NSPACE}(s(n)) \subseteq \mathbf{DSPACE}\left(s^2(n)\right)$$

משפט 7.16 (משפט Immerman) $\mathbf{NL} = \text{co-}\mathbf{NL}$.

טענה 7.17 אם קיימת רדוקציית log-space מ-L_1 ל-L_2, ו-$L_2 \in \mathbf{NL}$ אזי $L_1 \in \mathbf{NL}$.

טענה 7.18 תהי L^* שפה $\mathbf{NL}$-שלמה, וכן $L^* \in \text{co-}\mathbf{NL}$[5] אזי, $\mathbf{NL} = \text{co-}\mathbf{NL}$.

הגדרה 7.22 נגדיר את המחלקות

$$\mathbf{PSPACE} = \bigcup_{k=1}^{\infty} \mathbf{DSPACE}\left(n^k\right)$$
$$\mathbf{NPSPACE} = \bigcup_{k=1}^{\infty} \mathbf{NSPACE}\left(n^k\right)$$

מסקנה 7.23 קל לראות כי $\mathbf{PSPACE} \subseteq \mathbf{NPSPACE}$, אבל אפשר להשיג תוצאה יותר טובה. לפי משפט Savitch[7], מתקיים

$$\mathbf{NSPACE}\left(n^k\right) \subseteq \mathbf{DSPACE}\left(n^{2k}\right)$$

ולכן

$$\mathbf{PSPACE} = \mathbf{NPSPACE}$$

מסקנה 7.24 נגדיר את המחלקה $\mathbf{EXP}$ להיות,

$$\mathbf{EXP} = \bigcup_{c} \mathbf{DTIME}\left(2^{n^c}\right)$$

כעת, נשים לב שמתקיים $\mathbf{PSPACE} \subseteq \mathbf{EXP}$, וזאת לפי טענה **7.3** האומרת כי

$$\mathbf{DSPACE}\left(s(n)\right) \subseteq \mathbf{DTIME}\left(n \cdot 2^{\mathcal{O}(s(n))}\right)$$

טענה 7.25 מתקיים כי $\mathbf{PH} \subseteq \mathbf{PSPACE}$.

הגדרה 7.26 נאמר כי A היא $\mathbf{PSPACE}$-שלמה אם

1. $A \in \mathbf{PSPACE}$
2. לכל $B \in \mathbf{PSPACE}$ קיימת רדוקציית קארפ מ-B ל-A. כלומר, קיימת פונקציה f, חשיבה בזמן פולינומי[8], כך ש-

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

להלן קבוצה שהיא $\mathbf{PSPACE}$-שלמה,

$$\mathrm{QBF} = \{\varphi \mid \varphi \text{ is a quantified boolean formula that returns true}\}$$

דוגמא. למשל,

$$\mathrm{QBF} \ni \varphi = \exists x_1 \forall x_2 (x_1 \vee x_2)$$
$$\mathrm{QBF} \not\ni \psi = \forall x_1 \forall x_2 \exists x_3 (x_1 \vee x_3) \wedge (x_2 \vee \neg x_3)$$

טענה 7.27 QBF היא $\mathbf{PSPACE}$-שלמה.

אלגוריתמים ראנדומיים:

טענה 8.1 תהי M מ"ט הסתברותית להכרעת A אשר על כל קלט x מחזירה תשובה נכונה בהסתברות 1. אזי קיימת מ"ט M' דטרמיניסטית המכריעה את A בעלת זמן ריצה זהה לזה של A.

הגדרה 8.2 נאמר שקבוצה A שייכת ל-$\mathbf{RP}$ אם קיימת מ"ט הסתברותית M העוצרת בזמן פולינומי ומקיימת

$$\forall x \in A \quad \Pr_r\left[M(x,r) = 1\right] \geq \tfrac{1}{2}$$
$$\forall x \notin A \quad \Pr_r\left[M(x,r) = 0\right] = 1$$

(בעצם יש טעות חד צדדית)

טענה 8.3 $\mathbf{RP} \subseteq \mathbf{NP}$

הגדרה 8.4 נאמר ש-$L \in \mathbf{RP}_1$ אם קיימת מ"ט פולינומית הסתברותית M ופולינום $p(\cdot)$ כך ש-

$$x \in L \implies \Pr_r\left[M(x,r) = 1\right] \geq \tfrac{1}{p(|x|)}$$
$$x \notin L \implies \Pr_r\left[M(x,r) = 0\right] = 1$$

ונאמר ש-$L \in \mathbf{RP}_2$ אם קיימת מ"ט פולינומית הסתברותית M ופולינום $p(\cdot)$ כך ש-

$$x \in L \implies \Pr_r\left[M(x,r) = 1\right] \geq 1 - 2^{-p(|x|)}$$
$$x \notin L \implies \Pr_r\left[M(x,r) = 0\right] = 1$$

טענה 8.5 $\mathbf{RP}_1 = \mathbf{RP}_2$

הגדרה 8.6 נאמר כי קבוצה $A \in \mathrm{BPP}$ אם קיימת מ"ט הסתברותית M הרצה בזמן פולינומי ומקיימות

$$\forall x: \ \Pr_r\left[M(x,r) = \chi_A(x)\right] \geq \tfrac{2}{3}$$

כאשר χ_A האינדיקטור של A. כלומר,

$$\chi_A(x) = \begin{cases} 1 & x \in A \\ 0 & x \notin A \end{cases}$$

מסקנה 8.7 נשים לב לאבחנות הבאות,

1. $\mathrm{RP} \subseteq \mathrm{BPP}$, וזה קל לראות.
2. $\mathrm{BPP} \subseteq \mathrm{PSPACE} \subseteq \mathrm{EXP}$, כאשר ההסבר להכלה של $\mathrm{BPP} \subseteq \mathrm{PSPACE}$ הוא שאפשר לעבור על כל ה-rים האפשריים ולבדוק עבור איזה אחוז מתוכם מתקבל ש-$M(x,r) = 1$ ועבור איזה אחוז מתוכם מתקבל ש-$M(x,r) = 0$ ונענה עפ"י הרוב. מהגדרת BPP מובטח כי אם נענה עפ"י הרוב נקבל תשובה שנכונה עבור שייכות x לשפה עבור כל x.

NP ? BPP

טענה 8.8 תהי $A \in \mathrm{BPP}$. אזי לכל פולינום $p(\cdot)$ ישנה מ"ט M^* הסתברותית העוצרת בזמן פולינומי המקיימת

$$\forall x: \Pr_r\left[M^*(x,r) = \chi_A(x)\right] \geq 1 - \tfrac{1}{2^{p(|x|)}}$$

למה 8.9 (חסם צ'רנוב) יהיו $X_1, \ldots, X_n$ משתנים מקריים בלתי תלויים שווי התפלגות המקבלים ערכים ב-$\{0,1\}$, ותהי μ התוחלת של כ"א מהם. אזי, עבור כל $\varepsilon > 0$

$$\Pr\left[\frac{\sum_{i=1}^{k} X_i}{k} \geq \mu + \varepsilon\right] < e^{-2\varepsilon^2 k}$$

משפט 8.10 $\mathrm{BPP} \subseteq \mathrm{P/poly}$

משפט 8.11 $\mathrm{BPP} \subseteq \Sigma_2 \cap \Pi_2$.

#P:

תהי $A \in \mathrm{NP}$ כלומר קיים מוודא פולינומי $V(.)$ ופולינום $P(.)$ נגדיר יחס:

$R_A = \{(x,y) | V(x,y) = 1, |y| \leq P(|x|)\}$

$R_A \in PC$

עבור $R_A \in PC$ יחס חסום פולינומית נגדיר:

$f_R(x) = |\{y | (x,y) \in R\}|$

$f_R(x): \{0,1\}^* \to \mathbb{N}$

$\#P = \{f_R | PC$ – יחס ב R}

טענה: $NP \subseteq P^{\#P}$

טענה: $BPP \subseteq P^{\#P}$

$PH \subseteq P^{\#P}$

גרסת ההכרעה של #P

f - פונ' ספירה

f_R - בעיית הכרעה

תהי $f \in \#P$ נגדיר בעיית הכרעה:

$Sf = \{(x,N) | N > f(x)\}$

- קיימת רדו' פולי' מ f ל Sf נעשה חיפוש בינארי(על N) עד שנגיע לN הנכון. מSf ל f $2^{P(|x|)}$ (מס' האופציות) והסיבוכיות $\log 2^{P(|x|)}$

F היא #P שלמה אם:

- $f \in \#P$
- קיימת רדו' פולי' מכל $g \in \#P$ ל f.

רדוק' משמרת מס' עדים - רדו' פארסמונית

הגדרה: $R_1, R_2 \in PC$

S_{R_1}, S_{R_2} בעיות ההכרעה המתאימות ליחסים כלומר:

$S_{R_i} = \{x | (x,y) \in R_i\} \ \ i = 1,2$

$R_i(x) = \{y | (x,y) \in R_i\} \ \ i = 1,2$

נאמר ש g רדו' משמרת מס' עדים מ S_{R_1} ל- S_{R_2} אם:

$g(x) \in S_{R_2} \Leftrightarrow x \in S_{R_1}$ (כלומר g היא רדוקצית קארפ)

$|R_2(g(x))| = |R_1(x)|$

טענה:
$R_A \in PC$ אם $A \in NP$ וגם עבור כל $R_B \in PC, B \in NP$
קיימת רדוקציה פארסמונית מ-R_B ל-R_A אזי fR_A היא $\#P$ שלמה.

טענה:
$\#SAT$ בעיית הספירה של SAT היא #P שלמה.

משפט:
ישנו $R \in PC$ כך שלכל fR היא #P שלמה אבל S_R (בעיית ההכרעה) היא ב-P
(דוג' - בעיית הזיווג המושלם היא ב-P ובעיית הספירה המתאימה לה היא #P שלמה)

- אי אפשר לקרב בעיות ספירה ביעילות כי זה היה גורר $NP \subseteq BPP$
- כן אפשר לקרב בעיות ספירה תוך שימוש באורקל לNP

הגדרה קירוב:
$x \in \{0,1\}^*$, $f \in \#P$
$\Pi(x)$ יהיה אלגו' הסתברותי פולי' שהוא $(\frac{1}{3},10)$ (טיב הקירוב, שגיאה) - קירוב ל- $f(x)$
$\Pr_r\left[\frac{f(x)}{10} \le \Pi(x) \le 10 * f(x)\right] \ge 1 - \frac{1}{3}$

טענה:
אם ל $f \in \#P$ יש $(\frac{1}{3},10)$ קירוב אזי $NP \subseteq BPP$ (ואנו לא מצפים שזה יקרה)

$\#P = \{f_R | R \in PC\}$,$f_R: \{0,1\}^* \to \mathbb{N}$, $R \in PC$
Π יהיה אלגו' הסתברותי פולי' שהוא (c,δ) - קירוב ל- f_R
$Pr\left[\frac{f_R(x)}{c} \le \Pi(x) \le c * f_R(x)\right] \ge 1 - \delta$ (הטלות המטבע של Π)

משפט:
עבור כל $R \in PC$ קיים אלגו' הסתברותי פולינומי בעל גישת אורקל ל-NP הנותן $(16,\frac{1}{3})$ קירוב לfR

תכונות הנדרשות ממשפחת פונקציות ב- hash:
1. $h \in H$ נתנת ליצוג בגודל $P(|x|) \ge$
2. בהינתן y, $h(y)$ חשיב בזמן פולינומי ב- $|y|$
3. ניתן להגריל פונ' אקראית $h \in H$ בזמן פולינומי ב-$|x|$
4. ל-H יש תכונת המסננת האקראית.

טענה:
לכל $i \ge 1$ קיימת משפחה של פונ' hash H_l^i כך ש:
$h \in H_l^i \;\; h: \{0,1\}^l \to \{0,1\}^i \;\; 1 \le i \le l$
בעלות התכונות הבאות:
א) ל $h \in H_l^i$ יש תאור פולינומי ב-l.
ב) $h(y)$ ניתן לחישוב בזמן פולינומי ב- $|y|$
ג) ניתן לבחור $h \in H_l^i$ אקראית בזמן פולינומי ב-l.
ד) תכונת המסננת:
לכל $S \subseteq \{0,1\}^l$ יתקיים:
$\Pr[(1-\epsilon)\frac{|s|}{2^i} < |\{y \in S | h(y) = 0^m\}| < (1-\epsilon)\frac{|s|}{2^i}] \ge 1 - \frac{2^i}{\epsilon^2 |S| (\text{השגיאה})}$

הגדרות:
$S_{R,H}^* \in NP = \{(x,h,i) | \exists y \in R(x) \wedge h(y) = 0\}, S_R \in NP = \{x | \exists y (x,y) \in R\}$

שאלות ליצחק

יום רביעי 13 יולי 2016 19:26

- איך עוברים את המבחן הזה???????
- משפט לדנר
- **משפט 5.9** לכל $k \geq 0$, $\Sigma_{k+1} = \mathrm{NP}^{\Sigma_k}$.

(הכלה לצד השני - הניחושים)

טענה 6.5 $\mathrm{P}/1$ מכילה שפות **שאינן כריעות**, ולכן $\mathrm{P} \subsetneq \mathrm{P}/1$.

- האם מעגל יכול להחזיר תשובה לא נכונה, ולמה?
  - כן, כמו שיכול להיות עצה לא טובה
- 2014 מועד א' שאלה 2
- אם יש P^{BPP} האם האורקל מחזיר בהכרח תשובה נכונה?
  - כן.

משפט 7.16 (משפט Immerman) $\mathbf{NL} = \mathbf{co\text{-}NL}$.

-

טענה 7.17 אם קיימת רדוקציית log-space מ-L_1 ל-L_2, ו-$L_2 \in \mathbf{NL}$ אזי $L_1 \in \mathbf{NL}$.

($TR(G,S)$)

- **טענה 7.27** QBF היא $\mathbf{PSPACE}$-שלמה.
- יחס שאין לו רדוקציה עצמית תרגול 3

משפטים

יום שישי 15 יולי 2016 11:43

$PF \nsubseteq PC$
$PC \subseteq PF \Leftrightarrow NP \subseteq P(NP = P)$

טענה 3.6 כל יחס $R \in \mathrm{PC}$ שבעיית ההכרעה שלו S_R היא NP-שלמה הוא **בעל רדוקציה עצמית**. כלומר, קיימת רדוקציה מ-R ל-S_R.
משפט 3.7 (*Ladner*) אם $\mathrm{P} \neq \mathrm{NP}$ אזי קיימת קבוצה $A \in \mathrm{NP}$, $A \notin \mathrm{P}$ וכן $A \notin \mathrm{NPC}$. כלומר, A אינה NP-שלמה.
השערה 1. $\mathrm{P} \neq \mathrm{NP}$.
השערה 2. $\mathrm{NP} \neq \text{co-NP}$.

אם $P \neq NP \cap coNP$ אזי קיים יחס בחיתוך שלא ניתן לרדוקציה עצמית.

$NP \neq coNP \Rightarrow P \neq NP$
טענה 4.2 לא תמיד קיימת רדוקציית קארפ בין $L \in \mathrm{NP}$ ל-$\overline{L} \in \text{co-NP}$.
טענה 4.3 עבור $L \in \mathrm{NP}$ תמיד קיימת רדוקציית קוק מ-L ל-$\overline{L}$.
נשים לב כי ידוע ש־$\mathrm{P} \subseteq \mathrm{NP} \cap \text{co-NP}$.

השערה 3. $\mathrm{P} \subsetneq \mathrm{NP} \cap \text{co-NP}$.

טענה 4.4 אם $\mathrm{NP} \cap \text{co-NP}$ מכיל קבוצות שהן NP-קשות, אזי $\mathrm{NP} = \text{co-NP}$.
תזכורת. (מחישוביות) NP סגור לרדוקציות קארפ. כלומר, אם קיימת רדוקציית קארפ מ-L' ל-L וכן $L \in \mathrm{NP}$ אזי $L' \in \mathrm{NP}$.
NP אינו סגור (כנראה) לרדוקציית קוק. ז"א, אם קיימת רדוקציית קוק מ-L' ל-L וכן $L \in \mathrm{NP}$, אזי לא ניתן להסיק $L' \in \mathrm{NP}$.

טענה 5.4 $S \in \Sigma_{k+1}$ אם ורק אם קיים פולינום $P(\cdot)$ וקבוצה $S' \in \Pi_k$ כך ש-

$$S = \{x \mid \exists y, y < P(|x|), (x, y) \in S'\}$$

טענה 5.5 עבור $k \geq 1$, אם $\Pi_k \subseteq \Sigma_k$ אזי $\Sigma_k = \Sigma_{k+1}$.
טענה 5.6 אם $\Sigma_{k+1} = \Sigma_k$ אזי $\mathrm{PH} = \Sigma_k$.
מסקנה 5.7 $\mathrm{P} = \mathrm{PH} \iff \mathrm{P} = \mathrm{NP}$.

משפט 5.9 לכל $k \geq 0$, $\Sigma_{k+1} = \mathrm{NP}^{\Sigma_k}$.
$(NP^{\Pi_k} = NP^{\Sigma_k})$
טענה 5.10 תהי $S \in \mathrm{NP}$. תהי S' כך שקיימת רדוקציית קוק מ-S' ל-S. אזי, $S' \in \Sigma_2$.
נשים לב שמכאן נוכל להסיק בצורה דומה את סגירות PH לרדוקציות קוק, ע"י הוכחה הזהה לזו של טענה **5.10**.

טענה 6.5 $\mathrm{P}/1$ מכילה שפות **שאינן כריעות**, ולכן $\mathrm{P} \subsetneq \mathrm{P}/1$.
משפט 6.7 קבוצה A שייכת ל־$\mathrm{P/poly}$ $\iff$ A ניתנת לפתרון ע"י משפחת מעגלים בגודל פולינומי.
טענה 6.8 אם $\mathrm{NP} \subseteq \mathrm{P/poly}$ אזי $\mathrm{PH} = \Sigma_2$.

טענה 7.2 לכל פונקציה t, $\mathrm{DTIME}(t(n)) \subseteq \mathrm{DSPACE}(t(n))$.
טענה 7.3 מתקיים

$$\mathrm{DSPACE}(s(n)) \subseteq \mathrm{DTIME}\left(n \cdot 2^{\mathcal{O}(s(n))}\right)$$

הגדרה 7.5 נגדיר את המחלקה המתאימה

$$\mathrm{L} = \bigcup_c \mathrm{DSPACE}(\ell_c)$$

כאשר $\ell_c = c \log n$.

מסקנה 7.6 $\mathrm{L} \subseteq \mathrm{P}$.

הגדרה 7.7 נאמר שבעיה שייכת למחלקה $\mathbf{NSPACE}(s(n))$ עבור פונקציה s כלשהי, אם בהינתן קלט לבעיה באורך n ניתן להכריע את הבעיה ע"י מ"ט ל"ד במודל ה־`On-line` ע"י שימוש בזיכרון מתוך סרט העבודה החסום ע"י $s(n)$.

אבחנה. מתקיים[3]

$$\mathbf{DSPACE}(s(n)) \subseteq \mathbf{NSPACE}(s(n))$$
$$\mathbf{NTIME}(t(n)) \subseteq \mathbf{NSPACE}(t(n))$$

הגדרה 7.8 המחלקה הלא דטרמיניסטית המקבילה ל-$\mathbf{L}$ היא

$$\mathbf{NL} = \bigcup_c \mathbf{NSPACE}(\ell_c)$$

כאשר $\ell_c = c \log n$.

טענה 7.9 $\mathbf{L} \subseteq \mathbf{NL} \subseteq \mathbf{P}$.

משפט 7.14 (משפט Savitch) מתקיים כי

$$\mathbf{NL} \subseteq \mathbf{DSPACE}\left(\log^2 n\right)$$

כלומר, $\mathbf{NSPACE}(\log n) \subseteq \mathbf{DSPACE}\left(\log^2 n\right)$.

משפט 7.15 (משפט Savitch המוכלל) עבור $s(n) \geq \log n$, מתקיים

$$\mathbf{NSPACE}(s(n)) \subseteq \mathbf{DSPACE}\left(s^2(n)\right)$$

משפט 7.16 (משפט Immerman) $\mathbf{NL} = \text{co-}\mathbf{NL}$.

טענה 7.17 אם קיימת רדוקציית log-space מ-L_1 ל-L_2, ו-$L_2 \in \mathbf{NL}$ אזי $L_1 \in \mathbf{NL}$.

הגדרה 7.22 נגדיר את המחלקות

$$\mathbf{PSPACE} = \bigcup_{k=1}^{\infty} \mathbf{DSPACE}\left(n^k\right)$$
$$\mathbf{NPSPACE} = \bigcup_{k=1}^{\infty} \mathbf{NSPACE}\left(n^k\right)$$

מסקנה 7.23 קל לראות כי $\mathbf{PSPACE} \subseteq \mathbf{NPSPACE}$, אבל אפשר להשיג תוצאה יותר טובה. לפי משפט Savitch[7], מתקיים

$$\mathbf{NSPACE}\left(n^k\right) \subseteq \mathbf{DSPACE}\left(n^{2k}\right)$$

ולכן

$$\mathbf{PSPACE} = \mathbf{NPSPACE}$$

מסקנה 7.24 נגדיר את המחלקה $\mathbf{EXP}$ להיות,

$$\mathbf{EXP} = \bigcup_c \mathbf{DTIME}\left(2^{n^c}\right)$$

כעת, נשים לב שמתקיים $\mathbf{PSPACE} \subseteq \mathbf{EXP}$, וזאת לפי טענה **7.3** האומרת כי

$$\mathbf{DSPACE}\left(s(n)\right) \subseteq \mathbf{DTIME}\left(n \cdot 2^{\mathcal{O}(s(n))}\right)$$

טענה 7.25 מתקיים כי $\mathbf{PH} \subseteq \mathbf{PSPACE}$.

טענה 7.27 QBF היא $\mathbf{PSPACE}$-שלמה.

טענה 8.1 תהי M מ"ט הסתברותית להכרעת A אשר על כל קלט x מחזירה תשובה נכונה בהסתברות 1. אזי קיימת מ"ט M' דטרמיניסטית המכריעה את A בעלת זמן ריצה זהה לזה של A.

טענה 8.3 $\mathbf{RP} \subseteq \mathbf{NP}$

הגדרה 8.4 נאמר ש-$L \in \mathbf{RP}_1$ אם קיימת מ"ט פולינומית הסתברותית M ופולינום $p(\cdot)$ כך ש-

$$x \in L \implies \Pr_r\left[M(x,r) = 1\right] \geq \frac{1}{p(|x|)}$$
$$x \notin L \implies \Pr_r\left[M(x,r) = 0\right] = 1$$

ונאמר ש-$L \in \mathbf{RP}_2$ אם קיימת מ"ט פולינומית הסתברותית M ופולינום $p(\cdot)$ כך ש-

$$x \in L \implies \Pr_r\left[M(x,r) = 1\right] \geq 1 - 2^{-p(|x|)}$$
$$x \notin L \implies \Pr_r\left[M(x,r) = 0\right] = 1$$

טענה 8.5 $\mathrm{RP}_1 = \mathrm{RP}_2$
מסקנה 8.7 נשים לב לאבחנות הבאות,

1. $\mathrm{RP} \subseteq \mathrm{BPP}$, וזה קל לראות.
2. $\mathrm{BPP} \subseteq \mathrm{PSPACE} \subseteq \mathrm{EXP}$, כאשר ההסבר להכלה של $\mathrm{BPP} \subseteq \mathrm{PSPACE}$ הוא שאפשר לעבור על כל ה-rים האפשריים ולבדוק עבור איזה אחוז מתוכם מתקבל ש-$M(x,r) = 1$ ועבור איזה אחוז מתוכם מתקבל ש-$M(x,r) = 0$ ונענה עפ"י הרוב. מהגדרת BPP מובטח כי אם נענה עפ"י הרוב נקבל תשובה שנכונה עבור שייכות x לשפה עבור כל x.

טענה 8.8 תהי $A \in \mathrm{BPP}$. אזי לכל פולינום $p(\cdot)$ ישנה מ"ט M^* הסתברותית העוצרת בזמן פולינומי המקיימת

$$\forall x : \Pr_r \left[M^*(x,r) = \chi_A(x)\right] \geq 1 - \frac{1}{2^{p(|x|)}}$$

למה 8.9 (חסם צ'רנוב) יהיו $X_1, \ldots, X_n$ משתנים מקריים בלתי תלויים שווי התפלגות המקבלים ערכים ב-$\{0,1\}$, ותהי μ התוחלת של כ"א מהם. אזי, עבור כל $\varepsilon > 0$

$$\Pr\left[\frac{\sum_{i=1}^{k} X_i}{k} \geq \mu + \varepsilon\right] < e^{-2\varepsilon^2 k}$$

משפט 8.10 $\mathrm{BPP} \subseteq \mathrm{P/poly}$
משפט 8.11 $\mathrm{BPP} \subseteq \Sigma_2 \cap \Pi_2$.

טענה: $NP \subseteq P^{\#P}$

טענה: $BPP \subseteq P^{\#P}$

$PH \subseteq P^{\#P}$

טענה:
$R_A \in PC$ אם $A \in NP$ וגם עבור כל $R_B \in PC, B \in NP$
קיימת רדוקציה פארסמונית מ-R_B ל-R_A אזי fR_A היא $\#P$ שלמה.

טענה:
$\#SAT$ בעיית הספירה של SAT היא #P שלמה.

משפט:
ישנו $R \in PC$ כך fR היא #P שלמה אבל S_R (בעיית ההכרעה) היא ב-P

אם ל $f \in \#P$ יש $(\frac{1}{3},10)$ קירוב אזי $NP \subseteq BPP$ (ואנו לא מצפים שזה יקרה)

משפט:
עבור כל $R \in PC$ קיים אלגו' הסתברותי פולינומי בעל גישת אורקל ל-NP הנותן $(16,\frac{1}{3})$ קירוב לfR

NPC לא סגור לאיחוד

הקשר בין הגדרה 1 ל2-
$\Sigma_{k+1} = NP^{\Sigma_k}$ לכל $k \geq 0$
סימונים ותכונות:

1. $\pi_k = co\Sigma_k$
2. $\Delta_{k+1} = P^{\Sigma_k}$
3. $\Sigma_k \subseteq \Sigma_{k+1}$ ו- $\pi_k \subseteq \pi_{k+1}$
4. $\pi_k \subseteq \Sigma_{k+1}$ ו- $\Sigma_k \subseteq \pi_{k+1}$
5. $\pi_k \subseteq \Sigma_k \Rightarrow \Sigma_k = \Sigma_{k+1}$ (עבור $k \geq 1$)
6. $\Sigma_k = \Sigma_{k+1} \Rightarrow PH = \Sigma_k$
7. $\Sigma_k \subseteq \Delta_{k+1}$

משפט 1: $P \subseteq P/poly$ (אפשר לתת עצה ריקה)
משפט 2: $NP \nsubseteq P/poly \Rightarrow P \neq NP$

$NP \subseteq P/\log \Rightarrow NP = P$

שפה S תקרא דלילה אם קיים פולינום $p(.)$ כך שלכל $n \geq 0$ מתקיים $|S \cap \{0,1\}^n| \leq p(n)$
הוכיחו $NP \subseteq P/poly$ אמ"מ לכל $L \in NP$ קיימת רדוקצית קוק מ- L לשפה דלילה

משפט: לכל פונקציה $s:N\to N$, כך ש-logs היא space-constructible ולפחות לוגריתמית ב-n, מתקיים:
$NSPACE_{online}(s(n))=NSPACE_{offline}(\Theta(\log(s(n))))$

טענה: $SPACE(n) \neq P$
$BPP = coBPP$
$NP \subseteq BPP$ אז $NP = RP$

משפט: אי שיוויון מרקוב

יהי X מ"מ ו-a>0 אז מתקיים: $\mathbb{P}(|X| \geq a) \leq \frac{\mathbb{E}(|X|)}{a}$.

המחלקה ZPP:
הגדרה 1:
$L \in ZPP$ אם קיימת מ"ט הסתברותית M הרצה בזמן פולי' כל שמתקיים:
$\forall x \quad P_r[M(x,r) = '\perp'] \leq \frac{1}{2}$
$\forall x \quad P_r[M(x,r) = \chi_L(x) \ or \ M(x,r) = '\perp'] = 1$

הגדרה 2:
$L \in ZPP$ אם קיימת מ"ט הסתברותית M שמחזירה תמיד תשובה נכונה(0 או 1) ותוחלת זמן הריצה שלה פולינומית.
הגדרה 3:
$ZPP = RP \cap coRP$

שאלות מועד ב'

יום ראשון 07 אוגוסט 2016 18:53

- הוכחת $NP = P \Leftrightarrow PC \subseteq PF$

- הוכחת שפה דלילה תרגול 8
- משפט היררכית המקום
- הוכחה תרגול 13
- חישוב לא יוניפורמי - הכל + שקילות מכונות - הוכחה והוכחת מעגלים לוגים
- ניפוח - למה בבדיקת שייכות של x צריך $NPSACE(|S(n)|)$
- הוכחת st-conn למה $c \log n$ מס' קונפי'?
- $PH \subseteq PSPACE$
- הסתברויות
- הוכחת $NP \subseteq P/poly$ גורר $PH = \Sigma_2$
- $BPP \subseteq P/poly$
- $BPP \subseteq \Sigma_2 \cap \Pi_2$
- תרגיל 3 שאלה HOPE 3
- תרגיל 4 שאלה 1

תשובה ל6 ניסיון

יום רביעי 17 אוגוסט 2016 20:56

```
K = 8
While (G(a,k)=1)
   K *=8

Return k;
```

$$64 = 8^2$$

$$8^{i-1} \leq 8^i = k \leq 8^{i+2}$$

$L \in NP \;\; L \leq L^*$

אם זאת רדוקציית קארפ האם $L^* \in NP$