עמוס ביימל 23/01/04

סיבוכיות: שאלות חזרה

שאלה 1

סעיף א

נגדיר את השפה הבאה: $L_{\Sigma^*} = \{\langle M \rangle : L(M) = \Sigma^*\}$. הוכיחו כי $L_{\Sigma^*} \notin \mathcal{RE}$ וגם $\overline{L_{\Sigma^*}} \notin \mathcal{RE}$.
<u>הערה</u>: אפשר להוכיח את שתי הטענות על ידי רדוקציה אחת.

סעיף ב

המחלקה $\forall\mathcal{RE}$ מוגדרת באופן הבא:

שפה $L \in \forall\mathcal{RE}$ אם ורק אם קיימת $L_0 \in \mathcal{RE}$ כך ש-$L = \{ x : \forall y \ \ (x,y) \in L_0 \}$.

הוכיחו כי $L_{\Sigma^*} \in \forall\mathcal{RE}$.

סעיף ג

שפה B היא $\forall\mathcal{RE}$ קשה אם לכל $L \in \forall\mathcal{RE}$ מתקיים $L \le B$. הוכיחו כי L_{Σ^*} היא $\forall\mathcal{RE}$ קשה.

סעיף ד

הוכיחו כי אם שפה B היא $\forall\mathcal{RE}$ קשה, אזי $B \notin \mathcal{RE}$.

שאלה 2

תהי $L_{\text{EMP,not-EMP}} = \{<M_1>,<M_2> : \ L(<M_1>)=\phi \text{ and } L(<M_2>)\neq\phi \}$.
הראו כי לכל $L \in \mathcal{RE} \cup \text{co}\mathcal{RE}$ מתקיים $L \le L_{\text{EMP,not-EMP}}$.

שאלה 3

תהי A שפה. נגדיר את השפה C_A הבאה: $C_A = \{ <M> : \ A \subseteq L(M) \}$.

סעיף א

הוכיחו כי לכל שפה <u>סופית</u> A כאשר $A \neq \varnothing$ מתקיים $C_A \in \mathcal{RE} - \mathcal{R}$.

סעיף ב

הוכיחו כי לכל שפה <u>אינסופית</u> A מתקיים $C_A \notin \mathcal{RE}$.

שאלה 4

נגדיר את השפה L_{even}:

$L_{\text{even}} = \{$ <M> : מספר המילים בשפה $L(M)$ הוא זוגי $\}$.

הערה: אם יש אינסוף מילים ב- $L(M)$ אזי <M> $\notin L_{\text{even}}$.

סעיף א

הוכיחו כי $L_{\text{even}} \notin \mathcal{RE}$.

סעיף ב

הוכיחו $L_{\text{even}} \notin \text{co}\mathcal{RE}$.

שאלה 5

הוכיחו כי שפה $L \in \mathcal{RE}$ אם ורק אם קיימת שפה $L_0 \in \mathcal{R}$ כך ש- $L=\{ x : \exists y\ (x,y) \in L_0 \}$.

שאלה 6

הוכיחו או הפריכו את הטענות הבאות:

1. אם C היא תת-מחלקה לא טריביאלית של $\mathcal{RE}$ כאשר $\Sigma^* \in C$, אזי $L_C \in \mathcal{RE}$.
2. אם C היא תת-מחלקה לא טריביאלית של $\mathcal{RE}$ כאשר $\Sigma^* \in C$, אזי $L_C \notin \mathcal{RE}$.
3. אם C היא תת-מחלקה לא טריביאלית של $\mathcal{RE}$ כאשר $\Sigma^* \notin C$, אזי $L_C \in \mathcal{RE}$.
4. אם C היא תת-מחלקה לא טריביאלית של $\mathcal{RE}$ כאשר $\Sigma^* \notin C$, אזי $L_C \notin \mathcal{RE}$.

שאלה 7

סווגו כל אחת מהשפות הבאות לאחת מהאפשרויות הבאות:

1. $L \in \mathcal{P}$.
2. $L \in \mathcal{NP}$-comp (זכרו במקרה זה להוכיח כי $L \in \mathcal{NP}$).

יש להוכיח את תשובותיכם.

1. 3CLIQUE = $\{ G : G=(V,E)$ has a clique of size $|V|-3 \}$.
2. HALF-CLIQUE = $\{ G : G=(V,E)$ has a clique of size $|V|/2 \}$.
3. 4COLORING = $\{ G : G$ has a coloring with 4 colors $\}$.

שאלה 8

נגדיר את מחלקת השפות Δ_P:

$L \in \Delta_P$ אם ורק אם קיימות $L_1 \in \mathcal{NP}$ ו- $L_2 \in \text{co}\mathcal{NP}$ כך ש- $L = L_1 \cap L_2$.

שימו לב כי Δ_P <u>אינה</u> שווה ל- $\mathcal{NP} \cap \text{co}\mathcal{NP}$.

סעיף א

הוכיחו כי $\mathcal{NP} \cup \text{co}\mathcal{NP} \subseteq \Delta_P$.

סעיף ב

נגדיר את השפה SAT-noSAT: $\text{SAT-noSAT} = \{ (\varphi_1,\varphi_2) : \varphi_1 \in 3SAT, \varphi_2 \notin 3SAT \}$.
הוכיחו בקצרה כי SAT-noSAT היא Δ_P-שלמה ביחס לרדוקציות העתקה פולינומיאליות.

סעיף ג

הוכיחו כי $SAT \in co\mathcal{NP}$ אם ורק אם $\Delta_P = \mathcal{NP}$.

שאלה 9

3-צביעה של גרף $G=(V,E)$ היא פונקציה $c: V \to \{1,2,3\}$ המקיימת:

אם $(v_1,v_2) \in E$ אזי $c(v_1) \neq c(v_2)$.

הוכיחו בצורה ישירה כי אם קיים אלגוריתם יעיל הבודק אם גרף הוא 3-צביע אזי קיים אלגוריתם יעיל המוצא 3-צביעה של הגרף (אם היא קיימת).
הערה: בשאלה זו אין להשתמש במשפט קוק-לוין.

שאלה 10

בהינתן n קבוצות $S_1,\dots,S_n$, נאמר כי קבוצה $I \subseteq \{1,\dots,n\}$ היא אוסף של קבוצות לא-זרות אם לכל $i,j \in I$ מתקיים $S_i \cap S_j \neq \varnothing$. כלומר, כל שתי קבוצות באוסף נחתכות.
נגדיר:

- השפה XS: $\{$ ב- $S_1,\dots,S_n$ קיים אוסף של קבוצות לא-זרות בגודל k : $S_1,\dots,S_n,k\}$=XS.
- בעיית האופטימיזציה max-XS: בהינתן n קבוצות $S_1,\dots,S_n$, יש למצוא אוסף גדול ביותר של קבוצות לא-זרות.
- בעיית האופטימיזציה max-CLIQUE: בהינתן גרף G, יש למצוא קליק גדול ביותר ב- G.

סעיף א

הוכיחו כי XS היא $\mathcal{NP}$-שלמה.
רמז: רדוקציה מ- CLIQUE.

סעיף ב

הוכיחו כי אם אפשר לקרב את הבעיה max- CLIQUE עם יחס קירוב c, אזי אפשר לקרב את הבעיה max-XS עם יחס קירוב c.

שאלה 11

נתון גרף $G=(V,E)$ לא-מכוון מלא בו לכל קשת e יש משקל $w(e)$ שהוא שלם חיובי. מעגל המילטוני הוא מעגל פשוט המבקר בכל צומת בגרף בדיוק פעם אחת. נגדיר את בעיית האופטימיזציה TSP: בהינתן גרף G עם משקלים בתחום $\{1,\dots,w\}$, יש למצוא מעגל המילטוני ב- G שמשקלו קטן ביותר.

סעיף א

בהינתן גרף G עם משקלים בתחום $\{1,\dots,w\}$, הוכיחו כי כל מסלול המילטוני מקרב את בעיית ה-TSP בגרף G עם יחס קירוב w.

סעיף ב

גרף $G=(V,E)$ לא-מכוון מלא מקיים את אי-השוויון המשולש עם קבוע c אם לכל מסלול $x_1, x_2,\dots, x_k$ מתקיים: $w((x_1,x_k)) \leqslant c\,(w((x_1,x_2)) + w((x_2,x_3)) + \dots + w((x_{k-1},x_k)))$.

הראו איך לקרב עם יחס קירוב $1.5c$ את בעיית ה- TSP בגרף המקיים את אי-השוויון המשולש עם קבוע c.

סעיף ג

בהינתן גרף G עם משקלים בתחום $\{1,...,w\}$, הראו איך לקרב את בעיית ה- TSP בגרף G עם יחס קירוב $0.75w$.

שאלה 12

בהינתן גרף G נגדיר שתי בעיות אופטימיזציה:

- בעיית האופטימיזציה min-COLORING:

  בהנתן גרף G, יש למצוא צביעה של G במספר קטן ביותר של צבעים.

- בעיית האופטימיזציה min-COLOR-SUM:

  בהנתן גרף G, יש למצוא צביעה c של G כך ש- $\sum_{v\in V} c(v)$ קטן ביותר.

בסעיפים הבאים n הוא מספר הצמתים בגרף.

סעיף א

הוכיחו כי COLOR-SUM היא $\mathcal{NP}$-שלמה.

רמז: רדוקציה מ- SAT$\neq$.

סעיף ב

עבור גרף G נסמן ב- $S(G)$ את הערך המינימום של $\sum_{v\in V} c(v)$ מעל כל הצביעות $c: V \to \{1,...,n\}$.

הוכיחו כי $S(G) \geq n$ ואם קיימת צביעה של G עם k צבעים אזי מתקיים $S(G) \leq kn$.

סעיף ג

נסמן ב- $\chi(G)$ את המספר הקטן ביותר של צבעים הנדרש לצבוע גרף G. נניח כי קיים קבוע $a \geq 1$ וקיים אלגוריתם יעיל אשר לכל גרף G 3-צביע מחזיר צביעה של G בלכל היותר $a \cdot \chi(G)$ צבעים. הוכיחו כי תחת הנחה זו קיים אלגוריתם יעיל אשר לכל גרף G 3-צביע מחזיר צביעה של G שסכומה לכל היותר $3a \cdot S(G)$.

סעיף ד

הוכיחו כי אם קיימת צביעה c של G כך ש- $\sum_{v\in V} c(v) \leq s$ אזי קיימת קבוצה $U \subseteq V$ כך ש- $|U| \geq |V|/2$ ו- $c(u) \leq 2s/|V|$ לכל $u \in U$.

סעיף ה

הוכיחו כי אם נתונה צביעה c של G כך ש- $\sum_{v\in V} c(v) \leq s$ אזי ניתן בצורה יעילה לצבוע לפחות חצי מהצמתים בגרף על ידי $2s/|V|$ צבעים.

סעיף ו

יהי $1 \leq \alpha$. הוכיחו כי אם קיים אלגוריתם פולינומי ש α מקרב את בעיית min-COLOR-SUM, אזי קיים אלגוריתם פולינומי ש $O(\alpha \log n)$ מקרב את min-COLORING.

שאלה 13

סעיף א

תארו אלגוריתם יעיל אשר בהינתן גרף ובו קבוצה בלתי תלויה בגודל $3|V|/4$ מוצא קבוצה בלתי תלויה בגודל $|V|/2$.

<u>הדרכה</u>: השתמשו באלגוריתם ש- 2-מקרב את בעיית הכיסוי בצמתים.

סעיף ב

הסבירו מדוע אי-אפשר להשתמש באלגוריתם ש- 2-מקרב את בעיית הכיסוי בצמתים כדי לקרב את בעיית הקבוצה הבלתי תלויה הגדולה ביותר בגרף (ללא ההבטחה שיש קבוצה בלתי תלויה גדולה).

שאלה 14

גרף מכוון $G=(V,E)$ הוא גרף שכבות אם קיימת חלוקה של V ל- k קבוצות זרות $V_1,V_2,\ldots,V_k$ כך שהקשתות עוברות רק משכבה לשכבה שאחריה, כלומר,

$$E \subseteq V_1 \times V_2 \cup V_2 \times V_3 \cup \ldots \cup V_{k-1} \times V_k.$$

נגדיר:

DAG-CON={ G,s,t : G is a directed acyclic graph that contains a path from s to t }.

הוכיחו כי DAG-CON היא $\mathcal{NL}$ שלמה.

<u>הדרכה</u>: להוכיח כי DAG-CON היא $\mathcal{NL}$ קשה, בהינתן קלט ל- s,t-CON, בנו גרף בו כל צומת היא זוג (v,i) כאשר v הוא צומת בגרף המקורי ו- $1 \le i \le n$.

שאלה 15

הוכיחו כי אם s-t-CON $\in \mathcal{DL}$ אזי קיימת מ"ט M דטרמיניסטית המשתמשת בזיכרון $\log n$ כך שעל קלט גרף מכוון חסר מעגלים G וצמתים s ו- t המכונה M מחזירה מסלול מכוון מ- s ל- t בגרף (אם קיים).

שאלה 16

נגדיר את השפות הבאות:

d-s,t-CON = { G,u,v,d : G גרף לא מכוון שקיים בו מסלול באורך d מ u ל v },

min-odd-s,t-CON = { G,u,v : G גרף לא מכוון שאורך המסלול הקצר ביותר מ u ל v הוא אי זוגי }.

הערה: אם לא קיים מסלול מ u ל v ב G אזי $G,u,v \notin$ min-odd-s,t-CON.

סעיף א

הוכיחו כי d-s,t-CON $\in \mathcal{NL}$.

סעיף ב

הוכיחו כי min-odd-s,t-CON $\in \mathcal{NL}$.

סעיף ג

הוכיחו כי השפה min-odd-s,t-CON היא $\mathcal{NL}$-קשה.

שאלה 17

נתון גרף מכוון G. שני מסלולים ב- G הם שונים אם קיימת קשת המופיעה במסלול אחד ולא מופיעה במסלול השני (המסלולים לא בהכרח פשוטים). נגדיר את השפות הבאות:

2-s-t-CON = { G,s,t : ב- G קיימים לפחות שני מסלולים שונים מ- s ל- t }.

unique-s-t-CON = { G,s,t : ב- G <u>קיים</u> מסלול <u>יחיד</u> מ- s ל- t }.

סעיף א

הוכיחו כי השפה 2-s-t-CON היא $\mathcal{NL}$-קשה.

סעיף ב

הוכיחו כי השפה unique-s-t-CON היא $\mathcal{NL}$-קשה.

שאלה 18

תהי $T(n) \geq n$ פונקציה מהטבעיים לטבעיים. נגדיר את השפה

L_T = { $<M>$: M מ"ט דטרמיניסטית המקבלת את המילה $<M>$ בזמן $T(|<M>|)$ לכל היותר }.

הוכיחו כי לא קיימת מ"ט דטרמיניסטית המקבלת את L_T בזמן $T(n)$.

שאלה 19

נגדיר את השפה PBA:

PBA = { $<M>,x,1^n$: M היא מ"ט דטרמיניסטית המקבלת את x תוך לכל היותר n צעדים }.

סעיף א

הוכיחו כי PBA היא $\mathcal{P}$ שלמה תחת רדוקציות זיכרון לוגריתמי.

סעיף ב

נגדיר $\text{poly}\mathcal{L} = \bigcup_{c \geq 1} \mathcal{DSPACE}(\log^c n)$. הוכיחו כי אם PBA $\in$ poly$\mathcal{L}$ אזי קיים $c \geq 1$ כך ש- $\mathcal{P} \subseteq \mathcal{DSPACE}(\log^c n)$.

סעיף ג

הוכיחו כי $\mathcal{P} \neq$ poly$\mathcal{L}$.

<u>הדרכה</u>: השתמשו בסעיף ב' ובמשפט ההיררכיה עבור $\mathcal{DSPACE}$ כדי להגיע לסתירה.

שאלה 20

נגדיר את השפה B:

B = { $<M>,x$: M מ"ט דטרמינסטית המקבלת את x תוך לכל היותר $2^{|x|}$ צעדים }.

סעיף א

תהי $T(n) > 5n$ פונקציית-זמן. הוכיחו כי אם $B \in \mathcal{DTIME}(T(n))$, אזי $\mathcal{DTIME}(2^n) \subseteq \mathcal{DTIME}(T(n))$.

סעיף ב

הוכיחו כי $B \notin \mathrm{DTIME}(2^{0.5n})$.

שאלה 21

סעיף א

הוכיחו כי אם $\mathrm{SAT} \in \mathcal{BPP}$ אזי קיים אלגוריתם אקראי פולינומי שמקבל פסוק CNF, ומוצא הצבה מספקת לפסוק (אם קיימת).

סעיף ב

הוכיחו כי אם $\mathcal{NP} \subseteq \mathcal{BPP}$ אזי $\mathcal{NP} = \mathcal{RP}$.

שאלה 22

נגדיר את מחלקת השפות $\mathcal{PP}$:

$L \in \mathcal{PP}$ אם קיימת מ"ט מטילת מטבעות M הרצה בזמן פולינומי המקיימת:

1. אם $x \in L$ אזי $\Pr[\, M \text{ מקבלת את } x \,] > ½$,
2. אם $x \notin L$ אזי $\Pr[\, M \text{ מקבלת את } x \,] \leq ½$.

סעיף א'

הוכיחו כי $\mathcal{PP} \subseteq \mathcal{PSPACE}$.

סעיף ב'

תהי M מ"ט מטילת מטבעות. בנו מ"ט מטילת מטבעות M_1 כך שלכל קלט x
$\Pr[\, M_1 \text{ מקבלת את } x \,] = ½ + \Pr[\, M \text{ מקבלת את } x \,]/2$.

סעיף ג'

הוכיחו כי $\mathcal{NP} \subseteq \mathcal{PP}$.

שאלה 23

נגדיר את המחלקה $\mathcal{PP}$:

$L \in \mathcal{PP}$ אם קיימת מ"ט מטילת מטבעות הרצה בזמן פולינומי ומתקיים:

אם $x \in L$ אזי $\Pr[\, M \text{ מקבלת את } x \,] > ½$.

אם $x \notin L$ אזי $\Pr[\, M \text{ מקבלת את } x \,] \leq ½$.

כמו כן, נגדיר את השפות הבאות:

MAJ-SAT $= \{\, \varphi$: פסוק CNF עם n משתנים שיש לו יותר מ- 2^{n-1} הצבות מספקות $\}$.

THRESHOLD-SAT $= \{\, \varphi, k$: פסוק CNF שיש לו יותר מ- k הצבות מספקות $\}$.

סעיף א

הוכיחו כי MAJ-SAT $\in \mathcal{PP}$.

סעיף ב

הוכיחו כי השפה THRESHOLD-SAT היא $\mathcal{PP}$-קשה תחת רדוקציות פולינומיות.

הדרכה: בהנתן מ"ט פולינומית דטרמינסטית M המכריעה יחס המתאים לשפה וקלט x, הסתכלו על הפסוק $\varphi_{M,x}$ שבונה הרדוקציה ממשפט Cock-Levin.

שאלה 24

נגדיר את מחלקת השפות $\mathcal{ZPP}$:

$L \in \mathcal{ZPP}$ אם קיימת מ"ט מטילת מטבעות M הרצה בזמן פולינומי בעלת שלושה מצבים סופיים: מצב מקבל, מצב דוחה ומצב "לא ידוע" ומתקיים:

3. אם $x \in L$ אזי $\Pr[\,x$ מקבלת את $M\,] > ½$ ו- $\Pr[\,x$ דוחה את $M\,] = 0$.
4. אם $x \notin L$ אזי $\Pr[\,x$ דוחה את $M\,] > ½$ ו- $\Pr[\,x$ מקבלת את $M\,] = 0$.

כלומר M לכל קלט צודקת בהסתברות לפחות ½, לעולם אינה טועה, אך היא יכולה לעצור עם תשובה "לא ידוע".

הוכיחו כי $\mathcal{ZPP} = \mathcal{RP} \cap co\mathcal{RP}$.

שאלה 25

סעיף א

תזכורת: הבעיה MAX-SAT עבור פסוק CNF היא למצוא הצבה המספקת את המספר הגדול ביותר האפשרי של פסוקיות בפסוק. הבעיה MAX-EXACT-3SAT מוגדרת באופן זהה עבור פסוקי CNF בהם כל פסוקית מכילה בדיוק 3 ליטרלים שונים.

סעיף א

נתון פסוק CNF. הוכיחו כי לפחות אחת מההצבות 0^n או 1^n מספקת לפחות חצי מהפסוקיות בפסוק.

סעיף ב

הראו אלגוריתם פולינומי אקראי ש ½-מקרב את MAX-SAT (כלומר, בהסתברות לפחות ¾ האלגוריתם מחזיר הצבה "טובה").

סעיף ג

תהי C פסוקית המכילה 3 ליטרלים שונים. הוכיחו כי אם מגרילים הצבה למשתנים כך שכל משתנה מקבל ערך 1 בהסתברות ½, אזי בהסתברות ⅞ ההצבה תספק את C.

סעיף ד

יהי φ פסוק EXACT-3CNF עם m פסוקיות. הראו כי אם מגרילים הצבה באקראי אזי

- המספר הממוצע של פסוקיות המסתפקות ב- φ הוא $\frac{7}{8}m$.
- יהי $0 < \delta < 7/8$. ההסתברות שמספר הפסוקיות המסתפקות ב- φ הוא לפחות δm היא לפחות $\frac{7/8-\delta}{1-\delta}$.

סעיף ד

לכל $1/2 < \delta < 7/8$ קבוע הראו אלגוריתם פולינומי אקראי ש δ- מקרב את MAX- EXACT-3SAT.

שאלה 26

סעיף א

בסעיף זה נראה איך לממש "מונה אקראי" המשתמש בזיכרון $O(\log k)$ ומונה עד 2^k:

1. הטל מטבע k פעמים. אם כל ההטלות היו 0 אזי עצור, אחרת לך ל-1.

הוכיחו:

- האלגוריתם משתמש בזיכרון $O(\log k)$.
- ההסתברות שהאלגוריתם יבצע את צעד 1 פחות מ- 2^{k-1} פעמים היא לכל היותר ½.
  <u>הדרכה</u>: השתמשו בעובדה שהסתברות איחוד של מאורעות היא לכל היותר סכום ההסתברויות של המאורעות.
- ההסתברות שהאלגוריתם לא יעצור היא 0.

סעיף ב

הראה כי קיימת מ"ט מטילת מטבעות M פולינומית המשתמשת בזיכרון $O(\log n)$, כך שעל קלט גרף מכוון G וזוג צמתים s ו- t, מקיימת:

- אם $G,s,t \in$ s-t-CON אזי $P_M(G,s,t) \geq 1/n^n$,
- אם $G,s,t \notin$ s-t-CON אזי $P_M(G,s,t) = 0$.

סעיף ג

השתמשו בסעיפים א ו- ב כדי להוכיח כי $L \in \mathcal{NL}$ אם ורק אם קיימת מ"ט מטילת מטבעות M המשתמשת בזיכרון $O(\log n)$ המקיימת:

- אם $x \in \mathcal{L}$ אזי $P_M(x) \geq ½$,
- אם $x \notin \mathcal{L}$ אזי $P_M(x) = 0$.
- לכל x ההסתברות ש- M לא תעצור על x היא 0.

הערה: בשאלה זו $P_M(x)$ הוא ההסתברות שמ"ט M מקבלת קלט x.