מבחן באלגוריתמים קומבינטוריים 104291 – 2.2.15

משך המבחן שלוש שעות. אין שימוש בחומר עזר או מחשב. אנא נמק תשובותיך בקצור ובבהירות. ענה על כל חמש השאלות. **בהצלחה!**

1. תהא $u = (a_1, \ldots, a_n)$ סדרה של n מספרים ממשיים שונים.

א. (10 נקודות) נתון אלגוריתם השוואות B המקבל כקלט את u ומחשב מספר ממשי $b = B(u)$ המקיים

$$|\{1 \le i \le n : a_i > b\}| \ge \frac{n}{10} \quad , \quad |\{1 \le i \le n : a_i < b\}| \ge \frac{n}{10} \quad .$$

נתון כי הסיבוכיות של חישוב $B(u)$ הינה $O(n)$.
תן אלגוריתם M, המשתמש באלגוריתם B כקופסא שחורה, ומחשב את החציון של u בסבוכיות $O(n)$.

ב. (6 נקודות) האם קיים אלגוריתם השוואות שסיבוכיותו $O(n)$ המוצא את $\lfloor \frac{n}{3} \rfloor$ המספרים הקטנים ביותר ב־ u לפי סדרם? נמק.

ג. (4 נקודות) האם קיים אלגוריתם השוואות שסיבוכיותו $O(n)$ המוצא את $\lfloor \sqrt{n} \rfloor$ המספרים הקטנים ביותר ב־ u לפי סדרם? נמק.

2. יהיו $p_1, \ldots, p_m \ge 0$ כך ש־ $\sum_{i=1}^{m} p_i = 1$. יהיו $\ell_1, \ldots, \ell_m$ אורכי המילים בצופן רישא אופטימלי המתאים לוקטור ההתפלגות $p = (p_1, \ldots, p_m)$.
האורך הממוצע (הממושקל) של מילה בצופן אופטימלי זה נתון ע"י:

$$L(p) = \sum_{i=1}^{m} p_i \ell_i \quad .$$

א. (8 נקודות) יהא $m = 9$. מצא צופן רישא אופטימלי להתפלגות

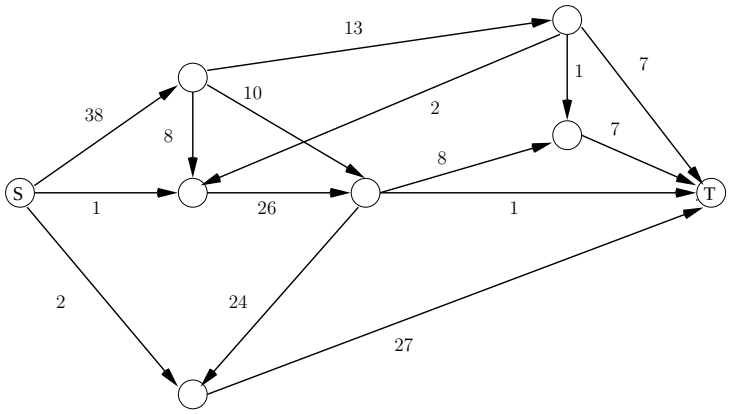
$$p = \frac{1}{18}(1, 1, 1, 2, 2, 2, 3, 3, 3) \quad .$$

ב. (12 נקודות) יהא $m = 9$. חשב את

$$\max\{L(p_1, \ldots, p_9) : \sum_{i=1}^{9} p_i = 1 \ , \ p_i \ge 0\} \quad .$$

יש למצוא חסם עליון ע"י דוגמא, ולהוכיח שהוא אופטימלי.

3. **א.** (10 נקודות) תהא $G = (V, E)$ רשת הזרימה המתוארת להלן עם מקור S, בור T וקיבולים המצויינים על הקשתות.
מצא חתך מינימלי וזרימה מקסימלית מ־ S ל־ T ע"י הפעלת אלגוריתם $Ford - Fulkerson$.



ב. (10 נקודות) נסח את משפט הזרימה המקסימלית והחתך המינימלי והוכח בעזרתו את הטענה הבאה: יהא $(k_1, \ldots, k_n)$ וקטור של מספרים טבעיים, ותהיינה $A_1, \ldots, A_n$ קבוצות סופיות כך שלכל $\emptyset \neq I \subset \{1, \ldots, n\}$ מתקיים

$$|\bigcup_{i \in I} A_i| \geq \sum_{i \in I} k_i \quad .$$

<u>אזי</u> קיימות קבוצות $B_1, \ldots, B_n$ זרות בזוגות כך ש־ $|B_i| = k_i$ ו־ $B_i \subset A_i$ לכל $1 \leq i \leq n$.

4. נגדיר פונקצית הצפנה $E : \mathbb{Z}_{315}^* \to \mathbb{Z}_{315}^*$ ע"י

$$E(x) = x^{103} (\text{mod } 315) \quad .$$

א. (10 נקודות) הראה כי E חח"ע ועל ומצא ביטוי מפורש לפונקצית הפענוח (כלומר לפונקציה ההפוכה) $D : \mathbb{Z}_{315}^* \to \mathbb{Z}_{315}^*$.

ב. (10 נקודות) מצא $x \in \mathbb{Z}_{315}^*$ המקיים $E(x) = 2^{21}$.

5. לגרף $G = (V, E)$ נסמן ב־ $\tau(G)$ את מספר הכסוי של G . (תזכורת: $\tau(G)$ הוא הגודל המינימלי של קבוצת קדקדים $S \subset V$ החותכת כל צלע ב־ G.)
נגדיר את השפות הבאות:
$L_1 =$ כל הזוגות (G, k), כאשר $G = (V, E)$ הוא גרף המקיים $\tau(G) \leq k$.
$L_2 =$ הגרפים $G = (V, E)$ המקיימים $\tau(G) \leq 0.1|V|$.
$L_3 =$ הגרפים הדו־צדדיים $G = (V, E)$ המקיימים $\tau(G) \leq 0.1|V|$.
$L_4 =$ הגרפים $G = (V, E)$ המקיימים $\tau(G) \leq |V| - 10$.

א. (10 נקודות) הגדר את היחס $L' \leq_P L$ בין זוג שפות $L', L \subset \{0,1\}^*$. הראה כי $L_1 \leq_P L_2$.

ב. (10 נקודות) הגדר את המחלקות P, NP, NPC. נניח כי $P \neq NP$. קבע לכל אחת מהשפות L_2, L_3, L_4 האם היא ב־ P, NP, NPC. (מותר להסתמך על כך ש־ $L_1 \in NPC$).

1. ב. נתון אלגוריתם $S(u,k)$ המוצא את ה k-מינימלי של $u=(a_1,\dots,a_n)$

ע"י שימוש באלגוריתם B: (i) חלק $B(u)=\lambda$ כנ"מ (ii) מצא C_n, כנ"מ

$C=\{a_i : a_i \le \lambda\}$ ו- $D=\{a_i : a_i>\lambda\}$ כנ"מ n.

(iii) $S(u,k)=\begin{cases} S(C,k) & |C|\ge k \\ S(D,k-|C|) & k>|C| \end{cases}$.

נסמן ב- $f(n,k)$ את סיבוכיות $S(u,k)$ ו- $F(n)=\max_k f(n,k)$.

מאחר ו- $|C|,|D|\le \frac{9n}{10}$ נקבל כי סיבוכיות (iii) $\le F(\frac{9n}{10})$

ולכן $F(n)\le Cn+n+F(\frac{9n}{10})$

$F(n)\le 10(C+1)n$.

נשלח את חלוקת האיברים לחמישיות, ונחשב $M(u)=S(u,\lfloor\frac{n}{2}\rfloor)$.

ג. נא ק"מ אלגוריתם לינארי המוצא את $\lfloor\frac{n}{3}\rfloor$ המספרים הקטנים ב-n לפי סדרם.

הוכחה: מס' המספרים הגדולים הוא

$n-(n-\lfloor\frac{n}{3}\rfloor+1) = \lfloor\frac{n}{3}\rfloor-1 \ge (\frac{2n}{3})^{2/3}$

ולכן לפי משפט האלגוריתם הנ"ל, קיבלנו שזמן הריצה הוא לפחות

$\Omega(n\log n)=\Omega((\frac{2n}{3})^{n/3}\log(\frac{2n}{3}))$.

ד. ק. מצא את החציון ב- $\frac{n}{5}$-קבוצות בזמן $O(n)$. מצא את

$\frac{n}{5}$ החציונים הקטנים בערך ב-n ר"ו האלגוריתם ל- $\frac{n}{5}$-מינימום בזמן $O(n)$,

ואח"כ עלות ב- $(\frac{n}{5}\log\frac{n}{5})10$.

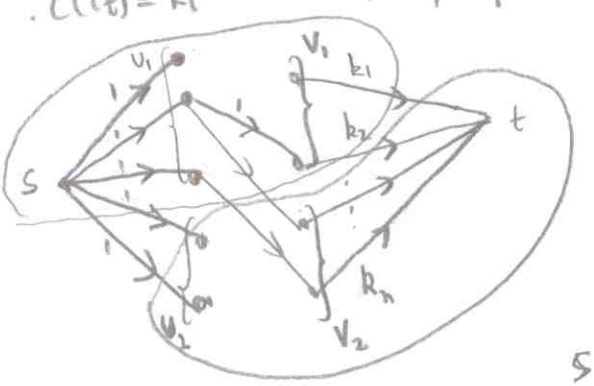
2. מ. תהא $q_1,\dots,q_8$ התפלגות כלשהי המקיימת כי $L(\frac{1}{9},\dots,\frac{1}{9}) = \frac{29}{9}$.

נניח כי $p_1 \geq \dots \geq p_8$ ו- $p_7 + p_8 \leq 2/9$. נוכיח כי $L(p_1,\dots,p_8) \leq \log_2 8 = 3$

לכל $\sum_{i=1}^{8} q_i = 1$ ו- $q_1,\dots,q_8 \geq 0$ מתקיים

$$L(p_1,\dots,p_8) = L(p_1,\dots,p_7,p_7+p_8) + p_7 + p_8 \leq 3 + \frac{2}{9} = \frac{29}{9}$$

3. יהי $U = \bigcup_{i=1}^{n} A_i$, $V = \{1,\dots,n\}$. נגדיר רשת זרימה על הקבוצות $V \cup U \cup \{s,t\}$ כך שקיבולת הקשתות $\{s,u\}_{u\in U}$ היא 1; קיבולת הקשתות $\{i,t\}_{i\in[n]}$ היא $c(it) = k_i$. קיבולת הקשתות $\{u,x\}$ היא 1 לכל $u \in U$, $x \in A_i$ כך ש- $i \in V$, וכן $c(xi) = 1$.



תהי $(S, \bar{S})$ חתך ברשת. כלומר $S \cup \bar{S} = V \cup U \cup \{s,t\}$, $s \in S$, $t \in \bar{S}$. אזי

$$\begin{aligned} Cap(S,\bar{S}) &= |U_2| + e(U_1,V_2) + \sum_{i\in V_1} k_i \\ &= |U_2| + \sum_{i\in V_2} |A_i - U_2| + \sum_{i\in V_1} k_i \geq |U_2| + |\bigcup_{i\in V_2} A_i - U_2| + \sum_{i\in V_1} k_i \\ &\geq |\bigcup_{i\in V_2} A_i| + \sum_{i\in V_1} k_i \geq \sum_{i=1}^{n} k_i \end{aligned}$$

לכן קיבול החתך המינימלי הוא $\sum_{i=1}^{n} k_i$. יהי f זרימה שגודלה $Val(f) = \sum_{i=1}^{n} k_i$ ו- $B_i = \{u \in U : f(ui) = 1\}$ הקבוצות המתאימות.

4. א. $n = 315 = 3^2 \cdot 5 \cdot 7$ $\varphi(n) = (3^2-3)(5-1)(7-1) = 144$

ב. $103^{-1} \pmod{144} = 7$ לכן $D(y) = y^7 \pmod{315}$ הוא ההופכי של E.

ג. $x = D(E(x)) \equiv D(2^{21}) \equiv 2^{21 \cdot 7} \equiv 2^{147} \equiv 2^{144} \cdot 2^3 \equiv 8 \ (315)$

5. א. נתאר עבור כל $k \geq 0$ ו- $G=(V,E)$ כלשהו את $\varphi(G,k) = (V', E')$ כך:

$$\varphi(G,k) = \begin{cases} G \cup \overbrace{\cdots}^{10k-n} & k \geq \frac{n}{10} \\ G \cup \overbrace{\cdots}^{\frac{n-10k}{8}} & k < \frac{n}{10} \end{cases} \qquad n = |V|$$

אז, $\tau(G) \leq k \iff \tau(\varphi(G,k)) \leq \frac{|V'|}{10}$.

φ הוא הפונקציה הפולינומית שמוכיחה כי $L_1 \leq_p L_2$.

ב. $L_2 \in NPC$ עבור k', $L_3 \in P$ כי אפשר לחשב את $\tau(G)$ בזמן פולינומי.

נניח בדרך השלילה כי G שקיים עבורה $L_4 \in P$. אלגוריתם A לכך.

אזי נוכל לבנות אלגוריתם המכריע את L_1 בזמן פולינומי באופן הבא:

$\binom{|V|}{|V|-10} \leq |V|^{10}$ הקלטים באורך $10-|V|$ ולכן מספר