מבחן באלגוריתמים קומבינטוריים 104291 – 18.2.14

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

1. יהא $k$ מספר טבעי. נתונים שני מערכים זרים $A = (a_1, \ldots, a_{k^2})$ באורך $k^2$ ו־ $B = (b_1, \ldots, b_{k^3})$ באורך $k^3$. נתון כי $A$ ו־ $B$ ממויינים, כלומר $a_1 < \cdots < a_{k^2}$ ו־ $b_1 < \cdots < b_{k^3}$.

   א. (12 נקודות) תן אלגוריתם יעיל ככל האפשר למיון של $A \cup B$ ונתח את סיבוכיותו.

   ב. (8 נקודות) האם קיים אלגוריתם למיון $A \cup B$ שסיבוכיותו $O(k^2)$? נמק.

2. יהא $G = (V, E)$ גרף על $|V| = n$ קדקדים עם משקלות אי־שליליים שונים $w(e)$ על הצלעות $e \in E$.

   א. (10 נקודות) הראה כי $G$ מכיל עץ פורש מינימלי יחיד $T = (V, E_1)$.
   הערה: יש להוכיח את הטענה במלואה מבלי להסתמך על תוצאות שהוכחנו בכיתה, למעט למת החילוף ליערות שאותה אפשר לצטט בלי הוכחה.

   ב. (10 נקודות) יהא $T = (V, E_1)$ העץ הפורש המינימלי היחיד ב־ $G$, ויהא $S = (V, E_2)$ עץ פורש ב־ $G$ שמשקלו הוא המינימלי מבין כל העצים הפורשים של $G$ השונים מ־ $T$.
   הוכח כי קיימות צלעות $e_1 \in E_1$ ו־ $e_2 \in E_2$ כך ש־ $E_2 = E_1 - \{e_1\} \cup \{e_2\}$.

**3.** יהיו $p_1, \ldots, p_m \geq 0$ כך ש־ $\sum_{i=1}^{m} p_i = 1$. יהיו $\ell_1, \ldots, \ell_m$ אורכי המילים בצופן רישא אופטימלי המתאים לוקטור ההתפלגות $p = (p_1, \ldots, p_m)$. יהא

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

האורך הממוצע (הממושקל) של מילה בצופן אופטימלי זה.

**א.** (6 נקודות) מצא צופן רישא אופטימלי להתפלגות

$$p = (\frac{3}{20}, \frac{3}{20}, \frac{3}{20}, \frac{3}{20}, \frac{1}{20}, \frac{1}{20}, \frac{1}{20}, \frac{1}{20}, \frac{1}{20}, \frac{1}{20}, \frac{1}{20}, \frac{1}{20}) \ .$$

**ב.** (7 נקודות) תרגיל זה הינו הכללה ל־ $k$ כללי של המקרה $k = 2$ המופיע בסעיף הקודם. יהא $k$ טבעי ויהא $m = 2^k + 2^{k+1}$. יהא $p = (p_1, \ldots, p_m)$ וקטור ההתפלגות הנתון ע"י:

$$p_i = \begin{cases} \frac{3}{5 \cdot 2^k} & 1 \leq i \leq 2^k \\ \\ \frac{1}{5 \cdot 2^k} & 2^k + 1 \leq i \leq 2^k + 2^{k+1} \end{cases}$$

מצא את אורכי המילים בצופן רישא אופטימלי המתאים להתפלגות $(p_1, \ldots, p_m)$, וחשב את $L(p_1, \ldots, p_m)$.

**ג.** (7 נקודות) האם קיימת התפלגות $p = (p_1, \ldots, p_7)$ המקיימת

$$? \quad L(p_1, \ldots, p_7) = 2.9$$

נמק.

**4.** נגדיר פונקציית הצפנה $E : \mathbb{Z}_{255}^* \to \mathbb{Z}_{255}^*$ ע"י

$$E(x) = x^{53} (\mathrm{mod}\ 255) \quad .$$

**א.** (10 נקודות) הראה כי $E$ חח"ע ועל ומצא ביטוי מפורש לפונקצית הפענוח (כלומר לפונקציה ההפוכה) $D : \mathbb{Z}_{255}^* \to \mathbb{Z}_{255}^*$.

**ב.** (5 נקודות) מצא $x \in \mathbb{Z}_{255}^*$ המקיים $E(x) = 2$.

**ג.** (5 נקודות) תהא $F : \mathbb{Z}_{255}^* \to \mathbb{Z}_{255}^*$ הפונקציה המוגדרת ע"י ההרכבה $F(x) = E(E(\cdots E(x)))$ כאשר $E$ מופעלת 64 פעמים.
מצא ביטוי מפורש פשוט ל־ $F(x)$.

**5. א.** (5 נקודות) נסח את משפט הזרימה המקסימלית והחתך המינימלי.

**ב.** (15 נקודות) נסמן ב־ $N = \{1, \ldots, n\}$ את קבוצת הסטודנטים בטכניון. בכל אחד מהימים $1 \leq j \leq m$ מתקיימת מסיבה. נסמן ב־ $S_j \subset N$ את קבוצת הסטודנטים היוצאים למסיבה ביום $j$ ונניח כי $|S_j| = k$ לכל $1 \leq j \leq m$. לכל $1 \leq i \leq n$ נסמן ב־

$$d_i = |\{1 \leq j \leq m : i \in S_j\}|$$

את מספר המסיבות בהן משתתף סטודנט $i$.
לכל $1 \leq j \leq m$ קבוצת הסטודנטים $S_j$ נוסעת למסיבה ברכב אחד ובוחרת סטודנט אחד כנהג תורן.

הוכח כי אפשר לבצע את $m$ הבחירות הנ"ל כך שלכל $1 \leq i \leq n$, סטודנט $i$ יתמנה לנהג תורן לכל היותר $\lceil \frac{d_i}{k} \rceil$ פעמים.
תן אלגוריתם יעיל המוצא $m$ בחירות כנ"ל. כלומר, מוצא מערכת נציגים $s_1 \in S_1, \ldots, s_m \in S_m$ כך שלכל $1 \leq i \leq n$ מתקיים

$$|\{1 \leq j \leq m : s_j = i\}| \leq \lceil \frac{d_i}{k} \rceil.$$

הדרכה: בנה רשת זרימה מתאימה הכוללת קדקד מקור, קדקד אחד לכל סטודנט, קדקד אחד לכל מסיבה, וקדקד בור.