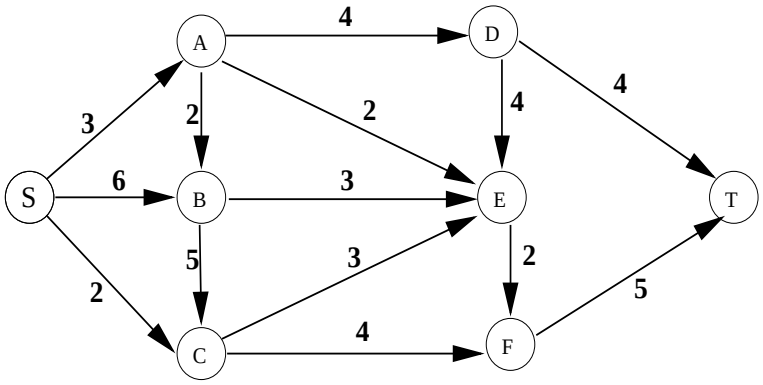
מבחן באלגוריתמים קומבינטוריים 104291 – 20.2.12

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

1. א. (10 נקודות) יהיו N, k, ℓ טבעיים המקיימים $N = k\ell$. נתונה סדרת מספרים (עם חזרות) $x_1, \ldots, x_N$ ונתון כי כל מספר בסדרה מופיע בה בדיוק ℓ פעמים (בפרט, הסדרה מכילה k מספרים שונים). תן אלגוריתם הממיין את הסדרה בזמן $O(N \log k)$.

ב. (10 נקודות) תן חסם תחתון למספר ההשוואות המירבי שיבצע כל אלגוריתם הפותר את הבעייה שבסעיף א.

2. 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) נתונות n קבוצות $A_1, \ldots, A_n$ ו־ n קבוצות נוספות $B_1, \ldots, B_n$.
תן אלגוריתם יעיל הקובע האם קיימת תמורה $\sigma = (\sigma(1), \ldots, \sigma(n))$ וקיימים n איברים שונים $x_1, \ldots, x_n$ כך שלכל $1 \leq i \leq n$ מתקיים $x_i \in A_i \cap B_{\sigma(i)}$.

3. נבצע חפוש עומק על הגרף המכוון $G=(V,E)$, ויהא T יער ה־ DFS המתקבל.
יהא $d(u)$ זמן הפתיחה (גילוי) של הקדקד u ו־ $f(u)$ זמן הסגירה של u .
ענה על השאלות בסעיפים הבאים (הסעיפים אינם תלויים זה בזה).

א. (6 נקודות) נתון כי הצלע $u \to v$ נמצאית ב־ G וכי $d(u) < d(v)$.
האם הצלע $u \to v$ נמצאית בהכרח גם ב־ T ?
האם v בהכרח צאצא של u ב־ T ?

ב. (7 נקודות) נתון כי קיים מסלול מכוון ב־ G מ־ u ל־ v וכי $f(u) < f(v)$.
האם u בהכרח צאצא של v ב־ T ?

ג. (7 נקודות) נניח כי G אינו מכיל מעגלים מכוונים,
וכי $u_1 \to u_2 \to u_3$ הוא מסלול מכוון ב־ G .
האם בהכרח $f(u_3) < f(u_1)$?

4. א. (8 נקודות) תאר את שיטת ההצפנה הציבורית RSA .

ב. (12 נקודות) תהא $E : \mathbb{Z}_{231}^* \to \mathbb{Z}_{231}^*$ הפונקציה הנתונה ע"י

$$E(x) = x^{13} (\mathrm{mod}\ 231) \quad .$$

הראה כי E חח"ע ועל.
מצא d כך שהפונקציה $D : \mathbb{Z}_{231}^* \to \mathbb{Z}_{231}^*$ הנתונה ע"י

$$D(y) = y^d (\mathrm{mod}\ 231)$$

מקיימת $D(E(x)) = x$ לכל $x \in \mathbb{Z}_{231}^*$.

5. קבוצת קדקדים $S \subset V$ תקרא <u>כיסוי</u> של גרף $G = (V, E)$ אם S חותכת כל צלע של G. נסמן:

$$\tau(G) = \min\{|S| : S \text{ כיסוי של } G\}$$

קבוצת קדקדים $S \subset V$ תקרא <u>כיסוי למחצה</u> של גרף $G = (V, E)$ אם S חותכת <u>לפחות מחצית</u> מסך כל הצלעות של G, כלומר

$$|\{e \in E : S \cap e \neq \emptyset\}| \geq \frac{|E|}{2} \quad .$$

נסמן:

$$\widehat{\tau}(G) = \min\{|S| : S \text{ כיסוי למחצה של } G\} \quad .$$

נגדיר את השפות הבאות:

$L_1 =$ כל הזוגות (G, k) המקיימים $\tau(G) \leq k$.
$L_2 =$ כל הזוגות (G, k) המקיימים $\widehat{\tau}(G) \leq k$.
$L_3 =$ הגרפים $G = (V, E)$ המקיימים $\tau(G) \leq |V| - 10$.

א. (5 נקודות) הגדר את היחס $L' \leq_P L$ בין זוג שפות $L', L \subset \{0,1\}^*$.
הגדר את המחלקות NPC , NP , P .

ב. (8 נקודות) הראה כי $L_1 \leq_P L_2$.

ג. (7 נקודות) קבע לכל אחת מהשפות L_2, L_3 האם היא ב־ NPC , NP , P . (מותר להסתמך על כך ש־ $L_1 \in NPC$).