אלגוריתמים (67504) תשס"ז מועד א'

<u>המרצה:</u> פרופ' בן-אור 11/2/07

יש לענות על 4 שאלות מתוך 5.
עליכם להוכיח נכונות של כל אלגוריתם אותו תיארתם, ולנתח את זמן הריצה שלו. על כל האלגוריתמים להיות יעילים. בשאלות 2-5 הניחו כי פעולות אריתמטיות על מספרים לוקחות O(1) זמן.
<u>ניקוד:</u> בשאלות 1-4, משקל הסעיף הראשון הוא 15 נק', ומשקל הסעיף השני הוא 10 נק'. משקל שאלה 5 הוא 25 נק'.

1. א) תאר את שיטת ההצפנה RSA. הוכיחו שהפיענוח עובד במקרה שההודעה זרה ל-n.
ב) נניח שלקבוצת אנשים המשתמשים ב-RSA מפתחות ציבוריים (n_i,e) עם n_i שונים. הודעה m נשלחת לכל האנשים בקבוצה. הראו כי אם מספר האנשים k גדול מ-e אז מאזין יכול לשחזר את ההודעה m.

2. נתונה רשת זרימה $G=(V,E,c,s,t)$
א) תאר אלגוריתם למציאת s-t cut בעל קיבולת מינימלית (~~אין צורך לנתח את זמן הריצה~~).
ב) תאר אלגוריתם הבודק האם יש בגרף s-t cut מינימלי **יחיד.**

3. א) נתון $c>0$. תאר אלגוריתם הסתברותי שמקבל מטריצה A בגודל nxn, שבכל איבר בה מופיע פולינום עם מקדמים שלמים מדרגה 1 במשתנים $x_1..x_m$, ומכריע האם הדטרמיננטה של A היא זהותית 0. על הסיכוי לטעות להיות קטן מ-c.
ב) זיווג בגרף לא מכוון הוא קבוצת צלעות שזרות בקודקודיהן. זיווג הוא מלא אם הוא מכסה את כל קודקודי הגרף. נניח שנתון לכם אלגוריתם הסתברותי A שמקבל גרף לא מכוון G ומחזיר 'לא' אם אין בגרף זיווג מלא, ומחזיר 'כן' בסיכוי ½ אם יש בגרף זיווג מלא. נתון $c>0$. תאר אלגוריתם הסתברותי שבסיכוי לפחות 1-c מוצא זיווג מלא בגרף, אם יש כזה, ומחזיר 'לא' אם אין. לאלגוריתם מותר להשתמש באלגוריתם A. תניחו שזמן הריצה של A הוא $f(V,E)$.

4. בשאלה זאת נתיחס למודל CRCW PRAM.
א) נתונות מטריצות 2x2 עם איברים שלמים $A_1,...,A_m$. הרישא ה-i-ית R_i מוגדרת כ-$R_i=A_1A_2..A_i$. תאר אלגוריתם מקבילי בעל זמן ריצה $T(n)=O(\log n)$ ומספר מעבדים $\frac{n}{\log n}$ שמחשב את כל הרישות.
ב) תאר אלגוריתם שמוצא מקסימום בין n מספרים $x_1..x_n$ עם n^{1+c} מעבדים וזמן ריצה $O(1/c)$.

5. נתון Σ א"ב סופי ואוסף W של מחרוזות $w_1..w_m$ מעל Σ. נתונה מחרוזת u מעל Σ ורוצים לקבלה כשירשור של מחרוזות מ-W (עם חזרות). במקרה ולא ניתן לקבל את u במדויק, נרצה למזער את העיוות:
לכל זוג תווים $a,b \in \Sigma$ נגדיר $c(a,b) \geq 0$ – מחיר החלפת a ב-b. העיוות בין שתי מחרוזות בעלות אורך זהה v,w- המכילות תווים מ- Σ הוא סכום מחירי ההחלפות של כל שני סימנים מתאימים.
דוגמא: נניח כי $\Sigma = \{a,b,c\}$, ונתונות שתי מחרוזות -

a	a	a	b	c
a	b	a	b	A

אז העיוות בין המחרוזות הוא $c(a,a)+c(a,b)+c(a,a)+c(b,b)+c(c,a)$
תאר אלגוריתם המוצא מילה v שהיא שירשור של מחרוזות מ-W בעלת עיוות מינימלי או מודיע כי אי-אפשר ליצור מילה באורך הנכון.