תרגיל מספר 11 באלגוריתמים

מועד הגשה: עד יום חמישי, 26.6.2025, בשעה 10:00 (בבוקר!) ישירות לאתר.

הנחיות: יש להגיש את התרגיל בצורה המכבדת את הכותב ואת הקורא. הקפידו על סדר בתרגיל – השתמשו בטיוטה קודם שאתם מכינים את התרגיל להגשה. פתחו את התרגיל בכותרת הכוללת את שם המקצוע, מספר התרגיל, תאריך **ושמות המגישים**. על התרגיל להיות בכתב קריא. הסריקה חייבת להיות טובה. תרגילים בלתי ראויים לא ייבדקו.

התרגיל יוגש בזוגות. על כל זוג להגיש עותק אחד בלבד. על שני המגישים להצהיר בראש התרגיל שהיו שותפים לפתרונו וששניהם אחראים להגשתו. ללא הצהרה כזו, לא ייבדק התרגיל ויקבל ציון 0. במקרה של כתיבה שאינה עצמאית עלולות שאלות (ואפילו תרגיל שלם) להיפסל (כמוסבר בסילבוס הקורס).

תזכורת: בדיקת השאלות היא מדגמית (רק חלק מהשאלות תבדקנה).

1. תהי $N=(V,E,c,s,t)$ רשת זרימה. יהיו (S',T') ו-(S'',T'') שני חתכים מינימליים ברשת זו. הוכיחו כי גם $(S'\cap S'',T'\cup T'')$ מהווה חתך מינימלי ברשת הנתונה.

2. נתון גרף דו-צדדי $G=(R\cup L,E)$. שבו $|R|=|L|=n$. נתאים לגרף מטריצה M מסדר $n\times n$ באופן הבא: לכל אחד מקדקודי R מתאימה שורה ולכל אחד מקדקודי L מתאימה עמודה. $m_{uv}=1$ אם בגרף יש צלע (u,v). אחרת: $m_{uv}=0$. נגדיר את הפרמנט של מטריצה A באופן הבא: $Per(A)=\sum_{\sigma\in S_n} a_{1\sigma(1)}a_{2\sigma(2)}\cdots a_{n\sigma(n)}$.
   א. הוכיחו כי $Per(M)$ שווה למספר השידוכים המושלמים בגרף.
   ב. הוכיחו כי $Per(M)\le n!$.

3. נתונה קבוצה בת n גברים ולצידה קבוצה בת m נשים. קיימות הכרויות (סימטריות) בין גברים לנשים. הציגו אלגוריתם יעיל המשדך גברים לנשים (בהתאם להכרויות) כך שיתקבל שידוך שבו סכום גילאי הגברים המשודכים יהיה מקסימלי. הוכיחו את נכונות האלגוריתם ונתחו את ביצועיו. המטרה היא להציג אלגוריתם פולינומיאלי בזמן קצר ככל שניתן.

4. $a\in\mathbb{Z}_n$ נקרא בשם שארית ריבועית, אם קיים $x\in\mathbb{Z}_n$, כך ש- $x^2=a \mod n$.
   א. כמה שאריות ריבועיות יש ב- $\mathbb{Z}_{17}$? הוכיחו.
   ב. כמה שאריות ריבועיות יש ב- $\mathbb{Z}_p$ כאשר p ראשוני? הוכיחו.
   ג. כמה שאריות ריבועיות יש ב- $\mathbb{Z}_n$ כאשר $n=pq$, ו- p,q ראשוניים שונים? הוכיחו.
   ד. הוכיחו כי $a\ne 0$ הוא שארית ריבועית ב- $\mathbb{Z}_p$ (כאשר p ראשוני) אם ורק אם $a^{\frac{p-1}{2}}=1 \mod p$.

יש להציג אלגוריתמים בצורה מילולית – לא כקוד או כתוכנית העתידה לעבור קומפילציה. הצגה שאינה מילולית לא תתקבל.