<u>תכנון אלגוריתמים תרגיל 5 – דף תשובות</u>

אנא הגישו רק חלק זה. <u>אל תחרגו מהמקום המוקצה לתשובה!</u>

ציון	

שם		ת.ז	
שם		ת.ז	

<u>שאלה 1:</u>

<u>סעיף א'</u>

יהיו $<i,j>$ זוג אינדקסים, $1 \le i,j \le n$ כך ש- $A^{ij}=B$. אזי, לכל $v \in \{0,\dots,r\}^k$ (בפרט, לכל וקטור v באורך k) מתקיים כי $A^{ij}v=Bv$. לכן, כאשר האלגוריתם יגיע לערך j בלולאה החיצונית (4) ולערך i בלולאה הפנימית (4.1) הוא יגלה שאכן $res=A^{ij}v$ ויוסיף את הזוג $<i,j>$ ל- S.

<u>סעיף ב'</u>

אנו בודקים האם B שווה ל- $(n-k)^2=O(n^2)$ מטריצות.

טענה 1 : לכל בדיקה כזו, יש סיכוי של לכל היותר $\frac{1}{r+1}$ להכשל.

נחסום את ההסתברות להצלחה בעזרת טענה 1.

אנו מעוניינים שהסיכוי שאף השוואה לא תיכשל יהיה לכל הפחות 1/2. ניתן לחסום הסתברות זו כדלהלן:

$$\Pr[fail] \le \Pr\begin{bmatrix}\exists <i,j> s.t.\\ A^{ij} \ne B, but\\ A^{ij}v=Bv\end{bmatrix} \le \sum_{<i,j>,A^{ij}\ne B} \Pr\left[A^{ij}v=Bv\right] \le \sum_{<i,j>,A^{ij}\ne B} \frac{1}{r+1} \le n^2\frac{1}{r+1}$$

מחסם האיחוד, נקבל שההסתברות שלפחות השוואה אחת מתוך n^2 השוואות יכשלו היא לכל היותר $n^2\left(\frac{1}{r+1}\right)$. לכן, נקבע $r=2n^2$. נקבל: $\frac{n^2}{2n^2+1}<\frac{1}{2}$.

ולכן, ההסתברות לכישלון קטנה ממש מ-1/2, וההסתברות להצלחה היא לכל הפחות 1/2, כנדרש.

הוכחת טענה 1: יהי $v \in \{0,\dots,r\}^k$, ויהיו $<i,j>$ זוג אינדקסים, $1 \le i,j \le n$ כך ש - $A^{ij} \ne B$. נניח ש- v הינו וקטור שקרן עבור A^{ij}, כלומר $A^{ij}v=Bv$. אזי, מתקיים:

$$A^{ij}v-Bv=0 \leftrightarrow \left(A^{ij}-B\right)v=0$$

נסמן $A^{ij}-B=D$. מכיוון ש- $A^{ij} \ne B$, נקבל $D \ne 0$. תהי $d_{l,m}$ כניסה במטריצה D, כך ש- $d_{l,m} \ne 0$. נבחן את וקטור התוצאה $\vec{w}$ המתקבל על ידי הכפלת D ב- v .

$\left(\vec{w}=Dv=\left(A^{ij}-B\right)v\right)$. מכיוון ש- v וקטור שקרן עבור A^{ij}, נקבל ש- $\vec{w}=\vec{0}$. נביט בערך w_l. מתקיים:

$w_l = d_{l,1}v_1 + d_{l,2}v_2 + \cdots + d_{l,m}v_m + \cdots + d_{l,k}v_k = 0$
ישנם r+1 ערכים אפשריים ל- v_m. אם נשנה את ערכו לאחת מ- r האפשרויות האחרות, בלי לשנות את שאר ערכי הוקטור v, נקבל וקטור הגון. כלומר, על כל וקטור שקרן יש לפחות r וקטורים הגונים. לכן, ההסתברות שבחרנו וקטור שקרן היא לכל היותר $\frac{1}{r+1}$, כנדרש.

סעיף ג

תיאור אלגוריתם

אינטואיציה: במקום לכפול מטריצות בכל איטרציה, ראשית, נחשב לכל "שורה" באורך k במריצה A את הערך שנקבל מלכפול אותה ב- v, ולאחר מכן בכל איטרציה נדרש רק להחסרת השורה הראשונה והוספת השורה הבאה.

1. $\emptyset \to S$
2. הגרל וקטור $v \in \{0, \dots, 2\mathrm{n}^2\}^k$ בהתפלגות אחידה.
3. חשב $res \leftarrow Bv$
4. אתחל $memo[n][n-k+1]$
5. עבור $j = 1, \dots, n-k+1$
   5.1. עבור $i = 1, \dots, n$
   5.1.1.1. $\sum_{m=j}^{j+k-1} a_{i,m}v_m \to memo[i,j]$
6. עבור $j = 1, \dots, n-k$
   6.1. עבור $i = 1, \dots, n-k$
   6.1.1. $[memo[i,j], memo[i+1,j], \dots, memo[i+k-1,j]] \to temp$
   6.1.2. אם $temp = res$
   6.1.2.1. $S \cup \{< i,j >\} \to S$
7. החזר את S

נכונות האלגוריתם

רעיון: האלגוריתם הנתון בשאלה מחשב בכל שלב את הערך $A^{ij}v$ ומשווה אותו לערך Bv .
נשים לב, שלמעשה הכפלת $[a_{i,j}, a_{i,j+1}, a_{i,j+2}, \dots, a_{i,j+k-1}]v$ מחושבת כעת על ידי האלגוריתם הנתון בשאלה גם כאשר נבדק האם $A^{ij}v = Bv$, אך גם כאשר נבדק האם $A^{i-1j}v = Bv$, $A^{i-2j}v = Bv$ וכו'. למעשה, הכפלת תת-השורה בוקטור מתבצעת מספר פעמים, כלומר, החישוב המתבצע הינו בזבזני.
בשורה 5.1.1.1 האלגוריתם מחשב את המכפלה של תת השורה $[a_{i,j}, a_{i,j+1}, \dots, a_{i,j+k-1}]$ ב-v, ושומר ערך זה בטבלה *memo* במיקום $[i,j]$. אם כן, בשורה 6.1.1 הוקטור המחושב *temp*, הינו בדיוק מכפלת המטריצה A^{ij} ב- v, ואנו משווים ערך זה ל- Bv, כמו באלגוריתם הנתון.

זמן ריצה

אתחול S ב- O(1)
הגרלת הוקטור v - הגרלת מספר בן n ביטים O(1), לכן סה"כ $\mathrm{O(k)}$
חישוב res– הכפלת מטריצה בגודל $k \times k$ בוקטור באורך k ב- $O(k^2)$.
אתחול $memo$ - $O(n^2)$
לולאה 5,5.1 – $O(n^2)$ איטרציות, בכל אחת נעשה חיבור של $O(k)$ איברים, סה"כ $\mathrm{O(n^2k)}$ זמן.
לולאה 6,6.1 – $O(n^2)$ איטרציות, בכל אחת נעשית השוואה בין שני וקטורים בגודל k ב-$O(k)$ זמן, ואולי הוספה לקבוצה ב- $O(1)$ זמן. סה"כ $\mathrm{O(n^2k)}$ זמן.
סה"כ זמן ריצת האלגוריתם הינו $\mathrm{O(n^2k + k^2)}$, מכיוון שמתקיים $k \leq n$, נקבל שזמן הריצה הינו $O(n^2k)$.

שאלה 2:

סעיף א

נשים לב כי אם בכל פעם שאליס מבקשת לדעת האם פולינום כלשהו שווה לפולינום האפס, האלגוריתם SZ מחזיר תשובה נכונה, אזי בסוף ריצת האלגוריתם, האלגוריתם מחזיר תשובה נכונה.

כלומר, בשביל שהאלגוריתם F_R יחזיר תשובה נכונה, מספיק לדרוש שהאלגוריתם SZ יחזיר תשובה נכונה על לכל היותר n שאילתות.

ההסתברות ש- SZ מחזיר תשובה נכונה עבור שאילתא אחת גדולה שווה מחצי. לכן, ההסתברות שהוא מחזיר תשובה נכונה על n שאילתות, כאשר הריצות השונות של SZ מתבצעות באופן ב"ת, גדולה שווה מ- $\frac{1}{2^n}$. כלומר, בהסתברות לפחות $\frac{1}{2^n}$ האלגוריתם מחזיר תשובה נכונה.

סעיף ב

נגדיר את האלגוריתם F_{R2} :

1. אליס מריצה את האלגוריתם F.
2. בכל פעם שהאלגוריתם מבקש לדעת עבור פולינום $p(x_1,\dots,x_k)$ האם $p(x_1,\dots,x_k)\equiv 0$:
   2.1. במשך t סיבובים: (t יקבע בהמשך)
      2.1.1. אליס מריצה את SZ על $p(x_1,\dots,x_k)$, ומקבלת תשובה ans.
      2.1.2. אם ans הינה "לא": אליס מזינה "לא" ל-F וממשיכה בחישוב.
   2.2. אם במשך t הסיבובים התשובה שהתקבלה היא "כן", אליס מזינה "כן" ל-F וממשיכה בחישוב.

נשים לב כי אם בכל פעם שאליס מזינה ל-F תשובה לגבי האם פולינום כלשהו שווה לפולינום האפס היא מזינה תשובה נכונה, אזי בסוף ריצת האלגוריתם, האלגוריתם מחזיר תשובה נכונה.

כלומר, בשביל שהאלגוריתם F_{R2} יחזיר תשובה נכונה, מספיק לדרוש שאליס תזין תשובה נכונה על לכל היותר n שאילתות.

נשים לב שלאלגוריתם SZ טעות חד כיוונית, כלומר, אם פולינום הקלט לאלגוריתם SZ הינו פולינום האפס, האלגוריתם מחזיר תשובה נכונה תמיד, ואילו אם הפולינום איננו פולינום האפס, האלגוריתם מחזיר תשובה נכונה בהסתברות לפחות חצי. כלומר, אם אלגוריתם SZ החזיר "לא" עבור קלט כלשהו, התשובה הנכונה היא בהכרח "לא" עבור קלט זה.

אליס טועה אמ"מ עבור פולינום כלשהו $p(x_1,\dots,x_k)$ כך שמתקיים $p(x_1,\dots,x_k)\neq 0$, האלגוריתם *SZ* החזיר תשובה שגויה *t* פעמים. ההסתברות ש-*SZ* טועה *t* פעמים בריצות ב"ת קטנה מ- $\frac{1}{2^t}$. מכיוון שישנן לכל היותר *n* פולינומים עליהם אליס יכולה לטעות, נקבל מחסם האיחוד:

$$\Pr[fail]\le \Pr\begin{bmatrix}\exists p(x)\ s.t.\, p(x)\not\equiv 0\\ but\ SZ\ returns\\ p(x)\equiv 0\ t\ times\end{bmatrix}\le \sum_{\forall p(x) that\ F\ produces}\frac{1}{2^t}\le\frac{\mathrm{n}}{2^t}$$

כלומר, ההסתברות שאליס מזינה ל-*F* תשובה שגויה קטנה מ- $\frac{n}{2^t}$. נדרוש $\frac{n}{2^t}<\frac{1}{2}$,

$$\frac{n}{2^t}<\frac{1}{2}\Leftrightarrow 2n<2^t\Leftrightarrow \log(2n)<\log(2^t)\Leftrightarrow \log(n)+1<t$$

כלומר, עבור $t=\log n+2$, בהסתברות קטנה מ-1/2 אליס מזינה ל-*F* תשובה שגויה עבור לפחות אחד מהפולינומים, לכן בהסתברות לפחות 1/2 האלגוריתם F_{R2} מחזיר תשובה נכונה.

זמן ריצה
האלגוריתם F רץ בזמן $O(n^2)$, פרט למימוש השאילתות.
במהלך הריצה, מתבצעות לכל היותר $O(n \log n)$ שאילתות באורך n לאלגוריתם SZ, שרץ בזמן $O(n^2)$. כלומר, זמן הריצה הכולל הוא $O(n^3 \log n)$.

<u>שאלה 3</u>

<u>סעיף א</u>
הטענה נכונה.
תהי N רשת זרימה $N = (G = (V, E), c, s, t)$ וזרימה כלשהי $f > 0$. צ"ל שב- G יש מסלול זרימה.

נניח בשלילה שלא קיים מסלול זרימה מ- s ל-t. נתבונן בגרף $G' = (V, E')$ כך ש- $E' = \{(u, v) | f(u, v) > 0\}$. מהנחת השלילה, נקבל שבגרף 'G לא קיים מסלול מ-s ל-t. נסמן: $S = \{u | there\ is\ a\ path\ from\ s\ to\ u\ in\ G'\}$. נשים לב כי $t \notin S$, וכן $s \in S$.

נביט בחתך $(S, V \backslash S = T)$.

טענה 1 : לכל קשת u, v כך ש- $u \in S\ and\ v \in T$, מתקיים $f(u, v) \leq 0$.

הוכחת טענה 1 : $u \in S$ ולכן קיים מסלול מ- s ל-u ב-G'. $v \notin S$, כלומר v לא נגיש מ- s ב- G'. לכן, לא יתכן שהקשת $(u, v) \in E'$, כי אז היה ניתן להרחיב את המסלול מ-s ל-u כך שיגיע גם ל-v, בסתירה להנחה ש- v לא נגיש מ-s. כלומר מהגדרת הגרף G' נקבל $f(u, v) \leq 0$.

מטענה 1, נובע שסכום הזרימה בחתך, $\sum_{(u,v) s.t. u \in Q, v \notin Q} f(u, v) \leq 0$. אבל, ממשפט שנלמד בכיתה, לכל חתך (S,T) כך ש- $s \in S, t \in T$, מתקיים שהזרימה בחתך שווה לזרימה ברשת, ומההנחה גודל הזרימה ברשת חיובי, כלומר $\sum_{(u,v) s.t. u \in Q, v \notin Q} f(u, v) = |f| > 0$, בסתירה.

<u>סעיף ב</u>

כפי שראינו בכיתה, בכל שלב בריצת אלגוריתם Ford – Fulkerson הזרימה הכללית ברשת גדלה. נשים לב שהזרימה המקסימלית ברשת חסומה על ידי הזרימה המקסימלית שניתן להזרים מ-s. מכיוון שדרגת s חסומה על ידי d_{max}, וכן הקיבול על כל קשת היוצאת מ-s חסום על ידי c_{max}, נקבל שהזרימה המקסימלית חסומה על ידי $c_{max} \cdot d_{max}$. מכיוון שכל הקיבולים שלמים, בכל מציאת מסלול שיפור הזרימה גדלה בלפחות 1, לכן לאחר לכל היותר $c_{max} \cdot d_{max}$ איטרציות, הריצה תסתיים.

שאלה 4:

סעיף א

(1) אין מסלול ברשת השיורית מ-u ל-s ← לכל v שכן של u, $f(u,v)=0$.

נניח שאין מסלול ברשת השיורית מ-u ל-s, וכן נניח בשלילה שקיים v שכן של u, כך ש-$f(u,v)\neq 0$. בה"כ $f(u,v)>0$.

נביט במסלול $p=(u_0,u_1,\dots,u_k=u,v=u_{k+1},\dots,u_l)$ מאורך מקסימלי בגרף G_f (גרף התשתית של הרשת השיורית), כך שכל קשתות המסלול (u_i,u_{i+1}) מקיימות $f(u_i,u_{i+1})>0$. קיים מסלול מקסימלי כזה, שכן בגרף G_f אין מעגלים. מאופן בניית הרשת השיורית, לכל קשת (x,y) כך שמתקיים $f(x,y)>0$, הקשת (y,x) שייכת לרשת השיורית*. כלומר, המסלול $p_r=(u_l,\dots,u_{k+1}=v,u_k=u,\dots,u_1,u_0)$ הינו מסלול ברשת השיורית.

מכיוון ש- p מקסימלי באורכו, נקבל שלכל קודקוד w שכן של u_0, מתקיים $f(w,u_0)\leq 0$, שכן אחרת היינו יכולים להוסיף את w לתחילת המסלול ולקבל מסלול ארוך יותר. אבל, $f(u_0,u_1)>0$, כלומר, קיימת זרימה חיובית שיוצאת מ-u_0, אבל אין זרימה הנכנסת ל- u_0 לכן, u_0 בהכרח שווה ל- s או ל- t, מאילוצי שימור זרימה. אם $u_0=s$, הסיפא של המסלול p_r החל מהקודקוד u, מהווה מסלול ברשת השיורית מ- u ל-s, בסתירה להנחה.

אם $u_0=t$, נשים לב ש- $u_0=t$ הינו הקודקוד הראשון במסלול p, כאמור, לא קיים קודקוד w כך ש- $f(w,u_0)=f(w,t)>0$. מכיוון שהזרימה $f(t,u_1)=f(u_0,u_1)>0$ ומשיקולי אנטי סימטריה נקבל $f(u_1,t)<0$. לכן, לא קיימת זרימה חיובית הנכנסת ל- t, ואילו קיימת זרימה חיובית היוצאת מ- t, ולכן, סכום הזרימה >0, בסתירה לכך ש- $|f|<0$. כלומר בסה"כ נקבל שלא יתכן שקיים v שכן של u כך ש- $f(u,v)\neq 0$.

(2) אין מסלול ברשת השיורית מ- t ל-v ← לכל u שכן של v, $f(u,v)=0$.

נניח שאין מסלול ברשת השיורית מ- t ל-v, וכן נניח בשלילה שקיים u שכן של v, כך ש-$f(u,v)\neq 0$. בה"כ $f(u,v)>0$.

נביט במסלול $p=(u_0,u_1,\dots,u_k=u,v=u_{k+1},\dots,u_l)$ מאורך מקסימלי בגרף G_f, כך שכל קשתות המסלול (u_i,u_{i+1}) מקיימות $f(u_i,u_{i+1})>0$. באופן דומה ל- (1), המסלול הנ"ל הינו מסלול חוקי, וכן המסלול $p_r=(u_l,\dots,u_{k+1}=v,u_k=u,\dots,u_1,u_0)$ הינו מסלול ברשת השיורית.

מכיוון ש- p מקסימלי באורכו, נקבל שלכל קודקוד w שכן של u_l, מתקיים $f(u_l,w)\leq 0$, שכן אחרת היינו יכולים להוסיף את w לסוף המסלול ולקבל מסלול ארוך יותר. אבל, $f(u_{l-1},u_l)>$ 0, כלומר, הזרימה היוצאת מ- u_l קטנה מהזרימה הנכנסת ל-u_l. לכן, u_l בהכרח שווה ל- t או ל- s, מאילוצי שימור זרימה. אם $u_l=t$, הרישא p_r עד לקודקוד v, מהווה מסלול ברשת השיורית מ- t ל-v, בסתירה להנחה. כלומר, לא יתכן שקיים u שכן של v, כך ש- $f(u,v)\neq 0$.

אם $u_l=s$ נשים לב ש- $u_l=s$ הינו הקודקוד האחרון במסלול p, כאמור, לא קיים קודקוד w כך ש- $f(u_l,w)=f(s,w)>0$. מכיוון שהזרימה $f(u_{l-1},s)=f(u_{l-1},u_l)>0$ ומשיקולי אנטי סימטריה נקבל $f(s,u_{l-1})<0$. לכן, לא קיימת זרימה חיובית היוצאת מ- s, ואילו קיימת זרימה שלילית היוצאת מ- s, ולכן, סכום הזרימה >0, בסתירה לכך ש- $|f|<0$. כלומר בסה"כ נקבל שלא יתכן שקיים u שכן של v כך ש- $f(u,v)\neq 0$.

* לכל קשת (x,y) כך שמתקיים $f(x,y)>0$, הקשת (y,x) שייכת לרשת השיורית- $f(x,y)>0$. משיקולי אנטי סימטריה נקבל $f(y,x)=-f(x,y)<0$. נבחן את הקיבול השיורי של קשת זו. $c_f(y,x)=c(y,x)-f(y,x)>0$ (שכן כל הקיבולים ≤ 0). כלומר, הקיבול השיורי של הקשת (y,x) גדול מ- 0, ולכן הקשת שייכת לרשת השיורית.

סעיף ב

תהי (v_i, v_j) קשת השייכת לחתך מינימלי כלשהו. כפי שראינו בכיתה, עבור זרימה מקסימלית f, לכל קשת (u, v) בחתך מינימלי מתקיים $f(u, v) = c(u, v)$. מכיוון ש-f זרימה מקסימלית ו-(v_i, v_j) שייכת לחתך מינימלי כלשהו, $f(v_i, v_j) = \mathrm{c}(v_i, v_j) > 0$. לכן, יש זרימה חיובית מ-v_i ל-v_j. נבחן את הזרימה $f(v_j, v_i)$. מאילוצי אנטי-סימטריה, נקבל $f(v_j, v_i) = -f(v_i, v_j) = -c(v_i, v_j) < 0$. כלומר, הזרימה על הקשת קטנה מ- 0. לכן, מהגדרת הרשת השיורית, נקבל ש- $c_f(v_j, v_i) = c(v_j, v_i) - f(v_j, v_i) > 0$ (שכן כל הקיבולים $\leq$ 0). ולכן הקשת (v_j, v_i) שייכת ל- E_f ומופיעה ברשת השיורית. אם כן, במיון הטופולוגי, בהכרח v_j מופיע לפני v_i, כלומר $j < i$.

סעיף ג

מכיוון ש- $|f| > 0$, ומשאלה 3 (א) נקבל שבהכרח יש מסלול זרימה מ-$s = v_{i_0}$ ל-$t = v_{j_0}$ ב-G. אם כן, ברשת השיורית יש מסלול מ- t ל-s. מחוקיות המיון הטופולוגי, נקבל $j_0 < i_0$.

סעיף ד

יהי k מספר כלשהו כך ש- $j_0 \leq k < i_0$. נגדיר את החלוקה (S, T) כך ש- $S = \{v_l | l > k\}$. צ"ל שהחלוקה הינה חתך מינימלי.

ראשית, מכיוון ש- $j_0 \leq k < i_0$ נקבל ש- $s = v_{i_0} \in S$, וכן ש- $t = v_{j_0} \in T$. כלומר, החלוקה הנ"ל אכן מגדירה חתך s-t חוקי. נותר להוכיח שהחתך הינו חתך מינימלי. נראה, שכל קשת החוצה את החתך הינה רוויה, ומכך נקבל שקיבול החתך שווה לזרימה. ממשפט min cut-max flow נקבל שהחתך הינו חתך מינימום. נשים לב, כי ברשת השיורית, לא קיימת קשת (u_i, u_j) כך ש- $i > j$, מחוקיות המיון הטופולוגי. לכן, לא קיימת ברשת השיורית קשת מהקבוצה S לקבוצה T. כלומר, כל הקשתות החוצות את החתך (S, T) הינן רוויות, והחתך הינו חתך מינימום כנדרש.

סעיף ה

←תהי $(v_k, v_l) \in E$ קשת כך שקיים חתך מינימלי המכיל אותה. צ"ל $j_0 \leq l < k \leq i_0$. מסעיף ב' נקבל שבהכרח $l < k$. נותר להראות כי $j_0 \leq l$, וכן כי $k \leq i_0$.

$j_0 \leq l$: נניח בשלילה ש- $j_0 > l$. מחוקיות המיון הטופולוגי, נקבל שאין מסלול מ- $t = v_{j_0}$ ל-v_l ברשת השיורית. מסעיף א' נקבל כי לכל u שכן של v_l, $f(u, v_l) = 0$, ובפרט $f(v_k, v_l) = 0 < c(v_k, v_l)$, לכן הקשת (v_k, v_l) איננה רוויה תחת f, בסתירה לכך שקיים חתך מינימלי המכיל אותה. לכן $j_0 \leq l$

$k \leq i_0$: נניח בשלילה ש- $k > i_0$. מחוקיות המיון הטופולוגי, נקבל שאין מסלול מ-v_k ל-s ברשת השיורית. מסעיף א', לכל v שכן של v_k, $f(v_k, v) = 0$.

$f(v_k, v_l) = 0 < c(v_k, v_l)$, לכן הקשת (v_k, v_l) איננה רוויה תחת f, בסתירה לכך שקיים חתך מינימלי המכיל אותה. לכן $k \leq i_0$.

→תהי $(v_k, v_l) \in E$ כך ש- $j_0 \leq l < k \leq i_0$. צ"ל כי קיים חתך מינימלי המכיל אותה.

לפי סעיף ד, נקבל שהחלוקה (S, T) כך ש- $S = \{v_m | m > k - 1\}$ הינה חתך s-t מינימלי. לפי ההגדרה, $v_k \in S, v_l \notin S$, כלומר הקשת (u_k, v_l) חוצה חתך מינימום כנדרש.