

## תכנון אלגוריתמים תרגיל 5 – דף תשובות

אנא הגישו רק חלק זה. אל תחרגו מהמקום המוקצה לתשובה!

	ציון
--	------

	ת.ז.		שם
	ת.ז.		שם

### שאלה 1

סעיף א

1. הגדרת הבעיה הליניארית בשלמים

נגדיר לכל $i = 1, \dots, m$ ולכל $j = 1, \dots, n$ את $a_{ij}$ כמשתנה אינדיקטור: אם $a_j \in s_i$ אז $a_{ij} = 1$ , אחרת,
$a_{ij} = 0$ . כעת, נגדיר את בעיית התכנון הליניארי הבאה:
$\min \sum_{i=1}^m c_{s_i} x_i$
s.t. $\sum_{i=1}^m a_{ij} x_i \geq 1, \quad j = 1, \dots, n$
$0 \leq x_i, \quad i = 1, \dots, m$
$-1 \leq -x_i, \quad i = 1, \dots, m$
$x_i \in \mathbb{Z}, \quad i = 1, \dots, m$

2. הגדרת הבעיה הדואלית

$\max \sum_{j=1}^n y_j$
s.t. $\sum_{j=1}^n a_{ij} y_j \leq c_{s_i}, \quad i = 1, \dots, m$
$0 \leq y_j, \quad j = 1, \dots, n$

## סעיף ב

## 1. הגדרת הבעיה הליניארית

נסתכל על הגרף הלא המכוון $G' = (V_1 \cup V_2, E')$ המוגדר באופן הבא: לכל $v \in V$ קיימים $v_1 \in V_1, v_2 \in V_2$ , ולכל $(u, v) \in E$ קיימת $\{u_1, v_2\} \in E'$ . נגדיר את $a_{ve}$ כמשתנה אינדיקטור: אם $e$ חלה על $v$ אז $a_{ve} = 1$ , אחרת $a_{ve} = 0$ . כעת, נגדיר את בעיית התכנון הליניארית הבאה:
$\max \sum_{e \in E'} w(e) \quad s.t. \quad \sum_{e \in E'} a_{ve} w(e) \leq 1, \quad \forall v \in V_1 \cup V_2$
$0 \leq w(e), \quad \forall e \in E'$
נשים לב כי $w(\{u_1, v_2\}) = w((u, v))$ בגרף $G$ .

## 2. הגדרת הבעיה הדואלית

$\min \sum_{v \in V_1 \cup V_2} y_v$
$s.t. \quad \sum_{v \in V_1 \cup V_2} a_{ve} y_v \geq 1, \quad \forall e \in E'$
$0 \leq y_v, \quad \forall v \in V_1 \cup V_2$

## 3.

נניח בשלילה כי לבעיה הליניארית מסעיף א' קיים פתרון בעל ערך גדול מ- $ E $ , ממשפט הדואליות החזקה
קיים פתרון בעל ערך גדול מ- $ E $ לבעיה הדואלית מסעיף א'. ניתן לראות כי הבעיה הדואלית
מסעיף א' זהה לבעיה מסעיף ב', ולכן ניתן להסיק כי קיימת פונקציית משקל בעל ערך גדול מ- $ E $ , אז על פי עקרון שוברך היונים קיימת צלע שמשקלה לפי $w$ גדול ממש מ-1, בסתירה לכך
שדרגת הכניסה והיציאה של כל קודקוד קטנה שווה מ-1.

## שאלה 2

### סעיף א – בעיית תכנון ליניארי

$\min\{10x_1 + 16x_2 + 12x_3 + 18x_4\}$
$s. t \quad x_1 + x_2 + x_3 + x_4 \geq 150$
$0x_1 + x_2 + 0x_3 + x_4 \geq 50$
$x_i \geq 0, \quad i = 1,2,3,4$

### סעיף ב – הגדרת התוכנית הדואלית

$\max\{150y_1 + 50y_2\}$
$s. t \quad y_1 + 0y_2 \leq 10$
$y_1 + y_2 \leq 16$
$y_1 + 0y_2 \leq 12$
$y_1 + y_2 \leq 18$
$y_j \geq 0, \quad j = 1,2$

### סעיף ג

<u>אבחנה:</u> $x_3 = x_4 = 0$ (אילוץ סוג 1,3 ואילוץ 2,4 זהים, לכן על מנת "לנמנם" את ערך פונקציית המטרה נעדיף לבחור ימים של 1 במקום 3 ושל 2 במקום 4).
עבור מערכת צירים בה הקורדינטה הראשונה היא $x_1$ והקורדינטה השנייה היא $x_2$ , התחום הפיזיכלי הינו הישר $f(x_1) = -x_2$ בין הנקודות $\{(0,150), (100,50)\}$ . נסמן נקודה $(a, b)$ על הישר בתחום הנ"ל, ונסתכל על הנקודה $(a + \Delta, b - \Delta)$ עבור $\Delta > 0$ נשים לב כי: $10a + 16b > 10(a + \Delta) + 16(b - \Delta) = 10a + 16b - 6\Delta$ .
לכן, הנקודה האופטימלית נמצאת בקצה הימני תחתון $(100,50)$ . בסה"כ קיבלנו כי הערך האופטימלי לבעיה מתקבל עבור $x_1 = 100, x_2 = 50, x_3 = x_4 = 0$ , וערכו 1,800.

### שאלה 3

#### סעיף א

אליס תשלח לבוב את המחרוזת $A \circ B$ . אם תת המחרוזת הנוצרת מ $n$ האיברים הראשונים
בהודעה שווה ל $C$ וגם קיים תו עליו תת המחרוזת הנוצרת מ $n$ האיברים האחרונים ו $D$
לא מסכימים החזר "כן", אחרת החזר "לא". ניתן לראות כי אורך ההודעה שאליס שולחת הינו $2n$ , ומכאן שסיבוכיות התקשורת הינה $O(n)$ .

#### סעיף ב

##### תיאור האלגוריתם

אליס מגרילה שני מספרים ראשוניים $q_1, q_2 < n^2$ ומחשבת $z_1 = A \bmod q_1, z_2 = B \bmod q_2$
אליס שולחת לבוב $q_1, z_1, q_2, z_2$ .
בוב מחזיר לאליס $(C \bmod q_1 == z_1) \& (D \bmod q_2 == z_2)$ .

##### סיבוכיות תקשורת

אליס שולחת $q_1, z_1, q_2, z_2 < n^2$ ולכן שולחת $4 \log(n^2) = 8 \log(n)$ ביטים, בוב שולח
כתשובה ביט יחיד וסה"כ סיבוכיות התקשורת של האלגוריתם הינה $O(\log(n))$ .

##### הוכחת הסתברות שגיאה

האלגוריתם נכשל אם $A \neq C$ וגם $(A - C) \bmod q_1 = 0$ או $B \neq D$ וגם $(B - D) \bmod q_2 = 0$ .
$P(A \neq C \text{ וגם } (A - C) \bmod q_1 = 0) = P(B \neq D \text{ וגם } (B - D) \bmod q_2 = 0) \leq$
$\leq \frac{\text{number of } q\text{'s dividing } w < n \text{ (} w \in \mathbb{N} < 2^n \text{)}}{\text{number of primes } < n^2} \leq \frac{n}{\log(n^2)} = \frac{2 \log(n)}{n} \leq (*) \frac{1}{8}$
(*) עבור $n$ מספיק גדול.
$P(A \neq C \text{ וגם } (A - C) \bmod q_1 = 0 \text{ או } B \neq D \text{ וגם } (B - D) \bmod q_2 = 0) =$ (זרים)
$P(A \neq C \text{ וגם } (A - C) \bmod q_1 = 0) + P(B \neq D \text{ וגם } (B - D) \bmod q_2 = 0) \leq \frac{1}{8} + \frac{1}{8} = \frac{1}{4}$


**בהצלחה!**