

## שיעור 4

### תמורות וצופן אניגמה

#### 4.1 תמורות

##### הגדרה 4.1 תמורה

תמורה על קבוצה סופית  $\Sigma = \{x_1, \dots, x_n\}$  היא פונקציה  $\pi : \Sigma \rightarrow \Sigma$  אשר היא חד-חד ערכית ו"על"  $\Sigma$ . בהינתן  $x_i \in \Sigma$  ותמורה  $\pi$ . אז

$$\pi(x_i) = x_j \in \Sigma .$$

תזכורת:

- $\pi$  חד-חד ערכית. ז"א אם  $x_i \neq x_j$  אז  $\pi(x_i) \neq \pi(x_j)$ .
- $\pi$  "על"  $\Sigma$ . ז"א לכל  $y \in \Sigma$  קיים  $x \in \Sigma$  כך ש-  $y = \pi(x)$ .

כתוצאה לכך, אם  $\pi$  פועלת על כל האיברים של  $\Sigma$  אז נקבל אותה קבוצה  $\Sigma$  רק לא באותו בסדר של הסדר המקורי:

$$\{\pi(x_1), \pi(x_2), \dots, \pi(x_n)\} .$$

##### דוגמה 4.1

$x$	1	2	3	4	5	6
$\pi(x)$	4	1	6	5	2	3

##### דוגמה 4.2

$x$	1	2	3	4	5	6
$\sigma(x)$	2	1	5	4	6	3

##### דוגמה 4.3

תהי  $\Sigma$  קבוצה סופית ותהי  $\Sigma \rightarrow \Sigma$  פונקציה. הוכחו: אם  $\pi$  חד-חד ערכית אז  $\pi$  תמורה.

##### פתרונות:

נתון לנו הפונקציה  $\pi : \Sigma \rightarrow \Sigma$  אשר  $\Sigma$  קבוצה נוצר סופית. כדי להוכיח כי  $\pi$  תמורה יש להראות כי  $\pi$  חד-חד-ערכית ו"על"  $\Sigma$ . כבר נתון לנו ש-  $\pi$  חד-חד-ערכית רק להראות כי  $\pi$  על  $\Sigma$ .

$\Sigma$  היא קבוצה סופית לכן קיימים שלם  $0 \leq n \leq |\Sigma|$ . תהיו  $(\Sigma)$  התמונה של  $\pi$ . מכיוון ש-  $\pi$  היא פונקציה מהקבוצה  $\Sigma$  אל הקבוצה  $\Sigma$ , אז התמונה שלה היא תת-קבוצה של  $\Sigma$ , כלומר:

$$\pi(\Sigma) \subseteq \Sigma .$$

לכן

$$|\pi(\Sigma)| \leq |\Sigma| = n .$$

נראה כי  $|\pi(\Sigma)| = |\Sigma|$ . נניח בשלילה כי  $|\pi(\Sigma)| < |\Sigma|$ . אז בהכרח קיימים איברים  $x_1, x_2 \in \Sigma$  כך ש-

בסטירה לכך ש:  $\pi$  חד-חד-ערכית. לכן הוכחנו דרך השיליה כי  $\Sigma(x_1) = \Sigma(x_2)$

$$|\pi(\Sigma)| = |\Sigma| = n.$$

הוכחנו כי  $\pi$  גם  $|\pi(\Sigma)| = |\Sigma|$  אז בהכרח

$$\pi(\Sigma) = \Sigma$$

ולפיכך  $\Sigma \rightarrow \pi$  היא פונקציה "על"  $\Sigma$ .



## הגדרה 4.2 הרכבה של תמורה

תהי  $\Sigma$  קבוצה נוצר סופית ותהינה  $\Sigma \rightarrow \Sigma : \pi \circ \sigma$  תמורה על הקבוצה  $\Sigma$ . ההרכבה של  $\pi$  ו-  $\sigma$  מוגדרת להיות הפונקציה שמסומנת  $\sigma \circ \pi$  ומוגדרת לפי התנאי:  
לכל  $x \in \Sigma$ , אם  $\pi(x) = y \in \Sigma$  ו-  $\sigma(y) = z \in \Sigma$  אז  $\sigma \circ \pi(x) = z$ .

הסימן  $\sigma \circ \pi(x)$  אומר "קודם  $\pi$  פועלת על  $x$  ואז  $\sigma$  פועלת על  $\pi(x)$ ".

### דוגמה 4.4

נתון התמורות  $\pi$  ו-  $\sigma$ :

$\begin{array}{c cccccc} x & 1 & 2 & 3 & 4 & 5 & 6 \\ \hline \pi(x) & 4 & 1 & 6 & 5 & 2 & 3 \end{array}$	$\begin{array}{c cccccc} x & 1 & 2 & 3 & 4 & 5 & 6 \\ \hline \sigma(x) & 3 & 5 & 4 & 2 & 6 & 1 \end{array}$
--	---

אזי ההרבה  $\sigma \circ \pi$  היא:

$\begin{array}{c cccccc} x & 1 & 2 & 3 & 4 & 5 & 6 \\ \hline \sigma \circ \pi(x) & 2 & 3 & 1 & 6 & 5 & 4 \end{array}$
---

לעומת זאת ההרבה ההפוכה  $\sigma \circ \pi$  היא:

$\begin{array}{c cccccc} x & 1 & 2 & 3 & 4 & 5 & 6 \\ \hline \pi \circ \sigma(x) & 6 & 2 & 5 & 1 & 3 & 4 \end{array}$
---

כלומר  $\sigma \circ \pi \neq \pi \circ \sigma$ .

## משפט 4.1 הרכבה של תמורה היא תמורה

תהי  $\Sigma$  קבוצה נוצר סופית ותהינה  $\Sigma \rightarrow \Sigma : \pi \circ \sigma$  תמורה על הקבוצה  $\Sigma$ . הרכבה  $\sigma \circ \pi$  היא תמורה על  $\Sigma$ .

**הוכחה:** מספיק להוכיח כי  $\sigma \circ \pi$  היא פונקציה חד-חד-ערכית ו"על"  $\Sigma$ .

### • חח"ע

נניח בשיליה כי  $\sigma \circ \pi$  לא חח"ע.

אזי קיימים  $x_1, x_2 \in \Sigma$  כך ש-  $\sigma(\pi(x_1)) = \sigma(\pi(x_2))$

נסמן  $y_1 = \pi(x_1)$  ו-  $y_2 = \pi(x_2)$ .

מכיוון ש-  $\pi$  תמורה אז  $\pi$  חח"ע ולכן  $y_1 \neq y_2$ . ומכיון ש-  $\sigma$  תמורה אזי  $\sigma(y_1) \neq \sigma(y_2)$ . לכן

$$\sigma(\pi(x_1)) \neq \sigma(\pi(x_2)),$$

בסתירה לכך ש-  $\sigma(\pi(x_1)) = \sigma(\pi(x_2))$ . לכן הוכחנו דרך השיליה כי  $\pi$  פונקציה חד-ע.

### • על

נניח בשלילה כי  $\pi$  לא פונקציה "על". נסמן  $(\Sigma)$   $\pi$  התמונה של  $\pi$ . אי-

$$\sigma\pi(\Sigma) \neq \Sigma .$$

ראשית מכיוון ש-  $(\Sigma)$   $\pi$  הוא התמונה של  $\pi$  אי-  $\Sigma \subseteq \sigma\pi(\Sigma)$ . לכן אם  $\Sigma \neq \sigma\pi(\Sigma)$ . מכאן

$$|\sigma\pi(\Sigma)| < |\Sigma| .$$

לכן בהכרח קיימים לפחות שני איברים  $x_1, x_2 \in \Sigma$  עבורם  $\pi(x_1) = \pi(x_2)$ . זאת בסתירה לכך ש-  $\pi$  חד-ע, שמכוח בסעיף הקודם.

לכן הוכחנו דרך השיליה כי הפונקציה  $\pi$  היא "על"  $\Sigma$ .



### הגדרה 4.3 תמורות מתחלפות

תהיינה  $\Sigma \rightarrow \Sigma : \sigma$  ו-  $\Sigma \rightarrow \Sigma : \pi$  תמורות. אומרים כי  $\pi$  ו-  $\sigma$  מתחלפות אם לכל  $x \in \Sigma$  מתקיים

$$\pi\sigma(x) = \sigma\pi(x) .$$

### הגדרה 4.4 תמורות מתחלפות

תהי  $\Sigma \rightarrow \Sigma : \pi$  תמורה על הקבוצה  $\Sigma$ . התמורה ההפכית של  $\pi$  מסומנת  $\pi^{-1}$  ומוגדרת:

$$\pi\pi^{-1}(x) = x = \pi^{-1}\pi(x)$$

לכל  $x \in \Sigma$ .

### דוגמה 4.5

נתונה התמורה  $\pi$ :

$x$	1	2	3	4	5	6	7	8
$\pi(x)$	6	3	5	1	2	4	8	7

התמורה ההפכית היא:

$x$	1	2	3	4	5	6	7	8
$\pi^{-1}(x)$	4	5	2	6	3	1	8	7

### הגדרה 4.5 נקודת שבת ונקודת זהה

תהי  $\Sigma \rightarrow \Sigma : \pi$  תמורה.

- אם קיימת נקודת  $\Sigma \in x$  כך ש-  $\pi(x) = x$  אז אומרים כי  $x$  היא נקודת שבת של  $\pi$ .
- אם קיימת נקודת  $\Sigma \in x$  כך ש-  $\pi(x) \neq x$  אז אומרים כי  $x$  היא נקודת זהה של  $\pi$ .

**הגדרה 4.6 תמורה זהה**

התמורהזהה מסומנת  $\Sigma \rightarrow \Sigma : \text{id}$  ומוגדרת כך שלכל  $\Sigma \in \Sigma$ :

$$\text{id}(x) = x .$$

במילים אחרות אם  $\Sigma \rightarrow \Sigma : \text{id}$  היא התמורהזהה אז כל נקודת  $\Sigma \in \Sigma$  היא נקודת שבת של  $\text{id}$ .

**משפט 4.2 תמורה ההפכית של תמורה מורכבת**

תהיינה  $\pi_t, \dots, \pi_1$  תמורות על הקבוצה  $\Sigma$ . אז

$$(\pi_1 \cdots \pi_t)^{-1} = \pi_t^{-1} \cdots \pi_1^{-1} .$$

**הוכחה:** נוכיח את הטענה באינדוקציה.

שלב הבסיס

עבור  $t=2$ , לכל  $\Sigma \in \Sigma$  יש לנו:

$$\pi_2^{-1} \pi_1^{-1} \pi_1 \pi_2(x) = \pi_2^{-1} \text{id} \pi_2(x) = \pi_2^{-1} \pi_2(x) = \text{id}(x) = x .$$

$$\text{לכן הוכחנו כי } (\pi_1 \pi_2)^{-1} = \pi_2^{-1} \pi_1^{-1} .$$

שלב האינדוקציה

נניח כי הטענה מתקיימת עבור  $t=k > 2$  (זאת היא ההנחה האינדוקציה). אז נראה כי הטענה נכונה גם במקרה  $t=k+1$  באופן הבא. נתבונן על התמורה המורכבת  $\pi_k \pi_{k+1} \cdots \pi_1$ . נסמן התמורה המורכבת מ-  $k$  תמורות כך:  $\pi_k \cdots \pi_1 = \sigma$ . הסימן הזה מאפשר לנו להביע את התמורה המורכבת מ-  $k+1$  תמורות כתמורה המורכבת מ-  $2$  תמורות באופן הבא:

$$\pi_1 \cdots \pi_k \pi_{k+1} = \sigma \pi_{k+1} .$$

מכאן ולפי שלב הבסיס מהופכית היא

$$(\sigma \pi_{k+1})^{-1} = \pi_{k+1}^{-1} \sigma^{-1} .$$

icut נזכיר את הגדרה  $\pi_k \cdots \pi_1 = \sigma$  ונשתמש בהנחה האינדוקציה שלנו כדי להוכיח את הטענה עבור  $t=k+1$ :

$$(\pi_k \pi_{k+1})^{-1} = \pi_{k+1}^{-1} (\pi_1 \cdots \pi_k)^{-1} = \pi_{k+1}^{-1} \pi_k^{-1} \cdots \pi_1^{-1}$$

כאשר במעבר האחרון השתמשנו בהנחה האינדוקציה.

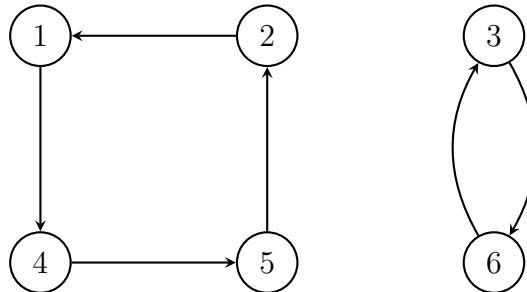
■

**4.2 פירוק למחזוריים של תמורה**

עד כה ראיינו תמורות בייצוג של טבלה. אבל המבנה האמתי של תמורה נגלה עם נציג תמורה כgraf. לדוגמה, תהי  $\pi$  תמורה הבאה על  $\Sigma = \{1, 2, 3, 4, 5, 6\}$ :

$x$	1	2	3	4	5	6
$\pi(x)$	4	1	6	5	2	3

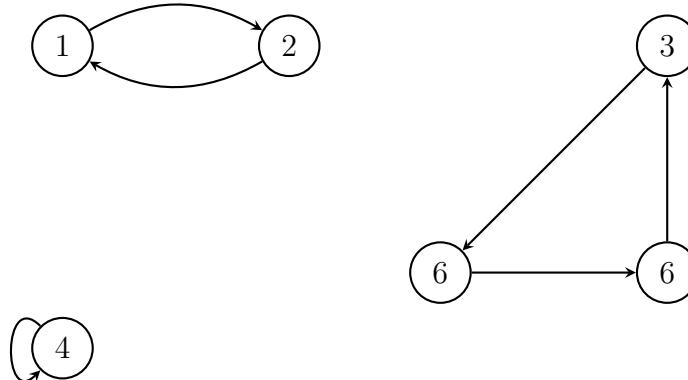
נדיר הגרף המכון  $G_\pi = (V, E)$  כאשר הקבוצה הקודקודים היא  $V = \Sigma$ , ולכל  $x \in \Sigma$  נגדיר צלע מ-  $x$  ל-  $\pi(x)$ . נ"א  $E = \{e_1, e_2, \dots, e_n\}$  היא הצלע מקודקод  $x_i$  לקודקוד  $\pi(x_i)$ . על פי ההגדרה הזו את הגרף  $G_\pi$  של התמורה  $\pi$  היא כמתואר באIOR למטה.



כדוגמה נוספת אם  $\sigma$  היא התמורה

$x$	1	2	3	4	5	6
$\sigma(x)$	2	1	5	4	6	3

אז הגרף  $G_\sigma$  הינו:



בגרף של תמורה, כל קודקוד שיעז לבזוק מעגל מכון אחד (שייתכן הוא עובר דרך קודקוד אחד בלבד). הרי קיימים התאמות אחדות-אחדות בין תמורה על  $\Sigma$  לבין גראף שמכסה כל המעגלים המכונים של  $\Sigma$ . התופעה זו היא המוטיבציה לסייעון מחזורי של תמורה.

#### הגדרה 4.7 מהזור

תהי  $\Sigma \rightarrow \Sigma$  :  $\pi$  תמורה על הקבוצה  $\Sigma$ . אם קיימים  $k$  איברים שונים  $\Sigma$  כך ש-

$$\pi(a_1) = a_2, \quad \pi(a_2) = a_3, \quad \dots \quad \pi(a_{k-1}) = a_k, \quad \pi(a_k) = a_1$$

אז אומרים כי קיימים מהזור באורך  $k$  ב-  $\pi$  שמסומנים:

$$(a_1 \ a_2 \ \dots \ a_k).$$

#### משפט 4.3 פירוק למחזורים של תמורה

כל תמורה  $\Sigma \rightarrow \Sigma$  :  $\pi$  על קבוצה סופית  $\Sigma$  מתפרקת למחזורים זרים.

**דוגמה 4.6**נתונה התמורה  $\pi$ :

$x$	1	2	3	4	5	6	7	8
$\pi(x)$	4	5	2	6	3	1	8	7

הפירוק למחזוריים הוא:

$$\pi = (1 \ 4 \ 6) (2 \ 5 \ 3) (8 \ 7)$$

**משפט 4.4**

תהי  $\Sigma \rightarrow \pi$  תמורה על קבוצה סופית  $\Sigma$  ויהי  $G_\pi = (V, E)$  הגרף של התמורה.  
 $\pi$  מכילה מחזור באורך  $k$  אם ורק אם הגרף  $G_\pi$  מכיל מעגל המילטוני באורך  $k$ .

הוכחה:  
כיוון אם

נניח ש-  $\pi$  מכילה מחזור באורך  $k$ .

$$\begin{aligned} & \left. \begin{aligned} & \text{קיימים איברים שונים } a_1, \dots, a_k \in \Sigma \text{ כך ש: } \\ & \pi(a_1) = a_2, \quad \pi(a_2) = a_3, \quad \dots \quad \pi(a_{k-1}) = a_k, \quad \pi(a_k) = a_1 \end{aligned} \right\} \Leftarrow \\ & \text{בגרף } G_\pi = (V, E) \text{ של התמורה קיימות הצלעות} \\ & a_1\pi(a_1), \ a_2\pi(a_2), \ \dots, \ a_{k-1}\pi(a_{k-1}), \ a_k\pi(a_k) \in E. \end{aligned}$$

 $\Leftarrow$  בגרף  $G_\pi = (V, E)$  קיימות הצלעות

$$a_1a_2, \ a_2a_3, \ \dots, \ a_{k-1}a_k, \ a_ka_1 \in E.$$

 $\Leftarrow$  מכילה מעגל המילטוני באורך  $k$ .

כיוון רק אם

נניח ש-  $G_\pi$  מכיל מעגל המילטוני באורך  $k$ . $\Leftarrow$  קיימים קבוצות  $a_1, \dots, a_k \in \Sigma$  עבורם

$$a_1a_2, \ a_2a_3, \ \dots, \ a_{k-1}a_k, \ a_ka_1 \in E.$$

 $\Leftarrow$  מכיוון ש-  $G_\pi$  הוא הגרף של התמורה  $\pi$  איזי

$$\pi(a_1) = a_2, \pi(a_2) = a_3, \quad \dots \quad \pi(a_{k-1}) = a_k, \pi(a_k) = a_1$$

$\Leftarrow$   $\pi$  מכילה מחזור באורך  $k$ :

$$(a_1 \ a_2 \ \dots \ \subseteq a_k) \subseteq \pi.$$



### הגדרה 4.8 המחלקה של תמורה

תהי  $\Sigma \rightarrow \pi$  תמורה. אומרים כי  $\pi$  שיכת למחלקה  $[1^{z_1} 2^{z_2} \cdots n^{z_n}]$  אם בפירוק למחזוריים של  $\pi$  יש בדיק  $z_1$  מחזוריים באורך-1,  $z_2$  מחזוריים באורך-2,  $z_3$  מחזוריים באורך-3, וכן הלאה.

במילים אחרות:

$$\pi \in [1^{z_1} 2^{z_2} \cdots n^{z_n}]$$

אם לכל  $n = 1, \dots, i$  בפירוק למחזוריים של  $\pi$  יש  $z_i$  מחזוריים באורך  $i$ .

### דוגמה 4.7

תהי  $. \Sigma = \{A, B, C, D, E, F\}$

$.(A \ B)(C \ D)(E \ F) \in [2^3]$

$.(A \ B \ C \ D) \in [1^2 4^1]$

$.(A \ D \ C)(E \ F) \in [1^1 2^1 3^1]$

## 4.3 תמורה צמודות

### הגדרה 4.9 תמורה צמודות

תהיינה  $\sigma, \pi$  תמורות על הקוצה סופית  $\Sigma$ . התמורה הצמודה של  $\sigma$  על ידי  $\pi$  היא המורה המורכבת  $\pi \sigma \pi^{-1}$ .

### משפט 4.5 משפט ההזזה של תמורות צמודות

תהיינה  $\Sigma \rightarrow \sigma : \Sigma \rightarrow \pi$  תמורות על הקוצה סופית  $\Sigma$ . לכל  $\Sigma$  אם  $\sigma(x) = y$  אז  $\pi(\sigma(x)) = \pi(y)$ .

$$\pi \sigma \pi^{-1}(\pi(\sigma(x))) = \pi(\sigma(x)) = \pi(y).$$

**הוכחה:** נניח ש:  $\sigma(x) = y$ . אז

$$\pi \sigma \pi^{-1}(\pi(\sigma(x))) = \pi \sigma \pi^{-1}\pi(x) = \pi \sigma(x) = \pi(y).$$

### משפט 4.6 פירוקים למחזוריים של תמורות צמודות שוויות

תהיינה  $\Sigma \rightarrow \sigma : \Sigma \rightarrow \pi$  תמורות על הקוצה סופית  $\Sigma$ . ונניח כי הפירוק למחזוריים של  $\sigma$  הוא

$$\sigma = (a_1 \ a_2 \ \cdots \ a_k) (b_1 \ b_2 \ \cdots \ b_l) \cdots .$$

אז הפירוק למחזוריים של  $\pi \sigma \pi^{-1}$  הוא:

$$\pi \sigma \pi^{-1} = (\pi(a_1) \ \pi(a_2) \ \cdots \ \pi(a_k)) (\pi(b_1) \ \pi(b_2) \ \cdots \ \pi(b_l)) \cdots .$$

**הוכחה:** עבור כל מהזור  $(a_1 \ a_2 \ \dots \ a_k)$  של  $\sigma$ , מתקיים

$$\sigma(a_i) = a_{i+1} \quad (1 \leq i \leq k-1), \quad \sigma(a_k) = a_1.$$

מנובע המשפט כי לכל מהזור של  $\sigma$  מתקיים:

$$\pi\sigma\pi^{-1}(\pi(a_i)) = \pi(a_{i+1}) \quad (1 \leq i \leq k-1), \quad \pi\sigma\pi^{-1}(\pi(a_k)) = \pi(a_1).$$

■

### משפט 4.7 המחלוקת של תמורה צמודות נשמרת

תהיינה  $\Sigma \rightarrow \Sigma : \sigma$  ו-  $\Sigma \rightarrow \Sigma : \tau$  תמורים על הקוצה סופית  $\Sigma$ .  
 $\tau$  צמודה ל-  $\sigma$  אם ורק אם  $\sigma \circ \tau$  שייכות לאותה מחלוקת.

**הוכחה:**

כיוון אם:

נניח ש-  $\sigma$  ו-  $\tau$  צמודות. אז קיימת תמורה  $\pi$  עבורה  $\tau = \pi\sigma\pi^{-1}$ . אם הפירוק למחוזרים של  $\sigma$  הוא

$$\sigma = (a_1 \ a_2 \ \dots \ a_k) (b_1 \ b_2 \ \dots \ \pi(b_l)) \dots$$

אז לפי משפט 4.6 הפירוק למחוזרים של  $\tau = \pi\sigma\pi^{-1}$  הוא

$$\pi\sigma\pi^{-1} = (\pi(a_1) \ \pi(a_2) \ \dots \ \pi(a_k)) (\pi(b_1) \ \pi(b_2) \ \dots \ \pi(b_l)) \dots$$

ולכן ל-  $\tau$  ול-  $\sigma$  יש אותו מבנה של מחוזרים וכך הוא שייכות לאותה מחלוקת.

כיוון רק אם:

■

## 4.4 צופן אניגמה

הgalלי האתחול של צופן אניגמה הם 3 תמורים קבועות שמוגדרות:

$x$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$\alpha_1(x)$	E	K	M	F	L	G	D	Q	V	Z	N	T	O	W	Y	H	X	U	S	P	A	I	B	R	C	J

$x$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$\alpha_2(x)$	A	J	D	K	S	I	R	U	X	B	L	H	W	T	M	C	Q	G	Z	N	P	Y	F	V	O	E

$x$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$\alpha_3(x)$	B	D	F	H	J	L	C	P	R	T	X	V	Z	N	Y	E	I	W	G	A	K	M	U	S	Q	O

המשקף הקבוע הוא תמורה הבאה:

$x$	$A$	$B$	$C$	$D$	$E$	$F$	$G$	$H$	$I$	$J$	$K$	$L$	$M$	$N$	$O$	$P$	$Q$	$R$	$S$	$T$	$U$	$V$	$W$	$X$	$Y$	$Z$
$\rho(x)$	$Y$	$R$	$U$	$H$	$Q$	$S$	$L$	$D$	$P$	$X$	$N$	$G$	$O$	$K$	$M$	$I$	$E$	$B$	$F$	$Z$	$C$	$W$	$V$	$J$	$A$	$T$

$$\begin{aligned} \alpha_1 &= (AELTPHQXRU)(BKNW)(CMOY)(DFG)(IV)(JZ)(S) && \in [1^1 2^2 3^1 4^2 10^1], \\ \alpha_2 &= (A)(JB)(CDKLHUP)(ESZ)(FIXVYOMW)(GR)(NT)(Q) && \in [1^2 2^3 3^1 7^1 8^1], \\ \alpha_3 &= (ABDHPEJT)(CFLVMZOYQIRWUKXSG)(N) && \in [1^1 8^1 17^1], \\ \rho &= (AY)(BR)(CU)(DH)(EQ)(FS)(GL)(IP)(JX)(KN)(MO)(TZ)(VW) && \in [2^{13}]. \end{aligned}$$

#### הגדרה 4.10 כלל מצפין וככלל מפענה של צופן אניגמה

יהי  $\pi$  משקף כלשהו מעל האלפבית  $Z = A, \dots, Z$ . הבחירה של המשקף מבהה את הלוח התקעiem. יהי  $w = x_1 x_2 \dots x_n$  מילה של טקסט גלי. לכל  $i = 1, \dots, n$ , הכלל מצפין והכלל מפענה של האות במקומות  $i$ -טקסט הם:

$$e(x_i) = \Delta_i(x_i) = d(x_i)$$

כאשר  $\Delta_i$  היא התמורה המורכבת

$$\Delta_i = \pi [\alpha_3^i]^{-1} \alpha_2^{-1} \alpha_1^{-1} \rho \alpha_1 \alpha_2 \alpha_3^i \pi(x_i)$$

כאשר

$$\alpha_3^i = \sigma_{-i} \alpha_3 \sigma_i, \quad [\alpha_3^i]^{-1} = \sigma_{-i} \alpha_3^{-1} \sigma_i.$$

אם נגדיר את התמורה המורכבת  $\pi$  אי  $\tau_i = \sigma_{-i} \alpha_3 \sigma_i \alpha_2 \alpha_1$  ולבסוף

$$\Delta_i = \tau_i^{-1} \rho \tau_i.$$

ז"א לכל  $i = 1, \dots, n$  התמורה המורכבת  $\Delta_i$  היא הצמודה של  $\rho$  על ידי  $\tau_i$ .

#### דוגמה 4.8 הצפנה על ידי צופן אניגמה

נתון הטקסט גלי,

hello .

נניח כי הלוח התקעiem הוא

$$\pi = (AX)(HF)(LP).$$

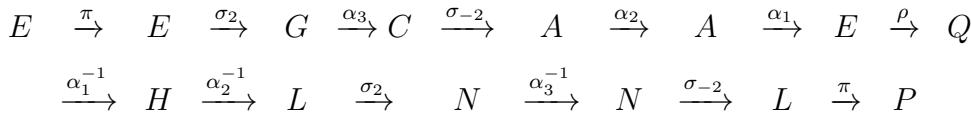
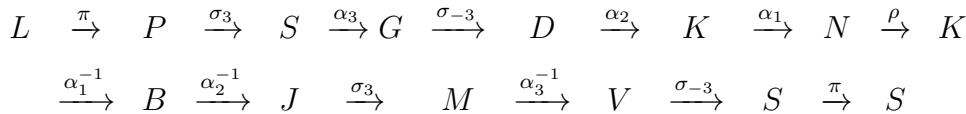
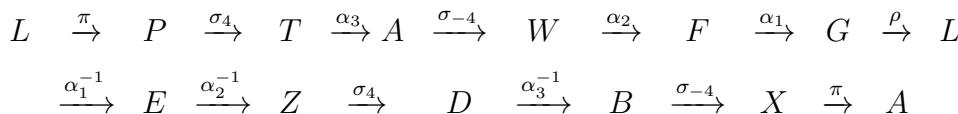
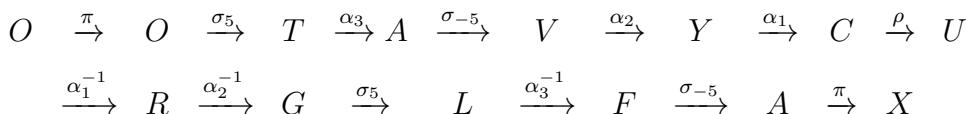
חשבו את הטקסט מוצפן.

פתרונות:

$$x_1 = H \quad (1)$$

$$\begin{array}{ccccccccc} H & \xrightarrow{\pi} & F & \xrightarrow{\sigma_1} & G & \xrightarrow{\alpha_3} C & \xrightarrow{\sigma_{-1}} & B & \xrightarrow{\alpha_2} J \xrightarrow{\alpha_1} Z \xrightarrow{\rho} T \\ & \xrightarrow{\alpha_1^{-1}} & L & \xrightarrow{\alpha_2^{-1}} & K & \xrightarrow{\sigma_1} & L & \xrightarrow{\alpha_3^{-1}} & F \xrightarrow{\sigma_{-1}} E \xrightarrow{\pi} E \end{array}$$

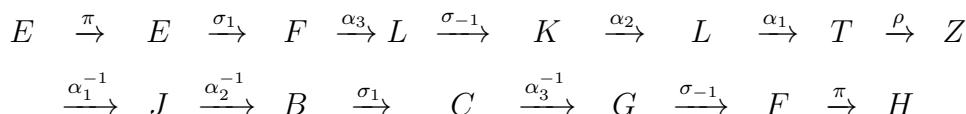
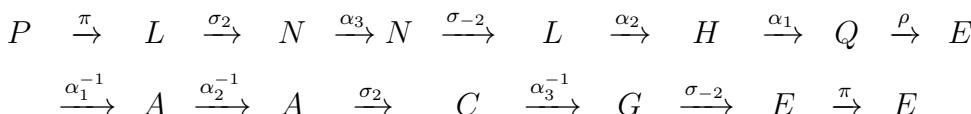
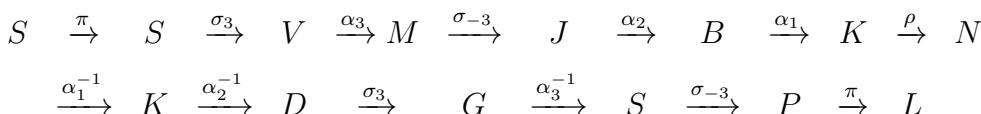
$$x_2 = E \quad (2)$$

 $x_3 = \text{L}$  (3) $x_4 = \text{L}$  (4) $x_5 = \text{O}$  (5)

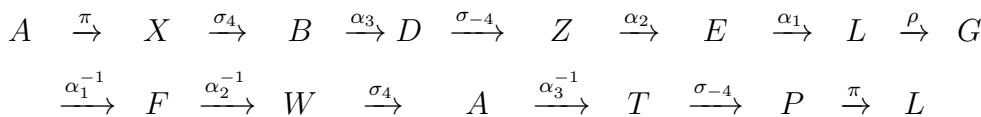
לפייך הטקסט מוצפן הוא: EPSAX.

**דוגמה 4.9 הצפנה על ידי צופן איניגמה**

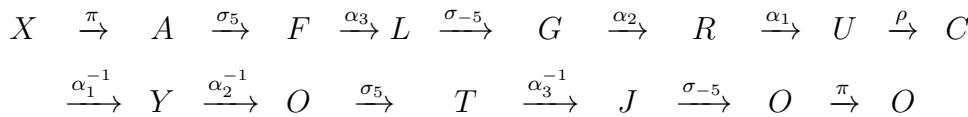
חשבו את הטקסט הגלוי של המילה המתקבלת בדוגמה הקודמת עם אותו לוח-התקעים.

**פתרונות:** $y_1 = \text{E}$  (1) $y_2 = \text{P}$  (2) $y_3 = \text{S}$  (3)

$$y_4 = A \quad (4)$$



$$y_5 = X \quad (5)$$



לפיכך הטקסט המקורי הוא: HELLO.

## 4.5 משפט ריבסקי

### הגדרה 4.11 תמורה משקפת

תהי  $\Sigma$  קבוצה נוצר סופית באורך זוגי. כלומר  $|\Sigma| = n$  זוגי. תהי  $\Sigma \rightarrow \Sigma : \rho$  תמורה. אומרים כי התמורה  $\rho$  היא משקף אם  $\rho \in [2^{n/2}]$ .

### משפט 4.8 תכונות של תמורה משקפת

תהי  $\Sigma$  קבוצה נוצר סופית באורך זוגי, ותהי  $\Sigma \rightarrow \Sigma : \rho$  תמורה. אז  $\rho$  היא משקף אם ורק אם התנאים הבאים מתקיימים:

$$\rho^{-1} = \rho \quad (1)$$

$$(2) \text{ לכל } \Sigma \in x \text{ מתקיים } \rho(x) \neq x.$$

הוכחה:

כיוון אם

נניח כי  $\rho$  משקף. נראה כי  $\rho^{-1} = \rho$  באופן הבא. נניח ש:

$$\rho = (x_1 \ y_1) (x_2 \ y_2) \cdots (x_{n/2} \ y_{n/2}).$$

לכל מחרוז  $(a_1 \ a_2 \ \cdots \ a_k)$  המחזור ההפוך הוא  $(a_k \ a_{k-1} \ \cdots \ a_1)$ . לכן

$$\begin{aligned} \rho^{-1} &= (x_1 \ y_1)^{-1} (x_2 \ y_2)^{-1} \cdots (x_{n/2} \ y_{n/2})^{-1} \\ &= (y_1 \ x_1) (y_2 \ x_2) \cdots (y_{n/2} \ x_{n/2}) \\ &= (x_1 \ y_1) (x_2 \ y_2) \cdots (x_{n/2} \ y_{n/2}) \\ &= \rho. \end{aligned}$$

כעת נראה שגם  $\rho(x) \neq x$  אז  $\rho(x) = x$ . נניח בשיילה שקיימת נקודה  $x \in \Sigma$  עבורה  $\rho(x) = x$ . אזי  $\rho \in [1^{z_1} \ \cdots \ z]$ , כאשר  $z > 0$ , כלומר  $\rho$  מכילה  $z$  מכוזרים לפחות אחד באורך 1, בסתרה לכך  $\rho$  היא משקף.

כיוון רק אם

נניח כי  $\Sigma \rightarrow \Sigma : \rho$  היא תמורה כך שלכל  $x \in \Sigma$  מתקיים  $x \neq \rho(x) \Leftrightarrow \rho^{-1}(\rho(x)) = x$ . נוכיח כי  $\rho$  היא משקף. בשלילה כי  $\rho$  לא משקף. אז  $\rho$  מכילה לפחות מחזור אחד באורך  $2 \neq k$ . נניח כי קיימים מחזור באורך 1. אז קיימת נקודת שבת של  $\rho$ , כלומר קיימת  $x \in \Sigma$  עבורו  $x = \rho(x)$ . והגענו לסתירה. מצד שני נניח כי קיימים מחזור באורך  $k > 2$ . אז ניתן לרשום  $\rho$  כהרכבה באופן הבא:

$$\rho = (x_1 \ x_2 \ x_3 \ \dots) \rho' ,$$

כאשר  $(\dots)$  הוא מחזור באורך  $k > 2$ . זו ההפכית של  $\rho$  היא

$$\rho^{-1} = \rho'^{-1} (x_1 \ x_2 \ x_3 \ \dots)^{-1} = \rho'^{-1} (\dots x_3 \ x_2 \ x_1) \neq \rho ,$$

בסתירה לכך שגם  $\rho^{-1} = \rho$ .

#### **משפט 4.9 הכלל מצפין של צופן האניגמה הוא תמורה משקפת על האלפבית האנגלית**

הכלל מצפין (והכלל מפענה) של צופן האניגמה הוא תמורה משקפת על האלפבית האנגלית.

**הוכחה:** הכלל מצפין והכלל מפענה של צופן האניגמה הם

$$e(x_i) = \Delta_i(x_i) = \tau_i^{-1} \rho \tau_i(x_i)$$

כאשר  $\pi \circ \rho$  המשקף הקבוע של צופן אניגמה.

$\Leftarrow$  לכל  $i = 1, \dots, n$  התמורה המורכבת  $\Delta_i$  היא הצמודה של  $\rho$  על ידי  $\tau_i$ .

$\Leftarrow$  מכיוון ש:  $\rho$  הוא משקף על האלפבית האנגלית אז  $\rho \in [2^{13}]$ .

$\Leftarrow$  לפי משפט 4.7  $\Delta_i \in [2^{13}]$ .

$\Leftarrow$  לפי הגדירה 4.11 התמורה  $\Delta_i$  היא תמורה משקפת.

#### **משפט 4.10 כלל של זוג תמורות משקפות**

יהיו  $\rho_1$  ו-  $\rho_2$  תמורות משקפות על הקבוצה סופית  $\Sigma$ .

קיימים  $\Sigma$  עברים  $x, y_1, y_2 \in \Sigma$  ורק אם  $\rho_1(x) = y_1$  וגם  $\rho_2(x) = y_2$ .

**הוכחה:**  
כיוון אם

תהיינה  $\rho_1, \rho_2$  תמורות משקפות ויהי  $x \in \Sigma$ .

$$\left. \begin{array}{l} y_1 = \rho_1(x) \\ y_2 = \rho_2(x) \end{array} \right\} \xrightarrow{\text{משקפת } \rho_1} x = \rho_1(y_1) \Rightarrow \rho_2(\rho_1(y_1)) = \rho_2(x) = y_2 .$$

כיוון רק אם

נניח ש:  $\rho_1(y_1) = \rho_2(y_2)$ . מכיוון ש-  $\rho_2$  תמורה משקפת איזומטרית  $x \in \Sigma$  קיים  $y_1, y_2 \in \Sigma$  כך ש:

$$\left. \begin{array}{l} \rho_1(y_1) = x = \rho_2(y_2) \\ \rho_2(y_2) = x \end{array} \right\} \xrightarrow{\text{משקפות } \rho_1, \rho_2} \left. \begin{array}{l} y_1 = \rho_1(x) \\ y_2 = \rho_2(x) \end{array} \right\} .$$

## 4.6 ההנחות של ריבסקי על צופן האניגמה

### הגדרה 4.12 ההנחות של ריבסקי

1) במהלך מלחמת העולם הראשונה והשנייה, כל הודעה שהוצפנה על ידי צופן האניגמה התחילה במילה סימטרית באורך 6 אותיות שנקראת **מילה משוכפלת**:

$$xyzxyz ,$$

במילה משוכפלת זו - 3 אותיות הראשונות היו זהות ל- 3 אותיות האחרונות.  
המילה הזאת נקראת המילה האופיינית של ההודעה.

2) ההצפנה של המילה המשוכפלת נקראת **המילה אופיינית**:

$$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \Delta_1(x)\Delta_2(y)\Delta_3(z)\Delta_4(x)\Delta_5(y)\Delta_6(z) .$$

3) הכלל מצפין אינו משתנה באותו יום.

### משפט 4.11 משפט ריבסקי I

יהי  $\sigma_6\sigma_5\sigma_4\sigma_3\sigma_2\sigma_1$  המילה האופיינית של טקסט מוצפן כלשהו שהוצפן ע"י צופן האניגמה. אז:

$$\begin{aligned} \sigma_4 &= \Delta_4\Delta_1(\sigma_1) , \\ \sigma_5 &= \Delta_5\Delta_2(\sigma_2) , \\ \sigma_6 &= \Delta_6\Delta_3(\sigma_3) . \end{aligned}$$

**הוכחה:**

תהי  $\sigma_6\sigma_5\sigma_4\sigma_3\sigma_2\sigma_1$  המילה האופיינית אשר היא ההצפנה של המילה המשוכפלת  $xyzxyz$ . נ"א

$$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \Delta_1(x)\Delta_2(y)\Delta_3(z)\Delta_4(x)\Delta_5(y)\Delta_6(z) .$$

נ"א

$$\left. \begin{array}{l} \sigma_1 = \Delta_1(x) \\ \sigma_4 = \Delta_4(x) \end{array} \right\} \Rightarrow x = \Delta_1(\sigma_1) \Rightarrow \Delta_4(x) = \Delta_4\Delta_1(\sigma_1) \Rightarrow \sigma_4 = \Delta_4\Delta_1(\sigma_1) .$$

$$\left. \begin{array}{l} \sigma_2 = \Delta_2(y) \\ \sigma_5 = \Delta_5(y) \end{array} \right\} \Rightarrow y = \Delta_2(\sigma_2) \Rightarrow \Delta_5(y) = \Delta_5\Delta_2(\sigma_2) \Rightarrow \sigma_5 = \Delta_5\Delta_2(\sigma_2) .$$

$$\left. \begin{array}{l} \sigma_3 = \Delta_3(z) \\ \sigma_6 = \Delta_6(z) \end{array} \right\} \Rightarrow z = \Delta_3(\sigma_3) \Rightarrow \Delta_6(z) = \Delta_6\Delta_3(\sigma_3) \Rightarrow \sigma_6 = \Delta_6\Delta_3(\sigma_3) .$$

**דוגמה 4.10**

נתונה הودעה מוצפנת שמתחלפת במילה אופיינית הבאה:

ICPWLV .

ז"א קיימת מילה מושכפלת  $xyzxyz$  כך ש:

$$\text{ICPWLV} = \Delta_1(x)\Delta_2(y)\Delta_3(z)\Delta_4(x)\Delta_5(y)\Delta_6(z) ,$$

לכן לפי משפט ריבסקי I :

$$\Delta_4\Delta_1(I) = W , \quad \Delta_5\Delta_2(C) = L , \quad \Delta_6\Delta_3(P) = V .$$

**דוגמה 4.11**

הטבלה הבאה מראה מיילים אופייניות מהודעות מוצפנות מאותו יום.

FDZWOW	YRVSNF	XASAIU	OYDFHH	PXFDBP	REQYUD
BLHGRR	LUBXKI	KGYEQA	APMCMO	JCENEM	KHREJS
HJNQSK	TTGMYL	SZWZXZ	ZFPRVX	QMUBZQ	IWIKFZ
NSXVT	DKJOGV	ENLTWY	CWAIFG	GITPAJ	WOOHDE
VQAU	MVKLLC	UBCJPN			

חשבו את התמורות  $\Delta_6\Delta_3$  ו-  $\Delta_5\Delta_2$  ו-  $\Delta_4\Delta_1$ .

**פתרונות:**

$$\Delta_4\Delta_1 = (ZRYS)(JNVU)(GPDOFWHQB)(ACIKETMLX) ,$$

$$\Delta_5\Delta_2 = (DO)(IA)(STYHJ)(BPMZX)(NWFVLR)(CEUKGQ) ,$$

$$\Delta_6\Delta_3 = (MOE)(CNK)(WBIZ)(AGLY)(VFPXTJ)(DHRSUQ) .$$

**משפט 4.12 משפט ריבסקי II**

- בכל תמורה כפולה  $\Delta_4\Delta_1$  של צופן אנigma קיים זוג מהזורים בסידור מסוים

$$(a_1 \ a_2 \ \cdots \ a_{k-1} \ a_k) (b_1 \ b_2 \ \cdots \ b_{k-1} \ b_k)$$

כך ש:

$$b_k = \Delta_1(a_1) , \quad b_{k-1} = \Delta_1(a_2) , \quad \dots \quad b_2 = \Delta_1(a_{k-1}) , \quad b_1 = \Delta_1(a_k) .$$

הסידור זהה של המהזרים נקרא **סדר ריבסקי**.

- בכל תמורה כפולה  $\Delta_5\Delta_2$  של צופן אנigma קיים זוג מוחזרים בסדר ריבסקי

$$(a_1 \ a_2 \ \cdots \ a_{k-1} \ a_k) (b_1 \ b_2 \ \cdots \ b_{k-1} \ b_k)$$

כך ש:

$$b_k = \Delta_2(a_1), \quad b_{k-1} = \Delta_2(a_2), \quad \dots \quad b_2 = \Delta_2(a_{k-1}), \quad b_1 = \Delta_2(a_k).$$

- בכל תמורה כפולה  $\Delta_6\Delta_3$  של צופן אנigma קיים זוג מוחזרים בסדר ריבסקי

$$(a_1 \ a_2 \ \cdots \ a_{k-1} \ a_k) (b_1 \ b_2 \ \cdots \ b_{k-1} \ b_k)$$

כך ש:

$$b_k = \Delta_3(a_1), \quad b_{k-1} = \Delta_3(a_2), \quad \dots \quad b_2 = \Delta_3(a_{k-1}), \quad b_1 = \Delta_3(a_k).$$

## דוגמה 4.12

$$\Delta_4\Delta_1 = (\text{OGKRYSD})(\text{ZUQWFIB})(\text{MJXCP})(\text{HILNVE})(\text{A})(\text{T})$$

ראשית נשים לב שהפירוק למוחזרים של  $\Delta_4\Delta_1$  הוא בדיקת המבנה הנקבע על ידי משפט ריבסקי. בפרט  $\Delta_4\Delta_1$  מכילה:

- זוג מוחזרים באורך 7,
- זוג מוחזרים באורך 5,
- זוג מוחזרים באורך 1.

לפי משפט ריבסקי II :

$$(\text{ZUQWFIB}) = \left( \Delta_1(\text{D}) \Delta_1(\text{S}) \Delta_1(\text{Y}) \Delta_1(\text{R}) \Delta_1(\text{K}) \Delta_1(\text{G}) \Delta_1(\text{O}) \right)$$

## דוגמה 4.13 קרייפטו-אנליזה של צופן אנigma

נתונות התמורות הבאות של צופן אנigma:

$$\Delta_4\Delta_1 = (\text{ZRYS})(\text{JNVU})(\text{GPDOFWHQB})(\text{ACIKETMLX}),$$

$$\Delta_5\Delta_2 = (\text{DO})(\text{IA})(\text{STYHJ})(\text{BPMZX})(\text{NWFVLR})(\text{CEUKGQ}),$$

$$\Delta_6\Delta_3 = (\text{MOE})(\text{CNK})(\text{WBIZ})(\text{AGLY})(\text{VFPXTJ})(\text{DHRSUQ}).$$

פענוו את הקסט מוצפן

ILBDA

**פתרונות:**

יהי הטקסט הגרפי

$$x_1x_2x_3x_4x_5.$$

אז

$$\text{ILBDA} = \Delta_1(x_1) \Delta_2(x_2) \Delta_3(x_3) \Delta_4(x_4) \Delta_5(x_5) .$$

אות 1

$$I = \Delta_1(x_1) \xrightarrow{\text{משקפת } \Delta_1} x_1 = \Delta_1(I) \xrightarrow{\text{משפט ריבסקי II}} x_1 = H .$$

אות 2

$$L = \Delta_2(x_2) \xrightarrow{\text{משקפת } \Delta_2} x_2 = \Delta_2(L) \xrightarrow{\text{משפט ריבסקי II}} x_2 = E .$$

אות 3

$$B = \Delta_3(x_3) \xrightarrow{\text{משקפת } \Delta_3} x_3 = \Delta_3(B) \xrightarrow{\text{משפט ריבסקי II}} x_3 = L .$$

אות 4

$$D = \Delta_4(x_4) \xrightarrow{\text{משקפת } \Delta_4} x_4 = \Delta_4(D)$$

$$\Delta_1(D) \xrightarrow{\text{משפט ריבסקי II}} M \xrightarrow{\text{משקפת } \Delta_1} D = \Delta_1(M) \Rightarrow \Delta_4(D) = \Delta_4\Delta_1(M) = L .$$

אות 5

$$A = \Delta_5(x_5) \xrightarrow{\text{משקפת } \Delta_5} x_5 = \Delta_5(A)$$

$$\Delta_2(A) \xrightarrow{\text{משפט ריבסקי II}} D \xrightarrow{\text{משקפת } \Delta_1} A = \Delta_1(D) \Rightarrow \Delta_5(A) = \Delta_5\Delta_2(D) = O .$$

תשובה סופית:

$$x_1x_2x_3x_4x_5 = HELLO .$$

