

## 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 מכך, 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  $\Sigma \rightarrow \Sigma$  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  $0 \leq n \leq |\Sigma|$ . תהי  $(\Sigma) \pi$  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-

$\Sigma$ , בסתירה לכך ש:  $\pi$  חד-חד-ערכית. לכן הוכחנו דרך השיליה כי

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

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

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

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



## הגדרה 4.2 הרכבה של תמורה

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

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

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

### דוגמה 4.4

נתון התרמוות  $\pi$  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 ההרבבה  $\sigma\pi$  היא:

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

לעומת זאת ההרבבה ההפוכה  $\pi\sigma$  היא:

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

כלומר  $\sigma\pi \neq \pi\sigma$ .

## משפט 4.1 הרכבה של תמורה היא תמורה

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

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

### • חח"ע

נניח בשיליה כי  $\sigma$  לא חח"ע. אזי קיימים  $x_1, x_2 \in \Sigma$  כך ש-  $(\pi(x_1)) = \sigma(\pi(x_2))$ . נסמן  $y_1 = \pi(x_1)$  ו-  $y_2 = \pi(x_2)$ . מכיוון ש-  $\pi$  תמורה אז  $\pi$  חח"ע ולכן  $y_1 \neq y_2$ . ומכיוון ש-  $\sigma$  תמורה אזי  $\sigma(y_1) \neq \sigma(y_2)$ . לכן

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

בסתירה לכך ש-  $\sigma$  חח"ע.

לכן הוכחנו דרך השיליה כי  $\sigma$  פונקציה חח"ע.

• על

נניח בשלילה כי  $\pi \sigma$  לא פונקציה "על". נסמן  $(\Sigma)$  התחמונה של  $\pi \sigma$ . אז  $\sigma \pi(\Sigma) \neq \Sigma$ .

ראשית מכיוון ש-  $(\Sigma)$  הוא התחמונה של  $\pi \sigma$  אז  $\Sigma \subseteq \pi \sigma(\Sigma)$ . לכן אם  $\Sigma \neq \pi \sigma(\Sigma)$  אז

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

לכן בהכרח קיימים לפחות שני איברים  $x_1, x_2 \in \Sigma$  עבורם  $\sigma \pi(x_1) = \sigma \pi(x_2)$ . זאת בסתיויה כך ש-  $\pi$  חח"ע, שMOVED בסייף הקודם.

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

### הגדרה 4.3 תמורהות מתחלפות

תהיינה  $\pi, \sigma$  תמורהות. אומרים כי  $\pi$  ו-  $\sigma$  מתחלפות אם

$$\pi \sigma = \sigma \pi .$$

### הגדרה 4.4 תמורהות מתחלפות

תהי  $\Sigma \rightarrow \Sigma$  תמורה על הקבוצה  $\Sigma$ . התמורה ההופכית 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 ההופכית 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  $\Sigma \rightarrow \Sigma$  תמורה.

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

### הגדרה 4.6 תמורה זהה

התמורה זהה מסומנת  $\Sigma \rightarrow \Sigma$  לפי ומוגדרת כך שלכל  $x \in \Sigma$ :

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

במילים אחרות אם  $\Sigma \rightarrow \Sigma$  היא התמורה זהה אז כל נקודת  $\Sigma \in x$  היא נקודת שבת של  $\text{id}$ .

**משפט 4.2 תמורה ההפכית של תמורה מורכבת**

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

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

**הוכחה:** נוכיח את הטענה באינדוקציה.

שלב הבסיס

עבור  $t = 2$ , לכל  $\Sigma \in x$  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 כ-  $\sigma$ :  $\sigma = \pi_1 \cdots \pi_k$ . הסימון 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 מההפכית היא

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

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

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

כאשר במעבר האחרון השתמשנו בהנחה האינדוקציה.

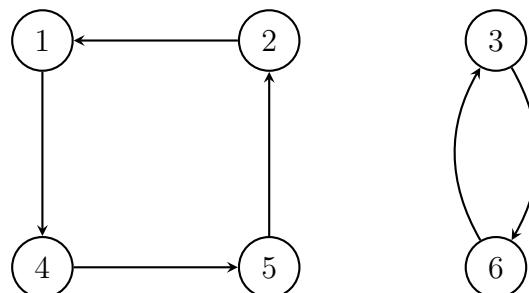
■

**4.2 פירוק למחזוריים של תמורה**

עד כה ראיינו תמורות ביצוג 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

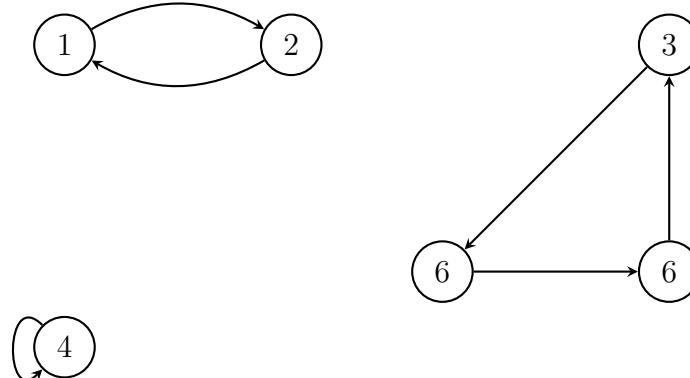
נדיר הgraf המכובן  $G_\pi = (V, E)$  כאשר הקבוצת הקודקודים היא  $V = \Sigma$ , ולכל  $x \in \Sigma$  נגידר צלע מ-  $x$  ל-  $\pi(x)$ . א"א  $E = \{e_1, e_2, \dots, e_n\}$  כאשר  $e_i = x_i \pi(x_i)$  הינה הצלע מקודקוד  $x_i$  לקודקוד  $\pi(x_i)$ . על פי ההגדרה זאת הgraf  $G_\pi$  של התמורה  $\pi$  היא כמתוארת באיור למטה.



כדוגמה נוספת אם  $\sigma$  היא התמורה

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

אזי הגרף  $G_\sigma$  הינו:



בגרף של תמורה, כל קודקוד שייך לבדיק מעגל מכוכן אחד (שייתכן הוא עובר דרך קודקוד אחד בלבד). הרי קיים התאמה אחת-אחד בין תמורה על  $\Sigma$  לבין גראף שמכסה כל המעגלים המכוכנים של  $\Sigma$ . התופעה זו היא המוטיבציה לשימוש מחזוריים של תמורים.

#### הגדרה 4.7 מחזור

תהי  $\Sigma \rightarrow \Sigma$  תמורה על הקבוצה  $\Sigma$  ויהיו  $\{x_1, \dots, x_n\}$  אם

$$\pi(x_1) = x_{i_1}, \pi(x_{i_1}) = x_{i_2}, \dots, x_{i_{k-1}} = x_k$$

או אומרים שבתמורה  $\pi$  קיים מחזור באורך  $k$ , מסומן

$$(x_{i_1} \ x_{i_2} \ \dots \ x_{i_k}).$$

#### משפט 4.3 פירוק למחזורים של תמורה

תהי  $\Sigma \rightarrow \Sigma$  תמורה על קבוצה סופית  $\Sigma$ . ניתן לרשום את  $\pi$  כהרכבה של מחזורים 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 למחזורים הוא:

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

#### הגדרה 4.8 החלוקת של תמורה

תהי  $\Sigma \rightarrow \Sigma$  תמורה. אומרים כי  $\pi$  שיכת לחלוקת  $[1^{z_1} 2^{z_2} \dots n^{z_n}]$  אם בפירוק למחזורים של  $\pi$  יש לבדוק  $z_1$  מחזורים באורך-1,  $z_2$  מחזורים באורך-2,  $z_3$  מחזורים באורך-3, וכן הלאה.

במילים אחרות:

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

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

### 4.7 דוגמה

- תהי  $\Sigma = \{A, B, C, D, E, F\}$
- התמורה  $(A \ B)(C \ D)(E \ F) \in [2^3]$
  - התמורה  $(A \ B \ C \ D) \in [1^2 4^1]$
  - התמורה  $(A \ D \ C)(E \ F) \in [1^1 2^1 3^1]$

## 4.3 תמורה צמודות

### הגדרה 4.9 תמורה צמודות

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

### משפט 4.4 משפט ההזזה של תמורה צמודות

תהיינה  $\Sigma : \sigma \rightarrow \Sigma : \pi \rightarrow \Sigma$  תמורה על הקבוצה סופית  $\Sigma$ . לכל  $x, y \in \Sigma$  אם  $\sigma(x) = y$  אז  $\pi(\sigma(x)) = \pi(y)$ .

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

**הוכחה:** נניח ש:  $y = \sigma(x)$ .

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



### משפט 4.5 פירוקים למחוזרים של תמורה צמודות שוויים

תהיינה  $\Sigma : \sigma \rightarrow \Sigma : \pi \rightarrow \Sigma$  תמורה על הקבוצה סופית  $\Sigma$ . ונניח כי הפירוק למחוזרים של  $\sigma$  הוא

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

אזי הפירוק למחוזרים 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 מחזיר  $(a_1 \ a_2 \ \dots \ a_k)$  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 מחזיר 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 4.6 המחלוקת של תמורה צמודות נשמרת

תהיינה  $\Sigma \rightarrow \Sigma : \sigma \circ \tau \rightarrow \Sigma$  תמורה על הקוצה סופית  $\Sigma$ .  
 $\tau$  צמודה ל-  $\sigma$  אם ורק אם  $\sigma \circ \tau = \tau \circ \sigma$  שוויון לאוותה מחלוקת.

הוכחה:

כיוון אם:

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

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

אז לפי משפט 4.5 הפירוק למחזוריים של  $\tau = \pi \sigma \pi^{-1}$  הוא

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

ולכן  $\tau \circ \sigma$  יש אותו מבנה של מחזוריים ולכן הן שוויון לאוותה מחלוקת.

כיוון רק אם:

## 4.4 צופן אנigma

הgalלי האתחל של צופן אנigma 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

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

**הגדירה 4.10 כל מיפוי וכל פעולה של צופן אניגמה**

יהי  $\pi$  משקף כלשהו מעל האלפבית  $Z = \{A, B, C\}$ . הבחירה של המשקף מhoeה את הלוח התקעים. יהי  $x_n \dots x_1 x_2 = w$  מילה של טקסט גלי. לכל  $n = 1, \dots, i$  הכלל מצפין והכלל מפענח של האות במיקום  $i$ - בטקסט ה- $\pi$ :

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

כאשר  $\Delta_i$  היא התמורה המורכבת

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

כאר

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

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

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

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

#### **דוגמה 4.8 הצפנה על ידי צופן אנigma**

נתון הטקסט גלי

hello .

**נניח כי הלוֹחַ הַתְקֻעִים הָוֶא**

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

חשבו את הטקסט מוצפן.

## **פתרונות:**

$$x_1 = \text{H} \quad (\mathbf{1})$$

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

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

$$\begin{array}{ccccccccc}
E & \xrightarrow{\pi} & E & \xrightarrow{\sigma_2} & G & \xrightarrow{\alpha_3} & C & \xrightarrow{\sigma_{-2}} & A & \xrightarrow{\alpha_2} & A & \xrightarrow{\alpha_1} & E & \xrightarrow{\rho} & Q \\
& \xrightarrow{\alpha_1^{-1}} & H & \xrightarrow{\alpha_2^{-1}} & L & \xrightarrow{\sigma_2} & N & \xrightarrow{\alpha_3^{-1}} & N & \xrightarrow{\sigma_{-2}} & L & \xrightarrow{\pi} & P
\end{array}$$

$$x_3 = L \quad (3)$$

$$\begin{array}{ccccccccc}
L & \xrightarrow{\pi} & P & \xrightarrow{\sigma_3} & S & \xrightarrow{\alpha_3} & G & \xrightarrow{\sigma^{-3}} & D & \xrightarrow{\alpha_2} & K & \xrightarrow{\alpha_1} & N & \xrightarrow{\rho} & K \\
& \xrightarrow{\alpha_1^{-1}} & B & \xrightarrow{\alpha_2^{-1}} & J & \xrightarrow{\sigma_3} & M & \xrightarrow{\alpha_3^{-1}} & V & \xrightarrow{\sigma^{-3}} & S & \xrightarrow{\pi} & S
\end{array}$$

$$x_4 = L \quad (4)$$

$$\begin{array}{ccccccccccccc}
 L & \xrightarrow{\pi} & P & \xrightarrow{\sigma_4} & T & \xrightarrow{\alpha_3} & A & \xrightarrow{\sigma_{-4}} & W & \xrightarrow{\alpha_2} & F & \xrightarrow{\alpha_1} & G & \xrightarrow{\rho} & L \\
 & \xrightarrow{\alpha_1^{-1}} & E & \xrightarrow{\alpha_2^{-1}} & Z & \xrightarrow{\sigma_4} & D & \xrightarrow{\alpha_3^{-1}} & B & \xrightarrow{\sigma_{-4}} & X & \xrightarrow{\pi} & A
 \end{array}$$

 $x_5 = \circ$  (5)

$$\begin{array}{ccccccccccccc}
 O & \xrightarrow{\pi} & O & \xrightarrow{\sigma_5} & T & \xrightarrow{\alpha_3} & A & \xrightarrow{\sigma_{-5}} & V & \xrightarrow{\alpha_2} & Y & \xrightarrow{\alpha_1} & C & \xrightarrow{\rho} & U \\
 & \xrightarrow{\alpha_1^{-1}} & R & \xrightarrow{\alpha_2^{-1}} & G & \xrightarrow{\sigma_5} & L & \xrightarrow{\alpha_3^{-1}} & F & \xrightarrow{\sigma_{-5}} & A & \xrightarrow{\pi} & X
 \end{array}$$

לפייך הטקסט מוצפן הוא: EPSAX.

**דוגמה 4.9 הצפנה על ידי צופן איניגמה**

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

**פתרונות:** $y_1 = E$  (1)

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

 $y_2 = P$  (2)

$$\begin{array}{ccccccccccccc}
 P & \xrightarrow{\pi} & L & \xrightarrow{\sigma_2} & N & \xrightarrow{\alpha_3} & N & \xrightarrow{\sigma_{-2}} & L & \xrightarrow{\alpha_2} & H & \xrightarrow{\alpha_1} & Q & \xrightarrow{\rho} & E \\
 & \xrightarrow{\alpha_1^{-1}} & A & \xrightarrow{\alpha_2^{-1}} & A & \xrightarrow{\sigma_2} & C & \xrightarrow{\alpha_3^{-1}} & G & \xrightarrow{\sigma_{-2}} & E & \xrightarrow{\pi} & E
 \end{array}$$

 $y_3 = S$  (3)

$$\begin{array}{ccccccccccccc}
 S & \xrightarrow{\pi} & S & \xrightarrow{\sigma_3} & V & \xrightarrow{\alpha_3} & M & \xrightarrow{\sigma_{-3}} & J & \xrightarrow{\alpha_2} & B & \xrightarrow{\alpha_1} & K & \xrightarrow{\rho} & N \\
 & \xrightarrow{\alpha_1^{-1}} & K & \xrightarrow{\alpha_2^{-1}} & D & \xrightarrow{\sigma_3} & G & \xrightarrow{\alpha_3^{-1}} & S & \xrightarrow{\sigma_{-3}} & P & \xrightarrow{\pi} & L
 \end{array}$$

 $y_4 = A$  (4)

$$\begin{array}{ccccccccccccc}
 A & \xrightarrow{\pi} & X & \xrightarrow{\sigma_4} & B & \xrightarrow{\alpha_3} & D & \xrightarrow{\sigma_{-4}} & Z & \xrightarrow{\alpha_2} & E & \xrightarrow{\alpha_1} & L & \xrightarrow{\rho} & G \\
 & \xrightarrow{\alpha_1^{-1}} & F & \xrightarrow{\alpha_2^{-1}} & W & \xrightarrow{\sigma_4} & A & \xrightarrow{\alpha_3^{-1}} & T & \xrightarrow{\sigma_{-4}} & P & \xrightarrow{\pi} & L
 \end{array}$$

 $y_5 = X$  (5)

$$\begin{array}{ccccccccccccc}
 X & \xrightarrow{\pi} & A & \xrightarrow{\sigma_5} & F & \xrightarrow{\alpha_3} & L & \xrightarrow{\sigma_{-5}} & G & \xrightarrow{\alpha_2} & R & \xrightarrow{\alpha_1} & U & \xrightarrow{\rho} & C \\
 & \xrightarrow{\alpha_1^{-1}} & Y & \xrightarrow{\alpha_2^{-1}} & O & \xrightarrow{\sigma_5} & T & \xrightarrow{\alpha_3^{-1}} & J & \xrightarrow{\sigma_{-5}} & O & \xrightarrow{\pi} & O
 \end{array}$$

לפייך הטקסט המקורי הוא: HELLO.

## 4.5 משפט ריבסקי והתקפה על הצופן האניגמה

### הגדלה 4.11 משקף

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

### משפט 4.7 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 מתקיים:

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

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

**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 מהזור  $(a_1 \ a_2 \ \cdots \ a_k)$  המוחזר 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 שאם  $\Sigma \in x$  אז  $x \neq \rho(x)$ . נניח בשילhouette שקיימות נקודה  $\Sigma \in x$  עבורות  $x$  ( $\rho(x) = x$ ). אזי  $\rho$  מכך  $\rho$  מכילה קיים לפחות אחד באורך 1, בסתרה לכך  $\rho$  היא משקף.

#### כיוון רק אם

נניח כי  $\Sigma \rightarrow \Sigma : \rho$  היא תמורה כך שלכל  $\Sigma \in x$  מתקיים  $\rho(\rho(\Sigma)) = \Sigma$ . נוכיח כי  $\rho$  היא משקף. נניח בשילhouette כי  $\rho$  לא משקף. אזי  $\rho$  מכילה לפחות אחד באורך  $k > 2$ . נניח כי קיים מוחזר באורך 1. אזי קיימת נקודת שבת של  $\rho$ , קלומר קיימת  $\Sigma \in x$  עבורות  $x$  ( $\rho(\rho(\Sigma)) = \Sigma$ ). והגענו לסתירה. מצד שני נניח כי קיים מוחזר באורך  $2 < k$ . אזי ניתן לרשום  $\rho$  כהרכבה באופן הבא:

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

כאשר  $(\dots \ x_1 \ x_2 \ x_3 \ \dots)$  הוא מוחזר באורך  $k$ . ז"א ההופכית של  $\rho$  היא

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

בסתרה לכך  $\rho^{-1} = \rho$ .

**משפט 4.8 הכלל מצפן של אניגמה הוא משקף על האלפבית האנגלית**

הכלל מצפן (והכלל מפענה) של צופן אניגמה הוא משקף על האלפבית האנגלית.

**הוכחה:** הכלל מצפן והכלל מפענה של צופן אניגמה הם

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

כאשר  $\pi$  ו-  $\rho$  המשקף הקבוע של צופן אניגמה.

$\Leftarrow$  לכל  $n = i$  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 4.6  $\Delta_i \in [2^{13}]$ .

$\Leftarrow$  לפי הדרה 4.11 התמורה  $\Delta_i$  היא משקף.

**משפט 4.9**

יהיו  $\rho_1$  ו-  $\rho_2$  משקפים על הקבוצה סופית  $\Sigma$ .  
לכל  $x \in \Sigma$ ,  $\rho_2\rho_1(y_1) = y_2$  אם  $\rho_1(x) = y_1$  ו-  $\rho_2(x) = y_2$  אזי  $\rho_1(x) = y_1$  ו-  $\rho_2(x) = y_2$ .

**הוכחה:** מכיוון ש-  $\rho_1$  משקף ו-  $\rho_1(x) = y_1$  אזי

$$\rho_1(x) = y_1 \iff \rho_1^{-1}(\rho_1(x)) = \rho_1^{-1}(y_1) \iff x = \rho_1^{-1}(y_1) \iff x = \rho_1(y_1) .$$

ז"א הוכחנו ש-  $x = \rho_1(y_1)$ . מכאן  $\rho_2\rho_1(y_1) = \rho_2(x) = y_2$ ,

כנדרש.

**דוגמה 4.10**

נניח שיש לנו טקסט שמוצפן ע"י צופן אניגמה שמתחל ב- ICPWLV. איזי אנחנו יודעים שקייםים כך ש:

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

כאשר ה-  $\Delta_i$  הוא הכלל מצפן של צופן אניגמה המורכב מהתמורות הנעלמות. מצד שני אנחנו כן יודעים שככל  $\Delta$  הוא משקף על פי. לכן, בזכות המשפט, אפשר להסיק כי:

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

**משפט 4.10 משפט ריבסקי**

יהיו  $\rho_1$  ו-  $\rho_2$  משקפים על הקבוצה סופית  $\Sigma$ . אם המוחזר

$$(a_1 \ a_2 \ \dots \ a_t)$$

מוופיע בפרק למחוזרים של התמורה המורכבת  $\rho_2\rho_1$ , אזי בהכרח המוחזר

$$(\rho(a_1) \quad \rho_1(a_2) \quad \cdots \quad \rho_1(a_t))$$

גם מוופיע בפרק למחוזרים של התמורה המורכבת  $\rho_1\rho_2$ , ובנוסף הוא שונה מהוחזר

$$(a_1 \quad a_2 \quad \cdots \quad a_t)$$