

## 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  $\pi$ , אזי

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

תזכורת:

•  $\pi$  חד-חד ערכית. ז"א אם  $x_i \neq x_j$  אזי  $\pi(x_i) \neq \pi(x_j)$ .

•  $\pi$  "על"  $\Sigma$ . ז"א לכל  $y \in \Sigma$  קיים  $x \in \Sigma$  כך ש-  $\pi(x) = y$ .

כתוצאה מכך, אם  $\pi$  פועלת על כל האיברים של  $\Sigma$  אזי 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  $\pi : \Sigma \rightarrow \Sigma$  פונקציה. הוכיחו: אם  $\pi$  חד-חד ערכית אזי היא תמורה.

##### פתרון:

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

$\Sigma$  היא קבוצה סופית לכן קיים שלם  $n \geq 0$  עבורו  $|\Sigma| = n$ . תהי  $\pi(\Sigma)$  התמונה של  $\pi$ . מכיוון ש-  $\pi$  היא פונקציה מהקבוצה  $\Sigma$  אל הקבוצה  $\Sigma$ , אזי 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:

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

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

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

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

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



## הגדרה 4.2 הרכבה של תמורות

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

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

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

## דוגמה 4.4

נתון התמורות  $\pi$  ו-  $\sigma$ :

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

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

אזי ההרכבה  $\sigma\pi$  היא:

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

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

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

כלומר  $\pi\sigma \neq \sigma\pi$ .

## משפט 4.1 הרכבה של תמורות היא תמורה

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

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

### • חח"ע

נניח בשלילה כי  $\sigma\pi$  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  $y_1 \neq y_2$ . 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-  $\sigma(\pi(x_1)) = \sigma(\pi(x_2))$ .

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

• על

נניח בשלילה כי  $\sigma\pi$  לא פונקצית "על". נסמן  $\sigma\pi(\Sigma)$  התמונה של  $\sigma\pi$ . אזי

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

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

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

לכן בהכרח קיים לפחות שני איברים  $x_1, x_2 \in \Sigma$  עבורם  $\sigma\pi(x_1) = \sigma\pi(x_2)$ . זאת בסתירה לכך ש-  $\sigma\pi$  חח"ע, שמוכח בסעיף הקודם.

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



### הגדרה 4.3 תמורות מתחלפות

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

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

### הגדרה 4.4 תמורות מתחלפות

תהי  $\pi : \Sigma \rightarrow \Sigma$  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 זזה

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

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

### הגדרה 4.6 תמורה הזהות

התמורה הזהות מסומנת  $\text{id} : \Sigma \rightarrow \Sigma$  ומוגדרת כך שלכל  $x \in \Sigma$ :

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

במילים אחרות אם  $\text{id} : \Sigma \rightarrow \Sigma$  היא התמורה הזהות אזי כל נקודה  $x \in \Sigma$  היא נקודת שבת של  $\text{id}$ .

**משפט 4.2 תמורה ההופכית 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  $x \in \Sigma$  יש לנו:

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

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 ההנחת האינדוקציה). אז נראה כי הטענה נכונה גם כן עבור  $t = k + 1$  באופן הבא. נתבונן על ההתמורה המורכבת  $\pi_1 \cdots \pi_k \pi_{k+1}$ . נסמן התמורה המורכבת מ- $k$  תמורות כך:  $\sigma = \pi_1 \cdots \pi_k$ . 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 השלב הבסיס מהופכית היא

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

כעת נחזיר את ההגדרה  $\sigma = \pi_1 \cdots \pi_k$  ונשתמש בהנחת 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 בהנחת האינדוקציה.

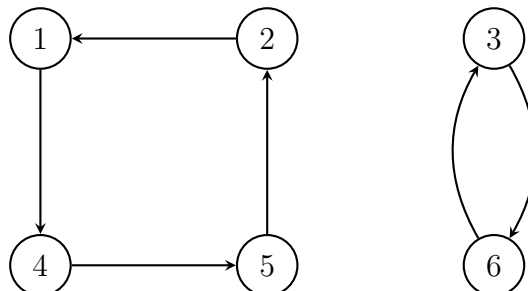
■

**4.2 פירוק למחזורים של תמורה**

עד כה ראינו תמורות בייצוג של טבלה. אבל המבנה האמיתי של תמורה נגלה עם נציג תמורה כגרף. 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

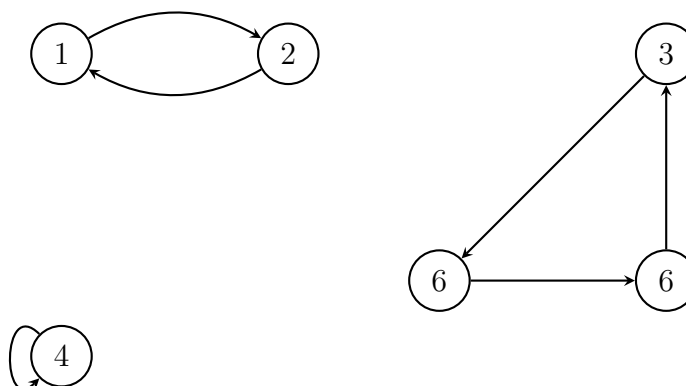
נגדיר הגרף המכוון  $G_\pi = (V, E)$  כאשר הקבוצת הקודקודים היא  $V = \Sigma$ , ולכל  $x \in \Sigma$  נגידר צלע מ- $x$  ל- $\pi(x)$ . אז  $E = \{e_1, e_2, \dots, e_n\}$  כאשר  $e_i = x_i \pi(x_i)$  היא הצלע מקודקוד  $x_i$  לקודקוד  $\pi(x_i)$ . על פי ההגדרה הזאת הגרף  $G_\pi$  של התמורה  $\pi$  היא כמתוארת 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 מכוון אחד (שייתכן הוא עובר דרך קודקוד אחד בלבד). הרי קיים התאמה אחת-אחת בין תמורה על  $\Sigma$  לבין גרף שמכסה כל המעגלים המכוונים של  $\Sigma$ . התופעה זו היא המוטיבציה לסימון מחזורים של תמורות.

#### הגדרה 4.7 מחזור

תהי  $\pi : \Sigma \rightarrow \Sigma$  תמורה על הקבוצה  $\Sigma$  והיו  $\Sigma = \{x_1, \dots, x_n\}$  אם

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

אז 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  $\pi : \Sigma \rightarrow \Sigma$  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 המחלקה של תמורה

תהי  $\pi : \Sigma \rightarrow \Sigma$  תמורה. אומרים כי  $\pi$  שייכת למחלקה  $[1^{z_1} 2^{z_2} \dots n^{z_n}]$  אם בפירוק למחזורים של  $\pi$  יש בדיק  $z_1$  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  $i = 1, \dots, n$  בפירוק למחזורים של  $\pi$  יש  $z_i$  מחזורים באורך  $i$ .

#### דוגמה 4.7

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 תמורות צמודות

#### הגדרה 4.9 תמורות צמודות

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

#### משפט 4.4 פירוקים למחזורים של תמורות צמודות שווים

תהי  $\sigma : \Sigma \rightarrow \Sigma$  תמורה ונניח כי הפירוק למחזורים שלה הוא

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

אזי להתמורה הצמודה  $\pi\sigma\pi^{-1}$  יש אותו פירוק למחזורים:

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

בלשון אחר, הצמודה של  $\sigma$  על ידי  $\pi$  פועלת על הפירוק למחזורים המקורי של  $\sigma$  על ידי להפעיל  $\pi$  על האיברים של המחזורים בנפרד.

**הוכחה:** אם  $\sigma(x) = y$  אזי  $\pi\sigma\pi^{-1}(\pi(x)) = \pi(y)$  באופן הבא:

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

■

#### משפט 4.5 תמוקות צמודות שייכות לאותה מחלקה

תהיינה  $\pi_1, \pi_2$  תמורות כלשהן על הקבוצה סופית  $\Sigma$ .

התמורה  $\pi_1$  והתמורה  $\pi_2$  הן צמודות אם ורק אם הן שייכות לאותה מחלקה.

**הוכחה:**

■

## 4.4 צופן אניגמה

הגלגלי האתחול של צופן אניגמה הם 3 תמורות 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

$$\alpha_1 = (AELTPHQXRU)(BKNW)(CMOY)(DFG)(IV)(JZ)(S) \in [1^1 2^2 3^1 4^2 10^1],$$

$$\alpha_2 = (A)(JB)(CDKLHUP)(ESZ)(FIXVYOMW)(GR)(NT)(Q) \in [1^2 2^3 3^1 7^1 8^1],$$

$$\alpha_3 = (ABDHPEJT)(CFLVMZOYQIRWUKXSG)(N) \in [1^1 8^1 17^1],$$

$$\rho = (AY)(BR)(CU)(DH)(EQ)(FS)(GL)(IP)(JX)(KN)(MO)(TZ)(VW) \in [2^{13}].$$

### הגדרה 4.10 כלל מצפין וכלל מפענח של צופן אניגמה

יהי  $\pi$  משקף כלשהו מעל האלפבית  $A, \dots, Z$ . הבחירה של המשקף מהווה את הלוח התקעים. יהי  $w = x_1 x_2 \dots x_n$  מילה של טקסט גלוי. לכל  $i = 1, \dots, n$  הכלל מצפין והכלל מפענח של האות במיקום  $i$ -ה בטקסט 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  $\tau_i = \sigma_{-i} \alpha_3 \sigma_i \alpha_2 \alpha_1 \pi$  אזי  $\tau_i^{-1} = \pi \alpha_1^{-1} \alpha_2^{-1} \sigma_{-i} \alpha_3^{-1} \sigma_i$  ולכן

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

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 גלוי

hello .

נניח כי הלוח התקעים הוא

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

חשבו את הטקסט מוצפן.

## פתרון:

$$\underline{x_1 = H} \quad (1)$$

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

$$\underline{x_2 = E} \quad (2)$$

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

$$\underline{x_3 = L} \quad (3)$$

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

$$\underline{x_4 = L} \quad (4)$$

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

$$\underline{x_5 = O} \quad (5)$$

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

לפיכך הטקסט מוצפן הוא: EPSAX.

## דוגמה 4.9 הצפנה על ידי צופן אניגמה

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

## פתרון:



$y_1 = E$  (1)

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

$y_2 = P$  (2)

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

$y_3 = S$  (3)

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

$y_4 = A$  (4)

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

$y_5 = X$  (5)

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



לפיכך הטקסט הגלוי הוא: HELLO.

## 4.5 משפט רייבסקי

### הגדרה 4.11 משקף

תהי  $\Sigma$  קבוצה נוצר סופית באורך זוגי. כלומר  $n = |\Sigma|$  זוגי. תהי  $\rho : \Sigma \rightarrow \Sigma$  תמורה. אומרים כי התמורה  $\rho$  היא משקף אם

$$\rho \in [2^{n/2}].$$

### משפט 4.6 תכונות של תמורה משקפת

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

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

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

## הוכחה:

### כיוון אם

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

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

לכל מחזור  $(a_1 \ a_2 \ \cdots \ a_k)$  המחזור ההפוכי 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  $x \in \Sigma$  אז  $\rho(x) \neq x$ . נניח בשלילה שקיימת נקודה  $x \in \Sigma$  עבורה  $\rho(x) = x$ . אזי  $\rho \in [1^{z_1} \cdots]$  כאשר  $z_1 > 0$ , כלומר  $\rho$  מכילה קיים לפחות מחזור אחד באורך 1, בסתירה לכך ש- $\rho$  היא משקף.

### כיוון רק אם

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

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

כאשר  $(x_1 \ x_2 \ x_3 \ \dots)$  הוא מחזור באורך  $k > 2$ . ז"א ההופכית של  $\rho$  היא

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

בסתירה לכך ש- $\rho^{-1} = \rho$ .

■

## משפט 4.7 הכלל מצפין של אניגמה הוא משקף על האלפבית האנגלית

הכלל מצפין של צופן אניגמה הוא משקף על האלפבית האנגלית

## הוכחה:

הכלל מצפין של צופן אניגמה היא מהצורה:

$$e(x_i) = \Delta_i$$

כאשר

$$\Delta_i = \pi \alpha_1^{-1} \alpha_2^{-1} \sigma_{-i} \alpha_3^{-1} \sigma_i \rho \sigma_{-i} \alpha_3 \sigma_i \alpha_2 \alpha_1 \pi .$$

אם נגדיר את התמורה המורכבת

$$\tau_i = \sigma_{-i} \alpha_3 \sigma_i \alpha_2 \alpha_1 \pi$$

אזי

$$\tau_i^{-1} = \pi \alpha_1^{-1} \alpha_2^{-1} \sigma_{-i} \alpha_3^{-1} \sigma_i$$

ולכן

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

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

■