

## 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.

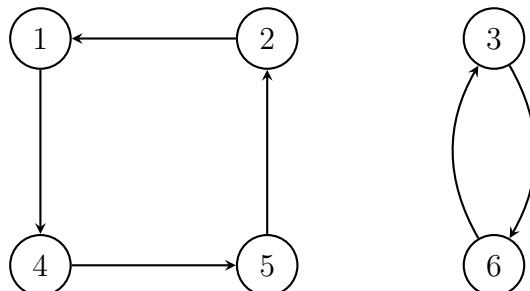
■

**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 |

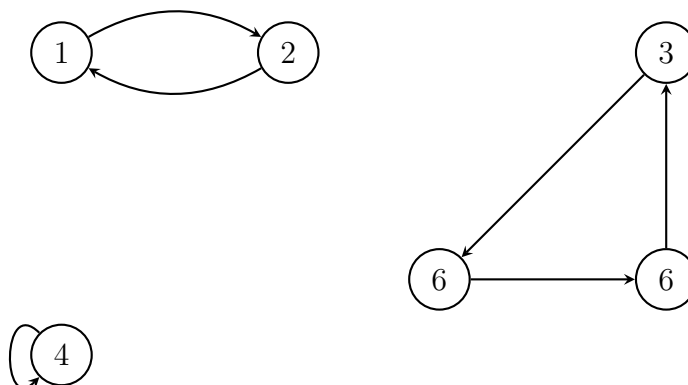
נגדיר הגרף המכוון  $G_\pi = (V, E)$  כאשר הקבוצת הקודקודים היא  $V = \Sigma$ , ולכל  $x \in \Sigma$  נגידר צלע מ- $x$  ל- $\pi(x)$ . אז  $E = \{e_1, e_2, \dots, e_n\}$  כאשר  $e_i = x_i \pi(x_i)$  היא הצלע מקודקוד  $x_i$  לקודקוד  $\pi(x_i)$ . על פי ההגדרה הזאת הגרף  $G_\pi$  של התמורה  $\pi$  היא כמתוארת 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 שייד 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  $\Sigma$ . אם קיימים  $k$  איברים שונים  $a_1, \dots, a_k \in \Sigma$  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 קיים מחזור באורך  $k$  ב- $\pi$  שמסומן:

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

#### משפט 4.3 פירוק למחזורים של תמורה

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

הוכחה: שאלה לעבודת הגשה.

#### 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:

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

#### משפט 4.4

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

הוכחה:

כיוון אם

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

$\Leftarrow$  קיימים איברים שונים  $a_1, \dots, a_k \in \Sigma$  כך ש:  $(a_1 \ a_2 \ \dots \ a_k) \in \pi$ .

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

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

$a_1\pi(a_1), a_2\pi(a_2), \dots, a_{k-1}\pi(a_{k-1}), a_k\pi(a_k) \in E$ .

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

$a_1a_2, a_2a_3, \dots, a_{k-1}a_k, a_k a_1 \in E$ .

$\Leftarrow G_\pi$  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

$a_1a_2, a_2a_3, \dots, a_{k-1}a_k, a_k a_1 \in E$ .

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

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

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

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

■

#### 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 בדיוק  $z_1$  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 4.5 משפט ההזזה של תמורות צמודות

תהיינה  $\sigma : \Sigma \rightarrow \Sigma$  ו- $\pi : \Sigma \rightarrow \Sigma$  תמורות על הקוצה סופית  $\Sigma$ . לכל  $x, y \in \Sigma$  אם  $\sigma(x) = y$  אזי

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

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

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

■

### משפט 4.6 פירוקים למחזורים של תמורות צמודות שווים

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

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

אזי הפירוק למחזורים של  $\pi\sigma\pi^{-1}$  הוא:

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

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

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

מנובע ממשפט כי לכל מחזור 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 המחלקה של תמורות צמודות נשמרת

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

הוכחה:

כיוון אם:

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

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

אזי לפי משפט 4.6 הפירוק למחזורים 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 ל- $\tau$  ול- $\sigma$  יש אותו מבנה של מחזורים ולכן הן שייכות לאותה מחלקה.

כיוון רק אם:

■

## 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 ה- $i$  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:**

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

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

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

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

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

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

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

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

$$\underline{x_5 = 0} \quad (5)$$

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



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:**

$$\underline{y_1 = E} \quad (1)$$

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

$$\underline{y_2 = P} \quad (2)$$

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

$$\underline{y_3 = S} \quad (3)$$

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

$$\underline{y_4 = A} \quad (4)$$

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

$$\underline{y_5 = X} \quad (5)$$

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



לפיכך הטקסט הגלוי הוא: HELLO.

## 4.5 משפט רייבסקי וההתקפה על הצופן האניגמה

### 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 4.8 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:

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

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

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 4.9 הכלל מצפין של אניגמה הוא משקף על האלפבית האנגלית**

הכלל מצפין (והכלל מפענח) של צופן אניגמה הוא משקף על האלפבית האנגלית.

**הוכחה:** הכלל מצפין והכלל מפענח של צופן אניגמה הם

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

כאשר  $\tau_i = \sigma_{-i} \alpha_3 \sigma_i \alpha_2 \alpha_1 \pi$  ו- $\rho$  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 אזי  $\rho \in [2^{13}]$ .

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

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

**משפט 4.10**

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

**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- $\rho(y_1) = x$  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 שמתחיל ב-ICPWLVB. אזי אנחנו יודעים שקיימים  $x, y, z \in \Sigma$  כך ש:

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

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

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

**משפט 4.11 משפט רייבסקי**

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

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

מופיע בפירוק למחזורים של התמורה המורכבת  $\rho_2\rho_1$ , אזי בהכרח המחזור

$$(\rho_1(a_t) \ \rho_1(a_{t-1}) \ \cdots \ \rho_1(a_2) \ \rho_1(a_1))$$

גם מופיע בפירוק למחזורים של התמורה המורכבת  $\rho_2\rho_1$ , ובנוסף הוא שונה מהחזור  $(a_1 \ a_2 \ \cdots \ a_t)$ .

#### דוגמה 4.11

נניח ש-

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

זה בדיוק הסוג של פירוק למחזורים הנקבע על ידי משפט רייבסקי: יש זוג מחזורים באורך 7, זוג מחזורים באורך 5, וזוג מחזורים באורך 1. מכיוון שיש רק שני מחזורים מכל אורך, אזי אנחנו יודעים כיצד להתאים אותם:

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

#### דוגמה 4.12 קריפטו-אנליזה של צופן אניגמה

נתונות התמורות הבאות של צופן אניגמה:

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

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

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

פענחו את הקסט מוצפן

ILBDA

**פתרון:**

**שלב 1) התמורה  $\Delta_4\Delta_1$**

ראשית נסתכל על התמורה  $\Delta_4\Delta_1$ .

|   | $\Delta_4\Delta_1$ | $\Delta_1$ | $\Delta_4$ |
|---|--------------------|------------|------------|
| A | C                  |            |            |
| B | G                  |            |            |
| C | I                  |            |            |
| D | O                  |            |            |
| E | T                  |            |            |
| F | W                  |            |            |
| G | P                  |            |            |
| H | Q                  |            |            |
| I | K                  |            |            |
| J | N                  |            |            |
| K | E                  |            |            |
| L | X                  |            |            |
| M | L                  |            |            |
| N | V                  |            |            |
| O | F                  |            |            |
| P | D                  |            |            |
| Q | B                  |            |            |
| R | Y                  |            |            |
| S | Z                  |            |            |
| T | M                  |            |            |
| U | J                  |            |            |
| V | U                  |            |            |
| W | H                  |            |            |
| X | A                  |            |            |
| Y | S                  |            |            |
| Z | R                  |            |            |

נתחיל עם הזוג תמורות (JNVU) (ZRYS). לפי משפט רייבסקי:

$\Delta_1 (U) = Z$  ,    $\Delta_1 (V) = R$  ,    $\Delta_1 (N) = Y$  ,    $\Delta_1 (J) = S$  .

|   | $\Delta_4\Delta_1$ | $\Delta_1$ | $\Delta_4$ |
|---|--------------------|------------|------------|
| A | C                  |            |            |
| B | G                  |            |            |
| C | I                  |            |            |
| D | O                  |            |            |
| E | T                  |            |            |
| F | W                  |            |            |
| G | P                  |            |            |
| H | Q                  |            |            |
| I | K                  |            |            |
| J | N                  |            |            |
| K | E                  |            |            |
| L | X                  |            |            |
| M | L                  |            |            |
| N | V                  |            |            |
| O | F                  |            |            |
| P | D                  |            |            |
| Q | B                  |            |            |
| R | Y                  |            |            |
| S | Z                  |            |            |
| T | M                  |            |            |
| U | J                  |            |            |
| V | U                  |            |            |
| W | H                  |            |            |
| X | A                  |            |            |
| Y | S                  |            |            |
| Z | R                  |            |            |

עבור הזוג תמורות  $(ACIKETMLX)$   $(GPDFQWHQB)$ , לפי משפט רייבסקי:

$\Delta_1(X) = G$  ,    $\Delta_1(L) = P$  ,    $\Delta_1(M) = D$  ,    $\Delta_1(T) = O$  ,    $\Delta_1(E) = F$  ,  
 $\Delta_1(K) = W$  ,    $\Delta_1(I) = H$  ,    $\Delta_1(C) = Q$  ,    $\Delta_1(A) = B$  .

|   | $\Delta_4\Delta_1$ | $\Delta_1$ | $\Delta_4$ |
|---|--------------------|------------|------------|
| A | C                  | B          |            |
| B | G                  |            |            |
| C | I                  | Q          |            |
| D | O                  |            |            |
| E | T                  | F          |            |
| F | W                  |            |            |
| G | P                  |            |            |
| H | Q                  |            |            |
| I | K                  | H          |            |
| J | N                  | S          |            |
| K | E                  | W          |            |
| L | X                  | P          |            |
| M | L                  | D          |            |
| N | V                  | Y          |            |
| O | F                  |            |            |
| P | D                  |            |            |
| Q | B                  |            |            |
| R | Y                  |            |            |
| S | Z                  |            |            |
| T | M                  | O          |            |
| U | J                  | Z          |            |
| V | U                  | R          |            |
| W | H                  |            |            |
| X | A                  | G          |            |
| Y | S                  |            |            |
| Z | R                  |            |            |

בנוסף  $\Delta_1$  הוא משקף, לכן, אם למשל  $\Delta_1(A) = B$  אז בהכרח  $\Delta_1(B) = A$ . על פי זה אפשר להשלים את העמודה של  $\Delta_1$  של הטבלה:



|   | $\Delta_4\Delta_1$ | $\Delta_1$ | $\Delta_4$ |
|---|--------------------|------------|------------|
| A | C                  | B          |            |
| B | G                  | A          |            |
| C | I                  | Q          |            |
| D | O                  | M          |            |
| E | T                  | F          |            |
| F | W                  | E          |            |
| G | P                  | X          |            |
| H | Q                  | I          |            |
| I | K                  | H          |            |
| J | N                  | S          |            |
| K | E                  | W          |            |
| L | X                  | P          |            |
| M | L                  | D          |            |
| N | V                  | Y          |            |
| O | F                  | T          |            |
| P | D                  | L          |            |
| Q | B                  | C          |            |
| R | Y                  | V          |            |
| S | Z                  | J          |            |
| T | M                  | O          |            |
| U | J                  | Z          |            |
| V | U                  | R          |            |
| W | H                  | K          |            |
| X | A                  | G          |            |
| Y | S                  | N          |            |
| Z | R                  | U          |            |

הערכים של התמורה  $\Delta_4$  נתונים ע"י העמודות  $\Delta_1$  ו- $\Delta_4\Delta_1$ . למשל, לפי השורה הראשונה:

$$\Delta_1(A) = B \quad \text{ו-} \quad \Delta_4(\Delta_1(A)) = C \quad \Rightarrow \quad \Delta_4(B) = C.$$

כדוגמה נוספת, לפי השורה השנייה:

$$\Delta_1(B) = A \quad \text{ו-} \quad \Delta_4(\Delta_1(B)) = G \quad \Rightarrow \quad \Delta_4(A) = G.$$

לפי השורה השלישית:

$$\Delta_1(C) = Q \quad \text{ו-} \quad \Delta_4(\Delta_1(C)) = I \quad \Rightarrow \quad \Delta_4(Q) = I,$$

וכן הלה. באופן הזה אפשר למצוא את כל הערכים של התמורה  $\Delta_4$  על האותיות של האלפבית:

|   | $\Delta_4\Delta_1$ | $\Delta_1$ | $\Delta_4$ |
|---|--------------------|------------|------------|
| A | C                  | B          | G          |
| B | G                  | A          | C          |
| C | I                  | Q          | B          |
| D | O                  | M          | L          |
| E | T                  | F          | W          |
| F | W                  | E          | T          |
| G | P                  | X          | A          |
| H | Q                  | I          | K          |
| I | K                  | H          | Q          |
| J | N                  | S          | Z          |
| K | E                  | W          | H          |
| L | X                  | P          | D          |
| M | L                  | D          | O          |
| N | V                  | Y          | S          |
| O | F                  | T          | M          |
| P | D                  | L          | X          |
| Q | B                  | C          | I          |
| R | Y                  | V          | U          |
| S | Z                  | J          | N          |
| T | M                  | O          | F          |
| U | J                  | Z          | R          |
| V | U                  | R          | Y          |
| W | H                  | K          | E          |
| X | A                  | G          | P          |
| Y | S                  | N          | V          |
| Z | R                  | U          | J          |

שלב 2) התמורה  $\Delta_5\Delta_2$

כעת נסתכל על התמורה  $\Delta_5\Delta_2$ :

|   | $\Delta_5 \Delta_2$ | $\Delta_2$ | $\Delta_5$ |
|---|---------------------|------------|------------|
| A | I                   |            |            |
| B | P                   |            |            |
| C | E                   |            |            |
| D | O                   |            |            |
| E | U                   |            |            |
| F | V                   |            |            |
| G | Q                   |            |            |
| H | J                   |            |            |
| I | A                   |            |            |
| J | S                   |            |            |
| K | G                   |            |            |
| L | R                   |            |            |
| M | Z                   |            |            |
| N | W                   |            |            |
| O | D                   |            |            |
| P | M                   |            |            |
| Q | C                   |            |            |
| R | N                   |            |            |
| S | T                   |            |            |
| T | Y                   |            |            |
| U | K                   |            |            |
| V | L                   |            |            |
| W | F                   |            |            |
| X | B                   |            |            |
| Y | H                   |            |            |
| Z | X                   |            |            |

נתחיל עם הזוג תמורות (IA) (DO). לפי משפט רייבסקי:

$$\Delta_2(A) = D, \quad \Delta_2(I) = O.$$

עבור הזוג תמורות (CEUKGQ) (NWFVLR), לפי משפט רייבסקי:

$$\Delta_2(Q) = N, \quad \Delta_2(G) = W, \quad \Delta_2(K) = F, \quad \Delta_2(U) = V, \quad \Delta_2(E) = L, \quad \Delta_2(C) = R.$$

עבור הזוג תמורות (BPMZX) (STYHJ), לפי משפט רייבסקי:

$$\Delta_2(X) = S, \quad \Delta_2(Z) = T, \quad \Delta_2(M) = Y, \quad \Delta_2(P) = H, \quad \Delta_2(B) = J.$$

|   | $\Delta_5\Delta_2$ | $\Delta_2$ | $\Delta_5$ |
|---|--------------------|------------|------------|
| A | I                  | D          |            |
| B | P                  | J          |            |
| C | E                  | R          |            |
| D | O                  |            |            |
| E | U                  | L          |            |
| F | V                  |            |            |
| G | Q                  | W          |            |
| H | J                  |            |            |
| I | A                  | O          |            |
| J | S                  |            |            |
| K | G                  | F          |            |
| L | R                  |            |            |
| M | Z                  | Y          |            |
| N | W                  |            |            |
| O | D                  |            |            |
| P | M                  |            |            |
| Q | C                  | N          |            |
| R | N                  |            |            |
| S | T                  |            |            |
| T | Y                  |            |            |
| U | K                  | V          |            |
| V | L                  |            |            |
| W | F                  |            |            |
| X | B                  | S          |            |
| Y | H                  |            |            |
| Z | X                  | T          |            |

בנוסף  $\Delta_2$  הוא משקף, לכן, אם למשל  $\Delta_2(A) = D$  אז בהכרח  $\Delta_2(D) = A$ . על פי זה אפשר להשלים את העמודה של  $\Delta_2$  של הטבלה:

|   | $\Delta_5 \Delta_2$ | $\Delta_2$ | $\Delta_5$ |
|---|---------------------|------------|------------|
| A | I                   | D          |            |
| B | P                   | J          |            |
| C | E                   | R          |            |
| D | O                   | A          |            |
| E | U                   | L          |            |
| F | V                   | K          |            |
| G | Q                   | W          |            |
| H | J                   | P          |            |
| I | A                   | O          |            |
| J | S                   | B          |            |
| K | G                   | F          |            |
| L | R                   | E          |            |
| M | Z                   | Y          |            |
| N | W                   | Q          |            |
| O | D                   | I          |            |
| P | M                   | H          |            |
| Q | C                   | N          |            |
| R | N                   | C          |            |
| S | T                   | X          |            |
| T | Y                   | Z          |            |
| U | K                   | V          |            |
| V | L                   | U          |            |
| W | F                   | G          |            |
| X | B                   | S          |            |
| Y | H                   | M          |            |
| Z | X                   | T          |            |

הערכים של התמורה  $\Delta_5$  נתונים ע"י העמודות  $\Delta_2$  ו- $\Delta_5 \Delta_2$ . למשל, לפי השורה הראשונה:

$$\Delta_2(A) = D \quad \text{ו-} \quad \Delta_5(\Delta_2(A)) = I \quad \Rightarrow \quad \Delta_5(D) = I.$$

כדוגמה נוספת, לפי השורה השנייה:

$$\Delta_2(B) = J \quad \text{ו-} \quad \Delta_5(\Delta_2(B)) = P \quad \Rightarrow \quad \Delta_5(J) = P.$$

לפי השורה השלישית:

$$\Delta_2(C) = R \quad \text{ו-} \quad \Delta_5(\Delta_2(C)) = E \quad \Rightarrow \quad \Delta_5(R) = E,$$

וכן הלה. באופן הזה אפשר למצוא את כל הערכים של התמורה  $\Delta_5$  על האותיות של האלפבית:

|   | $\Delta_5\Delta_2$ | $\Delta_2$ | $\Delta_5$ |
|---|--------------------|------------|------------|
| A | I                  | D          | O          |
| B | P                  | J          | S          |
| C | E                  | R          | N          |
| D | O                  | A          | I          |
| E | U                  | L          | R          |
| F | V                  | K          | G          |
| G | Q                  | W          | F          |
| H | J                  | P          | M          |
| I | A                  | O          | D          |
| J | S                  | B          | P          |
| K | G                  | F          | V          |
| L | R                  | E          | U          |
| M | Z                  | Y          | H          |
| N | W                  | Q          | C          |
| O | D                  | I          | A          |
| P | M                  | H          | J          |
| Q | C                  | N          | W          |
| R | N                  | C          | E          |
| S | T                  | X          | B          |
| T | Y                  | Z          | X          |
| U | K                  | V          | L          |
| V | L                  | U          | K          |
| W | F                  | G          | Q          |
| X | B                  | S          | T          |
| Y | H                  | M          | Z          |
| Z | X                  | T          | Y          |

שלב 3) התמורה  $\Delta_6\Delta_3$

כעת נסתכל על התמורה  $\Delta_6\Delta_3$ :

|   | $\Delta_6\Delta_3$ | $\Delta_3$ | $\Delta_6$ |
|---|--------------------|------------|------------|
| A | G                  |            |            |
| B | I                  |            |            |
| C | N                  |            |            |
| D | H                  |            |            |
| E | M                  |            |            |
| F | P                  |            |            |
| G | L                  |            |            |
| H | R                  |            |            |
| I | Z                  |            |            |
| J | V                  |            |            |
| K | C                  |            |            |
| L | Y                  |            |            |
| M | O                  |            |            |
| N | K                  |            |            |
| O | E                  |            |            |
| P | X                  |            |            |
| Q | D                  |            |            |
| R | S                  |            |            |
| S | U                  |            |            |
| T | J                  |            |            |
| U | Q                  |            |            |
| V | F                  |            |            |
| W | B                  |            |            |
| X | T                  |            |            |
| Y | A                  |            |            |
| Z | W                  |            |            |

נתחיל עם הזוג תמורות (CNK) (MOE). לפי משפט רייבסקי:

$\Delta_3(K) = M$  ,  $\Delta_3(N) = O$  ,  $\Delta_3(C) = E$  .

עבור הזוג תמורות (AGLY) (WBIZ), לפי משפט רייבסקי:

$\Delta_3(Y) = W$  ,  $\Delta_3(L) = B$  ,  $\Delta_3(G) = I$  ,  $\Delta_3(A) = Z$  .

עבור הזוג תמורות (DHRSUQ) (VFPXTJ), לפי משפט רייבסקי:

$\Delta_3(Q) = V$  ,  $\Delta_3(U) = F$  ,  $\Delta_3(S) = P$  ,  $\Delta_3(R) = X$  ,  $\Delta_3(H) = T$  ,  $\Delta_3(D) = J$  .

|   | $\Delta_6\Delta_3$ | $\Delta_3$ | $\Delta_6$ |
|---|--------------------|------------|------------|
| A | G                  | Z          |            |
| B | I                  |            |            |
| C | N                  | E          |            |
| D | H                  | J          |            |
| E | M                  |            |            |
| F | P                  |            |            |
| G | L                  | I          |            |
| H | R                  | T          |            |
| I | Z                  |            |            |
| J | V                  |            |            |
| K | C                  | M          |            |
| L | Y                  | B          |            |
| M | O                  |            |            |
| N | K                  | O          |            |
| O | E                  |            |            |
| P | X                  |            |            |
| Q | D                  | V          |            |
| R | S                  | X          |            |
| S | U                  | P          |            |
| T | J                  |            |            |
| U | Q                  | F          |            |
| V | F                  |            |            |
| W | B                  |            |            |
| X | T                  |            |            |
| Y | A                  | W          |            |
| Z | W                  |            |            |

בנוסף  $\Delta_3$  הוא משקף, לכן, אם למשל  $\Delta_3(A) = Z$  אז בהכרח  $\Delta_3(Z) = A$ . על פי זה אפשר להשלים את העמודה של  $\Delta_3$  של הטבלה:



|   | $\Delta_6\Delta_3$ | $\Delta_3$ | $\Delta_6$ |
|---|--------------------|------------|------------|
| A | G                  | Z          |            |
| B | I                  | L          |            |
| C | N                  | E          |            |
| D | H                  | J          |            |
| E | M                  | C          |            |
| F | P                  | U          |            |
| G | L                  | I          |            |
| H | R                  | T          |            |
| I | Z                  | G          |            |
| J | V                  | D          |            |
| K | C                  | M          |            |
| L | Y                  | B          |            |
| M | O                  | K          |            |
| N | K                  | O          |            |
| O | E                  | N          |            |
| P | X                  | S          |            |
| Q | D                  | V          |            |
| R | S                  | X          |            |
| S | U                  | P          |            |
| T | J                  | H          |            |
| U | Q                  | F          |            |
| V | F                  | Q          |            |
| W | B                  | Y          |            |
| X | T                  | R          |            |
| Y | A                  | W          |            |
| Z | W                  | A          |            |

הערכים של התמורה  $\Delta_6$  נתונים ע"י העמודות  $\Delta_3$  ו- $\Delta_6\Delta_3$ . למשל, לפי השורה הראשונה:

$$\Delta_3(A) = Z \quad \text{ו-} \quad \Delta_6(\Delta_3(A)) = G \quad \Rightarrow \quad \Delta_6(Z) = G.$$

כדוגמה נוספת, לפי השורה השנייה:

$$\Delta_3(B) = L \quad \text{ו-} \quad \Delta_6(\Delta_3(B)) = I \quad \Rightarrow \quad \Delta_6(L) = I.$$

לפי השורה השלישית:

$$\Delta_3(C) = E \quad \text{ו-} \quad \Delta_6(\Delta_3(C)) = N \quad \Rightarrow \quad \Delta_6(E) = N,$$

וכן הלה. באופן הזה אפשר למצוא את כל הערכים של התמורה  $\Delta_6$  על האותיות של האלפבית:

|   | $\Delta_6\Delta_3$ | $\Delta_3$ | $\Delta_6$ |
|---|--------------------|------------|------------|
| A | G                  | Z          | W          |
| B | I                  | L          | Y          |
| C | N                  | E          | M          |
| D | H                  | J          | V          |
| E | M                  | C          | N          |
| F | P                  | U          | Q          |
| G | L                  | I          | Z          |
| H | R                  | T          | J          |
| I | Z                  | G          | L          |
| J | V                  | D          | H          |
| K | C                  | M          | O          |
| L | Y                  | B          | I          |
| M | O                  | K          | C          |
| N | K                  | O          | E          |
| O | E                  | N          | K          |
| P | X                  | S          | U          |
| Q | D                  | V          | F          |
| R | S                  | X          | T          |
| S | U                  | P          | X          |
| T | J                  | H          | R          |
| U | Q                  | F          | P          |
| V | F                  | Q          | D          |
| W | B                  | Y          | A          |
| X | T                  | R          | S          |
| Y | A                  | W          | B          |
| Z | W                  | A          | G          |

**שלב 4) פענוח:**

$$\Delta_1(\sigma_1) = I, \quad \Delta_2(\sigma_2) = L, \quad \Delta_3(\sigma_3) = B, \quad \Delta_4(\sigma_4) = D, \quad \Delta_5(\sigma_5) = A.$$

לפיכך:

$$\sigma_1 = \Delta_1(I) = H,$$

$$\sigma_2 = \Delta_2(L) = E,$$

$$\sigma_3 = \Delta_3(B) = L,$$

$$\sigma_4 = \Delta_4(D) = L,$$

$$\sigma_5 = \Delta_5(A) = O.$$

