שיעור 4
תמורות וצופן אניגמה

4.1 תמורות

הגדרה 4.1 תמורה

תמורה על קבוצה סופית $\Sigma = \{x_1, \ldots, x_n\}$ היא פונקציה $\pi : \Sigma \to \Sigma$ אשר היא חד-חד ערכית ו "על" Σ. בהינתן $x_i \in \Sigma$ ותמורה π. אזי

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

תזכורת:

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

כתוצאה מכך, אם π פועלת על כל האיברים של Σ אזי נקבל אותה קבוצה Σ רק לא באותו בסדר של הסדר המקורי:

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

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 Σ קבוצה סופית ותהי $\pi : \Sigma \to \Sigma$ פונקציה. הוכיחו: אם π חד-חד ערכית אז היא תמורה.

פתרון:

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

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

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

לכן

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

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

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

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

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

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

ולפיכך $\pi : \Sigma \to \Sigma$ היא פונקציה "על" Σ.

■

הגדרה 4.2 הרכבה של תמורות

תהי Σ קבוצה נוצר סופית ותהיינה $\pi : \Sigma \to \Sigma$ ו- $\sigma : \Sigma \to \Sigma$ תמורות על הקבוצה Σ. ההרכבה של π ו- σ 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 π פועלת על x ואז σ פועלת על $\pi(x)$".

דוגמה 4.4

נתון התמורות π ו- σ:

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 ההרבה $\sigma\pi$ היא:

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

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

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

כלומר $\sigma\pi \neq \pi\sigma$.

משפט 4.1 הרכבה של תמורות היא תמורה

תהי Σ קבוצה נוצר סופית ותהיינה $\pi : \Sigma \to \Sigma$ ו- $\sigma : \Sigma \to \Sigma$ תמורות על הקבוצה Σ. ההרכבה $\sigma\pi$ היא תמורה על Σ.

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

- <u>**חח"ע**</u>

  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- π תמורה אז π חח"ע ולכן $y_1 \neq y_2$. ומכיוון ש- σ 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.

- **<u>על</u>**

ניח 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" Σ.

■

הגדרה 4.3 תמורות מתחלפות

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

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

הגדרה 4.4 תמורות מתחלפות

תהי $\pi : \Sigma \to \Sigma$ תמורה על הקבוצה Σ. התמורה ההופכית של π מסומנת π^{-1} ומוגדרת:

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

לכל $x \in \Sigma$.

דוגמה 4.5

נתונה התמורה π:

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 ונקודה זזה

תהי $\pi : \Sigma \to \Sigma$ תמורה.

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

הגדרה 4.6 תמורה הזהות

התמורה הזהות מסומנת $\mathrm{id}:\Sigma\to\Sigma$ ומוגדרת כך שלכל $x\in\Sigma$:

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

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

משפט 4.2 תמורה ההופכית של תמורה מורכבת

תהיינה $\pi_1,\cdots,\pi_t$ תמורות על הקבוצה Σ. אזי

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

הוכחה: נוכיח את הטענה באינדוקציה.

<u>שלב הבסיס</u>

עבור $t=2$, לכל $x\in\Sigma$ יש לנו:

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

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

<u>שלב האינדוקציה</u>

נניח כי הטעהה 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 בההנחת האינדוקציה שלנו כדי להוכיח את הטענה עבור $t=k+1$:

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

כאשר במעבר האחרון השתמשנו בההנחת האינדוקציה.

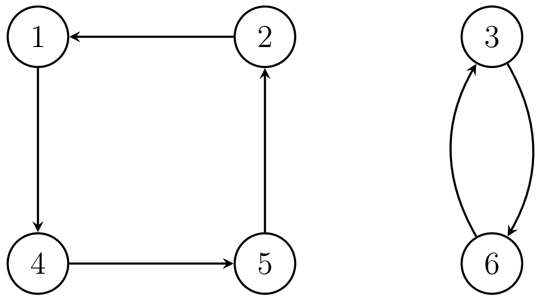
■

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 π 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

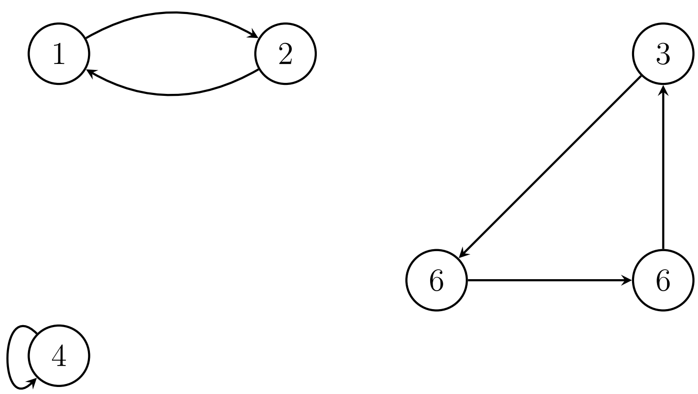
נגדיר הגרף המכוון $G_\pi = (V, E)$ כאשר הקבוצת הקודקודים היא $V = \Sigma$, ולכל $x \in \Sigma$ נגדיר צלע מ- x ל- $\pi(x)$. ז"א $E = \{e_1, e_2, \ldots, e_n\}$ כאשר $e_i = x_i\pi(x_i)$ היא הצלע מקודקוד x_i לקודקוד $\pi(x_i)$. על פי ההגדרה הזאת הגרף G_π של התמורה π היא כמתוארת באיור למטה.



כדוגמה נוספת אם σ היא התמורה

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

אזי הגרף G_σ הינו:



בגרף של תמורה, כל קודקוד שייך לבדיוק מעגל מכוון אחד (שייתכן הוא עובר דרך קודקוד אחד בלבד). הרי קיים התאמה אחת-אחת בין תמורה על Σ לבין גרף שמכסה כל המעגלים המכוונים של Σ. התופעה זו היא המוטיבציה לסימון מחזורים של תמורות.

הגדרה 4.7 מחזור

תהי $\Sigma \to \Sigma : \pi$ תמורה על הקבוצה Σ. אם קיימים k איברים שונים $a_1, \quad \ldots \quad, a_k \in \Sigma$ כך ש-

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

אז אומרים כי קיים מחזור באורך k ב- π שמסומן:

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_k \end{pmatrix} \ .$$

משפט 4.3 פירוק למחזורים של תמורה

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

הוכחה: שאלה לעבודת הגשה. ■

דוגמה 4.6

נתונה התמורה π:

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

הפירוק למחזורים הוא:

$$\pi = \begin{pmatrix} 1 & 4 & 6 \end{pmatrix}\begin{pmatrix} 2 & 5 & 3 \end{pmatrix}\begin{pmatrix} 8 & 7 \end{pmatrix}$$

משפט 4.4

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

הוכחה:

<u>כיוון אם</u>

נניח ש- π מכילה מחזור באורך k.

$\Leftarrow$ קיימים איברים שונים $a_1,\ldots,a_k \in \Sigma$ כך ש: $\begin{pmatrix} a_1 & a_2 & \ldots & \subseteq a_k \end{pmatrix} \in \pi$.

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

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

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

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

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

$\Leftarrow$ G_π מכילה מעגל המילטוני באורך k.

<u>כיוון רק אם</u>

נניח ש- G_π מכיל מעגל המילטוני באורך k.

$\Leftarrow$ קיימים קבוצות $a_1,\ldots,a_k \in \Sigma$ עבורם

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

$\Leftarrow$ מכיוון ש- G_π הוא הגרף של התמורה π אזי

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

$\Leftarrow$ π מכילה מחזור באורך k:

$$\begin{pmatrix} a_1 & a_2 & \ldots & \subseteq a_k \end{pmatrix} \subseteq \pi\ .$$

■

הגדרה 4.8 המחלקה של תמורה

תהי $\pi : \Sigma \to \Sigma$ תמורה. אומרים כי π שייכת למחלקה $[1^{z_1} 2^{z_2} \cdots n^{z_n}]$ אם בפירוק למחזורים של π יש בדיוק z_1 מחזורים באורך- 1, z_2 מחזורים באורך- 2, z_3 מחזורים באורך- 3, וכן הלה.

במילים אחרות:

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

אם לכל $i = 1, \ldots, n$ בפירוק למחזורים של π 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 π, σ תמורות על הקבוצה סופית Σ. התמורה הצמודה של σ על ידי π היא המורה המורכבת $\pi\sigma\pi^{-1}$.

משפט 4.5 משפט ההזזה של תמורות צמודות

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

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

הוכחה: נניח ש: $\sigma(x) = y$. אזי

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

■

משפט 4.6 פירוקים למחזורים של תמורות צמודות שווים

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

$$\sigma = \begin{pmatrix} a_1 & a_2 & \cdots & a_k \end{pmatrix} \begin{pmatrix} b_1 & b_2 & \cdots & b_l \end{pmatrix} \cdots \ .$$

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

$$\pi\sigma\pi^{-1} = \begin{pmatrix} \pi\left(a_1\right) & \pi\left(a_2\right) & \cdots & \pi\left(a_k\right) \end{pmatrix} \begin{pmatrix} \pi\left(b_1\right) & \pi\left(b_2\right) & \cdots & \pi\left(b_l\right) \end{pmatrix} \cdots \ .$$

הוכחה: עבור כל מחזור $\left(a_1 \quad a_2 \quad \ldots \quad a_k\right)$ של σ, מתקיים

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

מנובע ממשפט כי לכל מחזור של σ מתקיים:

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

■

משפט 4.7 המחלקה של תמורות צמודות נשמרת

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

הוכחה:

<u>כיוון אם:</u>

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

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

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

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

ולכן ל- τ ול- σ יש אותו מבנה של מחזורים ולכן הן שייכות לאותה מחלקה.

<u>כיוון רק אם:</u>

■

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

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

הגדרה 4.10 כלל מצפין וכלל מפענח של צופן אניגמה

יהי π משקף כלשהו מעל האלפבית $A,\ldots,Z$. הבחירה של המשקף מהווה את הלוח התקעים.
יהי $w=x_1x_2\ldots x_n$ מילה של טקסט גלוי. לכל $i=1,\ldots,n$ הכלל מצפין והכלל מפענח של האות במיקום ה-i בטקסט הם:

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

כאשר Δ_i היא התמורה המורכבת

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

כאשר

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

אם נגדיר את התמורה המורכבת $\tau_i=\sigma_{-i}\,\alpha_3\,\sigma_i\,\alpha_2\,\alpha_1\,\pi$ 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 $i=1,\ldots,n$ התמורה המורכבת, Δ_i היא הצמודה של ρ על ידי τ_i.

דוגמה 4.8 הצפנה על ידי צופן אניגמה

נתון הטקסט גלוי

$$\texttt{hello}\ .$$

נניח כי הלוח התקעים הוא

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

חשבו את הטקסט מוצפן.

פתרון:

(1 $x_1=\texttt{H}$

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

(2 $x_2=\texttt{E}$

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

3) $\underline{x_3 = \mathtt{L}}$

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

4) $\underline{x_4 = \mathtt{L}}$

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

5) $\underline{x_5 = \mathtt{O}}$

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

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:

1) $\underline{y_1 = \mathtt{E}}$

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

2) $\underline{y_2 = \mathtt{P}}$

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

3) $\underline{y_3 = \mathtt{S}}$

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

(4 $y_4 = \text{A}$

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

(5 $y_5 = \text{X}$

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

לפיכך הטקסט הגלוי הוא: HELLO. ∎

4.5 משפט רייבסקי

הגדרה 4.11 תמורה משקפת

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

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

משפט 4.8 תכונות של תמורה משקפת

תהי Σ קבוצה נוצר סופית באורך זוגי, ותהי $\rho:\Sigma\to\Sigma$ תמורה. אזי ρ 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 ρ משקף. נראה כי $\rho=\rho^{-1}$ באופן הבא. נניח ש:

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

לכל מחזור $\left(a_1\ a_2\ \cdots\ a_k\right)$ המחזור ההפוכי הוא $\left(a_k\ a_{k-1}\ \cdots\ a_1\right)=\left(a_1\ a_2\ \cdots\ a_k\right)^{-1}$. לכן

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

כעת נראה שאם $x\in\Sigma$ אז $\rho(x)\neq x$. נניח בשלילה שקיימת נקודה $x\in\Sigma$ עבורה $\rho(x)=x$. אזי $\rho\in\left[1^{z_1}\cdots\right]$ כאשר $z_1>0$, כלומר ρ מכילה קיים לפחות מחזור אחד באורך 1, בסתירה לכך ש- ρ היא משקף.

<u>כיוון רק אם</u>

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

$$\rho = (x_1\ x_2\ x_3\ \ldots\ )\,\rho' \quad ,$$

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

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

בסתירה לכך ש- $\rho = \rho^{-1}$. ■

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

הכלל מצפין (והכלל מפענח) של צופן אניגמה הוא תמורה משקפת 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- ρ המשקף הקבוע של צופן אניגנה.

⇐ לכל $i = 1, \ldots, n$ התמורה המורכבת Δ_i היא הצמודה של ρ על ידי τ_i.

⇐ מכיוון ש: ρ הוא משקף על האלפיבית האנגלית אזי $\rho \in [2^{13}]$.

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

⇐ לפי הגדרה 4.11 התמורה Δ_i היא תמורה משקפת.

■

משפט 4.10 כלל של זוג תמורות משקפות

יהיו ρ_1 ו- ρ_2 תמורות משקפות על הקבוצה סופית Σ.

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

הוכחה:

<u>כיוון אם</u>

תהיינה ρ_1, ρ_2 תמורות משקפות ויהי $x \in \Sigma$.

$$\left.\begin{aligned} y_1 &= \rho_1(x) \\ y_2 &= \rho_2(x) \end{aligned}\right\} \xRightarrow{\rho_1 \text{ משקפת}} \quad x = \rho_1(y_1) \quad \Rightarrow \quad \rho_2(\rho_1(y_1)) = \rho_2(x) = y_2 \ .$$

כיוון רק אם

נניח ש: $y_2 = \rho_2\left(\rho_1\left(y_1\right)\right)$. מכיוון ש- ρ_2 תמורה משקפת אזי $\rho_1\left(y_1\right)=\rho_2\left(y_2\right)$ לכן קיים $x\in\Sigma$ כך ש:

$$\left.\begin{aligned} y_1 &= \rho_1(x) \\ y_2 &= \rho_2(x) \end{aligned}\right\} \xRightarrow{\text{משקפות } \rho_1,\rho_2} \left.\begin{aligned} \rho_1(y_1) &= x \\ \rho_2(y_2) &= x \end{aligned}\right\} \quad\Rightarrow\quad \rho_1\left(y_1\right)=x=\rho_2\left(y_2\right) .$$

■

4.6 ההנחות של רייבסקי על צופן האניגמה

במהלך מלחמת העולם הראשונה כל הודעה שהוצפנה על ידי צופן האניגמה התחילה במילה משוכפלת בת 6 אותיות:

$$xyzxyz \ ,$$

כלומר ה- 3 אותיות הראשונות היו זהות ל- 3 אותיות האחרונות. המילה הזאת נקראת המילה האופיינית של ההודעה.

הגדרה 4.12 ההנחות של רייבסקי

1) כל הודעה מוצפנת מתחילה במילה האופיינית.

2) הכלל מצפין של כל אות הוא קבוע ואינו משתנה באותו יום.

דוגמה 4.10

נתונה הודעה מוצפנת שמתחילה במילה אופיינית הבאה:

$$\texttt{ICPWLV} \ .$$

על פי ההנחות של רייבסקי קיימים $x,y,z\in\Sigma$ עבורם:

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

כאשר Δ_i הוא הכלל מצפין של צופן האניגמה של אות ה- i של המילה. ז"א:

$$\begin{aligned} &\Delta_1(x)=\texttt{I} \ , &&\Delta_2(y)=\texttt{C} \ , &&\Delta_3(z)=\texttt{P} \ , \\ &\Delta_4(x)=\texttt{W} \ , &&\Delta_5(y)=\texttt{L} \ , &&\Delta_6(z)=\texttt{V} \ . \end{aligned}$$

Δ_i היא תמורה משקפת, לכן:

$$\Delta_1(\texttt{I})=x \ , \qquad \Delta_2(\texttt{C})=y \ , \qquad \Delta_3(\texttt{P})=z \ ,$$

לפיכך:

$$\Delta_4\Delta_1\left(\texttt{I}\right)=\texttt{W} \ , \qquad \Delta_5\Delta_2\left(\texttt{C}\right)=\texttt{L} \ , \qquad \Delta_6\Delta_3\left(\texttt{P}\right)=\texttt{V} \ .$$

דוגמה 4.11

הטבלה הבאה מראה מילים אופייניות מהודעות מוצפנות מאותו יום.

```
FDZWOW  YRVSNF  XASAIU  OYDFHH  PXFDBP  REQYUD
BLHGRR  LUBXKI  KGYEQA  APMCMO  JCENEM  KHREJS
HJNQSK  TTGMYL  SZWZXB  ZFPRVX  QMUBZQ  IWIKFZ
NSXVTT  DKJOGV  ENLTWY  CWAIFG  GITPAJ  WOOHDE
VQAUCG  MVKLLC  UBCJPN
```

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

פתרון:

$$\Delta_4\Delta_1 = (\mathtt{ZRYS})(\mathtt{JNVU})(\mathtt{GPDOFWHQB})(\mathtt{ACIKETMLX}) \ ,$$
$$\Delta_5\Delta_2 = (\mathtt{DO})(\mathtt{IA})(\mathtt{STYHJ})(\mathtt{BPMZX})(\mathtt{NWFVLR})(\mathtt{CEUKGQ}) \ ,$$
$$\Delta_6\Delta_3 = (\mathtt{MOE})(\mathtt{CNK})(\mathtt{WBIZ})(\mathtt{AGLY})(\mathtt{VFPXTJ})(\mathtt{DHRSUQ}) \ .$$

■

משפט 4.11 משפט רייבסקי

יהיו ρ_1 ו- ρ_2 משקפים על הקבוצה סופית Σ. אם המחזור

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_t \end{pmatrix}$$

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

$$\begin{pmatrix} \rho_1(a_t) & \rho_1(a_{t-1}) & \cdots & \rho_1(a_2) & \rho_1(a_1) \end{pmatrix}$$

גם מופיע בפירוק למחזורים של התמורה המורכבת $\rho_2\rho_1$, ובנוסף הוא שונה מהחזור $\begin{pmatrix} a_1 & a_2 & \cdots & a_t \end{pmatrix}$.

דוגמה 4.12

נניח ש-

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

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:

$$(\mathtt{OGKRYSD})(\mathtt{ZUQWFIB}) = (\mathtt{OGKRYSD})\Big(\Delta_1(\mathtt{D})\,\Delta_1(\mathtt{S})\,\Delta_1(\mathtt{Y})\,\Delta_1(\mathtt{R})\,\Delta_1(\mathtt{K})\,\Delta_1(\mathtt{G})\,\Delta_1(\mathtt{O})\Big)$$

דוגמה 4.13 קריפטו-אנליזה של צופן אניגמה

נתונות התמורות הבאות של צופן אניגמה:

$$\Delta_4\Delta_1 = (\mathtt{ZRYS})(\mathtt{JNVU})(\mathtt{GPDOFWHQB})(\mathtt{ACIKETMLX}) \ ,$$
$$\Delta_5\Delta_2 = (\mathtt{DO})(\mathtt{IA})(\mathtt{STYHJ})(\mathtt{BPMZX})(\mathtt{NWFVLR})(\mathtt{CEUKGQ}) \ ,$$
$$\Delta_6\Delta_3 = (\mathtt{MOE})(\mathtt{CNK})(\mathtt{WBIZ})(\mathtt{AGLY})(\mathtt{VFPXTJ})(\mathtt{DHRSUQ}) \ .$$

פענחו את הקסט מוצפן

ILBDA

פתרון:

שלב 1) התמורה $\Delta_4\Delta_1$

ראשית נסתכל על התמורה $\Delta_4\Delta_1$.

	$\Delta_4\Delta_1$	Δ_1	Δ_4
A	C		
B	G		
C	I		
D	O		
E	T		
F	W		
G	P		
H	Q		
I	K		

	$\Delta_4\Delta_1$	Δ_1	Δ_4
J	N		
K	E		
L	X		
M	L		
N	V		
O	F		
P	D		
Q	B		
R	Y		

	$\Delta_4\Delta_1$	Δ_1	Δ_4
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:

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

עבור הזוג תמורות (ACIKETMLX) (GPDOFWHQB), לפי משפט רייבסקי:

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

	$\Delta_4\Delta_1$	Δ_1	Δ_4
A	C	B	
B	G		
C	I	Q	
D	O		
E	T	F	
F	W		
G	P		
H	Q		
I	K	H	

	$\Delta_4\Delta_1$	Δ_1	Δ_4
J	N	S	
K	E	W	
L	X	P	
M	L	D	
N	V	Y	
O	F		
P	D		
Q	B		
R	Y		

	$\Delta_4\Delta_1$	Δ_1	Δ_4
S	Z		
T	M	O	
U	J	Z	
V	U	R	
W	H		
X	A	G	
Y	S		
Z	R		

בנוסף Δ_1 היא תמורה משקפת, לכן, אם למשל $\Delta_1(\mathtt{A}) = \mathtt{B}$ אז בהכרח $\Delta_1(\mathtt{B}) = \mathtt{A}$. על פי זה אפשר להשלים את העמודה של Δ_1 של הטבלה:

	$\Delta_4\Delta_1$	Δ_1	Δ_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 Δ_4 נתונים ע"י העמודות Δ_1 ו- $\Delta_4\Delta_1$. למשל, לפי השורה הראשונה:

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

כדוגמה נוספת, לפי השורה השנייה:

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

לפי השורה השלישית:

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

וכן הלה. באופן הזה אפשר למצוא את כל הערכים של התמורה Δ_4 על האותיות של האלפבית:

	$\Delta_4\Delta_1$	Δ_1	Δ_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 $\Delta_5\Delta_2$:

	$\Delta_5\Delta_2$	Δ_2	Δ_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 $(\mathtt{DO})(\mathtt{IA})$. לפי משפט רייבסקי:

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

עבור הזוג תמורות $(\mathtt{NWFVLR})(\mathtt{CEUKGQ})$, לפי משפט רייבסקי:

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

עבור הזוג תמורות $(\mathtt{STYHJ})(\mathtt{BPMZX})$, לפי משפט רייבסקי:

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

	$\Delta_5\Delta_2$	Δ_2	Δ_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	

	$\Delta_5\Delta_2$	Δ_2	Δ_5
J	S		
K	G	F	
L	R		
M	Z	Y	
N	W		
O	D		
P	M		
Q	C	N	
R	N		

	$\Delta_5\Delta_2$	Δ_2	Δ_5
S	T		
T	Y		
U	K	V	
V	L		
W	F		
X	B	S	
Y	H		
Z	X	T	

בנוסף Δ_2 הוא משקף, לכן, אם למשל $\Delta_2(\mathtt{A})=\mathtt{D}$ אז בהכרח $\Delta_2(\mathtt{D})=\mathtt{A}$. על פי זה אפשר להשלים את העמודה של Δ_2 של הטבלה:

	$\Delta_5\Delta_2$	Δ_2	Δ_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	

	$\Delta_5\Delta_2$	Δ_2	Δ_5
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	

	$\Delta_5\Delta_2$	Δ_2	Δ_5
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 Δ_5 נתונים ע"י העמודות Δ_2 ו- $\Delta_5\Delta_2$. למשל, לפי השורה הראשונה:

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

כדוגמה נוספת, לפי השורה השנייה:

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

לפי השורה השלישית:

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

וכן הלה. באופן הזה אפשר למצוא את כל הערכים של התמורה Δ_5 על האותיות של האלפבית:

	$\Delta_5\Delta_2$	Δ_2	Δ_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

	$\Delta_5\Delta_2$	Δ_2	Δ_5
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

	$\Delta_5\Delta_2$	Δ_2	Δ_5
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 $\Delta_6\Delta_3$:

	$\Delta_6\Delta_3$	Δ_3	Δ_6
A	G		
B	I		
C	N		
D	H		
E	M		
F	P		
G	L		
H	R		
I	Z		

	$\Delta_6\Delta_3$	Δ_3	Δ_6
J	V		
K	C		
L	Y		
M	O		
N	K		
O	E		
P	X		
Q	D		
R	S		

	$\Delta_6\Delta_3$	Δ_3	Δ_6
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:

$$\Delta_3(\mathtt{K}) = \mathtt{M}\ , \quad \Delta_3(\mathtt{N}) = \mathtt{O}\ , \quad \Delta_3(\mathtt{C}) = \mathtt{E}\ .$$

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

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

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

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

	$\Delta_6\Delta_3$	Δ_3	Δ_6
A	G	Z	
B	I		
C	N	E	
D	H	J	
E	M		
F	P		
G	L	I	
H	R	T	
I	Z		

	$\Delta_6\Delta_3$	Δ_3	Δ_6
J	V		
K	C	M	
L	Y	B	
M	O		
N	K	O	
O	E		
P	X		
Q	D	V	
R	S	X	

	$\Delta_6\Delta_3$	Δ_3	Δ_6
S	U	P	
T	J		
U	Q	F	
V	F		
W	B		
X	T		
Y	A	W	
Z	W		

בנוסף Δ_3 הוא משקף, לכן, אם למשל $\Delta_3(\texttt{A}) = \texttt{Z}$ אז בהכרח $\Delta_3(\texttt{Z}) = \texttt{A}$. על פי זה אפשר להשלים את העמודה של Δ_3 של הטבלה:

	$\Delta_6\Delta_3$	Δ_3	Δ_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	

	$\Delta_6\Delta_3$	Δ_3	Δ_6
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	

	$\Delta_6\Delta_3$	Δ_3	Δ_6
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 Δ_6 נתונים ע"י העמודות Δ_3 ו- $\Delta_6\Delta_3$. למשל, לפי השורה הראשונה:

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

כדוגמה נוספת, לפי השורה השנייה:

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

לפי השורה השלישית:

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

וכן הלה. באופן הזה אפשר למצוא את כל הערכים של התמורה Δ_6 על האותיות של האלפבית:

	$\Delta_6\Delta_3$	Δ_3	Δ_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

	$\Delta_6\Delta_3$	Δ_3	Δ_6
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

	$\Delta_6\Delta_3$	Δ_3	Δ_6
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) **<u>פענוח</u>:**

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

לפיכך:

$$\begin{aligned} \sigma_1 &= \Delta_1(\texttt{I}) &= \texttt{H} \ , \\ \sigma_2 &= \Delta_2(\texttt{L}) &= \texttt{E} \ , \\ \sigma_3 &= \Delta_3(\texttt{B}) &= \texttt{L} \ , \\ \sigma_4 &= \Delta_4(\texttt{D}) &= \texttt{L} \ , \\ \sigma_5 &= \Delta_5(\texttt{A}) &= \texttt{O} \ . \end{aligned}$$

■