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 $\Sigma\left(x_i\right)\neq\Sigma\left(x_j\right)$.
- 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:
$$\{\pi\left(x_1\right)\ ,\ \pi\left(x_2\right)\ ,\quad \ldots\quad \pi\left(x_n\right)\}\ .$$

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 $\pi\left(\Sigma\right)$ התמונה של π. מכיוון ש- π היא פונקציה מהקבוצה Σ אל הקבוצה Σ, אזי התמונה שלה היא תת-קבוצה של Σ, כלומר:
$$\pi\left(\Sigma\right)\subseteq\Sigma\ .$$

לכן
$$\left|\pi\left(\Sigma\right)\right|\leq|\Sigma|=n\ .$$

נראה כי $|\Sigma|=\left|\pi\left(\Sigma\right)\right|$. נניח בשלילה כי $|\Sigma|<\left|\pi\left(\Sigma\right)\right|$. 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
$\sigma(x)$	3	5	4	2	6	1

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

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.

- **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- 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.

- **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" Σ.

■

הגדרה 4.3 תמורות מתחלפות

תהיינה σ, π תמורות. אומרים כי π ו- σ מתחלפות אם

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

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 ונקודת 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 תמרה 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.

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

שלב האינדוקציה

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 $t=k+1$:

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

כאשר במעבר האחרון השתמשנו בההנחת האינדוקציה.

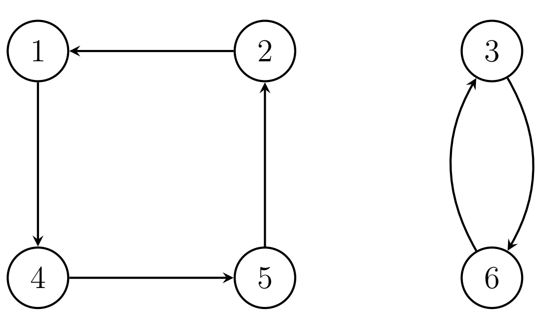
■

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

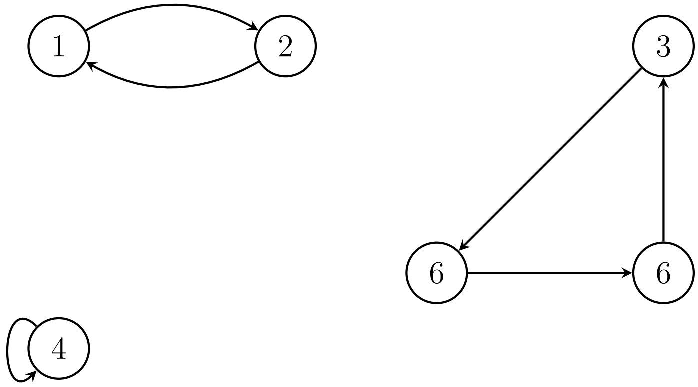
נגדיר הגרף המכוון $G_\pi=(V,E)$ כאשר הקבוצת הקודקודים היא $V=\Sigma$, ולכל $x\in\Sigma$ נגידר צלע מ- x ל- $\pi(x)$. ז"א $E=\{e_1,e_2,\ldots,e_n\}$ כאשר $e_i=x_i\pi(x_i)$ היא הצלע מקודקוד x_i לקודקוד $\pi(x_i)$. על פי ההגדרה הזאת הגרף G_π של התמורה π היא כמתוארת באיור למטה.



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 $\pi : \Sigma \to \Sigma$ תמורה על הקבוצה Σ ויהיו $\Sigma = \{x_1, \quad \ldots \quad , x_n\}$.
אם

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

אז אומרים שבתמורה π קיים מחזור באורך k, מסומן

$$\begin{pmatrix} x_{i_1} & x_{i_2} & \cdots & x_{i_k} \end{pmatrix} \ .$$

משפט 4.3 פירוק למחזורים של תמורה

תהי $\pi : \Sigma \to \Sigma$ תמורה על קבוצה סופית Σ. ניתן לרשום את π כהרכבה של מחזורים זרים.

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:

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

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 התמורה המורכבת $\pi\sigma\pi^{-1}$.

משפט 4.4 משפט ההזזה של תמורות צמודות

תהיינה $\sigma : \Sigma \to \Sigma$ ו- $\pi : \Sigma \to \Sigma$ תמורות על הקבוצה 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 4.5 פירוקים למחזורים של תמורות צמודות שווים

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

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

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

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

הוכחה: עבור כל מחזור $\begin{pmatrix} a_1 & a_2 & \ldots & a_k \end{pmatrix}$ של σ, מתקיים

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

מנובע ממשפט כי לכל מחזור של σ מתקיים:

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

■

משפט 4.6 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:
כיוון אם:

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

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

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

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

ולכן ל- τ ול- σ 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

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

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 $\underline{x_1=\mathtt{H}}$

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

(2 $\underline{x_2=\mathtt{E}}$

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

(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) $\underline{x_5 = \texttt{O}}$

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

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) $\underline{y_1 = \texttt{E}}$

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

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

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

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

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

4) $\underline{y_4 = \texttt{A}}$

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

5) $\underline{y_5 = \texttt{X}}$

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

לפיכך הטקסט הגלוי הוא: HELLO. ■

4.5 משפט רייבסקי

הגדרה 4.11 משקף

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

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

משפט 4.7 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:

<u>כיוון אם</u>

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

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

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

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

כעת נראה שאם $x \in \Sigma$ אז $\rho(x) \neq x$. נניח בשלילה שקיימת נקודה $x \in \Sigma$ עבורה $\rho(x) = x$. אזי $\rho \in [1^{z_1} \cdots]$ 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- $\rho^{-1} = \rho$. 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:

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

כאשר $(x_1\ x_2\ x_3\ \dots\ )$ הוא מחזור באורך $k > 2$. ז"א ההופכית של ρ 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 4.8 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- 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 4.6 $\Delta_i \in [2^{13}]$.

⇐ לפי הגדרה 4.11 התמורה Δ_i היא משקף.

■

משפט 4.9 משפט רייבסקי

הוכחה: ■