

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" Σ . בהינתן $x_i \in \Sigma$ ותמורה π . אז

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

תזכורת:

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

כתוצאה לכך, אם π פועלת על כל האיברים של Σ אז נקבל אותה קבוצה Σ 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 Σ קבוצה סופית ותהי $\Sigma \rightarrow \Sigma$ פונקציה. הוכחו: אם π חד-חד ערכית אז π תמורה.

פתרונות:

נתון לנו הפונקציה $\pi : \Sigma \rightarrow \Sigma$ אשר Σ קבוצה נוצר סופית. כדי להוכיח כי π תמורה יש להראות כי π חד-חד-ערכית ו"על" Σ . כבר נתון לנו ש- π חד-חד-ערכית רק להראות כי π על Σ .

Σ היא קבוצה סופית לכן קיימים שלם $0 \leq n \leq |\Sigma|$. תהיו (Σ) התמונה של π . מכיוון ש- π היא פונקציה מהקבוצה Σ אל הקבוצה Σ , אז התמונה שלה היא תת-קבוצה של Σ , 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-

Σ , בסתירה לכך ש: π חד-חד-ערכית. לכן הוכחנו דרך השיליה כי

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

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

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

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



הגדרה 4.2 הרכבה של תמורה

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

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

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

דוגמה 4.4

נתון התמורות π ו- σ :

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

אזי ההרבה $\sigma\pi$ היא:

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

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

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

כלומר $\sigma\pi \neq \pi\sigma$.

משפט 4.1 הרכבה של תמורה היא תמורה

תהי Σ קבוצה נוצר סופית ותהינה $\Sigma \rightarrow \Sigma : \pi \circ \sigma$ תמורה על הקבוצה Σ . הרכבה $\sigma\pi$ היא תמורה על Σ .

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

• חח"ע

נניח בשיליה 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 $y_1 \neq y_2$. ומכיון 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 השיליה כי π פונקציה חד-ע.

• על

נניח בשלילה כי π לא פונקציה "על". נסמן (Σ) π התמונה של π . אי-

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

ראשית מכיוון ש- (Σ) π הוא התמונה של π אי- $\Sigma \subseteq \sigma\pi(\Sigma)$. לכן אם $\Sigma \neq \sigma\pi(\Sigma)$. מכאן

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

לכן בהכרח קיימים לפחות שני איברים $x_1, x_2 \in \Sigma$ עבורם $\pi(x_1) = \pi(x_2)$. זאת בסתירה לכך ש- π חד-ע.

לכן הוכחנו דרך השיליה כי הפונקציה π היא "על" Σ .



הגדרה 4.3 תמורות מתחלפות

תהיינה $\Sigma \rightarrow \Sigma : \sigma$ ו- $\Sigma \rightarrow \Sigma : \pi$ 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 $\Sigma \rightarrow \Sigma : \pi$ תמורה על הקבוצה Σ . התמורה ההפכית 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 ההפכית היא:

| | | | | | | | | |
|---------------|---|---|---|---|---|---|---|---|
| x | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| $\pi^{-1}(x)$ | 4 | 5 | 2 | 6 | 3 | 1 | 8 | 7 |

הגדרה 4.5 נקודת שבת ונקודת זהה

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

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

הגדרה 4.6 תמורה זהה

התמורהזהה מסומנת $\Sigma \rightarrow \Sigma : \text{id}$ ומוגדרת כך שלכל $\Sigma \in \Sigma$:

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

במילים אחרות אם $\Sigma \rightarrow \Sigma : \text{id}$ היא התמורהזהה אז כל נקודת $\Sigma \in \Sigma$ היא נקודת שבת של id .

משפט 4.2 תמורה ההפכית של תמורה מורכבת

תהיינה π_t, \dots, π_1 תמורות על הקבוצה Σ . אז

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

הוכחה: נוכיח את הטענה באינדוקציה.

שלב הבסיס

עבור $t=2$, לכל $\Sigma \in \Sigma$ יש לנו:

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

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

שלב האינדוקציה

נניח כי הטענה מתקיימת עבור $t=k > 2$ (זאת היא ההנחה האינדוקציה). אז נראה כי הטענה נכונה גם במקרה $t=k+1$ באופן הבא. נתבונן על התמורה המורכבת $\pi_k \pi_{k+1} \cdots \pi_1$. נסמן התמורה המורכבת מ- k תמורות כך: $\pi_k \cdots \pi_1 = \sigma$. הסימן הזה מאפשר לנו להביע את התמורה המורכבת מ- $k+1$ תמורות כתמורה המורכבת מ- 2 תמורות באופן הבא:

$$\pi_1 \cdots \pi_k \pi_{k+1} = \sigma \pi_{k+1} .$$

מכאן ולפי שלב הבסיס מהופכית היא

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

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

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

כאשר במעבר האחרון השתמשנו בהנחה האינדוקציה.

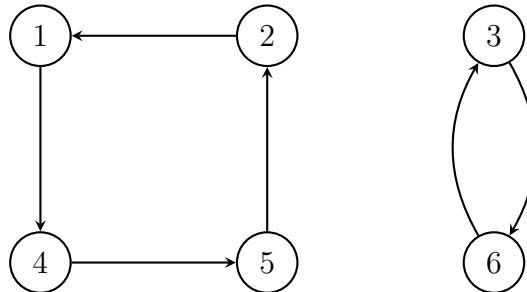
■

4.2 פירוק למחזוריים של תמורה

עד כה ראיינו תמורות בייצוג של טבלה. אבל המבנה האמתי של תמורה נגלה עם נציג תמורה כgraf. 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 |

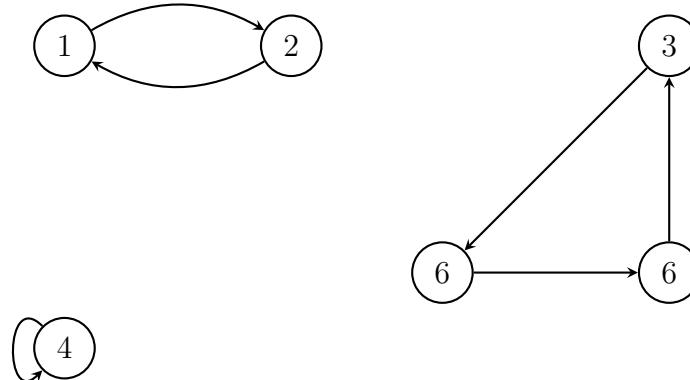
נדיר הגרף המכון $G_\pi = (V, E)$ כאשר הקבוצה הקודקודים היא $V = \Sigma$, ולכל $x \in \Sigma$ נגדיר צלע מ- x ל- $\pi(x)$. נ"א $E = \{e_1, e_2, \dots, e_n\}$ היא הצלע מקודקוד x_i לקודקוד $\pi(x_i)$. על פי ההגדרה הזו את הגרף G_π של התמורה π היא כמתואר באIOR למטה.



כדוגמה נוספת אם σ היא התמורה

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

אז הגרף G_σ הינו:



בגרף של תמורה, כל קודקוד שיעז לבזוק מעגל מכון אחד (שייתכן הוא עובר דרך קודקוד אחד בלבד). הרי קיימים התאמות אחת- אחת בין תמורה על Σ לבין גראフ שמכסה כל המעגלים המכונים של Σ . התופעה זו היא המוטיבציה לסייעון מחזורי של תמורות.

הגזרה 4.7 מחזור

תהי $\Sigma \rightarrow \Sigma$: π תמורה על הקבוצה Σ . אם קיימים k איברים שונים Σ 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 קיימים מחזור באורך k ב- π שמסומן:

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

משפט 4.3 פירוק למחזורים של תמורה

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

דוגמה 4.6נתונה התמורה π :

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

הפירוק למחזוריים הוא:

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

משפט 4.4

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

הוכחה:
כיוון אם

נניח ש- π מכילה מחזור באורך k .

$$\begin{aligned} & \left. \begin{aligned} & \text{קיימים איברים שונים } a_1, \dots, a_k \in \Sigma \text{ כך ש: } \\ & \pi(a_1) = a_2, \quad \pi(a_2) = a_3, \quad \dots \quad \pi(a_{k-1}) = a_k, \quad \pi(a_k) = a_1 \end{aligned} \right\} \Leftarrow \\ & \text{בגרף } G_\pi = (V, E) \text{ של התמורה קיימות הצלעות} \\ & a_1\pi(a_1), \ a_2\pi(a_2), \ \dots, \ a_{k-1}\pi(a_{k-1}), \ a_k\pi(a_k) \in E. \end{aligned}$$

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

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

 \Leftarrow מכילה מעגל המילטוני באורך k .

כיוון רק אם

נניח ש- G_π מכיל מעגל המילטוני באורך k . \Leftarrow קיימים קבוצות $a_1, \dots, a_k \in \Sigma$ עבורם

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

 \Leftarrow מכיוון ש- G_π הוא הגרף של התמורה π איזי

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

\Leftarrow π מכילה מחזור באורך k :
 $\left(a_1 \ a_2 \ \dots \ \subseteq a_k \right) \subseteq \pi$.



הגדרה 4.8 המחלקה של תמורה

תהי $\Sigma \rightarrow \pi$ תמורה. אומרים כי π שיכת למחלקה $[1^{z_1} 2^{z_2} \cdots n^{z_n}]$ אם בפירוק למחזוריים של π יש בדיק z_1 מחזוריים באורך-1, z_2 מחזוריים באורך-2, z_3 מחזוריים באורך-3, וכן הלאה.

במילים אחרות:

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

אם לכל $n = 1, \dots, i$ בפירוק למחזוריים של π יש z_i מחזוריים באורך i .

דוגמה 4.7

תהי $. \Sigma = \{A, B, C, D, E, F\}$

$.(A \ B)(C \ D)(E \ F) \in [2^3]$

$.(A \ B \ C \ D) \in [1^2 4^1]$

$.(A \ D \ C)(E \ F) \in [1^1 2^1 3^1]$

4.3 תמורה צמודות

הגדרה 4.9 תמורה צמודות

תהיינה σ, π תמורות על הקוצה 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 $\Sigma \rightarrow \sigma : \Sigma \rightarrow \pi$ תמורות על הקוצה סופית Σ . לכל Σ אם $\sigma(x) = y$ אז $\pi(\sigma(x)) = \pi(y)$.

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

הוכחה: נניח ש: $\sigma(x) = y$. אז

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

משפט 4.6 פירוקים למחזוריים של תמורות צמודות שוויות

תהיינה $\Sigma \rightarrow \sigma : \Sigma \rightarrow \pi$ תמורות על הקוצה סופית Σ . ונניח כי הפירוק למחזוריים של σ הוא

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

אז הפירוק למחזוריים של $\pi \sigma \pi^{-1}$ הוא:

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

הוכחה: עבור כל מהזור $(a_1 \ a_2 \ \dots \ a_k)$ של σ , מתקיים

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

מנובע המשפט כי לכל מהזור של σ 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 המחלוקת של תמורה צמודות נשמרת

תהיינה $\Sigma \rightarrow \Sigma : \sigma$ ו- $\Sigma \rightarrow \Sigma : \tau$ תמורים על הקוצה סופית Σ .
 τ צמודה ל- σ אם ורק אם $\sigma \circ \tau$ שייכות לאותה מחלוקת.

הוכחה:

כיוון אם:

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

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

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

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

ולכן ל- τ ול- σ יש אותו מבנה של מחוזרים וכך הוא שייכות לאותה מחלוקת.

כיוון רק אם:

■

4.4 צופן אניגמה

הgalלי האתחול של צופן אניגמה הם 3 תמורים קבועות שמוגדרות:

| x | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---------------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\alpha_1(x)$ | E | K | M | F | L | G | D | Q | V | Z | N | T | O | W | Y | H | X | U | S | P | A | I | B | R | C | J |

| x | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---------------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\alpha_2(x)$ | A | J | D | K | S | I | R | U | X | B | L | H | W | T | M | C | Q | G | Z | N | P | Y | F | V | O | E |

| x | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---------------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\alpha_3(x)$ | B | D | F | H | J | L | C | P | R | T | X | V | Z | N | Y | E | I | W | G | A | K | M | U | S | Q | O |

המשקף הקבוע הוא תמורה הבאה:

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

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

הגדרה 4.10 כלל מצפין וככלל מפענה של צופן אניגמה

יהי π משקף כלשהו מעל האלפבית $Z = A, \dots, Z$. הבחירה של המשקף מבהווה את הלוח התקעiem. יהי $w = x_1 x_2 \dots x_n$ מילה של טקסט גלי. לכל $i = 1, \dots, n$, הכלל מצפין והכלל מפענה של האות במקומות i -טקסט הם:

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

כאשר Δ_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 π אי $\tau_i = \sigma_{-i} \alpha_3 \sigma_i \alpha_2 \alpha_1$ ולבסוף

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

ז"א לכל $i = 1, \dots, n$ התמורה המורכבת Δ_i היא הצמודה של ρ על ידי τ_i .

דוגמה 4.8 הצפנה על ידי צופן אניגמה

נתון הטקסט גלי,

hello .

נניח כי הלוח התקעiem הוא

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

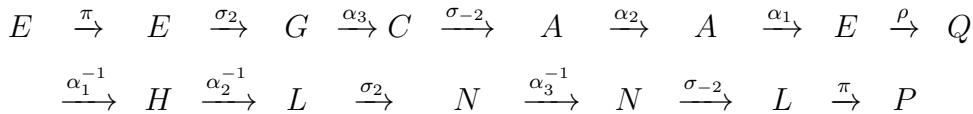
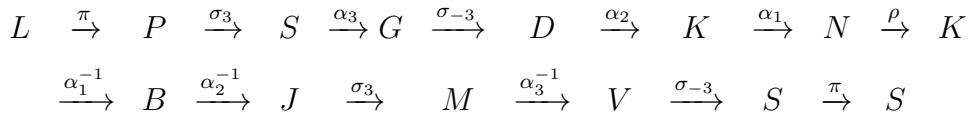
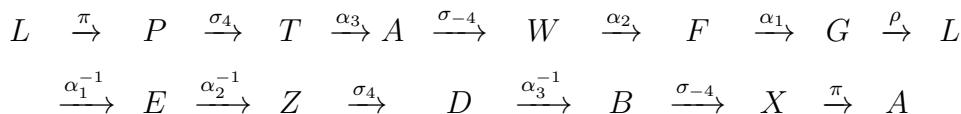
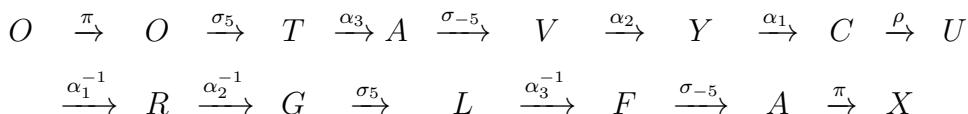
חשבו את הטקסט מוצפן.

פתרונות:

$$x_1 = H \quad (1)$$

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

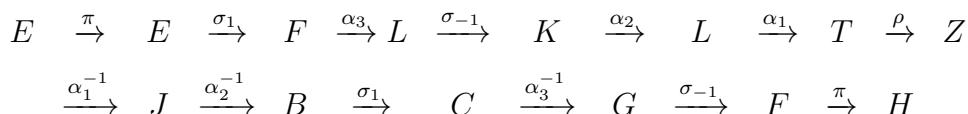
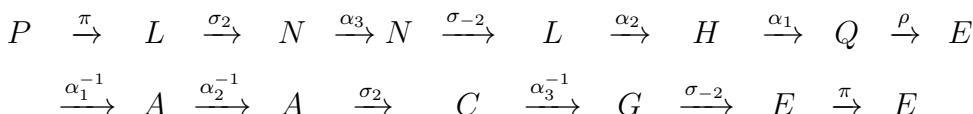
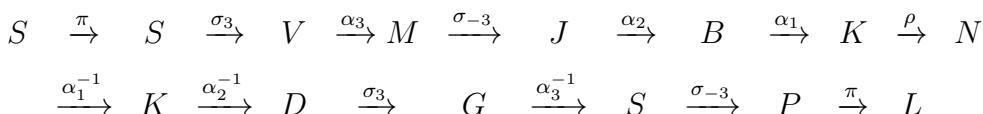
$$x_2 = E \quad (2)$$

 $x_3 = \text{L}$ (3) $x_4 = \text{L}$ (4) $x_5 = \text{O}$ (5)

לפייך הטקסט מוצפן הוא: EPSAX.

דוגמה 4.9 הצפנה על ידי צופן איניגמה

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

פתרונות: $y_1 = \text{E}$ (1) $y_2 = \text{P}$ (2) $y_3 = \text{S}$ (3)

$$y_4 = A \quad (4)$$

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

$$y_5 = X \quad (5)$$

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

לפיכך הטקסט המקורי הוא: HELLO.

4.5 משפט ריבסקי והתקפה על הצופן האניגמה

הגדרה 4.11 תמורה משקפת

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

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

משפט 4.8 תכונות של תמורה משקפת

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

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

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

הוכחה:

כיוון אם

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

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

לכל מחרוז $(a_1 \ a_2 \ \cdots \ a_k)$ המוחזר ההפוך הוא $(a_k \ a_{k-1} \ \cdots \ a_1)$. לכן

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

כעת נראה שאם $x \in \Sigma$ אז $\rho(x) \neq x$. נניח בשיילה שקיים נקודה $x \in \Sigma$ עבורה $\rho(x) = x$. אזי $\rho(x) = x$ מכילת ρ מחייבת מחרוז אחד באורך 1, בסתרה לכך ρ היא משקף.

כיוון רק אם

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

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

כאשר (\dots) הוא מחזור באורך $k > 2$. זו ההפכית 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 4.9 הכלל מצפין של צופן האניגמה הוא תמורה משקפת על האלפבית האנגלית

הכלל מצפין (והכלל מפענה) של צופן האניגמה הוא תמורה משקפת על האלפבית האנגלית.

הוכחה: הכלל מצפין והכלל מפענה של צופן האניגמה הם

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

כאשר $\pi \circ \rho$ המשקף הקבוע של צופן אניגמה.

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

\Leftarrow מכיוון ש: ρ הוא משקף על האלפבית האנגלית אז $\rho \in [2^{13}]$.

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

\Leftarrow לפי הגדירה 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 Σ עוברים $x, y_1, y_2 \in \Sigma$ ורק אם $\rho_1(x) = y_1$ וגם $\rho_2(x) = y_2$.

הוכחה:
כיוון אם

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

$$\left. \begin{array}{l} y_1 = \rho_1(x) \\ y_2 = \rho_2(x) \end{array} \right\} \xrightarrow{\text{משקפת } \rho_1} x = \rho_1(y_1) \Rightarrow \rho_2(\rho_1(y_1)) = \rho_2(x) = y_2 .$$

כיוון רק אם

נניח ש: $\rho_1(y_1) = \rho_2(y_2)$. מכיוון ש- ρ_2 תמורה משקפת איזומטרית $x \in \Sigma$ קיים $y_1, y_2 \in \Sigma$ כך ש:

$$\left. \begin{array}{l} \rho_1(y_1) = x = \rho_2(y_2) \\ \rho_2(y_2) = x \end{array} \right\} \xrightarrow{\text{משקפות } \rho_1, \rho_2} \left. \begin{array}{l} y_1 = \rho_1(x) \\ y_2 = \rho_2(x) \end{array} \right\} .$$
**דוגמה 4.10**

נניח שיש לנו טקסט שמוספן ע"י צופן אניגמה שמתחליל ב- ICPWLV. איזי אנחנו יודעים שקיימים:

כך ש:

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

כאשר ה- Δ_i הוא הכלל מצפין של צופן אניגמה המורכב מהתמורות הנעלמות. מצד שני אנחנו כן יודעים שכל Δ_i הוא משקפי 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 ריבסקי

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

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

מורפיע בפירוק למחרוזים של התמורה המורכבת $\rho_2\rho_1$, איזי בהכרח המחרוז

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

גם מופיע בפירוק למחרוזים של התמורה המורכבת $\rho_1\rho_2$, ובנוסף הוא שונה מהחרוז

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

זה בדיק הסוג של פירוק למחרוזים הנקבע על ידי משפט ריבסקי: יש זוג מחרוזים באורך 7, זוג מחרוזים באורך 5, זוג מחרוזים באורך 1. מכיוון שיש רק שני מחרוזים מכל אורך, איזי אנחנו יודעים כיצד להתאים אותם:

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

דוגמה 4.12 קרייפטו-אנליזה של צופן אניגמה

נתונות התמורות הבאות של צופן אניגמה:

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

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

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

פענו את הקסט מוצפן

פתרונות:**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 | | |
| 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 (ZRYS)(JNVU). לפי משפט ריבסקי:

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

| | $\Delta_4 \Delta_1$ | Δ_1 | Δ_4 |
|---|---------------------|------------|------------|
| A | C | | |
| B | G | | |
| C | I | | |
| D | O | | |
| E | T | | |
| F | W | | |
| G | P | | |
| H | Q | | |
| I | K | | |
| 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 (GPDOFWHQB) (ACIKETMLX), לפי משפט ריבסקי:

$$\Delta_1(X) = G, \quad \Delta_1(L) = P, \quad \Delta_1(M) = D, \quad \Delta_1(T) = O, \quad \Delta_1(E) = F,$$

$$\Delta_1(K) = W, \quad \Delta_1(I) = H, \quad \Delta_1(C) = Q, \quad \Delta_1(A) = B.$$

| | $\Delta_4 \Delta_1$ | 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 | |
| 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 | | |

בנוסח Δ_1 הוא משקף, כלומר, אם למשל $\Delta_1(A) = B$ אז בהכרח $\Delta_1(B) = A$. 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:

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

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 הלא. באופן זה 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 תמורהות (IA) (DO). לפי משפט ריבסקי:

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

עבור הזוג תמורהות (CEUKGQ) (NWFVLR), לפי משפט ריבסקי:

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

עבור הזוג תמורהות (BPMZX) (STYHJ), לפי משפט ריבסקי:

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

| | $\Delta_5 \Delta_2$ | 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 | |
| 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 | |

בנוסך Δ_2 הוא משקף, כלומר אם למשל $\Delta_2(A) = D$ אז בהכרח $\Delta_2(D) = A$. על פי זה אפשר להשלים את העמודה של Δ_2 של ה таблицה:

| | $\Delta_5 \Delta_2$ | 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 | |
| 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 Δ_5 נתונים ע"י העמודות Δ_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 הלא. באופן זה אפשר למצוא את כל הערךם 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 |
| 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: $\Delta_6 \Delta_3$:

| | $\Delta_6 \Delta_3$ | Δ_3 | Δ_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 תמורהות (CNK) (MOE). לפי משפט ריבסקי:

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

עבור הזוג תמורהות (AGLY) (WBIQ), לפי משפט ריבסקי:

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

עבור הזוג תמורהות (DHRSUQ) (VFPXTJ), לפי משפט ריבסקי:

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

| | $\Delta_6 \Delta_3$ | 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 | | |
| 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 | | |

בנוסך Δ_3 הוא משקף, כלומר אם למשל $Z = \Delta_3(A)$ אז בהכרח $\Delta_3(Z) = A$. על פי זה אפשר להשלים את העמודה של Δ_3 של ה таблицה:

| | $\Delta_6 \Delta_3$ | 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 | |
| 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 Δ_6 נתונים ע"י העמודות Δ_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 הלא. באופן זה 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 |
| 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:

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

