

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 $0 \leq n \leq |\Sigma|$. תהי (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 $x, x_2 \in \Sigma$ כך ש-:

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

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

הוכחנו כי π גם $|\pi(\Sigma)| = |\Sigma|$ אז בהכרח

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

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



הגדרה 4.2 הרכבה של תמורה

תהי Σ קבוצה נוצר סופית ותהינה $\Sigma \rightarrow \Sigma : \pi$ ו- $\Sigma \rightarrow \Sigma : \sigma$ תמורות על הקבוצה Σ . ההרכבה של π ו- σ מוגדרת להיות הפונקציה שמסומנת $\sigma\pi$ ומוגדרת לפי התנאי:
לכל $x \in \Sigma$, אם $\pi(x) = y \in \Sigma$ וגם $\sigma(y) = z \in \Sigma$ 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 הרכבה 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 $\sigma\pi$ 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 $\Sigma \rightarrow \Sigma : \pi$ ו- $\Sigma \rightarrow \Sigma : \sigma$ 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 בשיליה כי $\sigma\pi$ לא חח"ע. אזי קיימים $x_1, x_2 \in \Sigma$ כך ש- $(\pi(x_1)) = \sigma(\pi(x_2))$. 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

$$\sigma(\pi(x_1)) \neq \sigma(\pi(x_2)),$$

$$\sigma(\pi(x_1)) = \sigma(\pi(x_2))$$

בסתירה לכך ש- $\sigma\pi$ פונקציה חח"ע.

• על

נניח בשילילה כי $\pi \sigma$ לא פונקציה "על". נסמן (Σ) התחמונה של $\pi \sigma$. אז $\sigma \pi(\Sigma) \neq \Sigma$.

ראשית מכיוון ש- (Σ) הוא התחמונה של $\pi \sigma$ אז $\Sigma \subseteq \pi(\Sigma) \neq \sigma \pi(\Sigma)$. לכן אם Σ מכון

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

לכן בהכרח קיימים לפחות שני איברים $x_1, x_2 \in \Sigma$ עבורם $\sigma \pi(x_1) = \sigma \pi(x_2)$. זאת בסתיויה כך ש- π חח"ע, שMOVED בסייף הקודם.

לכן הוכחנו דרך השילילה כי הפונקציה $\pi \sigma$ היא "על" Σ .

הגדירה 4.3 תמורות מתחלפות

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

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

הגדירה 4.4 תמורות מתחלפות

תהי $\Sigma \rightarrow \Sigma$ 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

הגדירה 4.5 נקודת שבת ונקודת זהה

תהי $\Sigma \rightarrow \Sigma$ 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 .

הגדירה 4.6 תמורה זהה

התמורה זהה מסומנת $\Sigma \rightarrow \Sigma$ לפי ומוגדרת כך שלכל $x \in \Sigma$:

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

במילים אחרות אם $\Sigma \rightarrow \Sigma$ היא התמורה זהה אז כל נקודת $\Sigma \in x$ היא נקודת שבת של id .

משפט 4.2 תמורה ההפכית של תמורה מורכבת

תהיינה π_1, \dots, π_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 $\Sigma \in x$ 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 כ- σ : $\sigma = \pi_1 \cdots \pi_k$. 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 שלב הבסיס מההפכית היא

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

כעת נזכיר את ההגדרה $\sigma = \pi_1 \cdots \pi_k$ ונסתמש בהhnחת האינדוקציה שלנו כדי להוכיח את הטענה עבור $t = k + 1$:

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

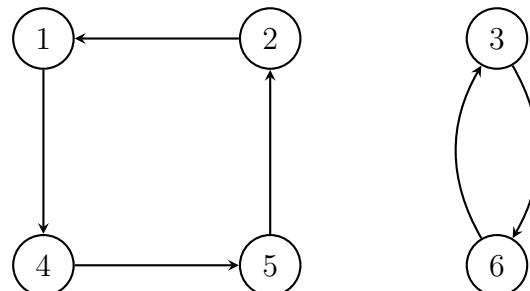
כאשר במעבר האחרון השתמשנו בהhnחת האינדוקציה. ■

4.2 פירוק למחזורים של תמורה

עד כה ראיינו תמורות ביצוג 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

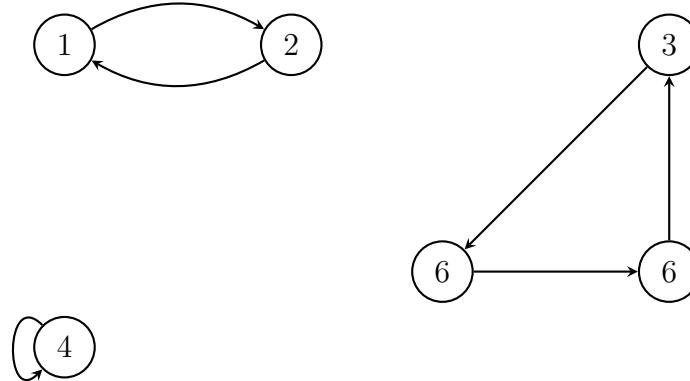
נדיר הgraf המכובן $G_\pi = (V, E)$ כאשר הקבוצת הקודקודים היא $V = \Sigma$, ולכל $x \in \Sigma$ נגידר צלע מ- x ל- $\pi(x)$. א"א $E = \{e_1, e_2, \dots, e_n\}$ כאשר $e_i = x_i \pi(x_i)$ הינה הצלע מקודקוד x_i לקודקוד $\pi(x_i)$. על פי ההגדרה זאת הgraf G_π של התמורה π היא כמתוארת באיור למטה.



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 לבדיק מעגל מכוכן אחד (שייתכן הוא עובר דרך קודקוד אחד בלבד). הרי קיים התאמה אחת-אחד בין תמורה על Σ לבין גראף שמכסה כל המעגלים המכוכנים של Σ . התופעה זו היא המוטיבציה לשימוש מחזוריים של תמורים.

הגדירה 4.7 מחזור

תהי $\Sigma \rightarrow \Sigma$ תמורה על הקבוצה Σ ויהיו $\{x_1, \dots, x_n\}$ אם

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

או אומרים שבתמורה π קיים מחזור באורך k , מסומן

$$(x_{i_1} \ x_{i_2} \ \dots \ x_{i_k}).$$

משפט 4.3 פירוק למחזוריים של תמורה

תהי $\Sigma \rightarrow \Sigma$ תמורה על קבוצה סופית Σ . ניתן לרשום את π כהרכבה של מחזוריים 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 למחזוריים הוא:

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

הגדירה 4.8 החלוקת של תמורה

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

במילים אחרות:

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

אם לכל $n = 1, \dots, i$ בפרק למחוזרים של π יש z_i מחזורים באורך i .

4.7 דוגמה

- 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 תמורה צמודות

הגדרה 4.9 תמורה צמודות

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

משפט 4.4 פירוקים למחוזרים של תמורות צמודות שוים

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

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

אזי להטורה הצמודה $\pi \sigma \pi^{-1}$ יש אותו פירוק למחוזרים:

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

בלשון אחר, הצמודה של σ על ידי π פועלת על הפירוק למחוזרים המקורי של σ על ידי להפעיל π על האיברים של המחזורים בנפרד.

הוכחה: אם $y = \sigma(x)$ אזי $\pi(y) = \pi(\sigma(x)) = \pi(\pi(x)) = x$ באופן הבא:

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

משפט 4.5 תמוקות צמודות שיכות לאותה מחלוקת

תהיינה π_1, π_2 תמורות כlhsן על הקבוצה סופית Σ .

התמורה π_1 והטורה π_2 הן צמודות אם ורק אם הן שיכות לאותה מחלוקת.

הוכחה:

4.4 צופן אניגמה

הgelgi האתחול של צופן אניגמה הם 3 תמורה קבועות שМОגדרות:

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 קבוע 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

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

הגדרה 4.10 כלל מצפן וכלל מפענה של צופן אניגמה

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

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

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

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

אם נגדיר את התמורה המורכבת π $\tau_i^{-1} = \pi \alpha_1^{-1} \alpha_2^{-1} \sigma_{-i} \alpha_3^{-1} \sigma_i$ אז $\tau_i = \sigma_{-i} \alpha_3 \sigma_i \alpha_2 \alpha_1 \pi$ ולכן

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

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 גליי

hello .

נניח כי הלוח התקעים הוא

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

חשבו את הטקסט מוצפן.

פתרונות:

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

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

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

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

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

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

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

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

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

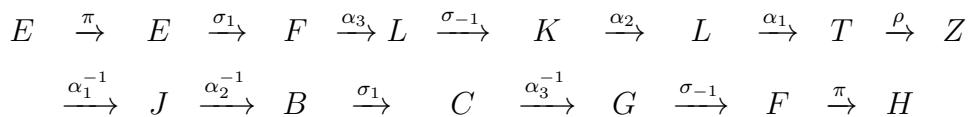
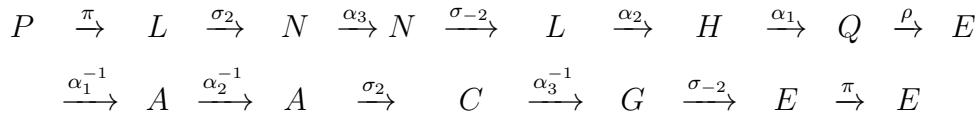
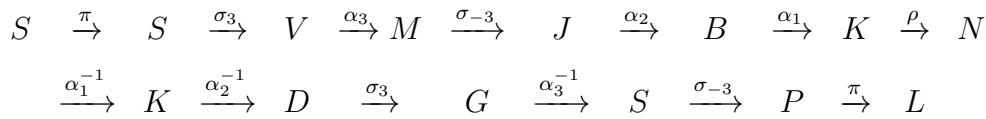
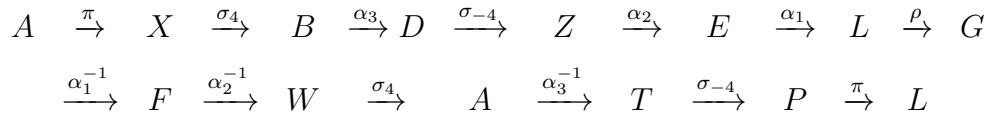
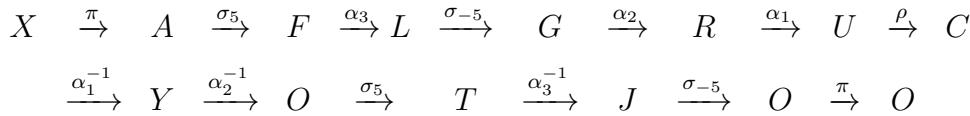
$$\begin{array}{ccccccccccccc} O & \xrightarrow{\pi} & O & \xrightarrow{\sigma_5} & T & \xrightarrow{\alpha_3} & A & \xrightarrow{\sigma_{-5}} & V & \xrightarrow{\alpha_2} & Y & \xrightarrow{\alpha_1} & C & \xrightarrow{\rho} & U \\ & \xrightarrow{\alpha_1^{-1}} & R & \xrightarrow{\alpha_2^{-1}} & G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

לפיכך הטקסט מוצפן הוא: EPSAX.

דוגמה 4.9 הצפנה על ידי צופן אניגמה

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

פתרונות:

$y_1 = E$ (1) $y_2 = P$ (2) $y_3 = S$ (3) $y_4 = A$ (4) $y_5 = X$ (5)

לפיכך הטקסט הגרפי הוא: HELLO.

4.5 משפט ריבסקי

הגדרה 4.11 משקל

תהי Σ קבוצה נוצר סופית באורך זוגי. ותהי $\Sigma \rightarrow \Sigma : \rho$ תמורה. אומרים כי התמורה ρ היא משקל אם $\rho \in [2^{n/2}]$.

משפט 4.6 תוכנות של תמורה משקלת

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

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

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

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 מהזור $(a_1 \ a_2 \ \cdots \ a_k)$ המחוור הפובי 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 שם $\Sigma \in x$ אז $x \neq \rho(x)$. נניח בשיילה שקיימת נקודה $x \in \Sigma$ עבורה $x = \rho(x)$. אזי $x \in \rho(\Sigma)$, כלומר ρ מכילה קיימים לפחות אחד באורך 1, בסתירה לכך ש- ρ היא משקף.

כיוון רק אם

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

$$\rho = (x_1 \ x_2 \ x_3 \ \cdots \)^{\rho'} ,$$

כאשר $(x_1 \ x_2 \ x_3 \ \cdots \)$ הוא מהזור באורך $k > 2$. א"א ההפכית של ρ היא

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

בסתירה לכך ש- $\rho^{-1} = \rho$.

משפט 4.7 הכלל מצפין של אניגמה הוא משקף על האלפבית האנגלית

הכלל מצפין של צופן אניגמה הוא משקף על האלפבית האנגלית

הוכחה:

הכלל מצפין של צופן אניגמה היא מהצורה:

$$e(x_i) = \Delta_i$$

כאשר

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

אם נגדיר את התמורה המורכבת

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

אזי

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

ולכן

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

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