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:

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

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

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

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

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

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

ולפיכך $\pi : \Sigma \to \Sigma$ 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 $\pi\sigma \neq \sigma\pi$.

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 $\sigma\pi\left(\Sigma\right)$ התמונה של $\sigma\pi$. אזי

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

ראשית מכיוון ש- $\sigma\pi\left(\Sigma\right)$ הוא התמונה של $\sigma\pi$ אזי $\sigma\pi\left(\Sigma\right) \subseteq \Sigma$. לכן אם $\sigma\pi\left(\Sigma\right) \neq \Sigma$ אז $\sigma\pi\left(\Sigma\right) \subset \Sigma$. מכאן

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

לכן בהכרח קיים לפחות שני איברים $x_1, x_2 \in \Sigma$ עבורם $\sigma\pi\left(x_1\right) = \sigma\pi\left(x_2\right)$. 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 תמרוה 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:

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

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

<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 $t = k+1$:

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

כאשר במעבר האחרון השתמשנו בההנחת האינדוקציה.

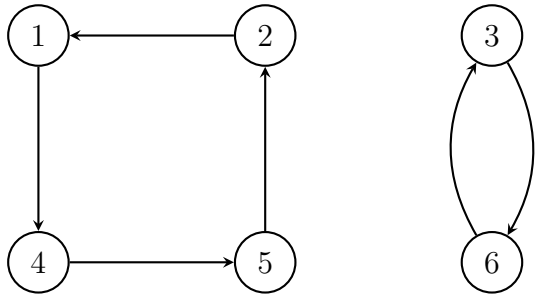
■

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 תמרוה הבאה על $\Sigma = \{1, 2, 3, 4, 5, 6\}$:

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

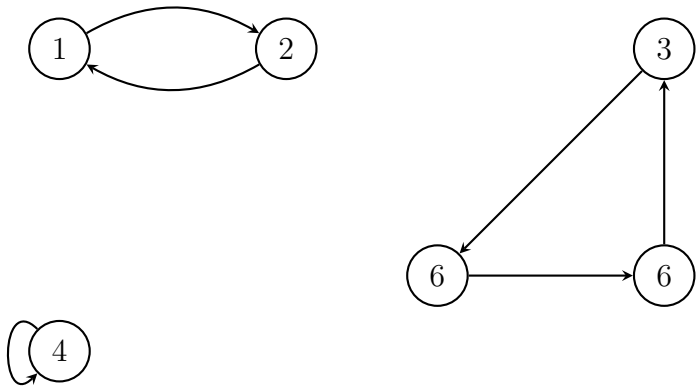
נגדיר הגרף המכוון $G_\pi = (V, E)$ כאשר הקבוצת הקודקודים היא $V = \Sigma$, ולכל $x \in \Sigma$ נגידר צלע מ- x ל- $\pi(x)$. ז"א $E = \{e_1, e_2, \ldots, e_n\}$ כאשר $e_i = x_i\pi(x_i)$ היא הצלע מקודקוד x_i לקודקוד $\pi(x_i)$. על פי ההגדרה הזאת הגרף G_π של התמורה π היא כמתוארת באיור למטה.



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 $\Sigma = \{x_1, \quad \dots \quad , x_n\}$.
אם

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

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

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