החבורה הסימטרית - הרצאה מס' 1

הגדרות בסיסיות

לכל n טבעי, $[n] := \{1, \dots, n\}$

תמורה (permutation) של $[n]$ היא פונקציה חח"ע ועל $\pi : [n] \to [n]$.

אוסף כל התמורות של $[n]$ מסומן

$$S_n := \{\pi \mid \pi : [n] \to [n] \text{ חח"ע ועל}\}.$$

על S_n מוגדרת באופן טבעי פעולת ההרכבה (של פונקציות):

$$\forall i \in [n] \quad (\pi \circ \sigma)(i) := \pi(\sigma(i))$$

לגבי פעולה זו, S_n היא חבורה הנקראת החבורה הסימטרית.

דרכים לרשום תמורה:

(I) כתיבה בשתי שורות

$$\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix} \in S_n$$

למשל

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

(II) כתיבה בשורה אחת (= השורה השנייה בכתיבה הנ"ל)

$$\pi = [2\ 6\ 1\ 4\ 3\ 5] \in S_n$$

הרכבת תמורות

$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \in S_3 \qquad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \in S_3$

$$\begin{array}{cccc} & 1 & 2 & 3 \\ \sigma\downarrow & 2 & 3 & 1 \\ \tau\downarrow & 1 & 3 & 2 \end{array} \Rightarrow \quad \tau\circ\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

מצד שני

$$\begin{array}{cccc} & 1 & 2 & 3 \\ \tau\downarrow & 2 & 1 & 3 \\ \sigma\downarrow & 3 & 2 & 1 \end{array} \qquad \sigma\circ\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

מסקנה:

לכל $n \geq 3$ S_n היא חבורה לא קומוטטיבית.

הערה: אם $k \leq n$, S_k איזומורפי לתת החבורה של S_n הקבועת (כלומר מקבעת במקום) את $n, \ldots, k+1$:

$\varphi : S_k \to S_n$

$$\pi \longmapsto \begin{pmatrix} 1 & \cdots & k & k+1 & \cdots & n \\ \pi(1) & & \pi(k) & \underbrace{k+1 \qquad n}_{} \end{pmatrix}$$

כל האיברים במקום שאחרי k נשארים במקום.

φ הומומורפיזם חח"ע של חבורות ("השיכון הטבעי" של S_k ב S_n).

- איבר היחידה של S_n הוא איבר הזהות

$e = id_n = \begin{pmatrix} 1 & 2 & \ldots & n \\ 1 & 2 & \ldots & n \end{pmatrix} \in S_n$

והתמורה ההופכית של $\pi \in S_n$ מתקבלת מסידור מחדש של סימונו

$\begin{pmatrix} \pi(1) & \pi(2) & \ldots & \pi(n) \\ 1 & 2 & & n \end{pmatrix}$

למשל: נניח שנתונה התמורה

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

$$\pi^{-1} = \begin{pmatrix} 3 & 2 & 5 & \boxed{1} & 4 \\ 1 & 2 & 3 & \boxed{4} & 5 \end{pmatrix} = \begin{pmatrix} \boxed{1} & 2 & 3 & 4 & 5 \\ \boxed{4} & 2 & 1 & 5 & 3 \end{pmatrix}$$

הגדרה – נקודת שבת (Fixed point)

$i\in[n]$ נקודת שבת של $\pi\in S_n$ אם $\pi(i)=i$.

חילוף (transposition)

הוא תמורה כך ש:

$$\#\{i\in[n] \mid \pi(i)\neq i\} = 2$$

כלומר קיים $i_1\neq i_2$ כך ש $\pi(i_1)=i_2$, $\pi(i_2)=i_1$

ולכל $i\neq i_1,i_2$, $\pi(i)=i$.

באופן כללי יותר, נגדיר K cycle:

K מחזור (או: מחזור באורך K) הוא תמורה $\pi\in S_n$ שעבורה קיימים $i_1,\dots,i_k\in[n]$ שונים זה מזה כך ש:

$$\pi(i_1)=i_2 \quad \pi(i_2)=i_3 \quad \dots \quad \pi(i_{k-1})=i_k, \quad \pi(i_k)=i_1$$

!

$$\pi(i)=i \quad \Big(\forall i\notin \underbrace{\{i_1,\dots,i_k\}}_{\text{support} = \text{התומך של } \pi}\Big)$$

(שימוש: סימון K מחזור כזה בכתיב מקוצר

$$\pi=(i_1,\dots,i_k)$$

למשל:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 6 & 4 & 3 & 2 \end{pmatrix} = (2\ 5\ 3\ 6)\in S_6$$

זהו 4-מחזור.

(חילוף = 2-מחזור).

טענה:

כל מחזור ב- S_n אפשר להציג כמכפלת מחזורים זרים.

הגדרה:

מחזורים $\sigma, \pi \in S_n$ נקראים זרים אם לכל $i \in [n]$
$\pi(i) = i$ או $\sigma(i) = i$, כלומר אין נקודה שבה
משתנים, פירוש הדבר הוא שהתומכים של π ו- σ
הם קבוצות זרות.

לדוגמה: $(1\,3\,2)$ זר ל- $(4\,5)$ כי

$$\pi = \underbrace{(1\,3\,2)}_{\text{תומך}}\underbrace{(4)(5)}_{\text{נקודות שבת}} \qquad \pi = \underbrace{(4\,5)}_{\text{תומך}}\underbrace{(1)(2)(3)}_{\text{נקודות שבת}}$$

(ניתן לראות שאין נקודות שבת משותפות)

יחידות ההצגה כמכפלת מחזורים זרים:

ההצגה כמכפלה היא יחידה עד כדי סדר הגורמים וסיבוב ציקלי של כל גורם (מחזור).

למשל:

$$S_7 \ni \pi = \begin{pmatrix}1&2&3&4&5&6&7\\3&2&6&7&5&1&4\end{pmatrix} = (1,3,6)(2)(4,7)(5) =$$

$$= (2)(5)(7,4)(6,1,3)$$ [שינוי סדר הגורמים ושינוי ציקלי].

כמובן ש: $(1,3,6) \neq (1,6,3)$

- לעיתים משמיטים בהצגה את המחזורים באורך 1 (נקודות השבת): $\pi = (1,3,6)(4,7)$
ואז צריך לומר במפורש מהו n.

היפוכים וסימן, הגדרה:

תהי $\pi \in S_n$ ויהי $1 \le i,j \le n$.

הזוג (i,j) נקרא היפוך (inversion) של π

אם $\boxed{i<j \quad \wedge \quad \pi(i) > \pi(j)}$

קבוצת ההיפוכים (inversion set):

קבוצת ההיפוכים של π מסומנת:

$$Inv(\pi) := \{(i,j) \mid i<j,\ \pi(i) > \pi(j)\}$$

וגודלה הוא <u>מספר ההיפוכים</u> (inversion number)

$$inv(\pi) = |Inv(\pi)| = \#\{(i,j) \mid i<j \wedge \pi(i) > \pi(j)\}$$

<u>למשל</u>:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 5 & 2 \end{pmatrix} \in S_5$$

$$Inv(\pi) = \{(1,2), (1,5), (3,5), (4,5)\}$$

$$\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 3 & 4 \end{pmatrix}$$

$$Inv(\pi^{-1}) = \{(1,3), (2,3), (2,4), (2,5)\}$$

כאן, $inv(\pi) = inv(\pi^{-1}) = 4$

<u>תרגיל</u>:

לכל $\pi \in S_n$, הוכח כי: $inv(\pi) = inv(\pi^{-1})$

- זו דוגמא ראשונה של <u>פרמטר</u> (statistic)
של תמורות.

הגדרה:

<u>הסימן</u> של תמורה $\pi \in S_n$ הוא

$$Sign(\pi) := (-1)^{inv(\pi)} \in \{1, -1\}$$

<u>טענה:</u>

$$\mathrm{Sign}(\pi) = \prod_{1\le i<j\le n} \frac{\pi(j)-\pi(i)}{j-i}$$

<u>הסבר:</u>

במונה ובמכנה מופיעים כל זוגות ההפרשים. במכנה - תמיד חיובי (כי תמיד $j>i$)
ואילו במונה - שליליות עד פי מספר ההיפוכים.

<u>מסקנה:</u> הסימן הוא <u>כפלי</u>

כלומר: $\mathrm{Sign}(\pi\circ\sigma) = \mathrm{Sign}(\pi)\cdot\mathrm{Sign}(\sigma)$ $\forall \pi,\sigma\in S_n$.

<u>הוכחת המסקנה:</u>

$$\mathrm{Sign}(\pi\circ\sigma) = \prod_{i<j}\left[\frac{\pi(\sigma(j))-\pi(\sigma(i))}{\sigma(j)-\sigma(i)}\cdot\frac{\sigma(j)-\sigma(i)}{j-i}\right] =$$

$$= \prod_{i<j}\frac{\pi(\sigma(j))-\pi(\sigma(i))}{\sigma(j)-\sigma(i)}\cdot\prod_{i<j}\frac{\sigma(j)-\sigma(i)}{j-i} = \mathrm{Sign}(\pi)\cdot\mathrm{Sign}(\sigma)$$

לסדר מחדש כי σ חח"ע ועל.

<u>תרגיל:</u>

ההפרש הסימטרי

$$\mathrm{Inv}(\pi\circ\sigma) = \mathrm{Inv}(\sigma)\,\triangle\,\sigma^{-1}(\mathrm{Inv}(\pi))$$

זוגות לא סדורים

$$(-1)^{\mathrm{inv}(\pi\circ\sigma)}$$

$$\mathrm{inv}(\pi\circ\sigma) \equiv \mathrm{inv}(\sigma)+\mathrm{inv}(\pi) \pmod 2$$

לבדוק פה.

<u>לברר</u>

משפט :

א) כל חילוף $\pi=(i_1,i_2)$ $\Leftarrow$ $Sign(\pi)=-1$.

ב) לכל k-מחזור π : $Sign(\pi)=(-1)^{k-1}$

ג) אם π היא מכפלת מחזורים זרים באורכים $k_1,\dots,k_t$ אז :

$$Sign(\pi)=(-1)^{\sum_{i=1}^{t}(k_i-1)}$$

הוכחה :

א) הוכחה ישירה :

$$\pi=(i_1,i_2)=\begin{pmatrix}\dots & i_1 & \dots & i_2\\ \dots\ \dots & i_2 & & i_1\end{pmatrix}\in S_n$$

כאשר $i_1<i_2$ אז

$$Inv(\pi)=\{(i_1,i_2)\}\cup\bigcup_{i_1<i<i_2}\{(i_1,i)\ (i,i_2)\}$$

ולכן $inv(\pi)$ אי-זוגי $Sign(\pi)=-1$

כלומר הקבוצה כוללת את ההיפוך הנוצר מהחילוף, ועוד היפוכים שבאים בזוגות. כל אינדקס i בין שני המוחלפים מוסיף שני היפוכים.

[אפשר גם ע״י $\begin{pmatrix}\dots & i_1 & \dots & i_2 \dots\\ \dots & i_2 & \dots & i_1 \dots\end{pmatrix}$ ולספור כמה היפוכים.]

ב) כל k מחזור הוא מכפלת $k-1$ חילופים (לא זרים).

$$(i_1,\dots,i_k)=(i_1,i_2)(i_2,i_3)\cdots(i_{k-1},i_k)$$

ומכלל הכפליות

$$Sign(\pi)=(-1)^{k-1}$$

ג) נובע ישירות מכפליות הסימן.

הערה:

בסעיף (ב) נותן את הדרך המהירה ביותר לחישוב הסימן ($O(n)$ צעדים, בהשוואה ל- $O(n^2)$ למציאת $inv(\pi)$).

למשל:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 6 & 4 & 2 & 1 \end{pmatrix} \implies sign(\pi) = (-1)^{2+1+0} = -1$$

כי:

$$\Downarrow$$

$$\underbrace{(1\ 3\ 6)}_{\substack{k=3 \\ \downarrow \\ k-1=2}} \underbrace{(2\ 5)}_{\substack{k=2 \\ \downarrow \\ k-1=1}} \underbrace{(4)}_{\substack{k=1 \\ \downarrow \\ k-1=0}} \implies$$

הערה:

אם נסמן את מספר המחזורים (cycle number) הזרים שמרכיבים את π (כולל מחזורים באורך 1) ב: $cyc(\pi)$

אז נקבל:

$$\boxed{sign(\pi) = (-1)^{n-cyc(\pi)}}$$

הסבר: אם $k_1,\dots,k_t$ הם אורכי המחזורים

$$\sum_i (k_i - 1) = \sum_i k_i - \sum_i 1 = n - cyc(\pi)$$

הגדרה: זוגיות התמורה

תמורה $\pi \in S_n$ נקראת זוגית (even) אם $sign\,\pi = 1$ (כלומר, אם $inv(\pi)$ זוגי). אחרת היא נקראת אי זוגית (odd).

אוסף כל התמורות הזוגיות ב- S_n שמסומן

$$A_n := \{\pi \in S_n \mid sign(\pi) = 1\}$$

ומהווה תת-חבורה (נורמלית) מאינדקס 2 של S_n הנקראת החבורה המתחלפת (Alternating Group) עבור $n \geq 2$.

הערה:

A_n הוא הגרעין של הפונקציה הסימן

$\text{Sign}: S_n \to \{1,-1\}$ (הומו')

לכן הוא תת חבורה נורמלית, והיא מאינדקס 2

(תזכורת: כל תת חבורה מאינדקס 2 היא נורמלית).

תת חבורות והצמדה ב S_n, A_n:

מה אפשר לומר על תת-חבורות של S_n?

משפט CALEY:

כל חבורה סופית איזומורפית לתת-חבורה של S_n עבור n מתאים.

הוכחה:

אם G חבורה סופית, $|G|=n$, נוכל להגדיר לכל $g\in G$ (כאשר G פועלת על עצמה):

$$\varphi_g : G \to G,\quad x \mapsto gx$$

(פעולה של G על עצמה זו כפל משמאל).

ברור ש φ_g היא תמורה על G ואם נמספר (שרירותית) את איברי G ב: $[n]$ נקבל $\varphi_g \in S_n$.

ויתר על כן, $\varphi: G \to S_n$, $g \mapsto \varphi_g$ היא הומו' של חבורות חח"ע

דוגמה:

$$G=\{z\in\mathbb{C}\mid z^4=1\}=\{1,i,-1,-i\}\quad(\cong \mathbb{Z}_4,+)$$

נראה היכן ישלח האיבר $i\in G$:

$$\rho_i:\ \begin{matrix}1\to i\\ i\to -1\\ -1\to -i\\ -i\to 1\end{matrix}\ \Bigg\}\implies \rho_i=\begin{pmatrix}1 & i & -1 & -i\\ i & -1 & -i & 1\end{pmatrix}$$

אם נמספר $[4]:\ 1\ 2\ 3\ 4$

$G:\ 1\ i\ -1\ -i$

אז:

$$\rho_i=\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}\in S_4$$

באותו אופן,

$$\rho_{-1}=\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}$$

ואכן מתקיים ש $\rho:G\to S_4$ מעתיקה את G לתת-חבורה של S_4 הנוצרת ע"י ρ_i $\rho_i=(1,2,3,4)$.

באמור $\rho:G\to S_4$ הומו' חח"ע ולכן G איזומורפי ל $\rho(G)$ שהיא תת חבורה של S_n.

שאלה: מה לגבי תת-חבורות נורמליות?

לשם כך נדבר תחילה על הצמדה ב S_n.

הגדרות:

אם $\pi,\sigma\in G$ אז $\pi^{-1}\sigma\pi\in G$ הוא **האיבר הצמוד** (conjugate) ל σ ע"י π.

אוסף האיברים הצמודים ל $g\in G$ נקרא **מחלקת הצמידות** של g

$$C_g:=\{h^{-1}gh\mid h\in G\}.$$

מחלקות הצמידות ב S_n.

שאלה

איך נראה מחלקי צמידות ב S_n ?

סימון

אם $\pi \in S_n$ היא מכפלת מחזורים זרים באורכים

$k_1,\dots,k_t$ כאשר $k_1 \geq \dots \geq k_t \geq 1$

$(k_1+\dots+k_t = n)$

אז נאמר ש π בעלת <u>מבנה מחזורי</u> כזה:

$$Cyc(\pi) = (k_1,\dots,k_t)$$

חלוקה של n (partition):

<u>למשל:</u>

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

אז

$$Cyc(\pi) = (3,2,2,1) \vdash 8$$

חלוקה של

- מספר החלקים ב $Cyc(\pi)$ הוא כמובן מספר המחזורים $cyc(\pi)$.

טענה:

עבור $\pi,\sigma \in S_n$ σ_1,σ_2 צמודים (כלומר $C_{\sigma_1} = C_{\sigma_2}$)

$\Longleftrightarrow$ ל σ_1,σ_2 אותו מבנה מחזורים, כלומר

$$Cyc(\sigma_1) = Cyc(\sigma_2)$$

הוכחה:

$$\sigma = (i_{11}, i_{12},\dots i_{1k_1})(i_{21},\dots i_{2k_2})\dots \in S_n$$

אז לכל $\pi \in S_n$

$$\pi\sigma\pi^{-1} = (\pi(i_{11}), \pi(i_{12}),\dots \pi(i_{1k_1}))(\quad)\dots$$

דוגמא:

$$\sigma = (1\,2\,3)(4\,5)(6\,7)$$

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 2 & 1 & 7 & 5 & 4 \end{pmatrix} \quad \left(= (1\,3\,2\,6\,5\,7\,4)\right)$$

אז

$$\pi\sigma\pi^{-1} = (3\,6\,2)(1\,7)(5\,4)$$

מכאן ברור שלתמורות צמודות יש אותו מבנה מחזורים וכן להפך: אם $Cyc(\sigma_1) = Cyc(\sigma_2)$ (נחשוב את σ_1, σ_2 כמכפלת מחזורים זרים באורכים לא עולים:

$$\sigma_1 = (i_{11}, \dots, i_{1k_1})(i_{21}, \dots, i_{2k_2})(\cdots)$$

$$\sigma_2 = (j_{11}, \dots, j_{1k_1})(j_{21}, \dots, j_{2k_2})(\cdots)$$

ונגדיר $\pi \in S_n$ ע"י $\pi(i_{11}) = j_{11}$ וכו'.

אז נקבל ש: $\sigma_2 = \pi\sigma_1\pi^{-1}$ כלומר σ_2 צמודה ל σ_1.

{כלומר כל טבלה למציאת המצמיד π המתאים

ספק לכן ש σ_1 ! σ_2 צמודות].

תרגיל:

מהן מחלקות הצמידות ב A_n.

תזכורת:

תת חבורה H של חבורה G היא נורמלית אם $\forall g \in G$ מתקיים: $g^{-1}Hg = H$

שאלה:

מהן אם כן תת החבורות הנורמליות של S_n (חוץ מ A_n)?

תשובה:

(א) עבור $n\neq 4$, תת-חבורות נורמליות של S_n הן: $S_n, A_n, \{Id\}$.

(ב) לכל $n\neq 4$, תת-החבורות הנורמליות של A_n הן: $A_n, \{id\}$.

מסקנה:

עבור $5\leq n$, A_n היא חבורה לא קומוטטיבית פשוטה.
(כלומר בלי תת-חבורות נורמליות לא טריוויאליות).
(A_n פשוטה גם עבור $n\leq 3$ אבל אז היא אבלית).

כיוון הוכחה של (ב) (דומה ל(א)):

טענת עזר:

לכל $3\leq n$, המחזורים $(123),(124),\dots,(12n)$ יוצרים את A_n.

הוכחת טענת העזר:

באינדוקציה על n, המעבר: אם $\sigma\in S_n$, $\sigma(n)\neq 1,2$, אז $\tilde{\sigma}=(1,2,n)^{-1}(1,2,\sigma(n))\sigma$ מקיים $\tilde{\sigma}(n)=n$ ואילו אם $\sigma(n)\in\{1,2\}$ אז זה עוד יותר קל.

- לכל $3\leq n$, אם H ת״ח נורמלית של A_n המכילה 3-מחזור אז $H=A_n$ (הוכחה קודמת).

מחזור להוכחת המשפט:

H ת״ח נורמלית של A_n ($5\leq n$), $H\neq\{id\}$. נוכיח כי $H=A_n$. ניקח $id\neq\sigma\in H$ עם מספר מקסימלי של נקודות שבת ונראה כי σ היא 3-מחזור (פירוק למקרים).

- הערה: שלח הוכחות מלאות ל(א) ו(ב) בנפרד.