©צוות קורס "תורת המספרים האלגוריתמית" סמסטר א תש״ף:
בר אלון, מיכאל פרי, שמואל שמעוני, איברהים שאהין, דורון מור,
ד״ר חיה קלר, ד״ר אלעד אייגנר-חורב
נכתב ע"י בר אלון

מעגלים בפרמוטציות

הגדרה:

עבור פרמוטציה (תמורה) $\sigma \in S_X$ *נסמן*

$$M_\sigma = \{x \in X : \sigma(x) \neq x\}$$

להיות קבוצת הנקודות שאינן נקודות שבת של σ.

הגדרה:

יהי $\sigma \in S_X$. *אם* $M_\sigma = \{i_1, i_2, \dots, i_r\}$ *וגם*

$$i_1 \overset{\sigma}{\to} i_2, \dots, i_{r-1} \overset{\sigma}{\to} i_r$$

אזי נאמר שσ *הוא מעגל באורך* r, *ונכתוב אותו כ-*$(i_1, \dots, i_r)$.

מעגלים באורך 2 מחליפים זוגות של איברים ולכן נקרא להם *חילופים* (או טרנספוזיציות).

<u>דוגמה:</u>

הפרמוטציה

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

הינה מעגל באורך 4, על כן נוכל לכתוב אותה בכתיב המקוצר $(1\ 2\ 3\ 4)$.

הפרמוטציה

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

הינה מעגל באורך 5 אותה נכתוב כ-$(1\ 5\ 3\ 4\ 2)$. שתי הדוגמאות לעיל היו ללא נקודות שבת. הפרמוטציה

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

הינה מעגל באורך 3 אותה נכתוב כ-$(1\ 2\ 3)(4)(5) = (1\ 2\ 3)$.

(שימו לב כי משמעות הסימון (4) לעיל היא כי 4 עובר לעצמו. לפעמים מתייחסים לסימון זה כמעגל באורך 1.)

הכתיב המקוצר בו השתמשנו בדוגמה מהווה צורה נוחה לכתיבת פרמוטציות כשמתעניינים בהרכבה (הנקראת גם מכפלה) של פרמוטציות.

דוגמה:

יהי $\alpha = (1\ 2)$ ויהי $\beta = (1\ 3\ 4\ 2\ 5)$. אזי

$$\alpha\beta = (1\ 2)(1\ 3\ 4\ 2\ 5) = (1\ 3\ 4)(2\ 5)$$

כאשר שני המעגלים שנתקבלו זרים. (כלומר אף מספר לא מופיע בשני המעגלים.)

דוגמה:

נשים לב כי

$$S_3 = \{\mathbf{1}_{[3]}, (1\ 2\ 3), (1\ 3\ 2), (1\ 2), (1\ 3), (2\ 3)\}$$

לפיכך, S_3 מורכבת ממעגלים, דהיינו כל תמורה ב-S_3 מלבד תמורת הזהות היא מעגל באורך 2 או 3.

הפיכת התמורה המיוצגת כמעגל מסתכמת בהילוך על המעגל בכיוון ההפוך.

אבחנה:

אם σ מעגל באורך r אזי σ^{-1} מעגל באורך r גם כן. יתרה מכך, אם $\sigma = (i_1, \dots, i_r)$ אזי $\sigma^{-1} = (i_r, \dots, i_1)$.

אי-הבהירות הבאה עולה. בהינתן $\sigma = (1\ 2\ 4)$, האם היא בS_4 ומקבעת את 3, או שהפרמוטציה בS_5 ומקבעת את 3 ואת 5? לפעמים זה יהיה ברור מההקשר. כאשר זה לא המצב, המוסכמה בה נשתמש היא *שזה לא משנה*. בפרט, כל איבר בS_n נוכל להתייחס אליו כאל איבר בS_{n+1} כאשר $n+1$ מהווה נקודת שבת שלו, כלומר

$$S_1 \subseteq S_2 \subseteq S_3 \subseteq \cdots$$

לא כל פרמוטציה היא מעגל, כפי שהדוגמה הבאה מראה לנו.

דוגמה:

נשקול את הפרמוטציה הבאה

$$\sigma \coloneqq \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 1 & 7 & 6 & 10 & 4 & 2 & 5 & 9 & 8 \end{pmatrix}$$

נשים לב כי בפרמוטציה זו נמצאים המעגלים הזרים בזוגות $(1\ 3\ 7\ 2)$, $(4\ 6)$, $(5\ \ 10\ \ 8)$ ו(9). יתרה מזאת, נשים לב כי σ הינה המכפלה (דהיינו ההרכבה) של מעגלים אלו, כלומר

$$\sigma = (1\ 3\ 7\ 2)(4\ 6)(5\ 10\ 8)(9)$$

שימו לב כי גם יכולנו לבטא את σ כהרכבה של אותם מעגלים בסדר שונה, למשל

$$\sigma = (4\ 6)(1\ 3\ 7\ 2)(5\ 10\ 8)(9)$$

חופש הבחירה הזה נובע מכך שהמעגלים זרים.

מעגלים הינם אובייקטים מורכבים יותר מכפי שהם נראים. לדוגמה, חזקות של מעגלים לא בהכרח מהווים מעגלים. אכן, עבור $\alpha = (1\ 2\ 3\ 4)$ מתקיים $\alpha^2 = (1\ 3)(2\ 4)$. בדומה, ניתן להשתמש בחזקות על מנת לגרום לשני מעגלים להתלכד.

למה:
יהיו α ו β מעגלים בS_n. אם קיים $i \in M_\alpha \cap M_\beta$ עבורו $\alpha^k(i) = \beta^k(i)$, לכל $k \geq 1$, אזי $\alpha = \beta$.

<u>הוכחה:</u>
נשים לב תחילה ש$M_\beta = M_\alpha$. אכן, אם זה לא מתקיים, אזי קיימת $j \in M_\alpha \setminus M_\beta$ נקודת שבת של β, אך לא של α. מכיוון שα מעגל, נובע שקיים k כך ש

$\alpha^k(i) = j$, ולכן על פי ההנחה $\beta^k(i) = j$. מכיוון שj היא נקודת שבת של β נובע כי $\beta^{k+1}(i) = \beta\left(\beta^k(i)\right) = \beta(j) = j$, אך j אינה נקודת שבת של α ולכן $\alpha^{k+1}(i) = \alpha\left(\alpha^k(i)\right) = \alpha(j) \neq j$, סתירה.

העובדה כי $M_\beta = M_\alpha$ יחד עם ההנחה ש$\alpha^k(i) = \beta^k(i)$ לכל $k \geq 1$, גוררת כי כל איבר נמצא במרחק שווה מi לאורך שני המעגלים, ולכן α וβ מתלכדים כמתבקש. ■

לפרמוטציות של קבוצות סופיות יש את התכונה שכל איבר בקבוצה, או שהוא מהווה נקודת שבת, או שהוא שייך למעגל כלשהו. לכן המשפט הבא אינו מפתיע.

משפט:
כל פרמוטציה $\alpha \in S_n$ הינה מעגל או ניתנת לכתיבה כמכפלה של מעגלים זרים בזוגות.

<u>הוכחה:</u>
ההוכחה באינדוקציה על $|M_\alpha|$. עבור בסיס נשקול את המקרה כאשר $|M_\alpha| = 0$.

אכן, הטענה מתקיימת, שכן $\alpha = \mathbf{1}_{[n]}$ במקרה זה. נניח כעת כי הטענה נכונה לכל הפרמוטציות α עבורן $|M_\alpha| \le k$ עבור $k \in Z^+$ כלשהו, ונוכיח את הטענה עבור פרמוטציה α המקיימת $1 \le |M_\alpha| = k+1$. נבחר $i_1 \in M_\alpha$ שרירותית, ונשקול את המעגל $(i_1, \dots, i_r)$ באורך r היחיד המכיל אותו (מעגל זה קיים שכן נוכל לבחור את r להיות השלם החיובי הקטן ביותר עבורו

$\alpha(i_1) = i_2, \alpha(i_2) = i_3, \dots, \alpha(i_r) = i_1$). אם $r = n$ אזי α הינה מעגל. נניח אם כן כי $r < n$, ונסמן בY את קבוצת $n - r$ האיברים שאינם במעגל שנבחר. אזי $\alpha(Y) = Y$ וגם $\alpha(\{i_1, \dots, i_r\}) = \{i_1, \dots, i_r\}$. (שימו לב כי בסימון הזה אנו מפעילים באגף שמאל תמורה על קבוצת ערכים, ואגף ימין מבטא את קבוצת הערכים המתקבלים כתמונות.) מהנחת האינדוקציה נובע כי $\alpha|_Y$ הינה מעגל או ניתנת למכפלה של מעגלים זרים בזוגות. העובדה כי Y ו$\{i_1, \dots, i_r\}$ זרים גוררת ש$\alpha =$ $(\alpha|_Y)(i_1, \dots, i_r)$ היא מכפלה של מעגלים זרים בזוגות, כפי שנתבקש להוכיח.

הייצוג של פרמוטציה כמכפלה של מעגלים זרים מכונה *פירוק (פקטוריזציה)* של הפרמוטציה. המשפט הנ"ל קובע כי כל פרמוטציה ניתנת לפירוק שכזה. בפירוקים אלו לא ברור האם יש צורך לוותר על הרישום של נקודות שבת. המושג *פירוק שלם* מופיע בספרות לעיתים על מנת לתאר פירוק בו כל נקודת שבת i מופיעה כ(i) בפירוק. ביתר הקורס, אם לא נאמר אחרת, נניח כי פירוק הינו פירוק שלם. המשפט הבא קובע כי פירוק הוא למעשה יחיד. לצורך הוכחת המשפט ניעזר בשתי הטענות הבאות.

הגדרה: שתי פרמוטציות $\sigma, \tau \in S_X$ תיקראנה זרות אם $M_\sigma \cap M_\tau = \emptyset$.

טענה:

כל שתי פרמוטציות $\sigma, \tau \in S_X$ זרות הינן מתחלפות, כלומר $\sigma\tau = \tau\sigma$.

<u>הוכחה:</u>

יהי $x \in X$. נראה כי $\sigma\tau(x) = \tau\sigma(x)$. מכיוון ש$M_\sigma \cap M_\tau = \emptyset$ קיימים שלושה מקרים לגבי הימצאותו של x.

<u>מקרה 1:</u> אם $x \in M_\sigma$ אזי $\sigma(x) \in M_\sigma$. לכן $x, \sigma(x) \notin M_\tau$, כלומר הן מהוות נקודות שבת של τ. לכן

$$\tau\sigma(x) = \tau\big(\sigma(x)\big) = \sigma(x) = \sigma\big(\tau(x)\big) = \sigma\tau(x)$$

מקרה 2: המקרה בו $x \in M_\tau$ ניתן לטיפול באופן דומה למקרה 1.
מקרה 3: כעת נניח כי $x \notin M_\sigma \cup M_\tau$, ולכן מהווה נקודות שבת של שתי הפרמוטציות. לכן
$$\tau(\sigma(x)) = \tau(x) = x = \sigma(x) = \sigma(\tau(x))$$

טענה:
יהי $\alpha = \beta\gamma \in S_n$, כאשר β ו-γ פרמוטציות זרות. אם $i \in M_\beta$ אזי $\alpha^k(i) = \beta^k(i)$ לכל $k \geq 0$.

הוכחה:
נשים לב כי הזרות של β ו-γ גוררת כי $\gamma|_{M_\beta} = \mathbf{1}_{M_\beta}$. לכן על כל איברי M_β מתקיים כי α מתלכד עם β, ובפרט אם $i \in M_\beta$ אז $\alpha^k(i) = \beta^k(i)$ לכל $k \geq 0$.

משפט:
יהי $\alpha \in S_n$ ויהי $\alpha = \beta_1 \cdots \beta_t$ פירוק כלשהו של α למעגלים זרים בזוגות. אזי פירוק זה יחיד עד כדי שינוי הסדר של ה-β_i במכפלה.

הוכחה:
נניח כי $\alpha = \gamma_1 \cdots \gamma_s$ הינו פירוק נוסף של α למעגלים זרים בזוגות. על פי חוק הצמצום נוכל להניח ללא הגבלת הכלליות כי אף β_i אינו מתלכד אם אף γ_j. יהי $i \in M_{\beta_t}$. אזי על פי הטענה השנייה נובע כי $\alpha^k(i) = \beta_t^k(i)$ לכל $k \in \mathbb{Z}^+$. מכיוון ש$M_{\beta_t} \subseteq M_\alpha$, נקבל ש$i \in M_\alpha$ ולכן קיים γ_j עבורו $i \in M_{\gamma_j}$. הטענה הראשונה גוררת כי ה-γ_ℓ-ות ניתנות לחילוף, ולכן על פי הטענה השנייה נובע כי $\gamma_j^k(i) = \alpha^k(i) = \beta_t^k(i)$ לכל $k \in \mathbb{Z}^+$. לפי הלמה אותה הוכחנו בעמוד 3 בתרגול זה, נובע כי $\beta_t = \gamma_j$, סתירה. ■

יהי $\alpha \in S_n$ מעגל באורך r. תכונה נחמדה של מעגלים היא ש$\alpha^r = \mathbf{1}_{[n]}$. למעשה, $\alpha^k = \mathbf{1}_{[n]}$לכל $r|k$. יתרה מכך, אם $\beta = \alpha_1 \cdots \alpha_t$ פירוק של β כאשר α_i מעגל באורך r_i, אזי $\beta^k = \mathbf{1}_{[n]}$ כאשר $r_i|k$ לכל $i \in [t]$. לכן נובעת הטענה הבאה.

טענה:

יהי $\beta \in S_n$ ויהי $\beta = \alpha_1 \cdots \alpha_t$ הפירוק של β למעגלים זרים בזוגות, כאשר α_i הינו מעגל באורך r_i. אזי השלם $\ell \in \mathbb{Z}^+$ הקטן ביותר המקיים $\beta^\ell = \mathbf{1}_{[n]}$ הוא $\ell = \mathrm{lcm}(r_1, \dots, r_t)$.

<u>תרגיל בית 1:</u>
תהי X קבוצה, ותהי $\tau \in S_X$. אזי ההעתקות הבאות מ-S_X ל-S_X מהוות פרמוטציות על S_X.

1. $\sigma \mapsto \sigma^{-1}$
2. $\sigma \mapsto \tau\sigma$
3. $\sigma \mapsto \sigma\tau$

<u>פתרון:</u>

1. נראה כי ההעתקה $\vartheta(\sigma) = \sigma^{-1}$ היא פרמוטציה על S_X. מכיוון ש$\sigma \in S_X$ ההופכית שלה היא פרמוטציה מוגדרת היטב בS_X. לכן ϑ היא העתקה מS_X לעצמה. נראה כעת כי ϑ היא חח״ע. נקבע שתי פרמוטציות $\xi_1, \xi_2 \in S_X$ עבורן $\vartheta(\xi_1) = \vartheta(\xi_2)$. אזי $\xi_1^{-1} = \xi_2^{-1}$. מכיוון ש $(\sigma^{-1})^{-1} = \sigma$ לכל פרמוטציה σ, נקבל שמתקיים כי
$$\xi_1 = (\xi_1^{-1})^{-1} = (\xi_2^{-1})^{-1} = \xi_2$$
ולכן ϑ חח״ע. העובדה כי $\vartheta(\sigma^{-1}) = (\sigma^{-1})^{-1} = \sigma$ גוררת שϑ היא על. לכן נוכל להסיק כי ϑ היא פרמוטציה על S_X.
2. נראה כי ההעתקה $\vartheta(\sigma) = \tau\sigma$ היא פרמוטציה על S_X. מכיוון ש$\tau\sigma \in S_X$ לכל $\sigma, \tau \in S_X$, נובע כי ϑ היא העתקה מS_X לעצמה.

נראה כעת כי ϑ היא חח״ע. נקבע שתי פרמוטציות $\xi_1, \xi_2 \in S_X$ עבורן $\vartheta(\xi_1) = \vartheta(\xi_2)$. אזי $\tau\xi_1 = \tau\xi_2$. מכלל הצמצום, אשר ניתן להשתמש בו שכן $\tau^{-1} \in S_X$ מוגדרת היטב, נובע כי $\xi_1 = \xi_2$ ולכן ϑ חח״ע. נעיר כי את הטיעון הנ"ל היה ניתן לעשות בצורה ישירה באופן הבא
$$\xi_1 = (\tau^{-1}\tau)\xi_1 = \tau^{-1}(\tau\xi_1) = \tau^{-1}(\tau\xi_2) = (\tau^{-1}\tau)\xi_2 = \xi_2$$

על מנת לראות מדוע ϑ היא על, נשים לב כי לכל $\xi \in S_X$ מתקיים
$$\xi = \mathbf{1}_X\xi = (\tau\tau^{-1})\xi = \tau(\tau^{-1}\xi) = \vartheta(\tau^{-1}\xi)$$
לכן נוכל להסיק כי ϑ היא פרמוטציה על S_X.

3. ההוכחה סימטרית לחלוטין לסעיף 2.