

Diskretne strukture

Permutacije, izročki

Fakulteta za računalništvo in informatiko
Univerza v Ljubljani

3. januar 2023

Kaj so permutacije

Naj bo A poljubna množica. *Permutacija* na A je vsaka bijektivna preslikava $f : A \rightarrow A$.

Permutacija reda n je permutacija v $\{1, 2, \dots, n\}$. Množico vseh permutacij reda n imenujemo *simetrična grupa reda n* in jo označimo z S_n .

Primer

- $\pi_1 : \{1, 2, 3\} \rightarrow \{1, 2, 3\}$, $\pi_1(1) = 2$, $\pi_1(2) = 3$, $\pi_1(3) = 1$, je *permutacija reda 3*. V kompaktni obliki jo zapišemo kot

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

- $\pi_2 : \{1, \dots, 6\} \rightarrow \{1, \dots, 6\}$, $\pi_2(1) = 2$, $\pi_2(2) = 3$, $\pi_2(3) = 4$, $\pi_2(4) = 1$, $\pi_2(5) = 5$, $\pi_2(6) = 6$, je *permutacija reda 6*. V kompaktni obliki jo zapišemo kot

$$\pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 1 & 5 & 6 \end{pmatrix}.$$

Produkt permutacij

Naj bosta $\pi, \psi \in S_n$ permutaciji reda n .

Produkt $\pi * \psi$ permutacij π in ψ je permutacija reda n , definirana kot

$$(\pi * \psi)(i) = \psi(\pi(i)) \quad \text{za vsak } i = 1, \dots, n. \quad (1)$$

Opomba

*Kompozitum funkcij $f \circ g$ je definiran s predpisom $(f \circ g)(x) = f(g(x))$. Produkt permutacij pa interpretiramo kot produkt relacij, tako da $(\pi * \psi)(i) = j$ pomeni $i(\pi * \psi)j$ in zato $(\pi * \psi)(i)$ izračunamo kot v (1).*

Primer

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 1 & 7 & 6 & 5 \end{pmatrix} \quad \psi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 5 & 4 & 2 & 3 & 1 & 6 \end{pmatrix}$$

$$\pi * \psi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 1 & 7 & 6 & 5 \end{pmatrix} * \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 5 & 4 & 2 & 3 & 1 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 4 & 2 & 7 & 6 & 1 & 3 \end{pmatrix}$$

$$\psi * \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 5 & 4 & 2 & 3 & 1 & 6 \end{pmatrix} * \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 1 & 7 & 6 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 7 & 1 & 3 & 4 & 2 & 6 \end{pmatrix}$$

Produkt permutacij **ni** komutativna operacija.

Inverzna permutacija

Z id_n označimo *identično permutacijo* reda n , tj. $\text{id}_n(i) = i$ za vsak $i = 1, \dots, n$.

Inverzna permutacija π^{-1} permutacije π je permutacija reda n , ki zadošča

$$\pi * \pi^{-1} = \pi^{-1} * \pi = \text{id}_n.$$

Primer

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 1 & 7 & 6 & 5 \end{pmatrix} \quad \psi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 5 & 4 & 2 & 3 & 1 & 6 \end{pmatrix}$$

$$\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 1 & 2 & 3 & 7 & 6 & 5 \end{pmatrix} \quad \psi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 4 & 5 & 3 & 2 & 7 & 1 \end{pmatrix}$$

$$\pi * \pi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 1 & 7 & 6 & 5 \end{pmatrix} * \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 1 & 2 & 3 & 7 & 6 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix} = \text{id}$$

Velja tudi: $\pi^{-1} * \pi = \psi * \psi^{-1} = \psi^{-1} * \psi = \text{id}$

Trditev

Naj bosta $\pi, \psi \in S_n$. Velja $(\pi * \psi)^{-1} = \psi^{-1} * \pi^{-1}$.

Zapis permutacije z disjunktными cikli

Permutacijo lahko zapišemo tudi *z disjunktными cikli* in ne v obliki *tabelice*.

Primer

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 1 & 7 & 6 & 5 \end{pmatrix} \quad \psi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 5 & 4 & 2 & 3 & 1 & 6 \end{pmatrix}$$

$$\begin{aligned} \pi &= (1234)(57)(6) = (1234)(57) = (6)(57)(1234) \\ &= (3412)(75)(6) = (176)(2534), \end{aligned}$$

$$\psi = (176)(2534),$$

$$\pi * \psi = (1234)(57) * (176)(2534) = (156)(2473),$$

$$\psi * \pi = (176)(2534) * (1234)(57) = (1543)(276).$$

Zapis $(i_1 i_2 i_3 \dots i_{k-1} i_k)$ preberemo kot

$$i_1 \mapsto i_2, i_2 \mapsto i_3, \dots, i_{k-1} \mapsto i_k, i_k \mapsto i_1.$$

Števila, ki jih izpustimo, se slikajo same vase.

Ciklična struktura permutacije

Primer

$\pi = (1234)(57)(6)$ je produkt 4-cikla, 2-cikla in 1-cikla,
 $\psi = (176)(2534)$ pa je produkt 3-cikla in 4-cikla.

Ciklična struktura permutacije π je zaporedje dolžin ciklov v zapisu permutacije z disjunktnimi cikli.

Primer

Naj bosta π in ψ kot v primeru zgoraj.
Ciklična struktura permutacije π je $[4, 2, 1]$.
Ciklična struktura permutacije ψ je $[4, 3]$.

1-ciklu pravimo tudi *fiksna točka* permutacije,
2-ciklu pa *transpozicija*.

Potenciranje permutacij

Za potenciranje permutacij je ugodnejši zapis permutacije z *disjunktnimi cikli* kot pa zapis v obliki *tabelice*.

$$\pi = (1234)(57)$$

Kako izračunati $\pi^2, \pi^3, \pi^4, \dots$?

$$\pi^2 = (1234)(57) * (1234)(57)$$

$$= (1234)^2(57)^2$$

$$= (13)(24)(57),$$

$$\pi^2 = (1234)(57) * (1234)(57) * (1234)(57)$$

$$= (1234)^3(57)^3$$

$$= (1432)(57),$$

⋮

Za potenciranje permutacij je dovolj poznati potence *ciklov*.

Primer

Potencirajmo 5- in 6-cikel, $\alpha = (12345)$, $\beta = (123456)$:

$$\alpha^2 = (13524), \alpha^3 = (14253), \alpha^4 = (15432), \alpha^5 = \alpha.$$

$$\beta^2 = (135)(246), \beta^3 = (14)(25)(36), \beta^4 = (153)(264),$$

$$\beta^5 = (165432), \beta^6 = \beta.$$

Trditev

Naj bo α permutacija, sestavljena iz samo enega cikla dolžine n .

Permutacija α^k ima ciklično strukturo

$$\underbrace{\left[\frac{n}{\gcd(n, k)}, \dots, \frac{n}{\gcd(n, k)} \right]}_{\gcd(n, k) \text{ členov}}.$$

Torej je sestavljena iz $\frac{n}{\gcd(n, k)}$ disjunktnih ciklov, ki so vsi iste dolžine

$$\frac{n}{\gcd(n, k)}.$$

Primer

Naj bo α 6–cikel. Velja:

- *Ciklična struktura α^2 je $[3, 3]$, saj je $\gcd(6, 2) = 2$.*
- *Ciklična struktura α^3 je $[2, 2, 2]$, saj je $\gcd(6, 3) = 3$.*
- *Ciklična struktura α^4 je $[3, 3]$, saj je $\gcd(6, 4) = 2$.*
- *Ciklična struktura α^5 je $[6]$, saj je $\gcd(6, 5) = 1$.*
- *Ciklična struktura α^6 je $[1, 1, 1, 1, 1, 1]$, saj je $\gcd(6, 6) = 6$.*
- *Ciklična struktura α^7 je enaka ciklični strukturi α .*
- *Ciklična struktura α^8 je enaka ciklični strukturi α^2 .*

Red permutacije π je najmanjše naravno število $k \geq 1$, za katerega je

$$\pi^k = \text{id.}$$

Trditev

Naj bo α permutacija, sestavljena iz samo enega cikla dolžine n . Potem je red permutacije α enak n in $\alpha^{-1} = \alpha^{n-1}$.

Trditev

Red permutacije π je najmanjši skupni večkratnik dolžin ciklov v zapisu permutacije π z disjunktными cikli. Oznaka: $r(\pi)$.

Primer

- Če je ciklična struktura α enaka $[3, 2]$ je $r(\alpha) = 6$.
- Če je ciklična struktura α enaka $[4, 3, 2]$ je $r(\alpha) = 12$.
- Če je ciklična struktura α enaka $[4, 3, 3, 2, 2]$ je $r(\alpha) = 12$.
- Če je ciklična struktura α enaka $[8, 7, 5, 2]$ je $r(\alpha) = 8 \cdot 7 \cdot 5$.

Potenciranje permutacij in zapis s transpozicijami

Izrek

Naj bo

$$\pi = \alpha_1 * \alpha_2 * \cdots * \alpha_m,$$

kjer so α_i , $i = 1, \dots, m$, cikli v zapisu permutacije α z disjunktnimi cikli.

Potem je

$$\pi^k = \alpha_1^k * \alpha_2^k * \cdots * \alpha_m^k.$$

Komentar: Permutacijo potenciramo tako, da jo zapišemo z disjunktnimi cikli in potenciramo vsak cikel posebej.

Trditev

Vsako permutacijo (iz S_n , $n \geq 2$) lahko zapišemo kot produkt transpozicij (2-ciklov).

Dokaz.

Trditev sledi iz enakosti: $(i_1 i_2 i_3 \dots i_k) = (i_1 i_2)(i_1 i_3) \cdots (i_1 i_k)$. □

Opomba

Zapis kot produkt transpozicij ni enolično določen.

Parnost permutacije

Permutacija je *soda*, če jo lahko zapišemo kot produkt sodo mnogo transpozicij.

Permutacija je *liha*, če jo lahko zapišemo kot produkt liho mnogo transpozicij.

Primer

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

Pravimo, da sta (v permutaciji π) števili 1 in 2 v *inverziji*, ker sta v spodnji vrstici tabele v napačnem vrstnem redu: 1 je manjše kot 2, toda 2 je zapisana pred 1.

Permutacija π ima 6 inverzij: 12, 13, 14, 56, 57, 67.

Izrek (o parnosti permutacij)

Denimo, da lahko permutacijo π zapišemo kot produkt m transpozicij, pa tudi kot produkt (morda drugih) n transpozicij. Potem je

$$m \equiv n \pmod{2}.$$

Permutacijska potenčna enačba je enačba oblike

$$\varphi^k = \alpha, \quad (2)$$

kjer je α znana permutacija, $k \in \mathbb{N}$, φ pa neznana permutacija.

Vprašanje. Kaj lahko povemo o rešljivosti enačbe (2)?

- $k = 0$: (2) je rešljiva samo, če je $\alpha = \text{id}$.
- $k = 1$: (2) je rešljiva.
- $k = 2$: Če je (2) rešljiva, potem je permutacija α soda.

Trditev

Enačba (2) je rešljiva natanko tedaj, ko je ciklična struktura φ^k enaka ciklični strukturi α .

Primer

Rešujemo enačbo

$$\varphi^2 = (1, 2)(3, 4)(5, 6, 7, 8, 9, 10, 11) = \alpha. \quad (3)$$

Ciklična struktura α je enaka $[7, 2, 2]$. Ker mora biti c.s. φ^2 enaka $[7, 2, 2]$, je φ oblike

$$[m], \quad [m_1, m_2] \quad \text{ali} \quad [m_1, m_2, m_3].$$

- Če je c.s. φ enaka $[11]$, potem je c.s. φ^2 enaka $[11]$, kar ni c.s. α . Torej ni rešitve.
- Če je c.s. φ enaka $[m_1, m_2]$, potem mora biti $m_1 = 7$, $m_2 = 4$. Torej rešitev je. Ugibajmo z metodo nedoločenih koeficientov:

$$\varphi = (x_1 x_2 x_3 x_4)(x_5 x_6 x_7 x_8 x_9 x_{10} x_{11}).$$

Potem je

$$\varphi^2 = (x_1 x_3)(x_2 x_4)(x_5 x_7 x_9 x_{11} x_6 x_8 x_{10}).$$

Primer

- Če je c.s. φ enaka $[m_1, m_2, m_3]$, potem je tudi

$$\text{c.s. } \varphi^2 \text{ enaka } [m_1, m_2, m_3] = [7, 2, 2].$$

Toda, če je c.s. φ enaka $[7, 2, 2]$ sledi, da je c.s. φ^2 enaka $[7, 1, 1, 1, 1]$. Torej ni rešitev.

$\varphi^2 = \alpha$, kjer je c.s. α enaka $[m]$

Če je c.s. α enaka $[m]$ sledi, da mora biti tudi c.s. φ^2 enaka $[m]$.

Trditev

Če je c.s. α enaka $[m]$, je $\varphi^2 = \alpha$ rešljiva natanko tedaj, ko je $\gcd(2, m) = 1$.

V tem primeru je rešitev celo ena sama, kar se vidi iz naslednjega premisleka.

Linearna diofantska enačba

$$2k + m\ell = 1$$

je namreč rešljiva. Zato velja

$$\alpha^k = (\varphi^2)^k = \varphi^{1-m\ell} = \varphi * (\varphi^m)^{-\ell} = \varphi * \text{id} = \varphi.$$

Trditev

Če je $\varphi^2 = \alpha$ rešljiva, potem je rešitev ena sama in enaka $\varphi = \alpha^k$.

$\varphi^2 = \alpha$, kjer je c.s. α enaka $[m, \dots, m]$

Trditev

Naj bo c.s. α enaka $[m, \dots, m]$.

- 1 Če je $\gcd(m, 2) = 1$, potem je $\varphi^2 = \alpha$ rešljiva, rešitev pa je več. Rešitve imajo ciklično strukturo oblike

$$[2m, \dots, 2m, m, \dots, m].$$

- 2 Če je $\gcd(m, 2) = 2$, potem je $\varphi^2 = \alpha$ rešljiva, če je r sod. Ciklična struktura φ mora biti oblike

$$[2m, \dots, 2m].$$

Primer

Obravnavajte rešljivost enačbe $\varphi^2 = \alpha$ pri c.s. α enako $[3, 3, 3, 3, 3]$.

Velja $\gcd(3, 2) = 1$, zato obstajajo rešitve φ za vsako od naslednjih cikličnih struktur $[6, 6, 3]$, $[6, 3, 3, 3]$, $[3, 3, 3, 3, 3]$.

Naj bo

c.s. α enaka $[m_1, \dots, m_1, m_2, \dots, m_2, \dots, m_\ell, \dots, m_\ell]$.

V tem primeru rešimo enačbe

$$\varphi_j^2 = \alpha_1^{(j)} * \dots * \alpha_{i_j}^{(j)}, \quad j = 1, \dots, \ell,$$

pri čemer so $\alpha_i^{(j)}$ vsi cikli v α dolžine m_j .

Rešitev $\varphi^2 = \alpha$ je potem

$$\varphi = \varphi_1 * \dots * \varphi_\ell.$$

Primer

Reši enačbo $\varphi^2 = (123)(456)(789)(10, 11)(12, 13)(14)$.

Rešujemo $\varphi_1^2 = (123)(456)(789)$, $\varphi_2^2 = (10, 11)(12, 13)$ in $\varphi_3^2 = (14)$.

- Če je c.s. φ_1^2 enaka $[3, 3, 3]$ sledi, da je c.s. permutacije φ_1 enaka bodisi $[6, 3]$ bodisi $[3, 3, 3]$. V prvem primeru je rešitev npr. $\varphi_1 = (142536)(798)$, v drugem pa $\varphi_1 = (132)(465)(798)$.
- Če je c.s. φ_2^2 enaka $[2, 2]$ sledi, da je c.s. φ_2 enaka $[4]$. Torej je rešitev $\varphi_2 = (10, 12, 11, 13)$.
- Očitno je $\varphi_3 = (14)$.

Končni rešitvi sta

$$\varphi = (142536)(798)(10, 12, 11, 13)(14),$$

$$\varphi = (132)(465)(798)(10, 12, 11, 13)(14).$$