Diskretne strukture

Štirinajsti sklop izročkov

Fakulteta za računalništvo in informatiko
Univerza v Ljubljani

12. januar 2022

Kaj so permutacije

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

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

Primer

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

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

- $\pi_2 : \{1, \ldots, 6\} \to \{1, \ldots, 6\}$, $\pi_2(1) = 2$, $\pi_2(2) = 3$, $\pi_2(3) = 4$, $\pi_2(4) = 1$, $\pi_2(5) = 5$, $\pi_2(6) = 6$, *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

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

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

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

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

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

Produkt permutacij ni komutativna operacija.

Inverzna permutacija

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

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

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

Primer

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

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

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

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

Trditev

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

Zapis permutacije z disjunktnimi cikli

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

Primer

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

$$\begin{aligned} \pi &= (1234)(57)(6) = (1234)(57) = (6)(57)(1234) \\ &= (3412)(75)(6) = (176)(2534), \\ \psi &= (176)(2534), \\ \pi * \psi &= (1234)(57) * (176)(2534) = (156)(2473), \\ \psi * \pi &= (176)(2534) * (1234)(57) = (1543)(276). \end{aligned}$$

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

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

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 $\mathcal{C}(\pi)$ *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 $\pi^2, \pi^3, \pi^4, \ldots$?

$$\begin{aligned}
\pi^2 &= (1234)(57) * (1234)(57) \\
&= (1234)^2(57)^2 \\
&= (13)(24)(57), \\
\pi^2 &= (1234)(57) * (1234)(57) * (1234)(57) \\
&= (1234)^3(57)^3 \\
&= (1432)(57), \\
&\vdots
\end{aligned}$$

Za potenciranje permutacij je dovolj poznati potence *ciklov*.

Potenciranje 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*, tj.* $\mathcal{C}(\alpha) = [n]$*. Permutacija* α^k *ima ciklično strukturo*

$$\mathcal{C}(\alpha^k) = \underbrace{\left[\frac{n}{\gcd(n,k)}, \ldots, \frac{n}{\gcd(n,k)}\right]}_{\gcd(n,k)\ \text{členov}}.$$

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

Primer

Naj bo α 6–cikel, tj. $\mathcal{C}(\alpha) = [6]$. Velja:

- $\mathcal{C}(\alpha^2) = [3, 3]$, *saj je* $\gcd(6, 2) = 2$.
- $\mathcal{C}(\alpha^3) = [2, 2, 2]$, *saj je* $\gcd(6, 3) = 3$.
- $\mathcal{C}(\alpha^4) = [3, 3]$, *saj je* $\gcd(6, 4) = 2$.
- $\mathcal{C}(\alpha^5) = [6]$, *saj je* $\gcd(6, 5) = 1$.
- $\mathcal{C}(\alpha^6) = [1, 1, 1, 1, 1, 1]$, *saj je* $\gcd(6, 6) = 6$.
- $\mathcal{C}(\alpha^7) = \mathcal{C}(\alpha)$.
- $\mathcal{C}(\alpha^8) = \mathcal{C}(\alpha^2)$.

Red permutacije

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

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

Trditev

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

Trditev

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

Primer

- *Za* $\mathcal{C}(\alpha) = [3, 2]$ *je* $r(\alpha) = 6$.
- *Za* $\mathcal{C}(\alpha) = [4, 3, 2]$ *je* $r(\alpha) = 12$.
- *Za* $\mathcal{C}(\alpha) = [4, 3, 3, 2, 2]$ *je* $r(\alpha) = 12$.
- *Za* $\mathcal{C}(\alpha) = [8, 7, 5, 2]$ *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, $i = 1, \ldots, m$, *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: $(i_1 i_2 i_3 \ldots i_k) = (i_1 i_2)(i_1 i_3) \cdots (i_1 i_k)$. □

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 tabelice v napačnem vrstnem redu: 1 je manjše kot 2, toda 2 je zapisana pred 1.

Permutacija π ima 6 inverzij: $1\,2, 1\,3, 1\,4, 5\,6, 5\,7, 6\,7$.

Izrek (o parnosti permutacij)

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

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

Potenčna enačba s permutacijami

Permutacijska potenčna enačba je enačba oblike

$$\varphi^k = \alpha, \tag{2}$$

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

Trditev

Enačba (2) je rešljiva natanko tedaj, ko je $\mathcal{C}(\varphi^k) = \mathcal{C}(\alpha)$.

Metoda nedoločenih koeficientov

Primer

Rešujemo enačbo

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

Velja $\mathcal{C}(\alpha) = [7,2,2]$. *Ker mora biti* $\mathcal{C}(\varphi^2) = [7,2,2]$, *je* $\mathcal{C}(\varphi)$ *oblike*

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

- *Če je* $\mathcal{C}(\varphi) = [11]$, *potem je* $\mathcal{C}(\varphi^2) = [11] \neq \mathcal{C}(\alpha)$. *Torej ni rešitve.*
- *Če je* $\mathcal{C}(\varphi) = [m_1, m_2]$, *potem mora biti* $m_1 = 7$, $m_2 = 4$. *Torej rešitev je. Ugibajmo z metodo nedoločenih koeficientov:*

  $$\varphi = (x_1x_2x_3x_4)(x_5x_6x_7x_8x_9x_{10}x_{11}).$$

  Potem je

  $$\varphi^2 = (x_1x_3)(x_2x_4)(x_5x_7x_9x_{11}x_6x_8x_{10}).$$

  Torej je $\varphi = (1,3,2,4)(5,9,6,10,7,11,8)$.

Primer

- *Če je* $\mathcal{C}(\varphi) = [m_1, m_2, m_3]$, *potem je tudi*

$$\mathcal{C}(\varphi^2) = [m_1, m_2, m_3] = [7, 2, 2].$$

Toda iz $\mathcal{C}(\varphi) = [7, 2, 2]$ *sledi* $\mathcal{C}(\varphi^2) = [7, 1, 1, 1, 1]$. *Torej ni rešitev.*

$\varphi^2 = \alpha$, kjer je $\mathcal{C}(\alpha) = [m]$

Iz $\mathcal{C}(\alpha) = [m]$ sledi, da mora biti $\mathcal{C}(\varphi^2) = [m]$.

Trditev

Če je $\mathcal{C}(\alpha) = [m]$, *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

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

Trditev

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

$\varphi^2 = \alpha$, kjer je $\mathcal{C}(\alpha) = [m, \ldots, m]$

Trditev

Naj bo $\mathcal{C}(\alpha) = [m, \ldots, m]$.

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

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

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

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

Primer

Obravnavajte rešljivost enačbe $\varphi^2 = \alpha$ *za* $\mathcal{C}(\alpha) = [3, 3, 3, 3, 3]$.

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

$\varphi^2 = \alpha$, kjer je α poljubna

Naj bo

$$\mathcal{C}(\alpha) = [m_1, \ldots, m_1, m_2, \ldots, m_2, \ldots, m_\ell, \ldots, m_\ell].$$

V tem primeru rešimo enačbe

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

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

Rešitev $\varphi^2 = \alpha$ je potem

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

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* $\varphi_3^2 = (14)$.

- *Iz* $\mathcal{C}(\varphi_1^2) = [3,3,3]$ *sledi, da je* $\mathcal{C}(\varphi_1) = [6,3]$ *ali* $\mathcal{C}(\varphi_1) = [3,3,3]$. *V prvem primeru je rešitev npr.* $\varphi_1 = (142536)(798)$, *v drugem pa* $\varphi_1 = (132)(465)(798)$.
- *Iz* $\mathcal{C}(\varphi_2^2) = [2,2]$ *sledi, da je* $\mathcal{C}(\varphi_2) = [4]$. *Torej je rešitev* $\varphi_2 = (10,12,11,13)$.
- *Očitno je* $\varphi_3 = (14)$.

Končni rešitvi sta

$$\varphi = (142536)(798)(10,12,11,13)(14),$$
$$\varphi = (132)(465)(798)(10,12,11,13)(14).$$