Algebra ir geometrija informatikams. Paskaitų konspektas. Rimantas Grigutis

5 paskaita. *Keitiniai.*

Tegu π yra aibės $N_n = \{1, 2, ..., n\}$ kėlinys $(i_1, i_2, ..., i_n)$. Tuo pačiu žymeniu π žymėsime ir abipus vienareikšmišką funkciją iš N_n į N_n apibrėžtą lygybėmis:

$$\pi : N_n \to N_n,$$
$$\pi(1) = i_1, \pi(2) = i_2, ..., \pi(n) = i_n.$$

Taip apibrėžtą funkciją vadinsime *keitiniu* aibėje N_n. Aišku, kad galime sudaryti $n!$ skirtingų keitinių aibėje N_n (tiek kiek yra skirtingų aibės N_n kėlinių). Tokių keitinių aibę žymi S_n.

Pateiksime pagrindinius keitinio reiškimo būdus.

1. *Keitinio, kaip funkcijos apibrėžtos baigtinėje aibėje, reiškimas lentele:*

$$\begin{pmatrix} 1 & 2 & ... & n \\ i_1 & i_2 & ... & i_n \end{pmatrix}.$$

Keitinį

$$\begin{pmatrix} 1 & 2 & ... & n \\ 1 & 2 & ... & n \end{pmatrix}$$

vadinsime vienetiniu keitiniu ir žymėsime *1.*

2. Keitinio *reiškimas nepriklausomais ciklais.*

Tegu $i \in N_n$. Tada turime aibės N_n elementų seką

$$i, \pi(i), \pi^2(i) = \pi(\pi(i)), ..., \pi^{k-1}(i), \pi^k(i) = i.$$

Gauname k ilgio ciklą $\left(i, \pi(i), \pi^2(i), ..., \pi^{k-1}(i)\right)$.

Jeigu $k = n$, tai visi aibės N_n elementai yra šiame cikle. Kitu atveju, egzistuoja toks $j \notin \left(i, \pi(i), \pi^2(i), ..., \pi^{k-1}(i)\right)$, kuriam konstruojame savo ciklą:

$$\left(j, \pi(j), \pi^2(j), ..., \pi^{l-1}(j)\right) .$$

Jeigu $k+l=n$, ai visi aibės N_n elementai yra skaičių i ir j cikuose. Kitu atveju skaičiui, nepriklausančiam skaičių i ir j ciklams konstruojame ciklą ir t.t. Pagaliau visi aibės N_n elementai bus cikluose.

5.1 Teiginys. *Jeigu j nepriklauso skaičiaus i ciklui, tai skaičių i ir j ciklai neturi bendrų elementų.*

Įrodymas.Įrodysime prieštarų metodu**.** Sakykime kuris nors skaičiaus j ciklo elementas $\pi^r(j)$ priklauso skaičiaus i ciklui, t.y. $\pi^r(j) = \pi^s(i)$. Tada

$$\begin{gathered} \pi^{r+1}(j) = \pi^{s+1}(i) \\ \cdots \\ j = \pi^l(j) = \pi^{s+(l-r)}(i). \end{gathered}$$

Gavome, kad skaičius j priklauso skaičiaus i ciklui. Prieštaravimas sąlygai įrodo teoremą.

Tokiu būdu, visi aibės N_n elementai keitinio π atžvilgiu suskyla į nesikertančius ciklus, o patį keitinį π galima reikšti šių nepriklausomais ciklais :

$$\pi = \left(i, \pi(i), \pi^2(i), ..., \pi^{k-1}(i)\right)\left(j, \pi(j), \pi^2(j), ..., \pi^{l-1}(j)\right)\cdots\ .$$

5.2 Pavyzdys. $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 1 & 3 & 2 & 7 & 8 & 6 & 5 \end{pmatrix}.$
Skaičiaus 1 ciklas: 1, $\pi(1) = 4, \pi(4) = 2, \pi(2) = 1$, taigi $1, 2, 4$
Skaičiaus 3 cikle yra tik vienas skaičius 3, nes $\pi(3) = 3$.
Skaičiaus 5 ciklas: 5, $\pi(5) = 7, \pi(7) = 6, \pi(6) = 8, \pi(8) = 5$,taigi $5, 7, 6, 8$.
Keitinio π reiškimas nepriklausomais ciklais yra

$$\pi = (1, 4, 2)(3)(5, 7, 6, 8)$$

5.3 Pastabos.
1. Vientinis keitinys 1=$(1)(2)\cdots(n)$, todėl keitinio reiškime nepriklausomais ciklais nerašomi ciklai sudaryti tik iš vieno skaičiaus:

$$\pi = (1, 4, 2)(3)(5, 7, 6, 8) = (1, 4, 2)(5, 7, 6, 8).$$

2. Keitnio reiškime nepriklausomais ciklais pačių ciklų rašymo tvarka yra nesvarbi. Pavyzdžiui

$$\pi = (1,4,2)\,(5,7,6,8) = (5,7,6,8)\,(1,4,2)\,.$$

3. Ciklas nepasikeis jeigu jame esančius skaičius cikli*š*kai paslinksime į kurią nors pusę:

$$(i_1, i_2, ..., i_{r-1}, i_r) = (i_2, i_3, ..., i_r, i_1) = \cdots = (i_r, i_1, ..., i_{r-2}, i_{r-1})\,.$$

5.3 Apibrėžimas. *Tegu* ρ, π *- keitiniai aibėje* N_n*. Keitinių* ρ ir π *sandauga vadinsime keitinį* $\sigma = \rho\pi$*, apibrėžtą lygybe*

$$\sigma(i) = \rho(\pi(i)) \ , \forall i \in N_n.$$

Taigi, keitinio reiškimas nepriklausomais ciklais yra keitinio reiškimas nepriklausomų ciklų sandauga.

Pastebėsime, kad keitinių sandauga yra funkcijų kompozicija, o ji ne visada komutatyvi, t.y. ne visada $\pi\rho = \rho\pi$.

5.4 Pavyzdys. Kai $\pi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, o $\rho = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, tai

$$\rho\pi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \pi\rho.$$

Keitinių sandauga aibėje S_n pasižymi šiomis savybėmis:

Są. *Asociatyvumas*: $\tau(\rho\pi) = (\tau\rho)\pi$:

$$(\tau(\rho\pi))(i) = \tau((\rho\pi)(i)) = \tau(\rho(\pi(i))) = (\tau\rho)(\pi(i)) = ((\tau\rho)\pi)(i)\,.$$

S2. *Vienetinio keitinio 1 egzistavimas*: su visais $\pi \in S_n$

$$\mathit{1}\pi = \pi 1 = \pi$$

S3 *Atvirkštinio keitinio egzistavimas*: jei

$$\pi = \begin{pmatrix} 1 & 2 & ... & n \\ i_1 & i_2 & ... & i_n \end{pmatrix}$$

ir

$$\pi^{-1} = \begin{pmatrix} i_1 & i_2 & ... & i_n \\ 1 & 2 & ... & n \end{pmatrix},$$

tai

$$\pi\rho = \rho\pi = \mathit{1}.$$

5.5 Apibrėžimas. *Ciklas* (i, j) *vadinamas* ***transpozicija.***

5.6 Teiginys. *Kai* $n \geq 2$*, tai bet kurį keitinį iš* S_n *galima užrašyti transpozicijų sandauga.*

Įrodymas. Šį teiginį pakanka įrodyti k ilgio ciklui.

Kai $k = 1$, tai $(i) = (i, j)\,(i, j)$.

Kai $k = 2$, tai $(i, j) = (i, j)$,

o kai $k \geq 3$, tai $(1, 2, ..., k) = (1, 2)\,(2, 3) \cdots (k - 1, k)$. Sandaugoje yra $k - 1$ transpozicija.

Įrodyta.

Pastebėsime, kad keitinio reiškimas transpozicijų sandauga yra nevienareikšmiškas. Pavyzdžiui,

$$(1, 2) = (1, 2)\,(1, 2)\,(1, 2),$$

arba

$$(1, 2, ..., k) = (1, 2)\,(2, 3) \cdots (k - 1, k) = (1, k)\,(1, k - 1) \cdots (1, 3)\,(1, 2)\,.$$

5.7 Teorema *Kiekviename keitinio reiškime transpozicijomis pačių transpozicijų skaičius visada yra lyginis arba nelyginis.*

Be įrodymo.

5.8 Apibrėžimai. *Keitinys* π *vadinamas lyginiu, jeigu* π *reiškime transpozicijomis pačių transpozicijų skaičius yra lyginis. Keitinys* π *vadinamas nelyginiu, jeigu* π *reiškime transpozicijomis pačių transpozicijų skaičius yra nelyginis.*

Jei keitinio π *reiškime transpozicijomis pačių transpozicijų skaičius yra* k *, tai keitinio* π *ženklu vadinamas skaičius* $\operatorname{sign}(\pi) = (-1)^k$.

5.9 Išvados.

1. *Vienetinis keitinys 1 yra lyginis, o transpozicija yra nelyginys keitinys.*

2. Jei $\pi-$ *lyginis keitinys, tai* $\operatorname{sign}(\pi) = 1$, *jei* $\pi-$ *nelyginis keitinys, tai* $\operatorname{sign}(\pi) = -1$

3. r ilgio *ciklas* $\sigma = (i_1, i_2, ..., i_r)$ *yra lyginis tada ir tik tada, kai* r *yra nelyginis ir atvirkščiai. Šio keitinio ženklas* $\operatorname{sign}(\sigma) = (-1)^{r-1}$

4. (lyginis keitinys) (lyginis keitinys) = (lyginis keitinys) .
(nelyginis keitinys) (nelyginis keitinys) = (lyginiskeitinys) .
(nelyginis keitinys) (lyginis keitinys) = (nelyginis keitinys) .

5. $\operatorname{sign}(\pi\rho) = \operatorname{sign}(\pi) \cdot \operatorname{sign}(\rho)$.

Lyginių keitinų aibę žymima A_n ir vadina **alternuojančia keitinių aibe**.

5.10 Teiginys. *Lyginių keitinių skaičius yra lygus nelyginių keitinių skaičiui.*

Įrodymas. Apibrėžkime keitinių aibę

$$U_{(a,b)} = \{\pi \in S_n | \pi = \sigma \circ (a,b)\,, \sigma \in A_n\} \subseteq S_n - A_n.$$

Aibės $U_{(a,b)}$ visi keitiniai yra *nelyginiai* ir visi skirtingi, nes jei

$$\sigma_1 \circ (a,b) = \sigma_2 \circ (a,b)\,,$$

tai

$$\sigma_1 \circ (a,b) \circ (a,b) = \sigma_2 \circ (a,b) \circ (a,b)$$

ir

$$\sigma_1 = \sigma_2.$$

Tegu aibėje A_n yra m_1 keitinų, aibėje $S_n - A_n$ yar m_2 keitinų. Tada turime, kad $m_1 \leq m_2$

Analogiškai apibrėžkime keitinių aibę

$$V_{(a,b)} = \{\pi \in S_n | \pi = \rho \circ (a,b)\,, \rho \in S_n - A_n\} \subseteq A_n.$$

Aibės $V_{(a,b)}$ visi keitiniai yra lyginiai ir visi skirtingi. tada turime $m_2 \leq m_1$
Taigi

$$m_1 = m_2 = \frac{n!}{2}\ .$$

Įrodyta.