Permutace

Motivace

- Permutace jsou důležitou částí matematiky viz použití v pravděpodobnosti, algebře (např. determinanty) a mnoho dalších.
- Jsou zásadní také pro kryptografii viz např. monoalfabetické a polyalfabetické šifry, enigma.
- Pomocí permutací lze vydělat peníze viz pan Samuel Loyd.

Samuel Loyd a jeho hlavolam "15-ka"

1000$ tomu, kdo najde řešení:

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

$\rightarrow$

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

Definice

Nechť $\mathbf{n} = \{1, 2, 3, \ldots, n\}$ a S_n je množina všech bijekcí z $\mathbf{n}$ do $\mathbf{n}$. Pak S_n tvoří grupu $(S_n, \cdot, ^{-1}, id)$ s operací skládání funkcí $\cdot$ a neutrálním prvkem id. Grupa S_n se nazývá grupa permutací (nebo také symetrická grupa).

Konvence

- Permutace budeme skládat zleva do prava, tj. $f \cdot g = g \circ f$.
- Obraz prvku x permutací f značíme xf, tj. $xf = f(x)$.
- Permutaci $f \in S_n$ zapisujeme takto:

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ 1f & 2f & \cdots & nf \end{pmatrix}$$

Příklad

Mějme $f, g \in S_4$ definované:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}, \quad g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$$

Pak

$$f \cdot g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} \neq g \cdot f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

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

Definice

Mějme r různých prvků $x_1, \ldots, x_r \in \mathbf{n}$. Pak r-cyklus $(x_1\ x_2\ \cdots\ x_r)$ je permutace z S_n, která zobrazuje $x_1 \mapsto x_2$, $x_2 \mapsto x_3$, $\ldots$, $x_{r-1} \mapsto x_r$, $x_r \mapsto x_1$ a fixuje ostatní prvky z $\mathbf{n}$.
2-cykly se také nazývají transpozice.

Příklad

- Uvažujme permutační grupu S_5. Pak např. 3-cyklus (1 5 2) je následující permutace z S_5:

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

- Každý 1-cyklus je identická permutace id.

Definice

Dva r-cykly $(x_1\ x_2\ \cdots\ x_r)$ a $(y_1\ y_2\ \cdots\ y_r)$ se nazývají disjunktní, pokud

$$\{x_1, x_2, \ldots, x_r\} \cap \{y_1, y_2, \ldots, y_r\} = \emptyset\,.$$

Věta

Každá permutace se dá vyjádřit jako součin disjunktních cyklů.

Příklad

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

$$= (1\ 2\ 4\ 5)\cdot(7\ 8)$$

Příklad

Stejná metoda funguje i na výpočet součinu cyklů.

$$(1\ 4\ 5)\cdot(4\ 6)\cdot(6\ 4\ 7)\cdot(3\ 7) \quad = \quad (1\ 4\ 5)\cdot(3\ 7\ 6)$$

Tvrzení

Mějme r-cyklus $(x_1\ x_2\ \cdots\ x_r)$. *Pak*
$(x_1\ x_2\ \cdots\ x_r)^{-1} = (x_r\ x_{r-1}\ \cdots\ x_1)$.

Příklad

$$\begin{aligned}((1\ 2\ 4\ 5)\cdot(7\ 8)\cdot(3\ 6))^{-1} &= (3\ 6)^{-1}\cdot(7\ 8)^{-1}\cdot(1\ 2\ 4\ 5)^{-1}\\ &= (6\ 3)\cdot(8\ 7)\cdot(5\ 4\ 2\ 1)\\ &= (3\ 6)\cdot(7\ 8)\cdot(1\ 5\ 4\ 2)\end{aligned}$$

Tvrzení

Disjuntní cykly komutují, tj. $f \cdot g = g \cdot f$ pro disjunktní cykly f, g.

Tvrzení

Řád r-cyklu $(x_1\ x_2\ \cdots\ x_r)$ je r.

Příklad

Např. $(1\ 4\ 5)^3 = (1\ 4\ 5) \cdot (1\ 4\ 5) \cdot (1\ 4\ 5) = id$.

Věta

Nechť f je permutace a $f = f_1 \cdot f_2 \cdots f_k$ je její rozklad na součin disjunktních cyklů. Pak řád f je nejmenší společný násobek řádů f_1 až f_k.

Příklad

Spočtěte řád $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 6 & 5 & 1 & 3 & 8 & 7 \end{pmatrix} \in S_8$.

Máme $f = (1\ 2\ 4\ 5) \cdot (7\ 8) \cdot (3\ 6)$. Řád f je tedy $\mathrm{lcm}(4, 2, 2) = 4$.

Věta

Každá permutace lze vyjádřit jako součin transpozic.

Důkaz

Cyklus $(x_1\ x_2\ \cdots\ x_r)$ lze vyjádřit jako
$(x_1\ x_2)\cdot(x_1\ x_3)\cdot(x_1\ x_4)\cdots(x_1\ x_r)$.

Příklad

$f = (1\ 2\ 4\ 5)\cdot(7\ 8)\cdot(3\ 6) = (1\ 2)\cdot(1\ 4)\cdot(1\ 5)\cdot(7\ 8)\cdot(3\ 6)$.

Definice

Transpozici tvaru $(i\ i+1)$ budeme nazývat sousední transpozice.

Věta

Každou permutaci lze vyjádřit jako součin sousedních transpozic.

Důkaz

Pro $i < j$ platí $(i\ j) = \sigma \cdot (j-1\ j) \cdot \sigma^{-1}$, kde
$\sigma = (i\ i+1) \cdot (i+1\ i+2) \cdots (j-2\ j-1)$.

Příklad

Vyjádřete transpozici $(3\ 7) \in S_8$ jako součin sousedních transpozic.
Máme $\sigma = (3\ 4) \cdot (4\ 5) \cdot (5\ 6)$. Pak

$$(3\ 7) = (3\ 4) \cdot (4\ 5) \cdot (5\ 6) \cdot (6\ 7) \cdot (5\ 6) \cdot (4\ 5) \cdot (3\ 4)\,.$$

Definice

Permutaci f nazveme lichou (sudou), pokud lze vyjádřit jako součin lichého (sudého) počtu transpozic.

Lemma

Identická permutace id je sudá (a ne lichá).

Věta

Každá permutace je buď lichá nebo sudá (nikdy ne obojí). Tj. liché permutace jdou vyjádřit pouze jako součin lichého počtu transpozic a sudé permutace sudého počtu.

Definice

Definujme zobrazení $s\colon S_n \to \mathbb{Z}_2$ vztahem:

$$s(f) = \begin{cases} 0 & \text{pokud je } f \text{ sudá,} \\ 1 & \text{pokud je } f \text{ lichá.} \end{cases}$$

Věta

Nechť $f, g \in S_n$. Pak $s(f \cdot g) = s(f) + s(g)$, tj. s je homomorfismus grup.

15-ka

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

$\rightarrow$

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

Zadaný stav se liší o jednu transpozici. K řešení je tedy potřeba lichá permutace. Naopak na to aby se prázdné políčko vrátilo zpět na svoji pozici je potřeba sudá permutace.

Pan Loyd prodal mnoho svých 15-tek, aniž by musel někomu vyplatit slíbenou odměnu, protože řešení prostě neexistuje.

Enigma

Enigma je šifrovací přístroj používající symetrickou polyalfabetickou šifru. Chod přístroje je určen:

- 3 rotory — permutace $\varrho_1, \varrho_2, \varrho_3$, počáteční nastavení a nastavení zarážek,
- Plug board — součin disjunktních transpozic τ,
- Reflektor — součin disjunktních transpozic ϱ,

Pak j-té písmeno zprávy je šifrováno permutací:

$$\epsilon_j = \tau \cdot (\sigma^{i_1} \cdot \varrho_1 \cdot \sigma^{-i_1}) \cdot (\sigma^{i_2} \cdot \varrho_2 \cdot \sigma^{-i_2}) \cdot (\sigma^{i_3} \cdot \varrho_3 \cdot \sigma^{-i_3}) \cdot \\ \cdot \varrho \cdot (\sigma^{i_3} \cdot \varrho_3^{-1} \cdot \sigma^{-i_3}) \cdot (\sigma^{i_2} \cdot \varrho_2^{-1} \cdot \sigma^{-i_2}) \cdot (\sigma^{i_1} \cdot \varrho_1^{-1} \cdot \sigma^{-i_1}) \cdot \tau \,,$$

kde $\sigma = (ABCD \cdots Z)$ a i_1, i_2, i_3 závisí na j a nastavení rotorů.


Zur Beachtung!

UPOZORNĚNÍ!

Oficiální stránky předmětu:

`http://cs.cas.cz/~horcik`

1. Požadavky na zápočet
2. Průběh zkoušek
3. Studijní materiály (skripta a errata skript, sbírka příkladů a její errata)
4. Vzorky testů a písemné zkoušky
5. Handouts z přednášek