Cyklový index permutační grupy

Zápis některých výsledků, k nimž se později dostaneme, se zjednoduší, zavedeme-li pomocný pojem cyklového indexu permutační grupy.

Nechť M je nějaká neprázdná konečná množina mající m prvků. Pišme $M = \{a_1, a_2, \ldots, a_m\}$. Každou permutaci σ množiny M lze zapsat jako součin několika nezávislých cyklů ve tvaru

$$\sigma = (c_1^1 \ldots c_{k_1}^1) \circ (c_1^2 \ldots c_{k_2}^2) \circ \cdots \circ (c_1^q \ldots c_{k_q}^q).$$

Přitom $\{c_1^1, \ldots, c_{k_1}^1, c_1^2, \ldots, c_{k_2}^2, \ldots, c_1^q, \ldots, c_{k_q}^q\} = \{a_1, a_2, \ldots, a_m\}$ a k tomu $k_1 + k_2 + \cdots + k_q = m$. Čísla $k_1, k_2, \ldots, k_q$ jsou délky cyklů. Připouštíme i cykly délky jedna, které se objeví, když permutace σ zobrazí některý prvek na něj samotný. Cykly délky jedna tak jednoznačně odpovídají pevným bodům permutace σ. Výše uvedený zápis permutace σ je jednoznačný až na pořadí cyklů a způsob, jakým jsou zapsány jednotlivé cykly — cyklus délky k lze zapsat k způsoby podle toho, který prvek je postaven na začátek.

Množiny prvků $\{c_1^1, \ldots, c_{k_1}^1\}, \{c_1^2, \ldots, c_{k_2}^2\}, \ldots, \{c_1^q, \ldots, c_{k_q}^q\}$ vystupujících ve výše uvedeném rozkladu permutace σ na součin nezávislých cyklů tvoří rozklad množiny M. Označme tento rozklad symbolem $r(\sigma)$. Označme dále pro každé $i = 1, 2, \ldots, m$ symbolem $j_i(\sigma)$ počet cyklů permutace σ délky i.

Pak rozklad $r(\sigma)$ množiny M indukovaný permutací σ obsahuje pro každé $i = 1, 2, \ldots, m$ právě $j_i(\sigma)$ i-prvkových podmnožin. V této situaci řekneme, že rozklad $r(\sigma)$ je rozkladem typu $1^{j_1(\sigma)} 2^{j_2(\sigma)} \ldots m^{j_m(\sigma)}$. O samotné permutaci σ pak rovněž řekneme, že je permutací typu $1^{j_1(\sigma)} 2^{j_2(\sigma)} \ldots m^{j_m(\sigma)}$. Pak ovšem platí $\sum_{i=1}^{m} i j_i(\sigma) = m$.

Každé permutaci σ množiny M přiřadíme člen, to jest součin proměnných, v proměnných $t_1, t_2, \ldots, t_m$ následovně:

$$Z(\sigma) = t_1^{j_1(\sigma)} t_2^{j_2(\sigma)} \ldots t_m^{j_m(\sigma)}.$$

Pak pro dvě permutace σ a τ množiny M zřejmě platí $Z(\sigma) = Z(\tau)$ právě tehdy, když σ i τ indukují rozklad množiny M téhož typu.

Buď nyní H podgrupa v grupě S_M všech permutací množiny M. Pak říkáme, že H je permutační grupa. Cyklovým indexem této permutační grupy H pak nazýváme polynom $Z(H)$ v proměnných $t_1, t_2, \ldots, t_m$ definovaný rovností

$$Z(H) = \frac{1}{|H|} \sum_{\sigma \in H} Z(\sigma).$$

Přejeme-li si zvýraznit proměnné, píšeme někdy místo pouhého $Z(H)$ obšírněji $Z(H; t_1, t_2, \ldots, t_m)$.

Určíme cyklové indexy některých význačných permutačních grup.

Cyklovým indexem celé grupy S_M všech permutací množiny M je polynom

$$Z(S_M) = \sum_{\substack{(j_1, j_2, \dots, j_m) \\ 1j_1 + 2j_2 + \cdots + mj_m = m}} \frac{1}{j_1! j_2! \dots j_m! \, 1^{j_1} 2^{j_2} \dots m^{j_m}} t_1^{j_1} t_2^{j_2} \dots t_m^{j_m}.$$

Poznamenejme, že v této sumě se sčítá, de facto, přes všechny možné typy rozkladů množiny M. Sčítanci příslušnému m-tici $(j_1, j_2, \dots, j_m)$ odpovídají rozklady množiny M obsahující pro každé $i = 1, 2, \dots, m$ právě j_i i-prvkových podmnožin. V souladu s předchozím označením pak mluvíme o rozkladech typu $1^{j_1} 2^{j_2} \dots m^{j_m}$.

Podle definice cyklového indexu $Z(S_M)$ máme rovnost

$$Z(S_M) = \frac{1}{|S_M|} \sum_{\sigma \in S_M} Z(\sigma).$$

Zde $|S_M| = m!$. Přitom člen $Z(\sigma)$ nezávisí na permutaci σ samotné, závisí pouze na typu permutace σ. Sloučíme tedy do jednoho sčítance všechny členy odpovídající permutacím stejného typu. Budeme tak sčítat už nikoliv přes všechny permutace σ množiny M, ale přes všechny možné typy rozkladů množiny M. Máme-li rozklady typu $1^{j_1} 2^{j_2} \dots m^{j_m}$, pak v uvedené sumě bude člen $t_1^{j_1} t_2^{j_2} \dots t_m^{j_m}$ vystupovat s koeficientem, jímž bude počet permutací σ množiny M indukujících rozklad množiny M typu $1^{j_1} 2^{j_2} \dots m^{j_m}$.

Zbývá si ujasnit, že tento koeficient je roven číslu

$$\frac{m!}{j_1!j_2!\dots j_m!\,1^{j_1}2^{j_2}\dots m^{j_m}}.$$

Představme si tedy libovolnou permutaci σ množiny M typu $1^{j_1}2^{j_2}\dots m^{j_m}$ zapsanou ve tvaru součinu nezávislých cyklů tak, že nejprve jsou uvedeny cykly délky jedna, potom cykly délky dva, atd. V tomto zápisu se objeví prvky $a_1, a_2, \dots, a_m$ uvedené v nějakém určitém pořadí, tedy tvořící nějakou permutaci množiny M. Takových permutací prvků $a_1, a_2, \dots, a_m$ je celkem $m!$. Ne všechny tyto permutace ale zadávají zápisy různých permutací σ množiny M jako součinů nazávislých cyklů. Při takovém zápisu permutace σ totiž nezáleží na pořadí cyklů stejných délek, takže musíme číslo $m!$ vydělit součinem čísel $j_1!j_2!\dots j_m!$, a nezáleží ani na způsobu zápisu jednotlivých cyklů, jakými prvky tyto cykly začínají, takže musíme číslo $m!$ dále vydělit součinem čísel $1^{j_1}2^{j_2}\dots m^{j_m}$. Takto dospějeme ke shora uvedenému koeficientu.

Cyklovým indexem grupy A_M všech sudých permutací množiny M je polynom

$$Z(A_M) = Z(S_M; t_1, t_2, \dots, t_m) + Z(S_M; t_1, -t_2, t_3, -t_4, \dots, (-1)^{m-1} t_m).$$

Připomeňme, že cyklus liché délky je sudá permutace a cyklus sudé délky je lichá permutace. Pro paritu permutace σ zapsané jako součin nezávislých cyklů jsou tedy určující počty cyklů sudých délek.

Takže permutace σ je sudá, respektive lichá, je-li $j_2(\sigma) + j_4(\sigma) + \cdots$ sudé, respektive liché číslo. Poněvadž pro každou permutaci σ je

$$\begin{aligned}&Z(\sigma; t_1, t_2, \ldots, t_m) + Z(\sigma; t_1, -t_2, t_3, -t_4, \ldots, (-1)^{m-1} t_m)\\&= Z(\sigma; t_1, t_2, \ldots, t_m) + (-1)^{j_2(\sigma)+j_4(\sigma)+\cdots} Z(\sigma; t_1, t_2, \ldots, t_m),\end{aligned}$$

plyne z předchozí úvahy, že tento polynom je roven 0 pro lichou permutaci σ a je roven $2Z(\sigma)$ pro sudou permutaci σ. Poněvadž dále $|A_M| = \frac{|S_M|}{2}$, z definice cyklového indexu $Z(A_M)$ vychází

$$Z(A_M) = \frac{1}{|A_M|} \sum_{\sigma \in A_M} Z(\sigma) = \frac{2}{|S_M|} \sum_{\sigma \in A_M} Z(\sigma) = \frac{1}{|S_M|} \sum_{\sigma \in A_M} 2Z(\sigma).$$

Odtud a z předchozího pozorování pak vyplývá

$$\begin{aligned}Z(A_M) &= \frac{1}{|S_M|} \sum_{\sigma \in S_M} (Z(\sigma; t_1, t_2, \ldots, t_m)\\&\qquad\qquad + Z(\sigma; t_1, -t_2, t_3, -t_4, \ldots, (-1)^{m-1} t_m))\\&= \frac{1}{|S_M|} \sum_{\sigma \in S_M} Z(\sigma; t_1, t_2, \ldots, t_m)\\&\qquad + \frac{1}{|S_M|} \sum_{\sigma \in S_M} Z(\sigma; t_1, -t_2, t_3, -t_4, \ldots, (-1)^{m-1} t_m))\\&= Z(S_M; t_1, t_2, \ldots, t_m) + Z(S_M; t_1, -t_2, t_3, -t_4, \ldots, (-1)^{m-1} t_m),\end{aligned}$$

což bylo potřeba ukázat.

Nechť C_M značí cyklickou podgrupu v grupě S_M řádu m generovanou cyklem $\rho = (a_1\, a_2\, \ldots\, a_m)$.

Cyklovým indexem cyklické grupy C_M řádu m je polynom

$$Z(C_M) = \frac{1}{m} \sum_{d|m} \varphi(d)\, t_d^{\frac{m}{d}}\,.$$

Zde $\varphi(n)$ je Eulerova funkce udávající pro každé kladné celé číslo n počet kladných celých čísel, která nepřevyšují n a jsou s n nesoudělná.

Prvky grupy C_M jsou kladné mocniny ρ^k cyklu $\rho = (a_1\, a_2\, \ldots\, a_m)$. Každá taková mocnina ρ^k je zřejmě součinem několika nezávislých cyklů stejné délky. Označme symbolem d tuto délku. Pak $d|m$ a permutace ρ^k je součinem $\frac{m}{d}$ nezávislých cyklů délky d. Přispívá tedy tato permutace ρ^k do cyklového indexu $Z(C_M)$ sčítancem tvaru $t_d^{\frac{m}{d}}$. Zbývá tak jen určit, s jakým koeficientem se tento sčítanec v cyklovém indexu $Z(C_M)$ objeví. Tento koeficient je roven počtu těch exponentů $k \in \{1, 2, \ldots, m\}$, pro něž permutace ρ^k je součinem nezávislých cyklů stanovené délky d, po vydělení řádem m grupy C_M.

K dané délce d nezávislých cyklů, na něž se rozpadá mocnina ρ^k cyklu ρ délky m, uvažme ještě největšího společného dělitele c čísel k a m. Při řešení poslední úlohy o obarvení rulety jsme si ujasnili, že pak mocnina ρ^k je permutací téhož typu jako mocnina ρ^c cyklu ρ. Takže i mocnina ρ^c je součinem nezávislých cyklů délky d, a poněvadž c dělí m, je počet těchto nezávislých cyklů roven číslu c, takže máme rovnost $cd = m$, a tedy dostáváme $c = \frac{m}{d}$. Dále jsme si ujasnili, že pak počet těch exponentů $k \in \{1, 2, \ldots, m\}$, pro něž mocnina ρ^k je permutací téhož typu jako mocnina ρ^c, je roven hodnotě Eulerovy funkce $\varphi(d)$. To ukazuje, že koeficient, s nímž se sčítanec $t_d^{\frac{m}{d}}$ v cyklovém indexu $Z(C_M)$ objeví, je roven číslu $\varphi(d)$ vydělenému řádem m grupy C_M.

Nechť D_M značí dihedrální grupu stupně m, to jest grupu všech symetrií pravidelného m-úhelníka, jehož vrcholy jsou prvky $a_1, a_2, \ldots, a_m$. Tato grupa D_M je složena z m otočení (to jsou prvky cyklické podgrupy C_M) a dále z m osových souměrností. Je-li m liché, pak jde o souměrnosti podle os procházejících středem některé strany m-úhelníka a protilehlým vrcholem. Je-li m sudé, pak jde o $\frac{m}{2}$ souměrností podle os procházejících protilehlými vrcholy a $\frac{m}{2}$ souměrností podle os procházejících středy protilehlých stran m-úhelníka. Grupa D_M má tedy celkem $2m$ prvků.

Cyklovým indexem dihedrální grupy D_M je polynom

$$Z(D_M) = \frac{1}{2} Z(C_M) + \frac{1}{2}\, t_1 t_2^{\frac{m-1}{2}}$$

pro m liché a

$$Z(D_M) = \frac{1}{2} Z(C_M) + \frac{1}{4} \left(t_2^{\frac{m}{2}} + t_1^2 t_2^{\frac{m-2}{2}} \right)$$

pro m sudé.

Skutečně v obou případech symetrie pravidelného m-úhelníka, které jsou otočeními, tedy symetrie z cyklické podgrupy C_M, přispívají do cyklového indexu $Z(D_M)$ příspěvkem

$$\frac{1}{2m} \sum_{\sigma \in C_M} Z(\sigma) = \frac{1}{2} Z(C_M).$$

Je-li m liché, pak každá osová souměrnost m-úhelníka ponechá jeden vrchol na místě a zbývající vrcholy ve dvojicích, které si odpovídají podle dotyčné osy souměrnosti, si navzájem vymění místa. Jsou zde tedy jeden pevný vrchol a $\frac{m-1}{2}$ transpozic vrcholů. Člen $Z(\sigma)$ příslušný takové symetrii σ je tedy tvaru $Z(\sigma) = t_1 t_2^{\frac{m-1}{2}}$. Tyto osové souměrnosti tedy celkem přispívají do cyklového indexu $Z(D_M)$ příspěvkem

$$\frac{1}{2m}\, m\, t_1 t_2^{\frac{m-1}{2}} = \frac{1}{2}\, t_1 t_2^{\frac{m-1}{2}}\,.$$

Je-li m sudé, pak v osových souměrnostech m-úhelníka podle os procházejících středy protilehlých stran si všechny vrcholy po dvojicích navzájem vymění místa. Je zde tedy $\frac{m}{2}$ transpozic vrcholů. Člen $Z(\sigma)$ příslušný takové symetrii σ je tedy tvaru $Z(\sigma) = t_2^{\frac{m}{2}}$. Tyto osové souměrnosti tedy celkem přispívají do cyklového indexu $Z(D_M)$ příspěvkem

$$\frac{1}{2m}\frac{m}{2}\, t_2^{\frac{m}{2}} = \frac{1}{4}\, t_2^{\frac{m}{2}}\,.$$

V osových souměrnostech m-úhelníka podle os procházejících dvěma protilehlými vrcholy zůstanou tyto dva vrcholy na místě a zbývající vrcholy si po dvojicích navzájem vymění místa. Jsou zde tedy dva pevné vrcholy a $\frac{m-2}{2}$ transpozic vrcholů. Člen $Z(\sigma)$ příslušný takové symetrii σ je pak tvaru $Z(\sigma) = t_1^2 t_2^{\frac{m-2}{2}}$. Tyto osové souměrnosti tedy celkem přispívají do cyklového indexu $Z(D_M)$ příspěvkem

$$\frac{1}{2m}\frac{m}{2}\, t_1^2 t_2^{\frac{m-2}{2}} = \frac{1}{4}\, t_1^2 t_2^{\frac{m-2}{2}}\,.$$

Sečtením příslušných příspěvků pak dostaneme očekávaný tvar cyklového indexu $Z(D_M)$.