Pólyova enumerační teorie

Nechť M je neprázdná konečná množina mající m prvků a nechť Y je nějaká neprázdná konečná nebo spočetně nekonečná množina. Prvky množiny Y budeme nazývat obrazci. Nechť dále H je podgrupa v grupě S_M všech permutací množiny M. Uvažujme množinu Y^M, to jest množinu všech zobrazení $M \to Y$. Mějme dále nějakou podmnožinu $\mathcal{F}$ množiny Y^M s následující vlastností: Pro každou permutaci σ z H a pro každé zobrazení f z $\mathcal{F}$ také zobrazení $f \circ \sigma$ náleží do $\mathcal{F}$. O takové podmnožině $\mathcal{F}$ množiny Y^M budeme říkat, že je uzavřená vzhledem k podgrupě H.

Každému obrazci $\wp \in Y$ přiřaďme proměnnou $x_\wp$ a každému zobrazení $f \in \mathcal{F}$ přiřaďme člen, to jest součin proměnných, označený $v(f)$ a definovaný následovně:

$$v(f) = \prod_{a \in M} x_{f(a)}.$$

Ke každé permutaci $\sigma \in H$ uvažme zobrazení $\overline{\sigma} : \mathcal{F} \to \mathcal{F}$ definované tímto předpisem: pro každé $f \in \mathcal{F}$ klademe $\overline{\sigma}(f) = f \circ \sigma$. Tato definice je korektní, poněvadž podmnožina $\mathcal{F}$ je uzavřená vzhledem k podgrupě H. Ukážeme dále, že zobrazení $\overline{\sigma}$ je permutací podmnožiny $\mathcal{F}$. Je-li $g \in \mathcal{F}$ libovolné zobrazení, pak poněvadž $\sigma^{-1} \in H$, také zobrazení $g \circ \sigma^{-1}$ náleží do $\mathcal{F}$ a máme $\overline{\sigma}(g \circ \sigma^{-1}) = g \circ \sigma^{-1} \circ \sigma = g$. To ukazuje, že zobrazení $\overline{\sigma}$ je surjektivní.

Jsou-li dále $f, g \in \mathcal{F}$ libovolná dvě zobrazení taková, že $\overline{\sigma}(f) = \overline{\sigma}(g)$, to jest $f \circ \sigma = g \circ \sigma$, pak jistě $f \circ \sigma \circ \sigma^{-1} = g \circ \sigma \circ \sigma^{-1}$, takže $f = g$. To ale ukazuje, že zobrazení $\overline{\sigma}$ je injektivní. Celkem je tedy $\overline{\sigma}$ permutací podmnožiny $\mathcal{F}$.

Uvažme množinu permutací $E^H = \{\overline{\sigma} : \sigma \in H\}$. Ukážeme, že E^H je podgrupa grupy $S_{\mathcal{F}}$ všech permutací podmnožiny $\mathcal{F}$. Ukážeme totiž, že pro libovolné dvě permutace $\sigma, \tau \in H$ platí $\overline{\sigma} \circ \overline{\tau} = \overline{\tau \circ \sigma}$. Skutečně pro libovolné zobrazení $f \in \mathcal{F}$ vychází $(\overline{\sigma} \circ \overline{\tau})(f) = \overline{\sigma}(\overline{\tau}(f)) = \overline{\sigma}(f \circ \tau) = f \circ \tau \circ \sigma = \overline{\tau \circ \sigma}(f)$. Je tedy zobrazení přiřazující každé permutaci σ z podgrupy H permutaci $\overline{\sigma}$ podmnožiny $\mathcal{F}$ antihomomorfismem podgrupy H do grupy $S_{\mathcal{F}}$. Obrazem podgrupy H při tomto antihomomorfismu je pak právě množina permutací E^H. Je tedy E^H antihomomorfním obrazem podgrupy H, takže E^H je skutečně podgrupa grupy $S_{\mathcal{F}}$.

Je tedy E^H jistou podgrupou grupy permutací $S_{\mathcal{F}}$. Můžeme tedy zkoumat orbity prvků množiny $\mathcal{F}$, to jest zobrazení z $\mathcal{F}$, v této podgrupě E^H. Tyto orbity budeme nazývat konfiguracemi. Všimněme si, že jsou-li f, g dvě zobrazení z téže konfigurace, to jest, jsou-li f, g dva prvky náležející do téže orbity podgrupy E^H, takže platí $g = \overline{\sigma}(f)$ pro nějakou permutaci σ z H, pak pro členy $v(f)$ a $v(g)$ příslušné těmto zobrazením f, g vychází:

$$v(g) = v(\overline{\sigma}(f)) = v(f \circ \sigma) = \prod_{a \in M} x_{f(\sigma(a))} = \prod_{a \in M} x_{f(a)} = v(f),$$

poněvadž σ je permutací množiny M.

Můžeme tedy pro každou orbitu $\mathcal{O}$ v podgrupě E^H korektně definovat jí odpovídající člen $v(\mathcal{O})$ jako člen $v(f)$, kde f je některý (kterýkoliv) prvek orbity $\mathcal{O}$.

Označme $\mathfrak{M}_{\mathcal{F},H}$ množinu všech konfigurací, to jest množinu všech orbit prvků množiny $\mathcal{F}$ v podgrupě E^H. Dále definujme takzvaný enumerátor:

$$\gamma(\mathcal{F}, H) = \sum_{\mathcal{O} \in \mathfrak{M}_{\mathcal{F},H}} v(\mathcal{O}).$$

Všimněme si, že je-li množina Y nekonečná, pak i množina $\mathcal{F}$ může být nekonečná. Poněvadž ale podgrupa H je konečná, a tedy také podgrupa E^H je konečná, všechny orbity prvků množiny $\mathcal{F}$ v podgrupě E^H, to jest všechny konfigurace budou konečné. V takovém případě pak množina $\mathfrak{M}_{\mathcal{F},H}$ všech konfigurací bude nekonečná, takže potom i výše uvedená suma bude obsahovat nekonečný počet sčítanců. V této sumě se ale každý myslitelný člen vyskytuje jenom konečně mnohokrát. To je patrné z toho, že ke každé konečné podmnožině Y_0 množiny Y existuje jenom konečný počet zobrazení $M \to Y_0$. Lze tedy na výše uvedenou sumu pohlížet jako na sumu navzájem různých členů s koeficienty, jimiž budou nějaká nezáporná celá čísla. My budeme dále vedeni snahou enumerátor $\gamma(\mathcal{F}, H)$ určit. Poznamenejme už jen, že je-li naopak množina Y konečná, potom je konečná i množina $\mathfrak{M}_{\mathcal{F},H}$ všech konfigurací, takže má smysl ptát se na počet těchto konfigurací. Tento počet pak dostaneme dosazením hodnoty 1 za všechny proměnné do enumerátoru.

Na tomto místě bude užitečné si rozmyslet, jakým způsobem se právě zavedené pojmy a konstrukce promítnou do situace zkoumané v příkladě o obarvení stěn pravidelného osmistěnu z předchozího paragrafu. Naše nynější množina M bude množinou všech stěn pravidelného osmistěnu. Množina Y bude množinou všech n barev. Naše nynější grupa H bude grupou všech těch permutací množiny M všech stěn osmistěnu, které jsou indukovány symetriemi z grupy K všech přímých symetrií pravidelného osmistěnu. Dřívější množina M zavedená v předchozím příkladě bude v našem nynějším pojetí množinou Y^M všech zobrazení $M \to Y$, což je ovšem množina všech obarvení stěn nehybného osmistěnu. Podmnožinou $\mathcal{F}$ množiny Y^M bude v tomto příkladě celá množina Y^M. Dřívější grupa H uvažovaná v předchozím příkladě bude v našem nynějším pojetí odpovídat grupě E^H. To je teď totiž podgrupa grupy všech permutací množiny Y^M všech obarvení stěn nehybného osmistěnu, která pozůstává z těch permutací, které jsou vytvořeny permutacemi stěn osmistěnu pocházejícími z naší nynější grupy H. Řešení příkladu z předchozího paragrafu pak vede na nalezení počtu všech orbit prvků množiny Y^M v podgrupě E^H, to jest na nalezení počtu všech konfigurací.

Označme $\mathcal{U}(H)$ svaz všech podgrup grupy H a $\mathcal{P}(M)$ svaz všech rozkladů množiny M. Definujme zobrazení $\psi : \mathcal{P}(M) \to \mathcal{U}(H)$ tak, že pro každý rozklad π množiny M bude $\psi(\pi)$ podgrupou grupy H pozůstávající ze všech těch permutací množiny M obsažených v H, které nechávají třídy rozkladu π nehnuty.

To znamená, že $\psi(\pi)$ bude podgrupou grupy H složenou ze všech těch permutací $\sigma \in H$, které splňují podmínku, že $\sigma(N) = N$ pro každou třídu N rozkladu π.

Připomeňme ještě, že jádrem zobrazení $f : M \to Y$ rozumíme rozklad množiny M, jehož třídami jsou všechny podmnožiny tvaru $f^{-1}(\wp)$ pro všechny obrazce $\wp$ ležící v podmnožině $f(M)$ množiny Y. Jádro zobrazení f značíme symbolem $\ker f$.
V tomto kontextu máme následující pozorování:

Lemma.

Pro libovolné zobrazení $f : M \to Y$ platí:

$$\psi(\ker f) = \{\sigma \in H : f \circ \sigma = f\}.$$

Důkaz.

Permutace $\sigma \in H$ náleží podle definice zobrazení ψ do podgrupy $\psi(\ker f)$ právě tehdy, když σ ponechává nehnuty všechny třídy rozkadu $\ker f$. To nastane právě tehdy, když pro každý prvek $a \in M$ platí, že oba prvky a i $\sigma(a)$ patří do téže třídy rozkladu $\psi(\ker f)$. To je ale ekvivalentní tomu, že pro každý prvek $a \in M$ platí, že $f(a) = f(\sigma(a))$. To ale právě znamená, že $f = f \circ \sigma$. $\square$

Pro každé zobrazení $f \in \mathcal{F}$ označme fH orbitu prvku f v podgrupě E^H. Připomeňme, že $fH = \{f \circ \sigma : \sigma \in H\}$. Určíme počet prvků $|fH|$ orbity fH:

Lemma.

Pro libovolné zobrazení $f \in \mathcal{F}$ je počet prvků orbity fH roven

$$|fH| = \frac{|H|}{|\psi(\ker f)|}.$$

Důkaz.

Pro libovolné dvě permutace σ a τ z podgrupy H rovnost $f \circ \sigma = f \circ \tau$ platí právě tehdy, když platí $f \circ \sigma \circ \tau^{-1} = f$. Podle předchozího lemmatu je poslední rovnost ekvivalentní tomu, že $\sigma \circ \tau^{-1} \in \psi(\ker f)$. To ale nastává právě tehdy, když permutace σ a τ leží v téže pravé třídě grupy H podle její podgrupy $\psi(\ker f)$. Tato úvaha ukazuje, že prvky orbity fH vzájemně jednoznačně odpovídají pravým třídám grupy H podle podgrupy $\psi(\ker f)$. Je tedy počet prvků orbity fH roven počtu tříd pravého rozkladu grupy H podle podgrupy $\psi(\ker f)$. Na základě formule pro počet tříd pravého rozkladu takto dostáváme, že

$$|fH| = |H/\psi(\ker f)| = \frac{|H|}{|\psi(\ker f)|}. \qquad \square$$

Nyní jsme připraveni dokázat následující Pólyovu-de Bruijnovu větu, která je stěžejním výsledkem tohoto paragrafu:

Věta.

Enumerátor $\gamma(\mathcal{F}, H)$ je dán formulí

$$\gamma(\mathcal{F}, H) = \frac{1}{|H|} \sum_{\sigma \in H} \Big(\sum_{f \in \mathcal{F}, f \circ \sigma = f} v(f) \Big).$$

Důkaz.

Podle definice enumerátoru máme

$$\gamma(\mathcal{F}, H) = \sum_{\mathcal{O} \in \mathfrak{M}_{\mathcal{F},H}} v(\mathcal{O}).$$

Poněvadž množina konfigurací $\mathfrak{M}_{\mathcal{F},H}$ tvoří rozklad množiny $\mathcal{F}$, a poněvadž očividně pro každou konfiguraci $\mathcal{O}$ platí

$$v(\mathcal{O}) = \frac{\sum_{f \in \mathcal{O}} v(f)}{|\mathcal{O}|} = \sum_{f \in \mathcal{O}} \frac{v(f)}{|fH|},$$

jelikož pro každé zobrazení $f \in \mathcal{O}$ je $\mathcal{O} = fH$, dostáváme odtud rovnost

$$\gamma(\mathcal{F}, H) = \sum_{\mathcal{O} \in \mathfrak{M}_{\mathcal{F},H}} \Big(\sum_{f \in \mathcal{O}} \frac{v(f)}{|fH|} \Big) = \sum_{f \in \mathcal{F}} \frac{v(f)}{|fH|}.$$

Podle předchozího lemmatu odtud vyplývá

$$\gamma(\mathcal{F}, H) = \frac{1}{|H|} \sum_{f \in \mathcal{F}} |\psi(\ker f)| \, v(f).$$

Konečně podle předminulého lemmatu odtud vychází

$$\gamma(\mathcal{F}, H) = \frac{1}{|H|} \sum_{f \in \mathcal{F}} |\{\sigma \in H : f \circ \sigma = f\}| \, v(f).$$

Jinak zapsáno to znamená, že

$$\gamma(\mathcal{F}, H) = \frac{1}{|H|} \sum_{f \in \mathcal{F}} \Big(\sum_{\sigma \in H, f \circ \sigma = f} v(f) \Big).$$

Přehozením sum nakonec dostáváme

$$\gamma(\mathcal{F}, H) = \frac{1}{|H|} \sum_{\sigma \in H} \Big(\sum_{f \in \mathcal{F}, f \circ \sigma = f} v(f) \Big),$$

což jsme měli ukázat. $\square$

Vraťme se nyní k situaci, kdy množina obrazců Y je konečná. Viděli jsme, že pak také množina všech konfigurací $\mathfrak{M}_{\mathcal{F},H}$ je konečná, takže má smysl ptát se na počet těchto konfigurací. Jak již bylo řečeno, tento počet dostaneme dosazením hodnoty 1 za všechny proměnné do enumerátoru $\gamma(\mathcal{F}, H)$. Z předchozí Pólyovy-de Bruijnovy věty takto bezprostředně plyne tento její důsledek:

Důsledek.

Počet všech konfigurací, to jest počet všech orbit prvků množiny $\mathcal{F}$ v podgrupě E^H je roven

$$|\mathfrak{M}_{\mathcal{F},H}| = \frac{1}{|H|} \sum_{\sigma \in H} |\{f \in \mathcal{F} : f \circ \sigma = f\}|. \qquad \square$$

Na závěr se vraťme ještě jednou k příkladu o obarvení stěn pravidelného osmistěnu z předchozího paragrafu. Tam jsme úlohu najít počet orbit v příslušné permutační grupě řešili s použitím Burnsideova lemmatu. Mělo by být nyní zřejmé, že takřka totožný postup řešení obdržíme, použijeme-li místo toho výše uvedený důsledek Pólyovy-de Bruijnovy věty.