Enumerácia diskrétnych štruktúr

Prednášal Doc. Toman, zapísal P. Hanušiak, TEX J. Svitok

1. marca 2001

verzia 0.2

Obsah

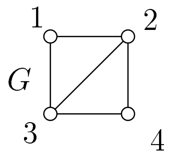
1 Určovanie počtu neoznačených objektov

1.1 Izomorfizmus grúp permutácií

Pri určovaní počtu neoznačených objektov úlohu formulujeme tak, aby sme mohli výsledok získať tým, že nájdeme počet orbít niektorej vhodnej grupy permutácií. Pomocou Burnsidovej lemy určíme počet orbít vyčíslením počtu identických prvkov vzhľadom na permutácie z uvažovanej grupy.

Definícia 1. Uvažujme množinu $X = \{1, 2, 3, \dots, n\}$; A nech je niektorá množina permutácií na množine X. Nech A je uzavretá vzhľadom na operáciu skladania permutácií. Potom A je *grupou permutácií* na množine A. *Rád grupy* A (budeme ho označovať $|A|$) je rovný počtu permutácií v množine A. *Stupeň grupy* A je rovný počtu prvkov množiny X.

Teoreticko-grupové pojmy môžeme skúmať spolu s grafmi, pričom využijeme názornosť a podnety z oblasti grafov.



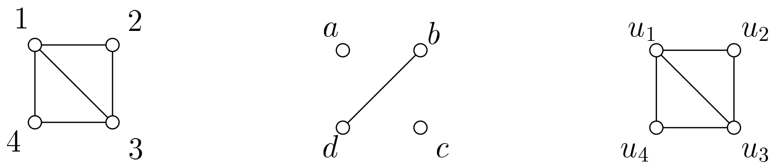
$$\begin{aligned}\alpha_1 &= (1)(2)(3)(4)\\ \alpha_2 &= (1)(3)(2\ 4)\\ \alpha_3 &= (1\ 3)(2)(4)\\ \alpha_4 &= (1\ 3)(2\ 4)\end{aligned}$$

Obr. 1: Graf G určuje „obraz“ svojej grupy automorfizmov.

Definícia 2. $\Gamma(G)$ — množina všetkých permutácií na $V(G)$, ktoré zachovávajú susednosť. Nazývame ju *grupa grafu* G a jej permutácie *automorfizmami.*

$\overline{G}$ — komplementárny graf; $\Gamma(G) = \Gamma(\overline{G})$

Kedy sú grupy permutácií rovnaké? na určenie tejto otázky potrebujeme jemnejšie kritérium ako je grupový izomorfizmus.



Obr. 2: Rozdiel medzi grafmi v doplnkovosti a označení

Definícia 3. Nech A,B sú dve grupy permutácií s množinami objektov X, resp. Y. Hovoríme, že sú *izomorfné* (zapisujeme $A \cong B$), ak existuje bijekcia $h : A \to B$ taká, že pre všetky permutácie α_1,α_2 z grupy A platí rovnosť $h(\alpha_1\alpha_2) = h(\alpha_1)h(\alpha_2)$. Ak okrem toho existuje bijekcia $\varphi : X \to Y$ taká, že pre každú permutáciu $\alpha \in A$ a pre každý prvok $x \in X$ platí rovnosť $\varphi(\alpha x| = h(\alpha)\varphi(x)$, potom grupy A, B sú identické a píšeme $A = B$.

Poznámka 4. Zobrazenie φ zamieňa označenie prvkov z grupy A za označenia zodpovedajúce grupe B.

1.2 Cyklový index grupy permutácií

Definícia 5. (Index je polynóm). Nech A je grupa permutácií, X množina objektov, $\alpha \in A$ permutácia. Každú permutáciu α môžeme jednoznačne napísať (až na poradie) v tvare súčinu po dvoch disjunktných cyklov.

$j_k(\alpha)$ je rovné počtu cyklov dĺžky k v permutácii α, kde $k = 1, 2, \dots, n$

Cyklový index $Z(A)$ — polynóm premenných $s_1, s_2, \dots, s_n$

$$Z(A) = Z(A, s_1, s_2, \ldots, s_n) = |A|^{-1} \sum_{\alpha \in A} \prod_{k=1}^{n} s_k^{j_k(\alpha)}$$

Príklad 6. Nech S_n je symetrická grupa na množine $\{1, 2, \ldots, n\}$.

$$Z(S_3) = \frac{1}{3!}(s_1^3 + 3s_1s_2 + 2s_3)$$

Najznámejšie cykl. grupy:

- symetrická
- alternujúca
- cyklická
- diadrálna
- identická

1.3 Všeobecný vzorec pre $Z(S_n)$ (Polya, Redfield)

Nech $\alpha \in A$ je ľub. permutácia množiny $X = \{1, 2, 3, \ldots, n\}$. Zadáme túto permutáciu nejakým vektorom $(j) = (j_1, j_2, \ldots, j_n)$, kde j_i je počet cyklov dĺžky i. Musí platiť $\sum k \cdot j_k = n$.

Definícia 7. $h(j)$ označíme počet permutácií z S_n, ktoré sú určené vektorom (j) — čiže keď máme $(j) = (j_1, j_2, \ldots, j_n)$ pre $\alpha \in S_n$ musí platiť $j_k(\alpha) = j_k$.

$$\begin{aligned} h(j) &= n!/\prod_{k=1}^{n} k^{j_k} j_k! && (1) \\ n &= \sum_{k=1}^{n} k j_k \end{aligned}$$

$$\underbrace{(\ ), (\ ), (\ )}_{\text{cykly dĺžky 1}}, \underbrace{(\ ,\ ), (\ ,\ ), \ldots, (\ ,\ )}_{2}, \underbrace{(\ ,\ ,\ ), (\ ,\ ,\ ), \ldots}_{3}$$

Do tejto „formy“ umiestňujeme prvky z $n!$. Niektoré pozície sú rovnocenné — takže opravíme poradie cyklov, to je $j_k!$, a rotáciu v cykle (k^{j_k}).

Veta 8 (Polya, Redfield). Cyklový index grupy S_n (symetrickej grupy) je určený formulou:

$$Z(S_n) = \frac{1}{n!} \sum_{\substack{(j) \\ \text{cez } \forall j}} h(j) \prod_{k=1}^{n} k^{j_k}$$

kde súčet berieme vzhľadom na všetky rozklady (j) čísla n a $h(j)$ je definované vzťahom (1).

1.4 Burnsideova lema

Definícia 9. Nech A je grupa permutácií na množine $X = \{1, 2, 3, \ldots, n\}$. Prvky $x, y \in X$ budeme nazývať *A–ekvivalentné* ak existuje permutácia $\alpha \in A$: $\alpha x = y$.

1. $x \in X$ (x, x) sú A–ekvivalentné (identická perm.)
2. ak x,y sú A–ekvivalentné, tak aj y,x sú A–ekvivalentné: $\alpha \in A$ $\alpha x = y$ $\alpha^{-1}\alpha x = \alpha^{-1} y$
3. ak x,y a y,z sú A–ekvivalentné, tak aj x,z sú A–ekvivalentné: $\beta\alpha x = \beta y$ $\beta y = z$ $\beta\alpha x = z$

Máme A–ekvivalenciu, ktorá je ekvivalenciou, a teda indukuje rozklad množiny X. Triedy rozkladu nazývame *orbitami* alebo *systém tranzitívnosti grupy.*

Definícia 10. Nech $x \in X$. Definujeme $A(x) = \{\alpha \in A | \alpha x = x\}$. $A(x)$ nazývame *stabilizátor prvku* x, alebo grupa izotropie prvku x.

Tvrdenie 11. Ak x a y patria do jednej orbity grupy A, tak platí $|A(x)| = |A(y)|$

Dôkaz. Nech x,y patria do orbity, t.j. musí existovať $\gamma \in A \gamma x = y \implies x = \gamma^{-1} y$

$$\begin{array}{rcl}
A(x) & = & \{\alpha_i | \alpha_i x = x\} \\
A(y) & = & \{\beta_j | \beta_j y = y\} \\
\alpha_i x & = & x \\
\gamma\alpha_i x & = & \gamma x = y \\
\gamma\alpha_i\gamma^{-1} y & = & y \implies \gamma\alpha_i\gamma^{-1} \in A(y) \\
\gamma\alpha_i\gamma^{-1} & \to & \beta_i \\
\alpha_i \neq \alpha_j & \implies & \beta_i \neq \beta_j
\end{array}$$

a ešte naopak a je to dokázané. □

Ďalší dôkaz. Nech $y \in Y \ldots$ TODO $\square$

Lema 12 (Burnsideova). Nech $N(A)$ je počet orbít grupy A, potom $N(A)$ je určený formulou:

$$N(A) = |A|^{-1} \sum_{\alpha \in A} j_1(\alpha)$$

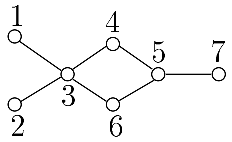
čiže priemerný počet 1–cyklov v každej permutácii.

Dôkaz. $X_1, X_2, \ldots, X_m$ sú orbity grupy A na množine $X = \{1, 2, 3, \ldots, n\}$.

$$\begin{aligned}
\bigcup_{i=1}^{m} X_i &= X \\
X_i \cup X_j &= \emptyset \qquad i \neq j \qquad X_i \neq \emptyset, i, j = 1, 2, \ldots, m \\
N(A) \cdot |A| &= \sum_{i=1}^{m} |A(x_i)|\,|X_i| = \sum_{x \in X} |A(x)| = \\
= \sum_{x \in X} \sum_{\substack{\alpha \in A \\ x = \alpha x}} 1 &= \sum_{x \in X} \sum_{\substack{x = \alpha x \\ \alpha \in A}} 1 = \sum_{\alpha \in A} j_1(\alpha)
\end{aligned}$$

$\square$

Príklad 13. Uvažujme graf G:



$$\begin{aligned}
\Gamma(G) \qquad \alpha_1 &= (1)(2)(3)(4)(5)(6)(7) \\
\alpha_2 &= (1\ 2)(3)(4)(5)(6)(7) \\
\alpha_3 &= (1)(2)(3)(4\ 6)(5)(7) \\
\alpha_4 &= (1\ 2)(3)(4\ 6)(5)(7) \\
|X| &= 7 \\
|\Gamma(G)| &= 4 \\
j_1(\alpha_1) &= 77 \\
j_1(\alpha_2) &= j_1(\alpha_3) = 5 \\
j_1(\alpha_4) &= 3 \\
N(\Gamma(G)) &= \frac{1}{4}(7 + 5 + 5 + 3) = 5
\end{aligned}$$

Orbity sú $\{1,2\},\{4,6\},\{3\},\{5\},\{7\}$. Počet orbít grupy grafu G je počet neoznačených zakorenených grafov z grafu G. Za koreň zvolíme ľubovoľný prvok orbity (je jedno ktorý prvok z orbity).

1.5 Ohraničená forma Burnsideovej lemy

A nech je grupa permutácií pôsobiacich na množine X. Grupu ohraničíme na množinu $Y \subseteq X$, spravidla Y sa berie ako zjednotenie nejakých orbít grupy A — označíme $A|Y$ — grupa permutácií pôsobiacich na množine Y.

$\alpha \in A$ nech je ľub. permutácia. Potom počet prvkov z Y identických vzhľadom na α označíme $j_1(\alpha|Y)$.

Lema 14. $N(A|Y) = |A|^{-1} \sum_{\alpha\in A} j_1(\alpha|Y)$, kde N je počet orbít.

Dôkaz. Analogicky ako bez $|$. □

1.6 Zvážená forma Burnsideovej lemy

R — komutatívny okruh, ktorý obsahuje množinu všetkých racionálnych čísel w — váhová funkcia, zobrazuje množinu X do okruhu R, kde A je grupa permutácií na množine X. V praktických aplikáciách je váhová funkcia w konštantná na orbitách grupy A — váha ľub. orbity X_i môžeme určiť ako váhu jej ľub. prvku. $w(X_i) = w(x)$, $x \in X_i$.

Veta 15. Súčet váh orbít grupy A sa určuje nasledujúcou formulou:

$$\sum_{i=1}^{m} w(X_i) = |A|^{-1} \sum_{\alpha\in A} \sum_{x=\alpha x} w(x)$$

TODO

Poznámka 16. Analogicky súčet cyklových indexov všetkých rôznych koreňových grafov, ktoré dostaneme z nejakého grafu G môže byť vyjadrený pomocou váh identických prvkov (vrcholov) grupy $\Gamma(G)$.

1.7 Polyova veta

Obmedzíme sa na verziu pre jednu premennú, verziu pre n premenných nebudeme zovšeobecňovať.

Definícia 17 (Mocninové grupy permutácií). Nech A je grupa permutácií na množine objektov $X = \{1,2,3,\ldots,n\}$, B konečná grupa permutácií so spočítateľnou množinou objektov Y^X — množina všetkých zobrazení z X do Y. Permutácie z B^A označujeme $(\alpha;\beta)$ kde $\alpha \in A$, $\beta \in B$ — aplikujeme ich na zobrazenia: nech $f \in Y^X : (\alpha;\beta)(x) = \beta f(\alpha x)$.

Položíme $B = E$ — identická grupa na Y, t.j. uvažujeme E^A s objektami Y^X.

$w : Y \to \{0, 1 \ldots n\}$

$|w^{-1}(k)|$ je konečné číslo pre každé $k \in \{0, 1 \ldots\}$, pričom $w^{-1}(k) = \{y | y \in Y, w(y) = k\}$

$c_k = |w^{-1}(k)|$ — počet „figúr" váhy k

$c(x) = \sum_{k=0}^{\infty} c_k x^k$ — rad vyčíslujúci figúry

$w(f) = \sum_{x \in X} w(f(x))$ — váha funkcie

Tvrdenie 18. Všetky funkcie, ktoré patria do tej istej orbity majú rovnakú váhu.

Dôkaz. Nech f,g patria do tej istej orbity ak existuje $\alpha \in A, \varepsilon \in E$ také, že $(\alpha, \varepsilon) f = g$

$w(f) = \sum_{x \in X} w(f(x))$; $w(g) = \sum_{x \in X} w(g(x))$; $g(x) = \varepsilon f(\alpha x)$; $g(x) = f(\alpha x) \implies \alpha x \in X \implies f(X) = g(X) \implies Y' \subseteq Y$ □

Váha orbity F je rovná váhe ľub. funkcie patriacej orbite — $w(F) = w(f)$, kde $f \in F$.

$|w^{-1}(k)|$ je konečné pre každé $k \in \{0, 1 \ldots\}$. Z toho vyplýva, že pre každé k existuje len konečný počet orbít rovnakej váhy. Počet orbít váhy k označíme C_k.

$C(x) = \sum_{k=0}^{\infty} C_k x^k$ — generujúca funkcia pre orbity každej váhy.

Veta 19 (Enumeračná Polyova veta). Rad $C(x)$ vyčísľujúci funkcie, dostaneme pomocou zámeny v cyklovom indexe $Z(A)$, keď za každú premennú s_k dosadíme rad $c(x^k)$ vyčíslujúci figúry. Symbolicky:

$$C(x) = Z(A, c(x^k)) \tag{2}$$

Dôkaz. Nech ε je identická permutácia na Y, $\alpha \in A$, $k = 0, 1, 2 \ldots$, $\varphi(\alpha, k)$ nech je počet funkcií váhy k pevných vzhľadom na permutáciu $(\alpha; \varepsilon)$, čiže takých f, ktoré spĺňajú

$$f(x) = (\alpha; \varepsilon) f(x) = \varepsilon f(\alpha x)$$

Ohraničíme E^A na funkcie váhy k. Z ohraničenej formy Burnsideovej lemy potom vyplýva:

$$
\begin{aligned}
C_k &= |A|^{-1} \sum_{\alpha \in A} \varphi(\alpha, k) \\
C(x) &= \sum_{k=0}^{\infty} |A|^{-1} \sum_{\alpha \in A} \varphi(\alpha, k) x^k \\
C(x) &= |A|^{-1} \sum_{\alpha \in A} \sum_{k=0}^{\infty} \varphi(\alpha, k) x^k \qquad (3)
\end{aligned}
$$

$\sum_{k=0}^{\infty} \varphi(\alpha, k) x^k$ vyčísluje všetky funkcie $f \in Y^X$ pevné vzhľadom na permutáciu $(\alpha; \varepsilon)$, teda také, že $\forall x \in X : f(x) = f(\alpha x)$ — funkcia f musí byť konštantná na disjunktných cykloch permutácie α a obrátene, všetky funkcie konštantné na cykloch permutácie α sú pevné vzhľadom na permutáciu α.

Nech z_r je cyklus dĺžky r permutácie α. Nech funkcia f zobrazuje elementy cyklu z_r na jeden z c_k elementov množiny Y, majúcich váhu k. Potom cyklus z_r prináša vklad do váhy funkcie f hodnotu rk.

Pre každé k je koeficient pri x^{rk} v rade $c(x^r) = \sum_{k=0}^{\infty} c_k x^{rk}$ je rovný počtu spôsobov ktorými môžeme určiť funkciu f na prvkoch cyklu z_r tak, aby bola pevná vzhľadom na permutáciu α a aby vklad do váhy $w(f)$ bol rk. Odtiaľ vyplýva, že rad

$$[c(x^r)]^{j_r(\alpha)}$$

vyčísluje všetky cykly dĺžky r.

$$\sum_{k=0}^{\infty} \varphi(\alpha, k) x^k = \prod_{\substack{k=1 \\ r}}^{n} [c(x^r)]^{j_r(\alpha)} \qquad (4)$$

□

Príklad 20. Koľko náhrdelníkov o 4 korálkach môžeme vytvoriť z koráliek dvoch farieb?

TODO