Burnsidova lema

Lovro Drofenik, Jan Genc, Tea Jeličić
Mentor: Jakob Jurij Snoj

Povzetek

V projektu smo se ukvarjali z iskanjem načina reševanja nalog, kjer moramo pri štetju različnih konfiguracij upoštevati rotacije ali simetrije.
V okviru tega smo spoznali osnove grup, nato pa smo podrobneje raziskali delovanja grup ter odkrili sredstva, s katerimi smo lahko dokazali Burnsidovo lemo, ki je za takšne naloge zelo uporabno orodje.

1 Uvod

V tabeli 7×7 pobarvamo dva kvadratka. Koliko različnih koknfiguracij lahko dobimo, če štejeta dve konfiguraciji za enaki, ko lahko iz ene dobimo drugo z rotacijami okrog središča za $90°$?

Če nalogo poskusimo rešiti na običajen način, hitro opazimo, da lahko z rotacijo nekaj barvanj dobimo več različnih konfiguracij kot z rotacijo drugih - če sta namreč pobarvana kvadratka simetrična čez središče tabele, lahko z rotacijo dobimo le dve različni konfiguraciji, sicer pa štiri. Čeprav bi lahko nalogo rešili tudi drugače, si bomo poskušali pomagati z grupami, da spoznamo Burnsidovo lemo - orodje, ki podobne naloge precej poenostavi.

2 Grupe

Da se lotimo problema, bomo torej najprej morali spoznati, kaj so grupe.

Definicija 1 *Grupa $(G, \cdot)$, je par množice G in operacije $\cdot$, ki poljubnima dvema elementoma množice G priredi nek element množice G. Veljati morajo še naslednje lastnosti:*

- *operacija je asociativna, torej: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, $\forall a, b, c \in G$.*
- *v G obstaja nevtralni element 1_G, tako da velja*

$$a \cdot 1_G = 1_G \cdot a = a, \ \forall a \in G.$$

- *vsak $a \in G$ ima svoj inverz a^{-1}, tako da*

$$a \cdot a^{-1} = a^{-1} \cdot a = 1_G.$$

Za dva elementa g in h bomo $g \cdot h$ pisali enostavno kot gh.

Primer grupe je $(\mathbb{Z}, +)$. Seštevanje je binarna asociativna operacija, imamo nevtralni element $1_G = 0$ in vsak element ima svoj inverz $a^{-1} = -a$, saj velja $a + a^{-1} = a + (-a) = 0 = 1_G$.

Operacija v grupah ni nujno komutativna, tj. za poljubna elementa $g, h \in G$ ne velja nujno $gh = hg$. Grupe s komutativno operacijo imajo posebno ime.

Definicija 2 ***Abelova grupa*** *je grupa, katere operacija je tudi komutativna.*

Zgled 1 $(\mathbb{Z}, +)$ *je Abelova grupa, ker je seštevanje komutativno.*

Navedimo še nekaj pomembnih primerov grup. Nekatere izmed njih bomo kasneje tudi uporabili.

Definicija 3 *Simetrična grupa* S_n *je množica vseh permutacij množice* $\{1, 2, \ldots, n\}$*. Operacija v tej grupi je kompozicija (na naši množici permutacije izvajamo eno za drugo).*

Definicija 4 *Diedrska grupa reda* $2n$*, ki jo označimo z* D_{2n}*, je grupa rotacij in zrcaljenj pravilnega* n*-kotnika. Operacija v tej grupi je prav tako kompozicija.*

Definicija 5 *Trivialna grupa* $\{1_G\}$ *je grupa, ki vsebuje le nevtralni element.*

Preden nadaljujemo, poglejmo nekaj osnovnih lastnosti grup.

Izrek 1 *V vsaki grupi sta nevtralni element in inverz posameznega elementa enolično določena.*

Dokaz: Dokažimo s protislovjem. Predpostavimo, da sta v grupi G dva različna nevtralna elementa in ju označimo z 1_{G_1} in 1_{G_2}. Potem velja:

$$\begin{aligned} 1_{G_1} \cdot 1_{G_2} =& 1_{G_1}, && (1_{G_2} \text{ je nevtralni element}) \\ 1_{G_1} \cdot 1_{G_2} =& 1_{G_2}, && (1_{G_1} \text{ je nevtralni element}) \\ \Rightarrow 1_{G_1} =& 1_{G_2}, \end{aligned}$$

kar je protislovje.

Podobno predpostavimo, da za nek element $a \in G$ obstajata dva različna inverza a_1^{-1} in a_2^{-1}. Potem zaradi asociativnosti velja:

$$(a_1^{-1} \cdot a) \cdot a_2^{-1} = 1_G \cdot a_2^{-1} = a_2^{-1}$$

$$a_1^{-1} \cdot (a \cdot a_2^{-1}) = a_1^{-1} \cdot 1_G = a_1^{-1}$$

$$\Rightarrow a_1^{-1} = a_2^{-1}$$

Spet smo prišli do protislovja in tako vemo, da je vsak inverz elementa iz G enolično določen. □

Enostavno lahko pokažemo tudi, da velja:

- $(a^{-1})^{-1} = a$
- $(ab)^{-1} = b^{-1}a^{-1}$

Lema 1 *Naj bo $g \in G$. Potem je preslikava $f : G \to G$, definirana s predpisom $f(x) = gx$, bijekcija.*

Dokaz: Najprej dokažimo injektivnost. Recimo, da obstajata taka x in y, $x \neq y$, da velja $f(x) = f(y)$. Potem sledi: $gx = gy \Rightarrow g^{-1}gx = g^{-1}gy \Rightarrow x = y$. Torej smo prišli do protislovja in funkcija je zato injektivna.
Dokažimo še surjektivnost. Vzemimo poljuben $a \in G$. Sedaj poglejmo $f(g^{-1}a)$. Vidimo da je $f(g^{-1}a) = gg^{-1}a = a$. Ker je tudi $g^{-1}a \in G$, so vsa števila iz G v zalogi vrednosti. Torej je funkcija surjektivna in zato tudi bijektivna. $\square$

Kot imajo množice svoje podmnožice, imajo tudi grupe svoje **podgrupe**. Seveda vsaka podmnožica s to operacijo ne tvori grupe.

Definicija 6 *Naj bo $(G, \cdot)$ grupa. $(H, \cdot)$ je* ***podgrupa*** *grupe $(G, \cdot)$ natanko tedaj, ko je tudi sama grupa in velja $H \subseteq G$.*

Podgrupa je **prava**, če je množica H strogo manjša od G. Vsaka grupa je podgrupa sama sebi. Vse grupe (z izjemo trivialne) imajo vsaj dve podgrupi: grupo samo in trivialno grupo.
Pred nadaljevanjem bomo spoznali še, kako lahko določene grupe zapišemo na enostavnejši način.

Definicija 7 *Naj bo G grupa in S njena podmnožica. Podgrupa $\langle S \rangle$, generirana z S, je množica elementov, ki jih lahko zapišemo kot končni produkt elementov v S in njihovih inverzov.*

Zgled 2 *Če je x generator grupe, je $\{\ldots, x^{-2}, x^{-1}, 1_G, x, x^2, \ldots\}$ grupa, generirana z x. Primer grupe z generatorjem $x = 1$ je $(\mathbb{Z}, +)$. Označimo jo lahko tudi kot $\langle 1 \rangle$.*

Včasih poleg generatorjev na grupah vključimo še kakšne dodatne pogoje, kar zapišemo za navpično črto. Denimo, zapis $\langle r \mid r^4 = 1 \rangle$ predstavlja ciklično grupo na štirih elementih.

3 Delovanje grup

Sedaj poznamo grupe in njihove osnovne lastnosti, kar je dovolj, da si lahko ogledamo delovanja grup - preslikave, s katerimi bomo na našem konkretnem primeru s pomočjo grup ponazorili rotacije.

Definicija 8 *Naj bo G grupa in X množica. Delovanje grupe G je preslikava $*$ iz $G \times X$ v X, za katero velja:*

- *za vsaka $g_1, g_2 \in G$ in $x \in X$ velja*
$$(g_1 g_2) * x = g_1 * (g_2 * x),$$
- $1_G * x = x$.

Definirali bomo še ekvivalenčno relacijo, ki nam bodo pomagali pri dokazovanju nekaterih pomembnih lastnosti.

Definicija 9 *Ekvivalenčna relacija $\sim$ je relacija med dvema elementoma a in b v množici, za katero velja:*

- $a \sim a$,
- $a \sim b \Rightarrow b \sim a$,
- $a \sim b \wedge b \sim c \Rightarrow a \sim c$.

Zgled 3 *Poglejmo si relacijo $=$, kot je definirana običajno. Enostavno preverimo, da zanjo veljajo vsi tri pogoji, torej je ekvivalenčna.*

Ekvivalenčna relacija razdeli množico na disjunktne **ekvivalenčne razrede**, tako da so v vsakem ekvivalenčnem razredu vsi elementi, ki so med seboj v relaciji.

Tudi pri delovanju grup lahko najdemo ekvivalenčno relacijo:

Definicija 10 *Naj bo G grupa, ki deluje na množici X. Definiramo ekvivalenčno relacijo $x \sim y$ s predpisom $x = g * y$ za nek $g \in G$. Ekvivalenčne razrede te relacije imenujemo* ***orbite****. Orbito, ki vsebuje element x, označimo z $\mathcal{O}_x$.*

Premislimo še enkrat o naši nalogi: v uvodu smo ugotovili, da barvanje dveh kvadratkov, simetričnih čez središče, ustvari konfiguracijo, ki se pri rotaciji za 180° ne spremeni. Podobno opažanje lahko prenesemo na delovanja grup.

Definicija 11 *Stabilizator* $stab_G(x)$ *elementa* x *množice* X*, na kateri deluje grupa* G*, je množica elementov* G*, ki pri delovanju* G *fiksirajo* x *- torej*

$$stab_G(x) = \{g \in G \mid g * x = x\}.$$

.

Izrek 2 *Stabilizator poljubnega elementa* $x \in X$ *je podgrupa v* G*.*

Dokaz: Očitno je, da je stabilizator podmnožica G. Dokazati moramo še, da je grupa. Za to mora množica imeti nevtralni element, inverz vsakega elementa in za vsaka g_1 in g_2 iz G mora veljati $(g_1 g_2) * x \in G$. Da prva dva pogoja zmeraj veljata, ni težko dokazati, zadnji pogoj pa množica izpolnjuje, saj velja

$$(g_1 * x) * g_2 = x * g_2 = x.$$

□

Orbite in stabilizatorje poljubnega elementa $x \in X$ povezuje pomemben izrek, ki ga sicer v tem članku ne bomo dokazali.

Izrek 3 ***Izrek o orbitah in stabilizatorjih.*** *Naj bo* G *končna grupa,* $O = \mathcal{O}_x$ *orbita poljubna elementa* $x \in X$ *ter* $S = stab_G(x)$*. Potem velja*

$$|O| \cdot |S| = |G|.$$

4 Burnsidova lema

Sedaj imamo vsa potrebna sredstva, da navedemo in dokažemo osrednji izrek našega članka, ki bo glavno orodje, s katerim bomo rešili nalogo iz začetka članka.

Izrek 4 ***Burnsidova lema*** *Naj bo* G *grupa, ki deluje na* X*. Naj bo* n *število različnih orbit. Potem je:*

$$n = \frac{1}{|G|} \cdot \sum_{g \in G} |Fix\ g|,$$

kjer $|Fix\ g|$ *predstavlja število različnih* $x \in X$*, za katere velja* $g * x = x$*.*

Dokaz: Najprej zapišimo $\sum_{g \in G} |Fix\ g|$ malo drugače.

$$\begin{aligned}\sum_{g\in G} |Fix\ g| = \sum_{g\in G} |\{x \in X \mid g * x = x\}| = \\ = |\{(g,x) \mid x \in X, g \in G, g * x = x\}| = \\ = \sum_{x\in X} |\{g \mid g \in G, g \in stab_G(x)\}| = \\ = \sum_{x\in X} |stab_G(x)|.\end{aligned}$$

Ker pa je $|stab_G(x)| = \frac{|G|}{|O_x|}$, velja:

$$\sum_{g\in G} |Fix\ g| = \sum_{x\in X} \frac{|G|}{|\mathcal{O}_x|}.$$

Zdaj pomnožimo obe strani z $\frac{1}{|G|}$:

$$\frac{1}{|G|} \cdot \sum_{g\in G} |Fix\ g| = \frac{1}{|G|} \cdot \sum_{x\in X} \frac{|G|}{|\mathcal{O}_x|} = \sum_{x\in X} \frac{1}{|\mathcal{O}_x|}.$$

Ker vsak x nastopa v natanko eni orbiti, se člen $\frac{1}{|\mathcal{O}_x|}$ pojavi natanko enkrat za vsak element orbite elementa x. Torej je vsota členov, ki jih prispevajo vsi elementi ene orbite, enaka 1. To velja za vsako orbito v G. Sledi, da je vsota $\sum_{x\in X} \frac{1}{|\mathcal{O}_x|}$ enaka številu različnih orbit n. $\square$

Sedaj se končno lahko lotimo naše naloge:

Zgled 4 *V tabeli* 7×7 *pobarvamo dva kvadratka. Koliko različnih konfiguracij lahko dobimo, če štejeta dve konfiguraciji za enaki, ko lahko iz ene pridemo v drugo z rotacijami okrog središča za* $90°$*?*

Rešitev: Definirajmo grupo $G = \langle r \mid r^4 = 1_G \rangle$ in naj bo X množica vseh možnih barvanj dveh različnh kvadratkov v tabeli 7×7. Delovanje grupe G na množici X naj predstavlja rotacijo - za vsak $x \in X$ naj $r * x$ predstavlja rotacijo elementa x za $90°$.

Število orbit nam tukaj predstavlja število različnih barvanj tabele, saj sta dve barvanji enaki natanko tedaj, ko sta v isti orbiti. Označimo število orbit s T. Uporabili bomo Burnsidovo lemo. Poglejmo, kaj se zgodi pri različnih rotacijah:

- Rotacija za $0°$ $(1_G x)$ vrne vse elemente v njihovo prvotno pozicijo. Takšnih barvanj x je $\binom{49}{2}$.

- Rotaciji za 90° (rx) in 270° (r^3x) v nobenem primeru ne vrneta dveh pobarvanih polj v prvotno pozicijo.
- Rotacija za 180° (r^2x) fiksira samo tista barvanja, pri katerih sta pobarvani polji zrcaljeni prek središča polja, takih barvanj je $\frac{48}{2}$ (vsako barvanje je enolično določeno z izbiro enega nesredinskega kvadratka, vsako barvanje pa smo šteli dvakrat - enkrat za en kvadratek in še enkrat za njegovo zrcalno sliko).

Po Burnsidovi lemi velja:

$$T = \frac{1}{4} \cdot \sum_{g \in G} |Fix\ g| = \frac{1}{4} \cdot \left(\binom{49}{2} + 0 + \frac{48}{2} + 0 \right) = \frac{1}{4} \cdot (1200) = 300.$$

Torej je takšnih barvanj natanko 300. □

Literatura

[1] E. Chen, *An Infinitely Large Napkin*, [ogled 8. 8. 2018], dostopno na `https://usamo.files.wordpress.com/2017/12/napkin-2017-12-11.pdf`