(Ne)rešljiva Rubikova kocka in grupe

Maša Lah, Sabina Boršić, Klara Drofenik
Mentor: Rok Gregorič

Matematično raziskovalno srečanje
24. avgust 2016

Povzetek

Cilj našega projekta je bil ugotoviti kriterij za rešljivost Rubikove kocke. Zato smo spoznali nekaj osnov grup, podrobneje simetrične in ciklične grupe ter generiranost. To znanje smo aplicirali na Rubikovo kocko in ugotovili, katere konfiguracije Rubikove kocke je možno dobiti s premiki stranic.

1 Uvod

Pri našem projektu smo raziskovali koliko je možnih konfiguracij Rubikove kocke. Želeli smo najti kriterij, ki bi nam povedal, ali je dana konfiguracija kocke rešlijva brez razstavljanja. Namreč, če bi kocko razstavili in jo ponovno sestavili, bi lahko ustvarili več konfiguracij, kot le z mešanjem rešene kocke.

Najprej preštejmo število vseh možnih konfiguracij, rešljivih ali ne. Rubikovo kocko velikosti $3 \times 3 \times 3$ sestavlja 27 kock. Od teh je ena skrita v sredini in ni vidna. Na vsakem licu leži ena sredinska kocka, torej skupno 6 sredinskih kock, ki ohranjajo svoj položaj, ne glede na to, kakšen premik naredimo. Imamo 8 vogalnih kock, ki imajo vsaka 3 vidna lica. Vsako od teh je pobarvano s svojo izmed šestih barv. Nazadnje ostane še 12 robnih kock z dvema vidnima in posledično pobarvanima licema. Skupaj imamo za prvo vogalno kocko 8 možnih

položajev, za naslednjo vogalno kocko imamo na izbiro 7 položajev, še za naslednjo 6, itd. Torej lahko vogalne kocke postavimo na celotno Rubikovo kocko na $8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 8!$ različnih načinov, če upoštevamo samo lego vogalne kocke, ne pa tudi, kako je obrnjena. Podobno lahko naredimo za robne kocke za katere dobimo 12! možnih postavitev. Upoštevati pa moramo še orientacijo barv na posamezni kocki. Za vogalno kocko, ki je tribarvna, imamo 3 različne orientacije in, ker je takšnih kock 8, obstaja 3^8 možnosti, za 12 dvobarvnih robnih kock pa 2^{12} možnosti. Ugotovimo, da je vseh možnih konfiguracij Rubikove kocke skupaj

$$8! \cdot 3^8 \cdot 12! \cdot 2^{12}.$$

To je precej veliko število, približno 10^{20}. Samo po sebi ni jasno ali lahko do vsake izmed teh konfiguracij tudi dejansko pridemo z mešanjem kocke ali je kocko, da pridemo do nekaterih postavitev, potrebno razstaviti.

2 Grupe

Da lahko matematično predstavimo vse poteze, ki jih lahko izvedemo na Rubikovi kocki, bomo uporabili grupe. Kaj je sploh grupa?

Definicija 1. ***Grupa*** *je množica G skupaj z binarno operacijo, tj. funkcijo $G \times G \to G$, ki jo bomo večinoma označevali kot $(x, y) \mapsto x \cdot y = xy$, za katero veljajo naslednje lastnosti:*

1. *asociativnost:*
$$(x \cdot y) \cdot z = x \cdot (y \cdot z),$$
za vse $x, y, z \in \mathbb{Z}$,
2. *enota: obstaja nek $e \in G$, da za vsak $x \in G$ velja*
$$e \cdot x = x \cdot e = x,$$
3. *obstoj inverza: za vsak $x \in G$ obstaja $x^{-1} \in G$, da velja*
$$x \cdot x^{-1} = x^{-1} \cdot x = e.$$

Primer 1. Preverili bomo, da je $(\mathbb{Z}, +)$, torej množica celih števil z operacijo seštevanja, grupa. Seštevanje je asociativno, saj že iz osnovne šole vemo, da velja

$$(x + y) + z = x + (y + z),$$

za vse $x, y, z \in \mathbb{Z}$. Enota je 0, saj velja $0 + x = x$, za vsak $x \in \mathbb{Z}$. Za vsako celo število x velja $x + (-x) = -x + x = 0$, zato je $-x$ njegov inverz. S tem smo zadostili vsem trem pogojem in tako dokazali, da je množica celih števil z operacijo seštevanja grupa.

Na enak način kot zgoraj bi lahko videli tudi, da so grupe $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ in $(\mathbb{C}, +)$.

Primer 2. Drug primer grupe je ciklična grupa $\mathbb{Z}/n$, ki vsebuje elemente $\{0, 1, \ldots, n-1\}$ in operacijo seštevanja ostankov števil pri deljenju z naravnim številom n. Razložimo to z več besedami. Vsak $x \in \mathbb{Z}$ lahko zapišemo kot $x = k \cdot n + r$, pri čemer je r ostanek pri deljenju x z n. Tedaj velja $x \pmod n = r$ in to je element množice $\mathbb{Z}/n$. Tedaj je grupna operacija na ciklični grupi, ki jo bomo tudi označevali $+$, definirana kot

$$x + y = x + y \pmod n,$$

pri čemer x in y na desni strani enačbe obravnavamo kot celi števili.

2.1 Simetrične grupe

Spoznali bomo poseben primer grup, ki jih imenujemo simetrične grupe. Te nam bodo pomagale pri razumevanju kriterija za rešljivost Rubikove kocke.

Definicija 2. ***Simetrično grupo*** S_n *tvorita množica vseh permutacij elementov* $1, 2, \ldots, n$*, torej bijektivnih preslikav* n*-elementne množice same vase, in operacije kompozituma.*

Trditev 1. *Simetrična grupa z operacijo kompozituma je grupa.*

Dokaz. Operacija kompozituma funkcij je asociativna, torej je temu pogoju zadoščeno. Enota je funkcija identiteta, oznaka id, ki slika vsak element v samega sebe. Po eni izmed ekvivalentnih karakterizacij bijektivnosti, ima vsak element S_n svoj inverz. □

Določimo moč simetrične grupe. Permutacijo lahko izrazimo kot postopek razvrščanja n elemetov na n mest. Če želimo n elementom pripisati svoje mesto, imamo za poljubnega prvega, ki ga slikamo, na voljo n mest, za naslednjega $n-1$ mest, in tako dalje, do zadnjega, za katerega imamo samo še eno možno mesto. To lahko zapišemo kot

$$|S_n| = n \cdot (n-1) \cdot \ldots \cdot 1 = n!.$$

Naj bosta i in j različni števili med 1 in n. Transpozicija (i, j) je element simetrične grupe, ki preslika i v j in j v i, ostale elemente pa ohrani enake. Vsaka permutacija je produkt transpozicij in parnost števila transpozicij v produktnem zapisu je enolična. Dokaz tega je mogoče najti v [2]. Zapisano s simboli, za vsak $\sigma \in S_n$ obstaja zapis $\sigma = (a_1 a_2)(a_3 a_4) \ldots (a_{k-1} a_k)$. Znak permutacije σ definiramo kot $\operatorname{sgn}(\sigma) = (-1)^k$. Če je k sodo število, rečemo, da je σ soda permutacija, če je k liho število, pa je liha.

2.2 Generiranost

Če je x element poljubne grupe, uvedemo pojem potence x^n za $n \in \mathbb{Z}$ kot

$$x^n = \underbrace{x \cdot x \cdot \ldots \cdot x}_{n},$$

če je $n > 0$, kot $x^0 = e$ za $n = 0$ in kot

$$x^n = \underbrace{x^{-1} \cdot x^{-1} \cdot \ldots \cdot x^{-1}}_{-n},$$

če je $n < 0$.

Definicija 3. *Pravimo, da elementi $x_1, \ldots, x_n \in G$ generirajo grupo G, če vsak $y \in G$ lahko zapišemo v obliki $y = x_{i_1}^{n_1} \cdot \ldots \cdot x_{i_k}^{n_k}$, za neke $i_1, \ldots, i_k \in \{1, \ldots, n\}$ in $n_1, \ldots, n_k \in \mathbb{Z}$. Tedaj elementom $x_1, \ldots, x_n$ pravimo generatorji grupe G.*

Primer 3. Oglejmo si primer množice celih števil in operacije seštevanja. Ugotovimo, da je $1 \in \mathbb{Z}$ generator za našo grupo, saj za vsak $n \in \mathbb{Z}$ velja

$$n = n \cdot 1 = \underbrace{1 + \cdots + 1}_{n},$$

če je $n > 0$, oziroma $0 = 0 \cdot 1$ za $n = 0$, oziroma

$$n = (-n) \cdot (-1) = \underbrace{(-1) + \cdots + (-1)}_{-n},$$

če je $n < 0$. Tudi vsaka podmnožica množice celih števil, ki vsebuje 1, generira našo grupo.

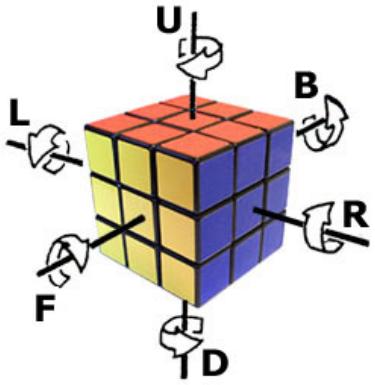
Primer 4. Generator ciklične grupe $\mathbb{Z}/n$ je 1, saj lahko vsak k med 0 in $n - 1$ lahko dobimo kot vsoto k enic.

Primer 5. Simetrično grupo S_n generirajo transpozicije, saj smo prej povedali, da lahko vsako permutacijo zapišemo kot njihov produkt.

3 Grupa Rubikove kocke

Vzemimo Rubikovo kocko $3 \times 3 \times 3$. Ima 6 ploskev, rotacije katerih v smeri urinega kazalca označimo glede na lego ploskve z začetnicami angleških imen zanje. Tako premik zgornje ploskve označimo z U, spodnje z D, desne z R, leve z L, sprednje s F in zadnje z B, kot je razvidno iz slike 1.

Označimo grupo premikov Rubikove kocke z $\mathbb{G}$. Kot množico jo tvorijo vsi premiki, s katerimi bi lahko poskusili reševati kocko. Vsak



Slika 1: Premiki Rubikove kocke

izmed njih je sestavljen iz končnega zaporedja osnovnih premikov F, B, L, U, D, L in R. Za $P, S \in \mathbb{G}$ definiramo premik $P \cdot S$ tako, da najprej opravimo premik P ter nato premik S. S tem smo podali grupno operacijo.

Trditev 2. *Množica premikov Rubikove kocke $\mathbb{G}$ z opisano operacijo je grupa.*

Dokaz. Operacija je asociativna, saj za premike P, S in T očitno velja $P \cdot (S \cdot T) = (P \cdot S) \cdot T$. Enoto podaja premik "ne naredimo nič", ki ohrani postavitev. V analogiji s simetrično grupo ga bomo označili z id. Pokažimo še, da za vsak premik P obstaja inverz P^{-1}.

Najprej si poglejmo primer, ko je P osnovni premik, brez škode za splošnost kar F. Njegov inverz dobimo tako, da sprednje lice zavrtimo obratno kot F, torej v obratni smeri urinega kazalca. To je enako, kot da bi opravili premik F^3.

Vsak element $P \in \mathbb{G}$ lahko zapišemo kot produkt osnovnih premikov. Postopajmo z indukcijo na dolžino tega zapisa. Če je zapis dolžine ena, potem je P osnovni premik in inverz že poznamo. Torej predpostavimo, da smo inverz našli že za vsak premik P, ki je produkt n osnovnih. Dovolj je pokazati, da tedaj obstaja inverz premika PF. To velja, saj premik

$$(PF)^{-1} = F^{-1}P^{-1} = F^3P$$

zadošča definiciji inverza. Po indukcijski predpostavki ima vsak element v $\mathbb{G}$ inverz. S tem smo dokazali, da gre za grupo. □

Opazko, da je vsako potezo za reševanje Rubikove kocke mogoče zapisati kot zaporedje osnovnih, lahko izrazimo v jeziku grup tako, da rečemo, da so osnovni premiki generatorji grupe $\mathbb{G}$.

Zanima nas, kako matematično zapisati konfiguracijo Rubikove kocke. Odvisna je od 4 postavitev, in sicer od lege osmih vogalnih kock, od lege dvanajstih robnih kock, od orientacije barv na vogalnih ter na robnih kockah. Natančno strukturo "faznega prostora" Rubikove kocke lahko opišemo s pojmi, ki smo jih spoznali tekom članka.

Trditev 3. *Množica vseh konfiguracij Rubikove kocke je v bijekciji z*

$$S_8 \times S_{12} \times (\mathbb{Z}/3)^8 \times (\mathbb{Z}/2)^{12}.$$

Dokaz. Lego osmih vogalnih kock lahko zapišemo s pomočjo simetrične grupe na osmih elementih S_8. Natančneje, če primerjamo dano konfiguracijo s konfiguracijo zmešane kocke, so položaji vogalnih kock premešani med sabo glede na to, kje so vogali v zmešani postavitvi. Na ta način konfiguracija podaja permutacijo n-elementne množice vozlišč oziroma nek element grupe S_8. Podobno naredimo za robne kocke, katerih lego določimo s S_{12}.

Zapisati moramo še orientacijo vseh kock, pri čemer bomo uporabili znanje o cikličnih grupah. Namreč, oštevičimo barve na dani vogalni kocki z 0, 1 in 2, tako da vrhnja oz spodnja barva sovpada s številom 0. Uporabimo premik $P \in \mathbb{G}$ in poglejmo, katero število je zdaj na vrhu prej izbrane vogalne kocke, kjerkoli se že ta zdaj morda nahaja. Če to naredimo za vsako vogalno kocko posebej, potem smo premiku P priredili osmerico elementov grupe $\mathbb{Z}/3$ oziroma ekvivalentno element produkta $(\mathbb{Z}/3)^8$. Orientacijo barv na vogalnih kockah torej označimo z elementi $(\mathbb{Z}/3)^8$, na robnih pa podobno z elementi $(\mathbb{Z}/2)^{12}$.

Glede na to, da podatki, kje ležijo vse kocke in kako so obarvane, enolično odločajo konfiguracijo, smo s tem dokazali trditev. □

Trditev bolj konkretno pomeni, da poljubno konfiguracijo Rubikove kocke predstavimo s četverico (σ, π, x, y), pri čemer σ in π označujeta permutacije položajev vogalnih in robnih kock, x in y pa orientacijo vogalnih in robnih kock.

Spomnimo se, da smo v uvodu s podobnim razmislekom izračunali število različnih konifiguracij Rubikove kocke kot $8! \cdot 12! \cdot 3^8 \cdot 2^{12}$. To ni naključje, saj je to število ravno moč opisane konfiguracijske množice.

Primer 6. Zapišimo konfiguracijo rešene kocke. Lego kock pri rešeni kocki označimo z identiteto, orientacijo barv pa z 0. Konfiguracija rešene kocke je tako $(\mathrm{id}, \mathrm{id}, \mathbf{0}, \mathbf{0})$, pri čemer je $\mathbf{0} = (0, 0, \ldots, 0)$ bodisi 8 bodisi 12 ničel v $(\mathbb{Z}/3)^8$ ali $(\mathbb{Z}/2)^{12}$.

Za zaključek bomo spoznali obljubljeni kriterij za to, ali lahko konfiguracijo dobimo z mešanjem rešene kocke.

Trditev 4. *Konfiguracija Rubikove kocke* (σ, π, x, y) *je rešljiva natanko tedaj, ko velja*

$$\begin{aligned} \operatorname{sgn}\sigma &= \operatorname{sgn}\pi \\ \sum_{i=1}^{8} x_i &= 0 \,(\mathrm{mod}\, 3) \\ \sum_{j=1}^{12} x_j &= 0 \,(\mathrm{mod}\, 2) \end{aligned}$$

kjer je $x = (x_1, x_2, \ldots, x_8)$ *za* $x_i \in \mathbb{Z}/3$ *in* $y = (y_1, y_2, \ldots, y_{12})$ *za* $y_j \in \mathbb{Z}/2$.

Dokaz kriterija si lahko ogledamo v [1]. Močno se opira na teorijo grup, specifično na lastnosti permutacijskih grup ter grupe $\mathbb{G}$, ki smo jo spoznali. S pomočjo tega kriterija bi lahko zgolj z opazovanjem in nekoliko računanja poljubne postavitve Rubikove kocke ugotovili, ali jo je sploh možno rešiti ali ne.

Iz kriterija trditve takoj sledi, da ni vsaka konfiguracija Rubikove kocke rešljiva. Še več, če bi izračunali, koliko četveric (σ, π, x, y) zadošča navedenim trem pogojem, bi ugotovili, da je rešljivih natanko $\frac{1}{12}$ konfiguracij (kar je še vedno zelo veliko, več kot milijarda milijard). Drugače povedano, če vam pade Rubikova kocka po tleh in se razleti ter jo nepozorno sestavite nazaj skupaj, potem je ena dvanajstina možnosti, da je kocko še vedno mogoče rešiti.

Literatura

[1] Janet Chen *Group Theory and the Rubik's Cube*[online.] [citirano 21. avgust 2016] Dostopno na spletnem naslovu: http://www.math.harvard.edu/ jjchen/docs/Group

[2] I. Vidav, *Algebra*, Ljubljana, Mladinska knjiga, 1962.