MaMS 2026

Matematično raziskovalno srečanje 2026

Piran, 26. julij – 1. avgust

DMFA Slovenije

Matematično raziskovalno srečanje 2026

Zbornik

Avtorji: *Manca Ernst, Jan Genc, Nives Gošnjak, Jaka Hedžet, Juš Kocutar, Jure Kreže, Matija Likar, Urban Merhar, Tim Milanez, Aleksander Simonič, Jasna Urbančič, Nejc Zajc, Domen Zevnik, Jakob Žorž*

Uredila: *Manca Ernst, Nejc Zajc*

Recenzenti: *Manca Ernst, Jan Genc, Nives Gošnjak, Juš Kocutar, Jure Kreže, Matija Likar, Tim Milanez, Nejc Zajc, Jakob Žorž*

Oblikoval: *Žan Hafner Petrovski*

Predstavnica: *doc. dr. Mojca Vilfan*

Kraj in leto izida: Ljubljana, 2026

Kazalo

UVOD

Uvodnik

Nejc Zajc

O taboru

Matematično raziskovalno srečanje, na kratko MaRS, je poletni matematični tabor za srednješolke in srednješolce. Zbornik, ki je pred vami, povzema vsebine in dogajanje letošnje izvedbe tabora.

Letošnji polet na MaRS je bil enaindvajseti zapored in prvi, ki nas je po začetnih letih tabora pripeljal nazaj na obalo. Potekal je med nedeljo, 26. julijem, in soboto, 1. avgustom, v CŠOD Breženka v Fiesi pri Piranu. Tabora se je udeležilo 20 dijakinj in dijakov iz vse Slovenije, ki so pod mentorstvom devetčlanske študentske posadke širili svoja matematična obzorja.

Strokovni program je bil kot vselej sestavljen iz treh sklopov. Osrednjo večdnevno delavnico je pripravil in vodil Domen Zevnik, ki je udeležencem predstavil kompleksne dinamične sisteme ene spremenljivke. Drugi del matematičnih vsebin so sestavljala večerna predavanja, ki so jih letos prispevali štirje gostje. Nekdanji MaRSovec dr. Aleksander Simonič nam je predaval o testih praštevilskosti, Jasna Urbančič je predstavila A/B teste, dr. Jaka Hedžet je spregovoril o ojačanem pronicanju v kvadratnih mrežah, Urban Merhar pa nas je popeljal v svet zavarovalništva in upravljanja tveganj.

Glavno matematično vsebino so, kot na MaRSu vedno, predstavljali projekti. Skupine dveh ali treh udeležencev so pod študentskim mentorstvom raziskale vnaprej pripravljen matematični problem. Delo na projektih je potekalo od ponedeljkovega dopoldneva do konca tabora in je zapolnilo večino ur strokovnega programa. Dijaki so se s temo najprej spoznali prek uvodnih primerov, jo nato z mentorjem raziskali in se dokopali do rešitve osrednjega problema. Ob tem so pripravili tudi članek, v katerem svoje delo podrobno opišejo, in kratko predstavitev za starše in ostale udeležence. Članki vseh projektov so zbrani v tem zborniku.

Poleg vseh omenjenih strokovnih vsebin smo za udeležence pripravili tudi pester družabni program, pri katerem so se dijaki preizkušali v spretnosti ocenjevanja velikih količin in poznavanju glasbe. Lokacija tabora nam je omogočala pogosto kopanje, ob večerih pa smo se vsi skupaj do poznih ur družili ob igranju družabnih iger. Izvedli smo tudi vse tradicionalne aktivnosti – sredin pohod ter petkovo Veliko MaRSovsko pustolovščino in MaRSovski piknik. Velika MaRSovska pustolovščina je orientacijski pohod, na katerem udeležence na kontrolnih točkah čakajo kratke in zabavne naloge.

Urnik tabora je bil tako tudi letos polno zaseden. Tabor je potekal pod okriljem DMFA Slovenije, finančno pa so nas podprli Zavarovalna skupina Sava, Fakulteta za matematiko in fiziko Univerze v Ljubljani, Fakulteta za naravoslovje in matematiko Univerze v Mariboru, Jane Street, Teads, AFLabs, Abelium in Akademija Panta Rei. Z njihovo pomočjo je bil letošnji polet uspešen, udeleženci pa so z nami preživeli teden, ki se ga bomo še dolgo z veseljem spominjali.

Beseda odgovorne osebe

Drage udeleženke, udeleženci in posadka, spoštovani predavatelji, podporniki in ostali bralci zbornika. Za nami je še en uspešen polet na MaRS. Novo lokacijo in priložnosti, ki jih je ponudila, smo izkoristili z odprtimi rokami. Za vso energijo, ideje in iznajdljivost bi se rad zahvalil prav vsakemu članu posadke posebej. Vzdušje, ki smo ga ustvarili, je ključno, da so poleti (in bodo še naprej) tako uspešni. Vseeno tabora ne zmoremo in si ga tudi ne želimo izvesti sami. Vsem predavateljem in podpornikom bi se iz srca zahvalil za pomoč in pripravljenost za sodelovanje.

Najpomembnejši del tabora ste seveda udeleženci. Vsako leto navdušujete z izjemno energijo in željo po spoznavanju novega. Ves naš trud ob pripravi tabora je poplačan, ko skupaj z vami poletimo v teden, poln nepozabnih trenutkov – večernih pogovorov, prvih partij taroka in iskanja izdajalcev sredi morja. Upam, da ste se v tednu z nami tudi vi zabavali, se veliko naučili in stkali nova prijateljstva. Udeleženci, ki ste s srednjo šolo že zaključili, želim vam veliko uspehov in MaRSovske energije še naprej. Z ostalimi pa upam, da se vidimo tudi naslednje leto.

Lep MaaaaRSovski pozdrav, Nejc!

Word of the president of the committee

Dear participants, crew members, respected lecturers, supporters and all other readers, yet another successful flight to MaRS is now behind us. As always, we welcomed the new location and all its opportunities with open arms. I want to thank every single crew member for your energy, great ideas and resourcefulness. The atmosphere we created was and will continue to be key to our success. Still, there is no way for us to run our camp completely by ourselves. I sincerely thank all our lecturers and supporters for their willingness to help and cooperate.

Our participants are with no doubt the most important part of the camp. You always manage to captivate us with your incredible energy and want for learning new things. Throughout our unforgettable week together – filled with moments ranging from late night conversations to games of tarock and figuring out impostors in the middle of the sea – we saw that our efforts were not in vain. I truly hope you too had fun, learned a lot and made many new friends. I also wish all our participants who finished high school this year every success and hope you will carry on with this energy wherever you go. And to all the rest – I definitely hope to see you again next year.

Greetings from MaaaaRS, Nejc!

Dnevnik

Manca Ernst in Matija Likar

Pestro dogajanje letošnjega tabora smo povzeli v tradicionalnem marsovskem dnevniku, ki smo ga dnevno objavljali na družbenih omrežjih. S tem smo želeli tabor približati javnosti ter hkrati ponuditi udeležencem hudomušen opis preteklih doživetij. Vendar pa naj vas nekonvencionalen slog dnevnika, ki je poln internih šal, ne zmede preveč. Uvidevni do nadarjenih udeležencev smo namreč dnevnik prepredli z mnogimi slovničnimi, slogovnimi ter vsebinskimi akrobacijami, ki so jih dijaki med branjem vedro razvozlavali. Za razlage preostalih, še nerazvozlanih, dnevniških nebuloz pa se priporočamo v komentarjih na takojšnji enoti mase.

Slika 1: Skupinska slika.

Nedeljek, 26. julij 2026

Ko se bralec na to veselo nedeljkovo popoldne ozre po vstali primorski, mu more v oči pasti skladovnica zrnatih usedlin, sestavljena iz menjajočih se plasti peska, peščenjaka, laporovca, redkeje tudi slojev apnenca in ilovice (bojda večinoma eocenske starosti, tako pravijo prijatelji s proste enciklopedije) — a na drugo stran zalivov fieških, kamor sonce med predavanji ne sije, tja ga je lokalna prometna škifofka napotila grta v breženko.

Tisti, ki nam guma ni počila in zaradi neznanih vzhodnoazijskih virusov nismo opravičeno izostali, smo svoje novačenje v marsovski kov pričeli z malopogovorno travmatično izkušnjo in miksom največjih svetovnih hitov (ne si pozabit pol neki za pisat vzet). Okolju prijazno pozdravljeni in s podrobnostmi seznanjeni smo se bolje spoznali s pomočjo priljubljene igre v malo manj priljubljenem krstilniku. Izkaže se, da vsak Velenjčan ne pozna gaserja.

Tako kot se nekateri ne morejo vzdržati vstopa v zbornico, se dnevnikopisci ne moremo odpovedati prehranskim komentarjem: nocoj so nas nasitili lokalni vretenčarji, a najbolj je dišal tvoj kisel krompir. Večerno radovednost je nato pogasil dr. Aleksander Simonič s predavanjem o testih praštevilskosti. Poleg seznanitve s svetovnimi kazinoji nam je z uporabo Miller-Rabinovega testa razkril življenjsko modrost. Z algoritmi je tako kot z ljudmi — večji, kot imaš k, počasneje tečeš.

Prežgano subsredozemsko vročino je razblinila poletna nevihta in nam obudila spomin na potopni MaRS 2023. Pridne ponočevalce ali pa tiste jutranje bralce naj še razvedrimo s prvenstvenim MaRSovskim anagramom, ki ga je najbolje užiti ob skodelici kave.

Garaška je dirka do vrha iz dna.
Kdor v cilju je prvi, TA PREJ ČAGO DA.

Ponedelja, 27. julij 2026

V kolikor bi snoč več razmišljali o posledicah svojih dejanj, bi lahko navzoči bolje začeli ponedeljin dnevniški sestavek. Tisti z manj sreče smo dan začeli malo za šalo, malo pa navkreber; a kot bi poetično djal g. Svetek-Zorin, smo v borbah, ponižanju, zmagah in trpljenju našli svoj pravi obraz (ga pa vsaj nismo našli mokri, kot tisti, ki so se prepustili novospečenemu knapovskemu vodstvu).

Toda glej, za vsakim švicom posije jasna kopalniška luč. Uradno smo zagnali najprej naše projekte, nato pa še Tomaževe železnice. Sledila je

Ni sledila. Nocoj ne bom govoričila. Skrila bom svojo ženo, šla po požirek vode in nato dokončala stavek. Zazrla se bom v nebo in ne bom videla zgolj beljakovin rastlinskega izvora, videla bom zvezde. Zakaj se še zdaj zafrkavam z osem? Vse me boli melancani so pet od deset ampak jaz grem jaz grem naprej. Ne morem živeti v temi trgovinica torek pri ne ne bom več jaz moram iti. Kdo je sonce in kako se ima jaz tega ne vem ona je zvezda JADRO, ne boji se on viharja. Ne – zdaj sedim na stolu – ni stola – mize ni – ničesar ni – koga poznam? Jaz sem Domen Zevnik. Jaz sem Domen Zevnik. Jaz sem Domen Zevnik. Ni rekel, da ni tranzitiven. Mati so mi včeraj poslali sliko ježa niso me vprašali kdo je jež ne poznajo ga a jaz vem, jaz ga vidim, on je na strehi in na balkonu in pod posteljo in v mojem kozarcu. To se je zgodilo. Kdaj bom šla naprej, ne vidim več zvezd, vidim sonce, ki mi žge v oči, a ga ne vidim, ne, kaj sem rekla, on je na drevesu, ne vidim ga, skril se je, pozabila ga bom, pozabila bom

Pavza.

Na večernem predavanju nam je Jasna Urbančič s podjetja Teads predstavila A/B teste.

Čakali smo dolga leta na tarok, kodne besede in ostale igre, ki smo jih igrali pozno v noč, ko smo čakali dolga leta in noči na tarok in igre besed in kode, ko se je čakalo na noč in na dan in igrali smo družabne igre in vse kar imamo od družabnih iger in vse pod nočjo in tarok je dolg in leta so kratka in vse pod soncem je majhno in midva sva tu in vsi smo v taroku in noč je med nama in sonce zakril je mesec.

Torek, 28. julij 2026

Spoštovani gospa predsednica, gospoda Kuzmana. To je marsovski dnevnik in prva jutranja kronika.

V večernem predavanju je dr. Jaka Hedžet s Fakultete za naravoslovje in matematiko v Mariboru predstavil problem ojačanega pronicanja v kvadratnih mrežah. Čeprav je predavanje sosede ločevalo po tistem, po čemer se ločevati ne sme, dnevniška redakcija vztraja, naj bralec le ljubi svojega soseda, čemur bivalci sobe 26 tudi dosledno sledijo.

Šport. Tekaška divizija je med jutranjo etapo okoli Fieškega ribnika uspela zmanjšati prednost tekaške sekcije sindikalnega doma Slovenskih železnic, ki je kljub vrhunski pripravljenosti sicer zamudila na štart. Plavalna reprezentanca je popoldan v disciplini 50 metrov prsno zanesljivo premagala ekipo OŠ Matije Čopa Kranj.

Sledijo čestitke in pozdravi. Za trenutek naj odloži delo Mariborka, ki ji naročniki oglasa želijo hitro okrevanje modric. Pozdravljamo tudi Luko Koper, ki se mu stanovalci sobe 25 zahvaljujejo za njegov obstoj v sredini. Prav tako pa ne smemo pozabiti na Uživalca faze REM in njegovih treh nog, ki danes godujejo. Iskrene čestitke!

Za konec si še poglejmo vreme. Jutri bo precej jasno. Na Primorskem bo pihal jugozahodnik. Najvišje dnevne temperature bodo od 31 do 36°C. Navkljub vremenu si bo Ježek nadel dolge nogavice z zimskim vzorcem. Opravo bo nadgradil z modro majico, s katero bo docela izpolnil svojo podobnost s Sonikom.

Poslušali ste prvo jutranjo kroniko.

Sredek, 29. julij 2026

Vrtni palčki in trobentice me kličejo, ko hodim navkreber. Zvončki in slani lasje pred mano frfotajo v vetru s kraške planote. Skozi gnečo zagledam beli križ. Vonj sončne kreme in poletnih počitnic. Drobtinice mandljevega kruha se razprostirajo po nebu. Prevračajo se in kotalijo. Sama črnina je okoli mene. Ne morem odpreti oči in ne čutim svojih nog. V suhih ustih okušam varuhe planeta. Spominjam se, da mi je nekdo povedal, kako skrbijo za plankton, a jaz se tega ne spomnim več. Želim si. Samorog me ne ustavi na vrhu griča. Pogledam gor v nebo in zagledam šahovnico, skozi katero pronicajo beli sončni žarki. Slišim ocean. Tržaški zaliv. Na starem parniku, ki prevaža sol, ga še zadnjič uzrem, preden z ostalimi prestopniki odplujemo na zahod. Vidim zvonik cerkve sv. Jurija in nato še piranski svetilnik. Vidim portoroške plaže, skladišče soli, neštete jadrnice, soline, bele avione, savudrijski svetilnik in galebe in citruse in luči in nič. Potem pa dolgo nič. Preko sobe vržem vrečko čipsa in je voda. Jokati se začnem. Slišim zvezde, ki mi šepetajo, naj hodim naprej. A moja stopala se ne dotikajo več tal. Na obzorju zagledam majhno belo luč. Veča se.

Urban Merhar iz pozavarovalnice Sava Re vodi večerno predavanje o zavarovalnicah in upravljanju tveganj.

Četrtje, 30. julij 2026

Nekje sredi dneva te začne boleti glava, ko se zaveš, da bo do večera bolečina prešla še na vrat in del tvojih ramen. Navajen si je. Kot detel te najprej kljuva le za očmi, potem pa čez čas, ne veš točno kdaj, začne utripati po vsem tvojem telesu. Ujet si v roju luči, ki nenehno sijejo v tvoj obraz, v tvoje oči, sijejo okoli tebe, sijejo skozi tebe, in te luči niso tople, ne, so kot žgoče črno sonce, ki ne pozna drugega, kot da sije vate in žge ... Poskušaš zatisniti veke, a nekako veš, da jih ne moreš, kajti njihova svetloba pronica v tvoje telo in skozi tvoje lase in vse do mene. Sonca ne poznaš, toda čutiš, veš, da on ne premore sovraštva, a žge prav tako. Ne veš več, ali je to, kar vidiš, resnično. Nikoli nisi vedel. Nekdo se pogovarja s tabo – morda se ti to le dozdeva – a ne slišiš njihovih besed, vse je le šum, prežet z bolečino, ki vztrajno sije in utripa nekje v tebi. Kako si želiš, da bi zaprl oči in pozabil … a ne moreš pozabiti, dokler tečeš. Vse je temno, a vse utripa, in ne moreš se ustaviti. Spominjaš se, kako si nekoč še mogel spati, a zdaj tega ne znaš več. Ne poznaš več vonja svoje odeje, ne čutiš več lahnega piša vetra, ki kdaj uide skozi okno tvoje sobe, in ne poznaš več teme,

ki te je tako rada objela. Nad tabo zdaj raste breza. Njene korenine segajo proti tlom in trgajo, režejo, da bi pognale. Ko bi le prepoznale spet črno zemljo, da bi v njej smele tiho ležati … Toda ne pustiš jim, kajti kam bi se usidrale, če tečeš? One so gozd in one bi vzele svojo žrtev.

Petje, 31. julij 2026

Petkovo jutro smo pričeli z zajtrkom, ki mu je kot običajno sledila še telovadba. Nato smo nadaljevali z delom na naših projektih, saj smo včeraj dobili kar nekaj popravkov naših mentorjev. Imeli smo tudi poskusne predstavitve. Po kosilu pa je bil čas za težko pričakovan vrhunec našega tedna — veliko marsovsko pustolovščino! Na njej smo se po skupinah podali na pot, na kateri so nas na svojih postojankah čakali mentorji z nalogami. Po pustolovščini je bil čas še za tradicionalen ~~mafijski~~ marsovski piknik. Takrat so zmagovalci prejeli čast razbiti ta veliko marsovsko čokolado, ki so jo potem tudi razdelili med ostale Marsovce. Večerno dogajanje se je zavleklo pozno v noč.

(Dodatek: zjutraj smo ugotovili, da to ni prvi petkov dnevnik, in da Jure ni edini, ki je ponesreči poljubil svojega najboljšega prijatelja. cmok)

Šestek, 1. avgust 2026

Kaj plakaš, ti dobri človek?
Dneva je konec —
kaj plakaš opolnoči?
Večer je — zbogom!
Z mano bolí ste in radost delili;
še dosti, dosti bi povedal …
na obali, ob jezeru,
kdo delil bo zdaj?
Spet cvetijo spominčice —
a vse besede v prsih mró …
Na obali, v mojem srcu,
preveč je sreče,
morda ga boš našel tudi ti!
Kaj plakaš, ti dobri človek,
je žalosti v njem preveč?
Zdaj ostal je le spomin …
morda ne bom vas videl več!
Z mano ves teden ste nosili …
ste ranjeni z ostjo spoznanj?
Poglej, saj ni prvič konec marsa …
zbogom! Morda boš našel me —
in glej! Ko rože ovenijo
morda ga boš našel tudi ti!

OSREDNJA DELAVNICA

Kompleksna dinamika

Domen Zevnik

Fakulteta za matematiko in fiziko, Univerza v Ljubljani

1 Osnovni pojmi in definicije

Pri obravnavi bomo uporabljali predvsem realna in kompleksna števila. Definicije, trditve in dokazi so zapisani tako, da jih lahko uporabljamo nad $\mathbb{R}$ ali $\mathbb{C}$. Zato pišemo $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$. Kadar kompleksnih števil ne potrebujemo, običajno vzamemo $\mathbb{F} = \mathbb{R}$.

Glavni vir pri pripravi teh zapiskov je bil spletni učbenik Marka McClura *Complex Dynamics* [1].

Definicija 1.1 (Dinamični sistem)**.** Dinamični sistem *je funkcija*

$$f \colon \mathbb{F} \longrightarrow \mathbb{F}.$$

Glavne in edine primere dinamičnih sistemov bomo dobili iz družine funkcij, ki jih določa parameter $c \in \mathbb{F}$*:*

$$f_c(x) = x^2 + c.$$

Definicija 1.2 (Orbita)**.** *Za* $x \in \mathbb{F}$ *definiramo* orbito točke x *z zaporedjem*

$$x_0 := x, \qquad x_1 := f(x_0), \qquad x_2 := f(x_1), \qquad \ldots, \qquad x_n := f(x_{n-1}).$$

Torej je $x_n = f^n(x_0)$*, kjer* f^n *pomeni* n*-kratno kompozicijo funkcije* f*.*

Definicija 1.3 (Periodična točka, fiksna točka in cikel)**.** *Točka* $x \in \mathbb{F}$ *je* periodična*, če obstaja* $m \in \mathbb{N}$*, za katerega je*

$$f^m(x) = x.$$

Najmanjšemu takemu m *pravimo* perioda *točke* x*. Periodično točko s periodo* 1 *imenujemo* fiksna točka*. Zanjo velja* $f(x) = x$*.*

Če ima x_0 *periodo* m *in označimo* $x_j = f^j(x_0)$*, množico*

$$\{x_0, x_1, \ldots, x_{m-1}\}$$

imenujemo m-cikel *oziroma* periodični cikel*.*

Če ima x periodo m, se njena orbita ciklično ponavlja:

$$x_0 \mapsto x_1 \mapsto \cdots \mapsto x_{m-1} \mapsto x_0.$$

Točka je zato fiksna točka funkcije f^m. Obrat ne velja brez dodatnega pogoja: fiksna točka f^m ima lahko periodo k, kjer $k \mid m$ in $k < m$.

Primer 1.1. *Naj bo* $\mathbb{F} = \mathbb{R}$ *in* $f(x) = x^2 - 1$. *Tedaj*

$$0 \mapsto -1 \mapsto 0 \mapsto -1 \mapsto \cdots,$$

zato imata 0 *in* -1 *periodo* 2.

Fiksne točke dobimo iz

$$x = x^2 - 1 \quad \Longleftrightarrow \quad x^2 - x - 1 = 0,$$

zato sta

$$x_{1,2} = \frac{1 \pm \sqrt{5}}{2}.$$

Za periodo 2 *rešimo*

$$f^2(x) = x, \qquad f^2(x) = (x^2 - 1)^2 - 1 = x^4 - 2x^2,$$

oziroma

$$x(x + 1)(x^2 - x - 1) = 0.$$

Po izločitvi fiksnih točk ostaneta 0 *in* -1.

1.1 Pajčevinasti diagrami

Pri realnih dinamičnih sistemih lahko iteracije ponazorimo s pajčevinastim diagramom. Začnemo v izbrani točki (x_0, x_0) na simetrali $y = x$. Iz (x_n, x_n) se navpično premaknemo do grafa $y = f(x)$, torej do (x_n, x_{n+1}), nato pa vodoravno nazaj do simetrale, v točko (x_{n+1}, x_{n+1}). Ponavljanje teh dveh korakov nariše orbito. Presečišča grafa $y = f(x)$ s simetralo $y = x$ so ravno fiksne točke.

1.1.1 Funkcija $f(x) = x^2 - \frac{1}{4}$

Fiksne točke dobimo enako kot pri funkciji $x^2 - 1$:

$$x = x^2 - \frac{1}{4} \quad \Longleftrightarrow \quad x^2 - x - \frac{1}{4} = 0.$$

Kvadratna formula da

$$x_\pm = \frac{1 \pm \sqrt{1 + 1}}{2} = \frac{1 \pm \sqrt{2}}{2},$$

torej

$$x_- \approx -0{,}20710678 \qquad \text{in} \qquad x_+ \approx 1{,}20710678.$$

Za začetno vrednost $x_0 = 0{,}97$ dobimo prve člene

$$0{,}97 \mapsto 0{,}6909 \mapsto 0{,}22734 \mapsto -0{,}19832 \mapsto -0{,}21067 \mapsto -0{,}20562 \mapsto \cdots.$$

Orbita se izmenično približuje fiksni točki x_-. Na pajčevinastem diagramu zato stopnice tvorijo vedno manjše pravokotnike okoli presečišča grafa in simetrale.

Slika 1 prikazuje celotni pajčevinasti diagram, slika 2 pa povečavo majhne okolice fiksne točke, v kateri postane izmenično približevanje še jasnejše. Zaporedni členi ležijo izmenično levo in desno od x_-, velikosti pravokotnikov pa se krčijo proti nič. Natančno merilo tega krčenja bomo v naslednjem razdelku opisali z odvodom.

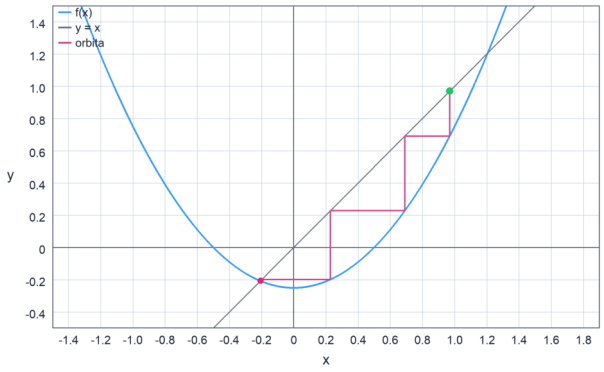
Za $x_0 = 1{,}21$ je položaj drugačen. Začetna vrednost je nekoliko večja od druge pozitivne fiksne točke:

$$x_0 = 1{,}21 > x_+ = \frac{1 + \sqrt{2}}{2} \approx 1{,}20710678.$$

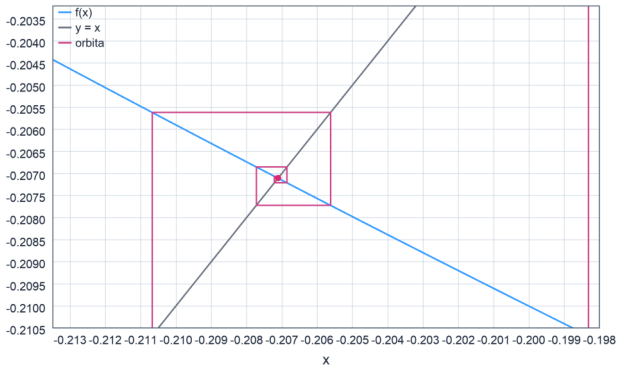
Iteracije se zato povečujejo,

$$\begin{aligned} 1{,}21 &\mapsto 1{,}2141 \mapsto 1{,}22404 \mapsto 1{,}24827 \mapsto 1{,}30818 \\ &\mapsto 1{,}46134 \mapsto 1{,}88550 \mapsto 3{,}30512 \mapsto 10{,}6738 \mapsto \cdots, \end{aligned}$$

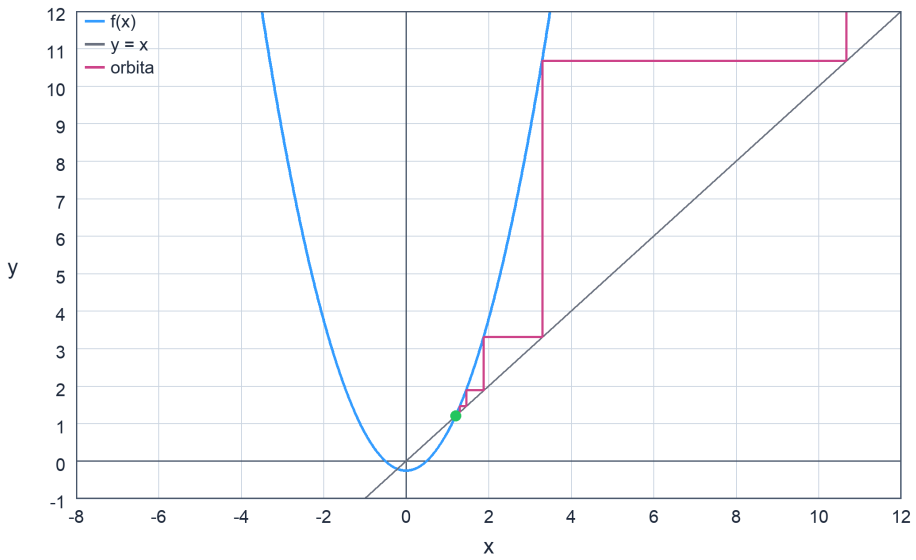
in orbita pobegne proti $+\infty$.



Slika 1: Celotni pajčevinasti diagram za $f(x) = x^2 - 1/4$ in $x_0 = 0{,}97$.



Slika 2: Povečava okoli $x_- \approx -0{,}2071$, ki je privlačna fiksna točka.



Slika 3: Za $f(x) = x^2 - 1/4$ in $x_0 = 1{,}21 > x_+$ pajčevinaste stopnice hitro zapustijo okolico fiksne točke in orbita pobegne v neskončnost.

1.1.2 Funkcija $f(x) = x^2 - 1$

Kot smo izračunali zgoraj, sta njeni fiksni točki

$$x_- = \frac{1-\sqrt{5}}{2} \approx -0{,}61803 \qquad \text{in} \qquad x_+ = \frac{1+\sqrt{5}}{2} \approx 1{,}61803.$$

Pri $x_0 = 1$ orbita že po prvem koraku pade na cikel

$$1 \mapsto 0 \mapsto -1 \mapsto 0 \mapsto -1 \mapsto \cdots .$$

Pajčevinasti diagram zato po prehodnem koraku ponavlja isti pravokotnik med točkama 0 in -1. Vidimo privlačni 2-cikel $\{0, -1\}$.

Začetna vrednost $x_0 = 1{,}6$ je še vedno manjša od pozitivne fiksne točke $x_+ \approx 1{,}61803$. Njena orbita zato *ne* pobegne:

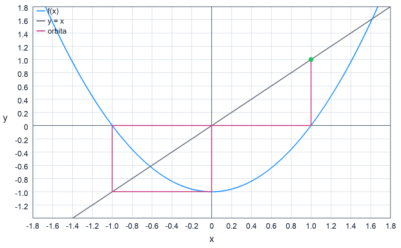
$$1{,}6 \mapsto 1{,}56 \mapsto 1{,}4336 \mapsto 1{,}05521 \mapsto 0{,}11347 \mapsto -0{,}98713 \mapsto -0{,}02558 \mapsto -0{,}99935 \mapsto \cdots ,$$

temveč se prav tako približuje ciklu $\{0, -1\}$.

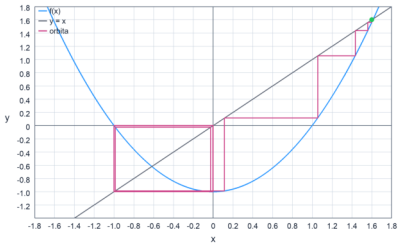
Za prikaz pobega moramo izbrati vrednost nad pozitivno fiksno točko, na primer $x_0 = 1{,}62 > x_+$. Tedaj

$$1{,}62 \mapsto 1{,}6244 \mapsto 1{,}63868 \mapsto 1{,}68526 \mapsto 1{,}84009 \mapsto 2{,}38593 \mapsto 4{,}69268 \mapsto 21{,}0213 \mapsto \cdots ,$$

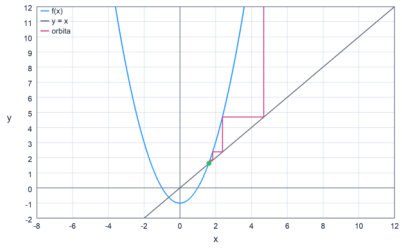
zato orbita pobegne proti $+\infty$.



Slika 4: $x_0 = 1$: orbita vstopi v 2-cikel $0 \leftrightarrow -1$.



Slika 5: $x_0 = 1{,}6 < x_+$: orbita se približa istemu 2-ciklu.



Slika 6: $x_0 = 1{,}62 > x_+$: orbita pobegne v neskončnost.

Ti primeri že pokažejo več različnih vrst obnašanja: konvergenco k fiksni točki, približevanje periodičnemu ciklu in pobeg v neskončnost. Pozneje bomo videli tudi bolj zapletene, kaotične orbite. V naslednjih podpoglavjih bomo ta obnašanja sistematično karakterizirali z odvodom v fiksni oziroma periodični točki.

2 Klasifikacija fiksnih točk

2.1 Karakterizacija z odvodom

Definicija 2.1. *Naj bo $f : \mathbb{F} \to \mathbb{F}$ odvedljiv dinamični sistem in naj bo x_0 njegova fiksna točka. Točka x_0 je*

1. privlačna, *če* $0 < |f'(x_0)| < 1$;
2. odbojna, *če* $|f'(x_0)| > 1$;
3. nevtralna, *če* $|f'(x_0)| = 1$;
4. superprivlačna, *če* $|f'(x_0)| = 0$.

Odvod je naklon najboljšega linearnega približka. Za x blizu x_0 velja

$$f(x) \approx f(x_0) + f'(x_0)(x - x_0),$$

napaka pa je višjega reda. Če je x_0 fiksna točka, dobimo

$$\begin{aligned} |f(x) - x_0| &= |f(x) - f(x_0)| \\ &\approx \big|f(x_0) + f'(x_0)(x - x_0) - \big(f(x_0) + f'(x_0)(x_0 - x_0)\big)\big| \\ &= |f'(x_0)|\,|x - x_0|. \end{aligned}$$

Zato se točke pri $|f'(x_0)| < 1$ približujejo x_0, pri $|f'(x_0)| > 1$ pa se od njega oddaljujejo. Če je $|f'(x_0)| = 1$, samo iz odvoda ne moremo sklepati, ali se orbita približuje ali oddaljuje.

Primer 2.1 ($f(x) = x^2 - 1/4$)**.** *Fiksni točki te funkcije smo že izračunali:*

$$x_- = \frac{1 - \sqrt{2}}{2} \qquad in \qquad x_+ = \frac{1 + \sqrt{2}}{2}.$$

Ker je $f'(x) = 2x$, v manjši fiksni točki dobimo

$$f'(x_-) = 1 - \sqrt{2} \qquad in \qquad |f'(x_-)| = \sqrt{2} - 1 \approx 0{,}4142 < 1.$$

Zato je x_- privlačna fiksna točka. V večji fiksni točki pa je

$$f'(x_+) = 1 + \sqrt{2} \qquad in \qquad |f'(x_+)| = 1 + \sqrt{2} \approx 2{,}4142 > 1,$$

zato je x_+ odbojna fiksna točka. S tem odvod pojasni obnašanje, ki smo ga opazili na pajčevinastih diagramih: orbite v okolici x_- se ji približujejo, orbite v okolici x_+ pa se od nje oddaljujejo.

3 Klasifikacija orbit

Periodična točka s periodo m je fiksna točka funkcije f^m, zato njeno orbito klasificiramo glede na odvod f^m.

Definicija 3.1. *Naj bo x_0 periodična točka s periodo m in naj bo $x_j = f^j(x_0)$. Orbita točke x_0 je* privlačna*,* odbojna*,* nevtralna *oziroma* superprivlačna*, kadar je x_0 ustrezne vrste fiksna točka funkcije f^m.*

Po verižnem pravilu

$$(g \circ f)'(x) = g'(f(x))f'(x)$$

in zato

$$(f^m)'(x_0) = f'(x_0)f'(x_1)\cdots f'(x_{m-1}).$$

Primer 3.1 ($f(x) = x^2 - 1$)**.** *Fiksni točki sta*

$$x_- = \frac{1 - \sqrt{5}}{2} \qquad in \qquad x_+ = \frac{1 + \sqrt{5}}{2}.$$

Ker je $f'(x) = 2x$, velja

$$\begin{aligned} |f'(x_-)| &= |1 - \sqrt{5}| = \sqrt{5} - 1 \approx 1{,}2361 > 1, \\ |f'(x_+)| &= 1 + \sqrt{5} \approx 3{,}2361 > 1. \end{aligned}$$

Obe fiksni točki sta torej odbojni.

Po drugi strani točki 0 *in* -1 *tvorita* 2*-cikel, saj*

$$f(0) = -1 \qquad in \qquad f(-1) = 0.$$

Odvod funkcije f^2 *v točki* 0 *je*

$$(f^2)'(0) = f'(-1)f'(0) = (-2) \cdot 0 = 0.$$

Enak rezultat dobimo, če cikel začnemo v -1*:*

$$(f^2)'(-1) = f'(0)f'(-1) = 0 \cdot (-2) = 0.$$

Zato je cikel $\{0, -1\}$ *superprivlačen, kar je močnejša oblika privlačnosti. To pojasni, zakaj se mu približujejo orbite, prikazane v pajčevinastih diagramih.*

4 Bifurkacijski diagram in orbite kritičnih točk

Definicija 4.1. *Naj bo* $f\colon \mathbb{F} \to \mathbb{F}$ *odvedljiv dinamični sistem. Točka* $x_0 \in \mathbb{F}$ *je* kritična točka*, če je*

$$f'(x_0) = 0.$$

Za $f_c(x) = x^2 + c$ je $f_c'(x) = 2x$, zato je $x_0 = 0$ edina kritična točka.

Izrek 4.1. *Naj bo* $f\colon \mathbb{C} \to \mathbb{C}$ *dinamični sistem s privlačno ali superprivlačno orbito. Tedaj ta orbita privlači vsaj eno kritično točko sistema* f*.*

Natančneje: če je $A = (x_j)_j$ privlačna orbita, obstaja kritična točka y, za katero

$$\lim_{k\to\infty} \operatorname{dist}\big(f^k(y), A\big) = 0 \qquad \text{in} \qquad \operatorname{dist}(z, A) = \min_{x\in A} |z - x|.$$

Posledica 4.1. *Kvadratni dinamični sistem* f_c *ima največ eno privlačno oziroma superprivlačno orbito.*

Posledica 4.1 nam pove, da lahko privlačne orbite kvadratnega sistema opišemo z orbito njegove kritične točke. Ker ima f_c le eno kritično točko, to je 0, diagram kritične orbite zazna vse privlačne režime kvadratne družine.

Za parameter c je orbita kritične točke 0 enaka

$$0 \longmapsto c \longmapsto c^2 + c \longmapsto (c^2 + c)^2 + c \longmapsto \cdots.$$

Za realni parameter c lahko iz teh orbit narišemo bifurkacijski diagram.

4.1 Kako diagram nastane

Za vsak izbrani parameter c začnemo v kritični točki $x_0 = 0$ in računamo

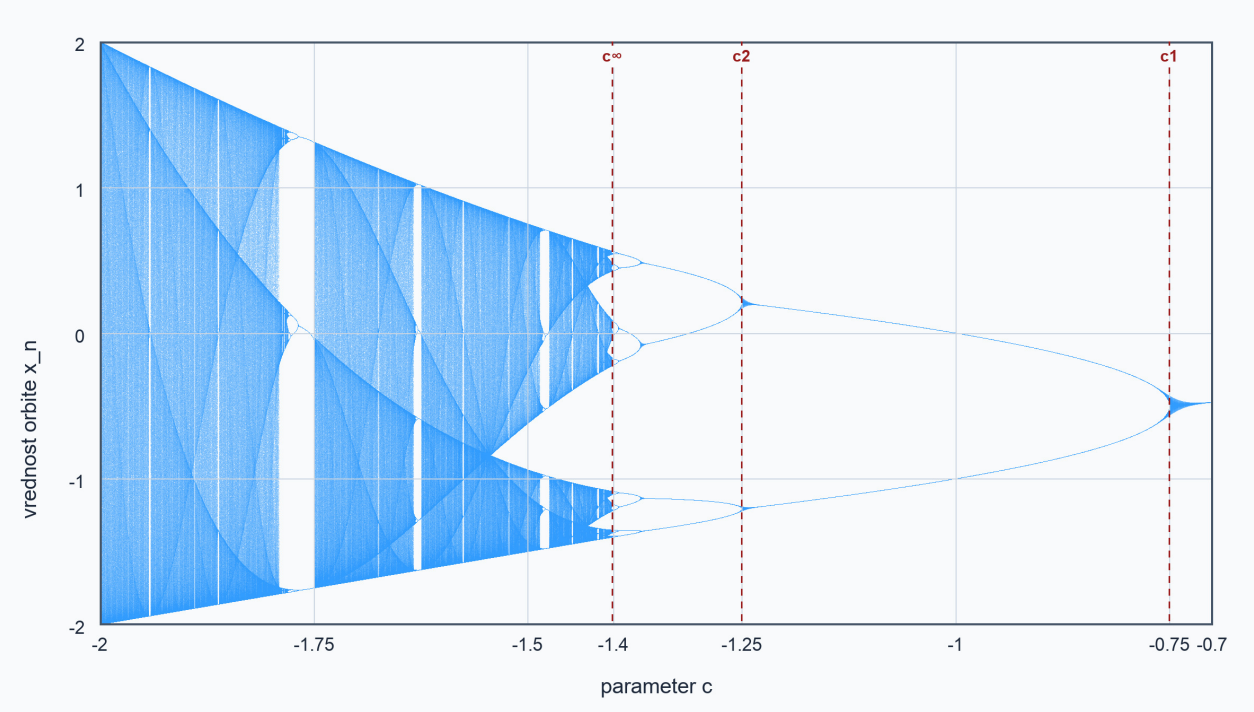
$$x_{n+1} = x_n^2 + c.$$

Prvih nekaj iteracij zavržemo, saj opisujejo le prehod do dolgoročnega obnašanja. Preostale vrednosti x_n narišemo v navpičnem stolpcu nad pripadajočim parametrom c. Postopek ponovimo za gosto mrežo parametrov. To je standardna konstrukcija bifurkacijskega diagrama.

Navpično rezino diagrama pri fiksnem c beremo takole:

- ena vidna vrednost pomeni, da kritična orbita konvergira k privlačni fiksni točki;
- dve, štiri oziroma osem vrednosti pomenijo privlačni cikel periode 2, 4 oziroma 8;

- širok pas mnogih vrednosti kaže na aperiodično, občutljivo oziroma kaotično dolgoročno obnašanje;
- tudi znotraj kaotičnega območja se pojavijo ozka *periodična okna*, v katerih zopet obstaja privlačni cikel.



Slika 7: Bifurkacijski diagram za $f_c(x) = x^2 + c$ na intervalu $-2 \leq c \leq -0{,}7$. Za vsakega od 4000 parametrov izvedemo 4000 iteracij kritične orbite, prvih 100 zavržemo, preostale pa narišemo. Črtkane navpičnice označujejo $c_1 = -3/4$, $c_2 = -5/4$ in akumulacijsko točko $c_\infty \approx -1{,}401155$.

4.2 Podvojitve periode

Pri $c_1 = -3/4$ privlačna fiksna točka izgubi privlačnost in nastane privlačni 2-cikel. Pri $c_2 = -5/4$ se njegova perioda ponovno podvoji in nastane privlačni 4-cikel. Nadaljnje podvojitve se vrstijo vedno hitreje:

$c_1 = -\frac{3}{4}$	prva podvojitev periode,
$c_2 = -\frac{5}{4}$	prehod iz 2-cikla v 4-cikel,
$c_3 \approx -1{,}36810$	prehod iz 4-cikla v 8-cikel,
$c_4 \approx -1{,}39405$	naslednja podvojitev periode,
$c_\infty \approx -1{,}401155$	Feigenbaumova točka oziroma meja kaskade.

Pri c_∞ se kaskada period $1, 2, 4, 8, \ldots$ zgosti. Neposredno onkraj nje se pojavijo kaotični režimi, prekinjeni s periodičnimi okni.

5 Kompleksna dinamika

5.1 Napolnjena Juliajeva množica

Oglejmo si kvadratni kompleksni dinamični sistem

$$f_c \colon \mathbb{C} \to \mathbb{C}, \qquad f_c(z) = z^2 + c, \qquad c \in \mathbb{C}.$$

Za začetno točko $z_0 \in \mathbb{C}$ iteriramo sistem. Orbita je bodisi omejena bodisi divergira oziroma »eksplodira«.

Trditev 5.1 (Radij pobega)**.** *Orbita točke z_0 divergira, če*

$$|z_0| > R_c := \max\{2, |c|\}.$$

Dokaz. Nastavimo

$$\lambda := |z_0| - 1 > 1.$$

Ker je $|z_0| > R_c$, velja tudi $|z_0| > |c|$. Iz obrnjene trikotniške neenakosti zato sledi

$$\begin{aligned} |z_1| &= |z_0^2 + c| \\ &\geq |z_0|^2 - |c| \\ &> |z_0|^2 - |z_0| = |z_0|(|z_0| - 1) = \lambda |z_0|. \end{aligned}$$

Posebej je $|z_1| > |z_0| > R_c$. Če je $|z_k| > |z_0|$, lahko enak razmislek uporabimo pri z_k in dobimo

$$\begin{aligned} |z_{k+1}| &\geq |z_k|^2 - |c| \\ &> |z_k|(|z_k| - 1) > \lambda |z_k|, \end{aligned}$$

saj je $|z_k| - 1 > |z_0| - 1 = \lambda$. Z indukcijo sledi

$$|z_n| > \lambda^n |z_0| \qquad \text{za vsak } n \geq 1.$$

Ker je $\lambda > 1$, zaporedje $\lambda^n |z_0|$ divergira proti neskončnosti, zato tudi $|z_n| \to \infty$. S tem je divergenca orbite zares dokazana. □

Če je $|z_0| \leq R_c$, orbita ni nujno omejena. Lahko šele po več iteracijah preseže R_c in nato pobegne.

Definicija 5.1 (Napolnjena Juliajeva množica)**.** Napolnjena Juliajeva množica *sistema f je*

$$FJ(f) := \{z \in \mathbb{C} : (f^n(z))_{n \geq 0} \textit{ je omejena orbita}\}.$$

Za kvadratni sistem velja $FJ(f_c) \subseteq \overline{B(0, R_c)}$.

5.1.1 Algoritem za risanje napolnjene Juliajeve množice

Napolnjeno Juliajevo množico numerično rišemo na naslednji način. Za izbrani parameter c izvedemo te korake.

1. V kompleksni ravnini izberemo pravokotno območje in ga razdelimo na mrežo pikslov. Vsak piksel predstavlja eno začetno točko z_0.
2. Izberemo največje število iteracij N in za vsako začetno točko računamo $z_{n+1} = z_n^2 + c$, dokler orbita ne preseže radija pobega $R_c = \max\{2, |c|\}$ ali dokler ne izvedemo vseh N iteracij.
3. Če orbita prvič pobegne pri koraku n, piksel pobarvamo glede na čas pobega n: hitreje pobegle točke dobijo drugačno barvo oziroma odtenek kakor počasneje pobegle točke.

4. Če po N korakih pobega ne zaznamo, piksel pobarvamo črno in začetno točko obravnavamo kot približen element $FJ(f_c)$.

Ker izvedemo le končno mnogo iteracij, je dobljena slika približek. Večji N praviloma izboljša predvsem prikaz točk blizu roba množice.

Juliajeve množice bomo narisali pozneje, ko bomo definirali tudi pojem Mandelbrotove množice (glej podrazdelek 6.2.2).

5.2 Primer $f_0(z) = z^2$

Označimo

$$\mathbb{D} = \{z \in \mathbb{C} : |z| < 1\}, \qquad \partial\mathbb{D} = \{z \in \mathbb{C} : |z| = 1\}, \qquad \overline{\mathbb{D}} = \mathbb{D} \cup \partial\mathbb{D}.$$

Če $z_0 \in \mathbb{D}$, je $|z_{n+1}| = |z_n|^2 < |z_n|$, zato $z_n \to 0$. Če $z_0 \notin \overline{\mathbb{D}}$, je $|z_0| > 1$ in orbita divergira. Če $z_0 \in \partial\mathbb{D}$, potem $|z_n| = 1$ za vsak n. Sledi

$$FJ(z^2) = \overline{\mathbb{D}}.$$

Poznamo tri tipe dinamike:

1. $z_0 \notin \overline{\mathbb{D}}$: orbita divergira v neskončnost;
2. $z_0 \in \mathbb{D}$: orbita konvergira k 0;
3. $z_0 \in \partial\mathbb{D}$: orbita ostane na krožnici in kaže občutljivo obnašanje.

5.2.1 Dinamika na robu krožnice

Za dinamiko na $\partial\mathbb{D}$ so ključne naslednje tri lastnosti.

1. Krožnica je invariantna: če je $|z_0| = 1$, potem je $|z_n| = 1$ za vsak n, zato orbita nikoli ne zapusti roba.
2. Vse odbojne periodične orbite funkcije z^2 ležijo na $\partial\mathbb{D}$, njihove točke pa so gosta podmnožica krožnice. Res, če ima točka periodo m, potem je

   $$\left|(f_0^m)'(z)\right| = 2^m > 1,$$

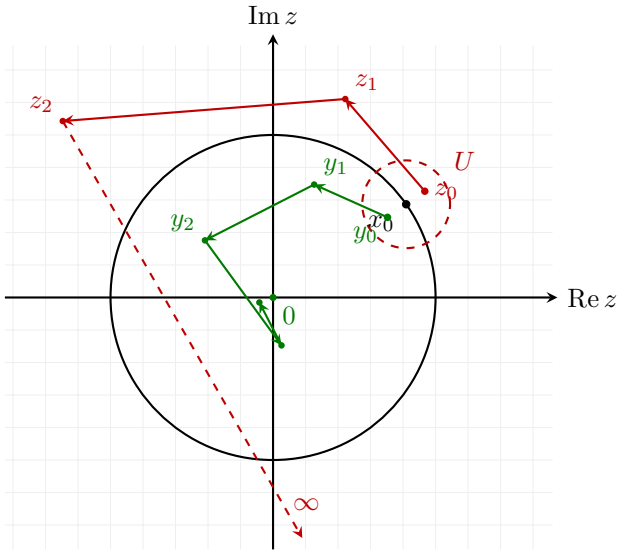
   zato je takšna periodična točka odbojna.
3. V vsaki okolici katerekoli točke roba sta točki z izjemno različnima dinamikama: orbita ene konvergira k 0, orbita druge pa pobegne v neskončnost.

Natančneje, naj bo $x_0 \in \partial\mathbb{D}$ in naj bo U poljubna njegova okolica. Za dovolj majhen $\varepsilon > 0$ sta v U tudi točki

$$y_0 = (1-\varepsilon)x_0 \in \mathbb{D}, \qquad z_0 = (1+\varepsilon)x_0 \notin \overline{\mathbb{D}}.$$

Njuni orbiti zadoščata

$$|f_0^n(y_0)| = (1-\varepsilon)^{2^n} \longrightarrow 0 \qquad \text{in} \qquad |f_0^n(z_0)| = (1+\varepsilon)^{2^n} \longrightarrow \infty.$$



Slika 8: V vsaki okolici U točke $x_0 \in \partial\mathbb{D}$ lahko izberemo $y_0 \in \mathbb{D}$ in $z_0 \notin \overline{\mathbb{D}}$. Zelena orbita konvergira k 0, rdeča pa pobegne v neskončnost.

5.3 Juliajeva množica in kaos

Definicija 5.2. *Naj bo $f\colon \mathbb{C} \to \mathbb{C}$ polinomski dinamični sistem,*

$$f(z) = a_m z^m + a_{m-1} z^{m-1} + \cdots + a_1 z + a_0.$$

Juliajeva množica *je rob napolnjene Juliajeve množice:*

$$J(f) := \partial F J(f).$$

Pri $f_0(z) = z^2$ je $J(f_0) = \partial\mathbb{D}$, krožnica. V splošnem je Juliajeva množica mnogo bolj zapletena in pogosto fraktalna. Na njej ima dinamika kaotičen značaj.

Za polinom f stopnje vsaj 2 dinamika na $J(f)$ zadošča podobnim lastnostim kakor dinamika preslikave z^2 na $J(z^2) = \partial\mathbb{D}$. Dinamiki z začetnimi točkami na $J(f)$ zato pravimo *kaotična*.

Prvi praktični indikator kaosa dobimo iz analogije s točko 3 razdelka 5.2.1. Tudi na splošni Juliajevi množici je dinamika občutljiva na začetne pogoje. To pomeni, da lahko poljubno bližnji začetni točki po dovolj iteracijah razvijeta zelo različni orbiti. V praksi je takšna občutljivost eden izmed prvih indikatorjev, s katerimi preverjamo, ali je opazovana dinamika kaotična.

5.4 Topološki opis s pomočjo kritične orbite

Izrek 5.1. *Fiksirajmo $c \in \mathbb{C}$ in naj bo $f_c(z) = z^2 + c$.*

1. *Če je kritična orbita $(f_c^n(0))_n$ omejena, sta $J(f_c)$ in $FJ(f_c)$ povezani množici.*
2. *Če je kritična orbita neomejena, je $J(f_c)$ enaka Cantorjevi množici.*[1]

Cantorjevo množico konstruiramo tako, da iz intervala $[0,1]$ odstranimo srednjo tretjino, nato srednji tretjini obeh preostalih intervalov in tako naprej:

$$C_0 = [0,1], \qquad C_1 = \left[0, \frac{1}{3}\right] \cup \left[\frac{2}{3}, 1\right], \qquad C_2 = \left[0, \frac{1}{9}\right] \cup \left[\frac{2}{9}, \frac{1}{3}\right] \cup \left[\frac{2}{3}, \frac{7}{9}\right] \cup \left[\frac{8}{9}, 1\right],$$

[1] Topološko natančneje množici nista nujno enaki, temveč sta homeomorfni.

in v splošnem

$$C = \bigcap_{n=0}^{\infty} C_n.$$

Cantorjeva množica je neprazna, popolnoma nepovezana in kompaktna.

6 Mandelbrotova množica

Mandelbrotova množica izraža temeljno odvisnost med Juliajevimi množicami in parametrom c.

Definicija 6.1. Mandelbrotova množica *je*

$$\mathcal{M} := \{c \in \mathbb{C} : (f_c^n(0))_{n\geq 0} \textit{ je omejena}\} = \{c \in \mathbb{C} : J(f_c) \textit{ je povezana}\}.$$

Druga enakost v definiciji je posledica izreka 5.1.

6.1 Algoritem za risanje Mandelbrotove množice

Mandelbrotovo množico numerično rišemo na naslednji način.

1. V ravnini parametrov izberemo pravokotno območje in ga razdelimo na mrežo pikslov. Vsak piksel predstavlja eno vrednost parametra c.
2. Izberemo največje število iteracij N. Za vsak parameter c začnemo v kritični točki $z_0 = 0$ in računamo
$$z_{n+1} = z_n^2 + c,$$
dokler ne dobimo $|z_n| > 2$ ali dokler ne izvedemo vseh N iteracij.
3. Če orbita prvič preseže radij 2 pri koraku n, piksel pobarvamo glede na čas pobega n: hitro pobegle parametre prikažemo z drugačno barvo oziroma odtenkom kakor počasneje pobegle parametre.
4. Če po N iteracijah pobega ne zaznamo, piksel pobarvamo črno in parameter c obravnavamo kot približno točko množice $\mathcal{M}$.

Ker izvedemo le končno mnogo iteracij, je dobljena slika približek. Pomembna je tudi razlika med obema algoritmoma: pri risanju Juliajeve množice fiksiramo c in spreminjamo začetno točko z_0, pri risanju Mandelbrotove množice pa spreminjamo parameter c in vedno začnemo v kritični točki $z_0 = 0$.

Iz algoritma je razvidno, da je $\mathcal{M} \subseteq \overline{B(0,2)}$. Množica $\mathcal{M}$ je zaprta in zato kompaktna, poleg tega pa tudi povezana. Vsaki točki $c \in \mathcal{M}$ pripada povezana Juliajeva množica, medtem ko imajo parametri zunaj $\mathcal{M}$ nepovezane Juliajeve množice.

6.2 Vizualizacija Mandelbrotove množice

Pri običajni vizualizaciji notranjost Mandelbrotove množice pobarvamo črno. Točke zunaj nje pobarvamo glede na čas pobega kritične orbite: različni odtenki zato ne predstavljajo različnih delov množice $\mathcal{M}$, temveč hitrost, s katero pripadajoče orbite pobegnejo v neskončnost. Takšno barvanje posebej dobro poudari zapletenost roba.

6.2.1 Fraktalna struktura in majhne kopije

Mandelbrotova množica je fraktalna: ob povečevanju njenega roba se vedno znova pojavljajo nove podrobnosti. Med njimi so tudi majhne kopije celotne Mandelbrotove množice. Te kopije niso zgolj grafični učinek ločljivosti, saj se ob nadaljnjem povečevanju okoli njih ponovno pojavijo kardioida[2], krožne komponente in razvejene strukture roba.

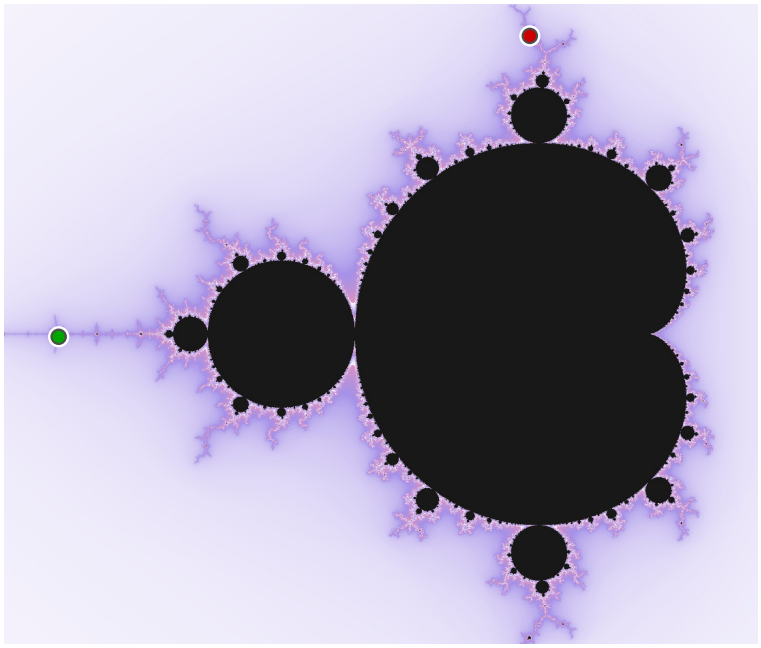
Najprej si oglejmo celotno Mandelbrotovo množico na sliki 9. Zelena točka označuje realni parameter

$$c_* \approx -1{,}754877666,$$

v okolici katerega se nahaja prva manjša kopija množice. Rdeča točka označuje parameter

$$c_{**} \approx -0{,}171021 + 1{,}024347i,$$

v okolici katerega bomo opazovali drugo manjšo kopijo.

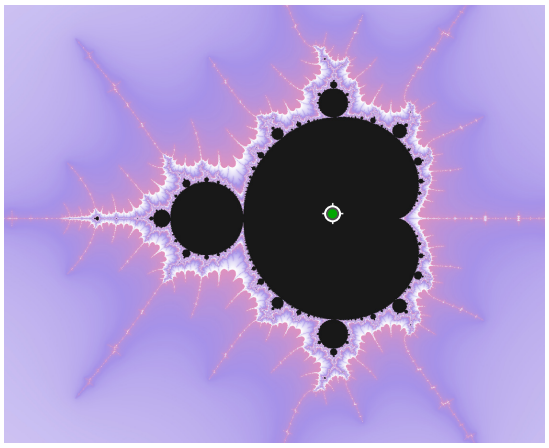


Slika 9: Pregled celotne Mandelbrotove množice. Zelena točka označuje lokacijo prve povečave, rdeča pa lokacijo druge povečave.

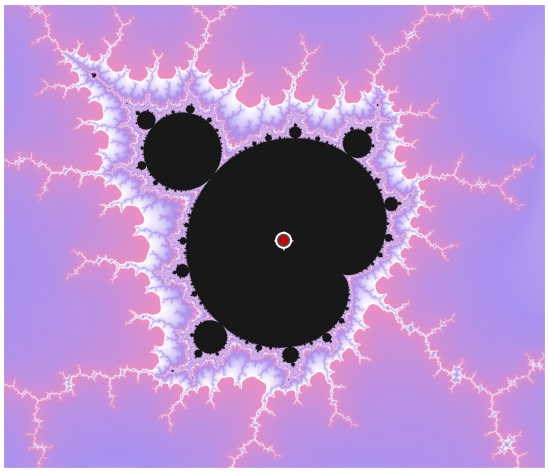
Povečava označenega območja je prikazana na sliki 10. V njej prepoznamo isto osnovno obliko z glavno kardioido in pripetimi komponentami, ob robu pa se pojavijo nove podrobnosti.

Drugi primer manjše kopije dobimo s povečevanjem okolice rdeče točke na sliki 9. Rezultat je prikazan na sliki 11. Ponovno se pojavi Mandelbrotovi množici podobna oblika, obdana z novimi, še drobnejšimi strukturami. Takšno ponavljanje na vedno manjših merilih je značilna lastnost fraktalne geometrije. Podobnost ni povsem geometrijsko natančna, saj vsako merilo prinese tudi drugače razporejene podrobnosti.

[2] Ime kardioida izhaja iz grških besed *kardía* (srce) in *eîdos* (oblika), saj je krivulja srčaste oblike.



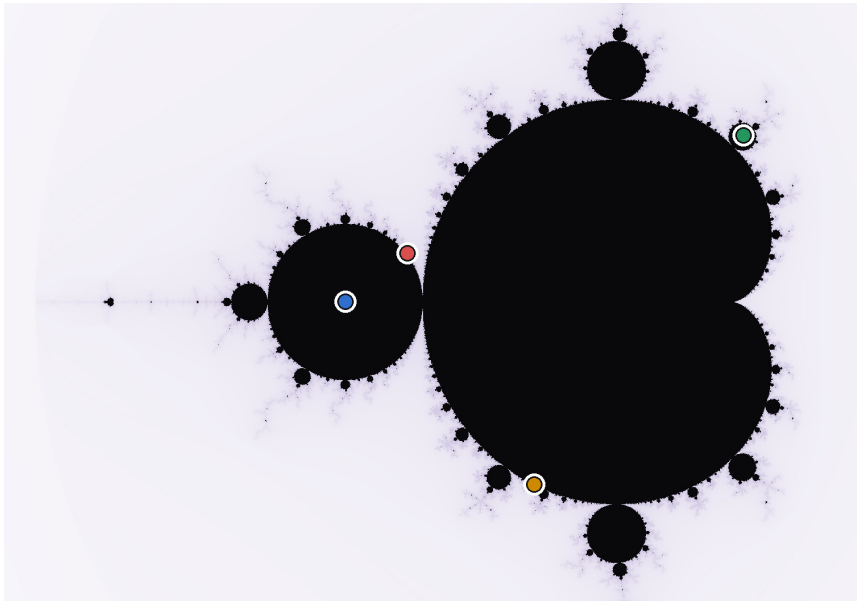
Slika 10: Prva manjša kopija Mandelbrotove množice pri $c_* \approx -1{,}754877666$.



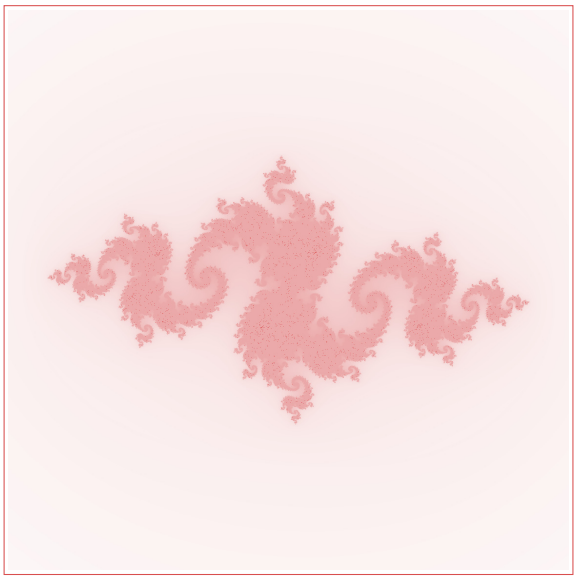
Slika 11: Povečava okolice rdeče točke s slike 9, v kateri se pokaže nova manjša kopija Mandelbrotove množice.

6.2.2 Izbrani primeri Juliajevih množic

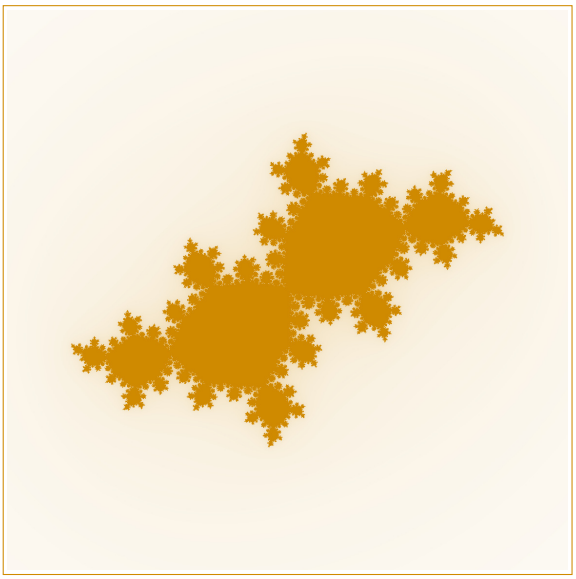
Vsak parameter $c \in \mathbb{C}$ določa svoj kvadratni dinamični sistem $f_c(z) = z^2 + c$ in s tem svojo Juliajevo množico. Na sliki 12 so na Mandelbrotovi množici označeni štirje parametri iz programa. Za lažje povezovanje ima vsak parameter svojo barvo. Z isto barvo je na sliki 13 pobarvana pripadajoča napolnjena Juliajeva množica. Juliajeva množica sama je rob pobarvanega območja.



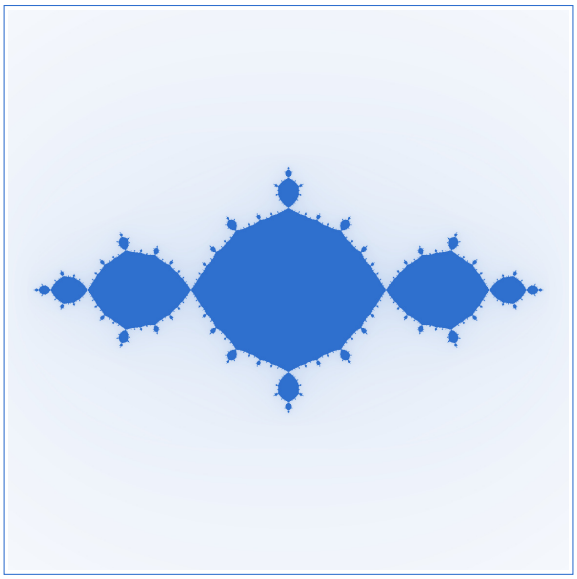
Slika 12: Štirje izbrani parametri v ravnini Mandelbrotove množice. Barva posamezne točke se ujema z barvo pripadajoče Juliajeve množice na naslednji sliki.



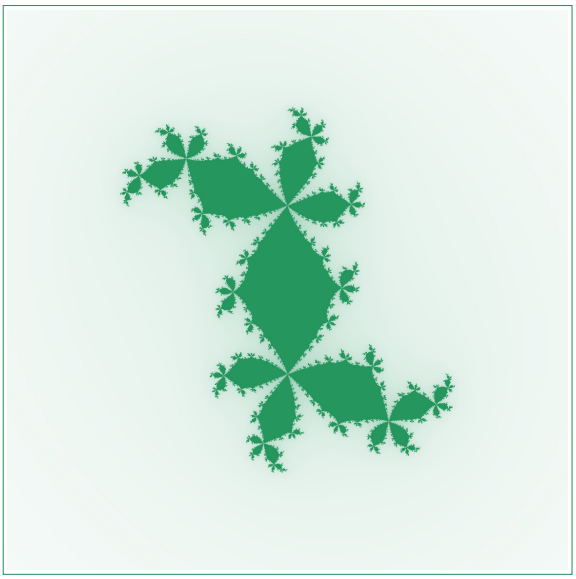
Spirala
$c = -0{,}8 + 0{,}156i$



Zlati Sieglov disk
$c \approx -0{,}391 - 0{,}587i$



Bazilika
$c = -1$

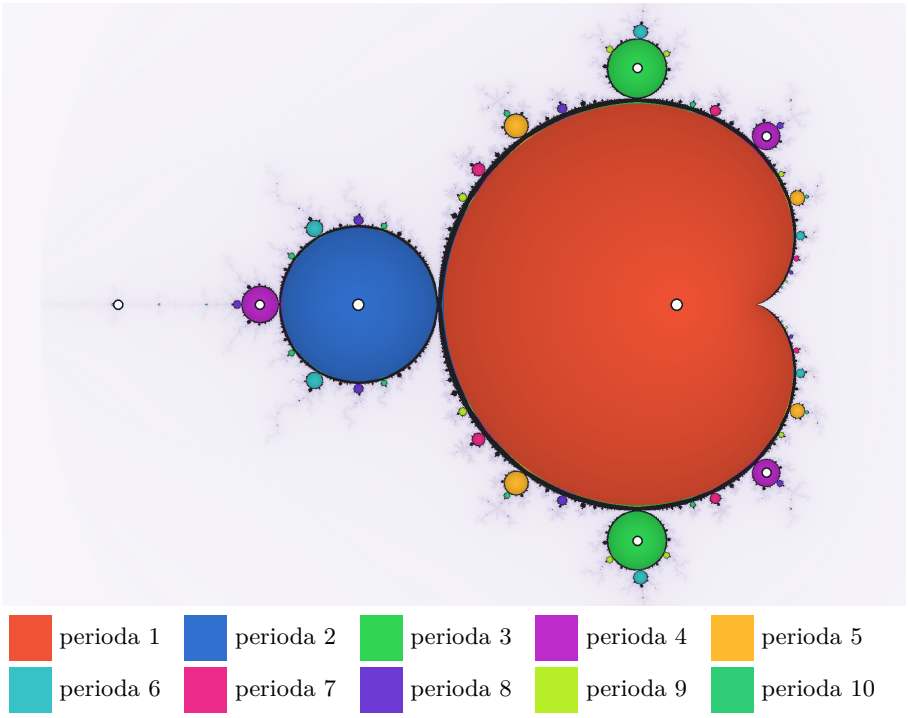


Fatoujev prah
$c = 0{,}285 + 0{,}535i$

Slika 13: Štiri napolnjene Juliajeve množice. Barve ustrezajo označenim parametrom na sliki 12.

6.3 Komponente Mandelbrotove množice

Notranjost Mandelbrotove množice razpade na povezana območja, ki jim pravimo *hiperbolične komponente*. V vsaki taki komponenti ima sistem $f_c(z) = z^2 + c$ privlačen periodični cikel, njegova perioda pa je po vsej komponenti enaka. Zato lahko komponente pobarvamo glede na periodo njihovega privlačnega cikla, kakor je prikazano na sliki 14.



Slika 14: Mandelbrotova množica s komponentami, pobarvanimi glede na periodo privlačnega cikla. Rdeča glavna kardioida ustreza periodi 1, modra komponenta periodi 2, zelene komponente periodi 3 in tako naprej. Bele točke s temnim robom označujejo izbrana superprivlačna središča komponent.

Rdeča glavna komponenta je kardioida. V njej so natanko tisti parametri, pri katerih ima f_c privlačno fiksno točko, torej privlačen cikel periode 1. Velika modra komponenta na levi vsebuje parametre s privlačnim 2-ciklom. Manjše zelene, vijolične, rumene in druge komponente ustrezajo višjim periodam. Črna oziroma nepobarvana območja na robu pomenijo, da pri uporabljeni ločljivosti in številu iteracij perioda ni bila zanesljivo prepoznana. Ta območja ne predstavljajo nove vrste dinamike.

Vsaka hiperbolična komponenta je konformno izomorfna odprtemu enotskemu disku $\mathbb{D}$, zato je zlasti topološko disk. To ne pomeni, da je njena podoba v ravnini parametra c nujno evklidski krog. Kot bomo dokazali v podrazdelku 6.3.1, je glavna komponenta natančna kardioida, komponenta periode 2 pa je natančen evklidski disk $B(-1, \frac{1}{4})$. Druge komponente so na sliki pogosto videti krožne ali kardioidne, vendar imajo lahko geometrijsko bolj zapletene meje. Vsaka ima enolično določeno središče.

6.3.1 Glavna kardioida in komponenta periode 2

Glavno kardioido sestavljajo parametri c, za katere ima f_c privlačno fiksno točko. Naj bo z taka točka. Rešujemo

$$z^2 + c = z, \qquad |f_c'(z)| = |2z| < 1.$$

Pišemo množitelj kot

$$2z = re^{i2\pi t}, \qquad 0 \le r < 1, \quad t \in [0, 1),$$

zato je

$$z = \frac{1}{2} re^{i2\pi t}$$

in

$$c = z - z^2 = \frac{1}{2} re^{i2\pi t} \left(1 - \frac{1}{2} re^{i2\pi t}\right).$$

Ta parametrična enačba opisuje glavno kardioido.

Na glavno kardioido so pripete komponente višjih period. Za komponento periode 2 rešujemo

$$f_c^2(z) = z, \qquad |(f_c^2)'(z)| < 1.$$

Simbolično dobimo krog s središčem v -1 in polmerom $1/4$:

$$c(t, r) = -1 + \frac{1}{4} r e^{i2\pi t}, \qquad 0 \leq r < 1, \quad t \in [0, 1).$$

6.3.2 Središča komponent in superprivlačni cikli

Središče hiperbolične komponente je natanko parameter, pri katerem privlačni cikel postane *superprivlačen*. Za kvadratni polinom je edina kritična točka 0. V središču komponente periode n je ta točka na periodičnem ciklu, zato velja

$$f_c^n(0) = 0.$$

Ta enačba nam omogoča poiskati središča komponent. Središče glavne kardioide je $c = 0$, središče modre komponente periode 2 pa je $c = -1$. Enako določimo tudi središča komponent višjih period. Bele točke na sliki 14 označujejo nekaj takih superprivlačnih središč.

Literatura

[1] Mark McClure, *Complex Dynamics*, spletni učbenik in zapiski predmeta, pomlad 2019. Dostopno na: `https://legacy.marksmath.org/classes/Spring2019ComplexDynamics/text/contents.html` (dostopano 16. avgusta 2026).

PREDAVANJA

Ojačano pronicanje v kvadratnih mrežah

Dr. Jaka Hedžet

Fakulteta za naravoslovje in matematiko, Univerza v Mariboru

1 Uvod

Ojačano pronicanje je proces, pri katerem se informacija oziroma določena lastnost postopoma širi po mreži ali grafu. V obravnavanem problemu si predstavljamo šahovnico, katere posamezna polja so pobarvana črno ali belo. Določena polja na začetku pobarvamo črno, nato pa se barva po vnaprej določenem pravilu širi na preostala polja. Osnovno vprašanje je, koliko črnih polj moramo izbrati na začetku, da bo po končanem procesu celotna šahovnica pobarvana črno.

Naloga: Naj bo dana kvadratna šahovnica velikosti $n \times n$. Belo polje se pobarva črno, če ima vsaj dve črni sosedi. Označimo s $p(n)$ najmanjše število začetno črnih polj, ki zagotavljajo, da bo na koncu celotna šahovnica črna. Za določitev natančne vrednosti parametra $p(n)$ moramo dokazati dve neenakosti:

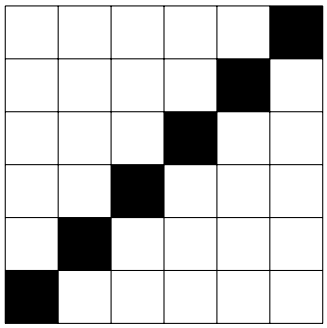
$$p(n) \leq k \qquad \text{in} \qquad p(n) \geq k.$$

Prva zahteva konstrukcijo, ki pokaže, da je k polj dovolj, druga pa dokaz, da z manj kot k polji procesa ni mogoče uspešno zaključiti.

2 Osnovni problem na kvadratni mreži

Za zgornjo mejo lahko uporabimo diagonalno konstrukcijo (slika 1). Za šahovnico velikosti $n \times n$ izberemo vsa polja na eni od diagonal. Tako dobimo n začetno črnih polj. Zaradi izbranega pravila se nato črnina postopoma širi po šahovnici. Enak princip lahko uporabimo za poljubno naravno število n, zato dobimo

$$p(n) \leq n.$$



Slika 1: Diagonalna konstrukcija.

Da bi pokazali, da je ta zgornja meja tudi optimalna, potrebujemo spodnjo mejo. Pri tem uporabimo geometrijski argument, ki temelji na obsegu črnega območja. Označimo obseg črnega območja z o. Ko se belo polje pobarva črno, ima že vsaj dve črni sosedi. Zaradi tega dodajanje novega polja ne poveča skupnega obsega črnega območja. Obseg se lahko ohrani ali zmanjša, nikoli pa se v procesu ne poveča. To pomeni, da mora začetni obseg biti vsaj tolikšen, kot je končni.

Na koncu procesa je črna celotna šahovnica. Njen obseg je

$$o = 4n.$$

Na začetku lahko vsako posamezno črno polje prispeva največ štiri enote k skupnemu obsegu. Če je začetno število črnih polj enako k, je zato začetni obseg največ $4k$. Ker se obseg med procesom ne more povečati, mora veljati

$$4k \geq 4n.$$

Od tod sledi

$$k \geq n,$$

oziroma

$$p(n) \geq n.$$

Skupaj z zgornjo mejo tako dobimo pomemben rezultat

$$\boxed{p(n) = n}.$$

To pomeni, da je za popolno pronicanje na kvadratni šahovnici velikosti $n \times n$ potrebnih natanko n začetno črnih polj.

3 Pravokotne mreže

Naravna nadgradnja osnovnega problema je, da namesto kvadratne mreže opazujemo pravokotno šahovnico velikosti $m \times n$. Označimo najmanjše potrebno število začetno črnih polj s $p(m, n)$ in predpostavimo, da je $m > n$.

Tudi v tem primeru lahko dobimo zgornjo mejo s konstrukcijo, ki temelji na diagonali. Na začetku izberemo n polj na diagonali. V preostalih $m - n$ stolpcih nato izberemo po eno črno polje iz vsakega drugega stolpca. če je $m - n$ sodo število, se konstrukcija lepo zaključi. če je $m - n$ liho, ostane en stolpec, v katerem moramo dodati še eno začetno črno polje. Tako dobimo

$$p(m, n) \leq n + \left\lceil \frac{m-n}{2} \right\rceil = \left\lceil \frac{m+n}{2} \right\rceil.$$

Za spodnjo mejo ponovno uporabimo argument z obsegom. Obseg celotne pravokotne šahovnice je

$$o = 2m + 2n.$$

Ker se obseg med procesom ne more povečati in lahko vsako začetno črno polje prispeva največ štiri enote k obsegu, mora biti začetno število črnih polj vsaj

$$\left\lceil \frac{2m+2n}{4} \right\rceil = \left\lceil \frac{m+n}{2} \right\rceil.$$

Zato dobimo

$$p(m, n) \geq \left\lceil \frac{m+n}{2} \right\rceil.$$

Kombinacija zgornje in spodnje meje vodi do rezultata

$$\boxed{p(m, n) = \left\lceil \frac{m+n}{2} \right\rceil.}$$

4 Sprememba pravila pronicanja

Nadalje lahko spremenimo osnovno pravilo. Namesto da se belo polje pobarva že takrat, ko ima vsaj dve črni sosedi, zahtevamo, da ima tri ali celo štiri črne sosede. Takšna sprememba bistveno oteži proces pronicanja, saj mora biti za spremembo barve izpolnjen strožji pogoj.

Pri pravilu s štirimi sosedi lahko iz začetne konfiguracije izpeljemo različne omejitve. Pri strožjih pravilih je pomembno, da začetna konfiguracija ne vsebuje določenih struktur belih polj. Pri pravilu s tremi črnimi sosedi lahko na primer opazimo naslednje pogoje:

- noben stolpec ne sme biti v celoti bel,
- na robu ne smeta biti dve zaporedni beli polji,
- če polja skupaj tvorijo pravokotnik, ne smejo biti vsa bela.

Problem lahko ponovno obravnavamo tako na kvadratnih kot na pravokotnih šahovnicah. Nov parameter označimo s $P(m, n)$. V nasprotju z osnovnim primerom problem v splošnem še ni rešen. Znani so posamezni delni rezultati, med drugim za mreže velikosti $3 \times m$ in $5 \times m$.

5 Imuna vozlišča

Naslednja nadgradnja problema je uvedba imunih polj. Imuno polje je takšno polje, ki se ne glede na število črnih sosed nikoli ne pobarva črno. Takšna polja predstavljajo dodatno oviro za širjenje procesa.

Prisotnost imunih polj lahko povzroči, da moramo na začetku izbrati več črnih polj kot v osnovnem problemu. Po drugi strani pa lahko pri ustrezni izbiri imunih polj začetna konfiguracija ostane dovolj učinkovita in dodatnih začetno črnih polj sploh ne potrebujemo.

Zato parameter ni več odvisen samo od velikosti mreže, temveč tudi od izbire imunih vozlišč. Zanimata nas lahko dve nasprotni situaciji: kako izbrati imuna vozlišča tako, da se vrednost parametra čim bolj poveča, ali pa tako, da ostane čim bližje prvotni vrednosti.

Tudi tukaj lahko uporabimo argument z obsegom. Če se na primer zaradi imunega polja spremeni končni obseg črnega območja, moramo primerjati začetni in končni obseg. Ustrezna izbira imunega polja lahko povzroči, da se obseg poveča. Ker notranje polje lahko poveča obseg za štiri enote, je v določenih konfiguracijah potrebno eno dodatno začetno črno polje. Če imamo k imunih vozlišč, pri čemer k ni prevelik, lahko tako dobimo spodnjo mejo oblike

$$p(n) \geq n + k.$$

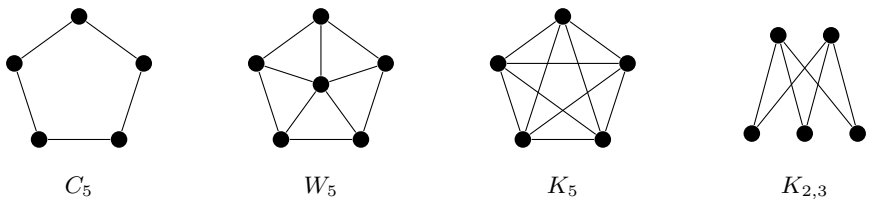
6 Povezava s teorijo grafov

Problem šahovnice lahko naravno prevedemo v jezik teorije grafov. Polja šahovnice predstavljajo vozlišča grafa, sosednja polja pa povežemo z ustreznimi povezavami. Proces barvanja tako postane proces na grafu.

V teoriji grafov se obravnavani proces imenuje r-sosedno ojačano pronicanje. Pri tem barvamo vozlišča grafa G s črno barvo, belo vozlišče pa se pobarva, če ima vsaj r črnih sosedov. Najmanjše število začetno črnih vozlišč, ki zagotavljajo, da bo na koncu celoten graf črn, označimo z

$$m(G, r).$$

Takšna formulacija omogoča, da problem posplošimo daleč preko kvadratnih mrež. Namesto šahovnic lahko obravnavamo različne družine grafov in poskušamo določiti njihove vrednosti $m(G, r)$. Naravni primeri so cikli, kolesa, polni grafi in polni dvodelni grafi.



Slika 2: Primeri grafov. Po vrsti si sledijo cikel, kolo, polni graf, polni dvodelni graf.

7 Zaključek

Ojačano pronicanje v kvadratnih mrežah je preprost problem za formulacijo, vendar omogoča številne zanimive matematične nadgradnje. Osnovni primer na šahovnici pokaže pomembno povezavo med konstrukcijskimi argumenti in invariantami. Z diagonalno konstrukcijo dobimo zgornjo mejo, medtem ko argument z obsegom zagotovi ustrezno spodnjo mejo. Na ta način dobimo natančen rezultat $p(n) = n$.

Nadaljnje spremembe problema, kot so pravokotne mreže, strožja pravila pronicanja in imuna vozlišča, odpirajo zahtevnejša vprašanja. Posebej zanimiv je prehod iz mrež v splošne grafe, kjer proces opišemo s parametrom $m(G, r)$. Tako se problem poveže s širšim področjem teorije grafov in postane mogoče raziskovati njegovo obnašanje na različnih družinah grafov.

Zavarovalnice in upravljanje tveganj

Urban Merhar

Sava Re

Zakaj se zavarujemo? Ker življenje prinaša negotovosti. Nesreče, bolezni, naravne ujme in drugi nepričakovani dogodki imajo lahko velike finančne posledice za posameznika, družino ali podjetje. Osnovna ideja zavarovanja je zato preprosta, a izjemno pomembna: tveganje, ki bi ga posameznik težko nosil sam, se prenese na širšo skupnost. S plačilom premije posameznik pridobi večjo finančno varnost, zavarovalnica pa prevzame odgovornost za izplačilo škode ob nastanku zavarovalnega primera.

Zavarovalništvo ima zelo dolge korenine. Že v zgodovini so se ljudje organizirali tako, da so posledice nesreč delili med širšo skupnost. Prve zgodovinsko dokumentirane zametke najdemo v Hamurabijevem zakoniku, ki je datiran okoli leta 1750 pr. n. št. Značilen primer iz zgodovine so trgovske karavane, kjer je škodo ob ropih nosila celotna karavana. Kitajski trgovci so na primer blago razporejali na več čolnov, da izguba enega čolna ne bi pomenila izgube vsega blaga. Podobno so delitev tveganj razumeli tudi v antični Grčiji, kjer sta ladjar in trgovec skupaj poravnala škodo, nastalo med plovbo. V vseh teh primerih prepoznamo isto načelo: solidarnost in razpršitev tveganja.

V sodobnem zavarovalništvu se ta ideja izraža skozi pogodbeni odnos med zavarovancem in zavarovalnico. Zavarovanec plača premijo, zavarovalnica pa ob dogovorjenem škodnem dogodku izplača zavarovalnino oziroma vzpostavi stanje pred škodo. Za zavarovanca to pomeni manjšo negotovost: namesto možnosti velike in nepredvidljive finančne izgube plača vnaprej znan strošek. Zavarovalnici pa veliko število podobnih tveganj omogoča, da škode ocenjuje statistično. Tako velike koeficiente variacije za posamezne zavarovance zamenja z majhnim koeficientom variacije za portfelj zavarovanj.

Posebno mesto v zavarovalniškem sistemu ima pozavarovanje. Če je zavarovalnica zaščita za posameznike in podjetja, je pozavarovalnica, poenostavljeno povedano, zavarovalnica za zavarovalnice. Njena vloga pride do izraza predvsem pri zelo velikih posameznih tveganjih ali katastrofalnih dogodkih, ko bi lahko ena večja škoda oziroma večje število majhnih škod povzročilo celo propad zavarovalnice. Pozavarovanje zavarovalnicam omogoča, da del presežnih tveganj prenesejo naprej, s tem pa varujejo svojo kapitalsko stabilnost in sposobnost izpolnjevanja obveznosti do zavarovancev.

Pri tem ima ključno vlogo upravljanje tveganj. Tveganje lahko razumemo kot vpliv negotovosti na cilje. V zavarovalništvu to pomeni možnost, da se dejanski prihodnji dogodki razlikujejo od pričakovanih in povzročijo finančno izgubo ali neugodno spremembo finančnega položaja družbe. Upravljanje tveganj zato ni zgolj kontrolna funkcija, temveč sistematičen proces prepoznavanja, merjenja, spremljanja in obvladovanja tveganj ter poročanja o njih.

V okviru evropske ureditve Solventnost II je finančna stabilnost zavarovalnic urejena skozi tri stebre. Prvi steber zajema kvantitativne kapitalske zahteve, kot so lastna sredstva, zahtevani solventnostni kapital in solventnostni količnik. Drugi steber poudarja kakovost sistema upravljanja, notranjih kontrol in lastne ocene tveganj ter solventnost. Tretji steber pa se nanaša na poročanje in razkritja, ki povečujejo preglednost poslovanja za nadzornike, trg in javnost.

Za dolgoročno finančno varnost zavarovalnice je posebej pomemben solventnostni količnik, ki kaže razmerje med razpoložljivimi lastnimi sredstvi in zahtevanim solventnostnim kapitalom. Gre za enega ključnih kazalnikov tega, ali ima družba dovolj kapitala za absorbiranje nepričakovanih izgub, izpolnjevanje obveznosti do zavarovancev in stabilno poslovanje tudi v neugodnih razmerah.

Upravljanje tveganj v zavarovalnici poteka na več ravneh. V proces so vključeni vsi zaposleni, saj se tveganja pojavljajo v vsakodnevnem poslovanju, produktih, naložbah, procesih, sistemih in strateških odločitvah.

Zavarovalnice se srečujejo z različnimi tveganji: zavarovalnimi, tržnimi, kreditnimi, likvidnostnimi, operativnimi in strateškimi. Vse pomembnejša postajajo tudi novonastajajoča tveganja, kot so kibernetska tveganja, geopolitična nestabilnost, tveganja, povezana z umetno inteligenco, ter trajnostna in podnebna tveganja. Prav razumevanje teh tveganj je ključno za odgovorno odločanje in dolgoročno odpornost zavarovalniškega sistema.

Pomemben primer takšnega sistema v regiji je Zavarovalna skupina Sava, katere matična družba je Sava Re. Skupina deluje na področju pozavarovanja, zavarovanja, pokojnin, upravljanja premoženja, asistenčnih storitev in drugih dopolnilnih dejavnosti. S svojo prisotnostjo v več državah regije, razvejano ponudbo ter poudarkom na stabilnosti, odgovornosti in trajnostnem razvoju predstavlja pomemben del zavarovalniškega okolja v Sloveniji in širši regiji Adria.

Če želite o zavarovalništvu in upravljanju tveganj izvedeti še več, vam predlagam, da na spletnih straneh Zavarovalne skupine Sava poiščete poročilo o solventnosti in finančnem položaju, v katerem je predstavljeno vse o sistemu upravljanja tveganj v Zavarovalni skupini Sava in še več.

Zavarovalništvo ni le prodajanje zavarovalnih polic, temveč sistem ustvarjanja gospodarske varnosti. Temelji na solidarnosti, statistiki, kapitalu, zaupanju in odgovornem upravljanju tveganj. V svetu, kjer so negotovosti vse večje in kompleksnejše, postaja sposobnost prepoznavanja, razumevanja in obvladovanja tveganj ena ključnih kompetenc tako za posameznike kot organizacije.

Najnujnejše o testih praštevilskosti

Dr. Aleksander Simonič

Fakulteta za matematiko, naravoslovje in informacijske tehnologije, Univerza na Primorskem

1 Uvod

Vsi poznamo pojem *praštevila*: to je tako naravno število $n \geq 2$, ki ima natanko dva pozitivna delitelja, 1 in n. Vsi tudi znamo našteti nekaj prvih praštevil, poleg tega pa sta iz osnovne šole zagotovo marsikomu v spominu ostali dve lastnosti: praštevil je neskončno mnogo in vsako naravno število $n \geq 2$ se da zapisati kot produkt potenc praštevil. Toda, kako *vemo*, ali je neko *veliko* število res praštevilo? Morda se komu zdi raziskovanje v tej smeri preveč "neuporabno" ali celo trivialno, toda temu ni tako. Javni ključi *RSA kriptografskega sistema* [12, Poglavje 6], ki je priljubljen za šifriranje kratkih sporočil in digitalno podpisovanje, so dobljeni kot produkt dveh 1024-bitnih praštevil. Kako bi v *doglednem času* našli tako velika praštevila? Če že ne moremo povedati z gotovostjo, ali lahko vsaj z neko verjetnostjo trdimo, da smo v naključnem iskanju po neki podmnožici naravnih števil res našli praštevilo? Na predavanju smo se podrobneje seznanili z algoritmom, ki reši slednje vprašanje.

2 Naivni pristop

Kako smo v šoli določili, ali je dano naravno število praštevilo? Postopek je bil morda tak: preverimo, ali katero od števil $d \in \{2, \ldots, \lfloor\sqrt{n}\rfloor\}$ deli $n \geq 4$. Če tak delitelj obstaja, potem je n sestavljeno število, drugače pa je n praštevilo. V najslabšem primeru, ko je n praštevilo, bomo s tem postopkom opravili $\lfloor\sqrt{n}\rfloor - 1$ deljenj. Če bi za vsako deljenje porabili le eno mikrosekundo, bi za celoten postopek na 1024-bitnem številu potrebovali vsaj $3 \cdot 10^{140}$ let! Tudi če bi vrednosti za d omejili le na praštevila, ki ne presegajo $\sqrt{n}$, bi še vedno imeli opravka s $\pi(\sqrt{n})$ deljenj, kar je po *praštevilskem izreku* [6, Poglavje 6.2] $\pi(x) \sim x/\log x$ asimptotično enako $2\sqrt{n}/\log n$. Torej, tudi to nam ne prinese izrazitega napredka, pa še seznam praštevil bi potrebovali (kar še s trenutno najboljšimi algoritmi ni hitro). Potrebujemo močnejše orodje. Morda je malce presenetljivo, da se skriva v znamenitem izreku iz elementarne teorije števil 17. stoletja.

3 Učinkoviti algoritmi

"Čas je denar" je vsem dobro znan pregovor, ki še kako drži v poslovnem svetu. Z algoritmi, še posebno tistimi, ki nam krojijo vsakdan, ni nič drugače. Algoritem iz prejšnjega sestavka tako v realnem svetu nima mesta. Pravimo, da je algoritem *učinkovit*, če je njegova časovna zahtevnost polinomska funkcija na parametru *velikosti* vhodnega podatka. Torej, če je vhod algoritma naravno število $n \geq 2$, mora potem algoritem delovati v največ $p(\log n)$ časovnih enotah, kjer je $p(x)$ neki polinom s konstantnimi koeficienti. Naivni algoritmi za štiri osnovne računske operacije so vsi učinkoviti, npr. pisno množenje dveh naravnih števil $n \geq 2$ in $m \geq 2$ zahteva $\ll (\log n)(\log m)$ bit-operacij. Nekatere pomembne operacije v teoriji števil imajo učinkovite algoritme, npr. največji skupni delitelj (a, b) in modularno potenciranje $a^c \bmod n$ za $1 \leq |a| < n$, $c \geq 2$ in $n \geq 2$, glej [4, Poglavji 4 in 5].

V skladu z uvodnimi vprašanji želimo najti *učinkovite* in *deterministične* algoritme, ki bi nam rešili naslednja odločitvena problema:

1. PRAŠTEVILA: Za podano naravno število $n \geq 2$, ali je n praštevilo?
2. SESTAVLJENA ŠTEVILA: Za podano naravno število $n \geq 2$, ali je n sestavljeno število?

Odločitvena problema PRAŠTEVILA in SESTAVLJENA ŠTEVILA sta si *komplementarna*: odgovor na en problem (da/ne) avtomatično poda odgovor na drug problem (ne/da). Kljub temu sta si z vidika teorije računske zahtevnosti, glej npr. [3] in [4, Poglavje 3], precej različna. Osrednja razreda problemov v tej teoriji sta P in NP, kjer razred P sestoji iz odločitvenih problemov, ki jih lahko rešimo z učinkovitimi in deterministični algoritmi, medtem ko razred NP sestoji iz tistih odločitvenih problemov, katerih rešitve lahko *preverimo* z učinkovitimi in deterministični algoritmi. Ker lahko vedno učinkovito preverimo pravilnost razcepa danega naravnega števila, ki nam je bil posredovan kot dokaz za njegovo sestavljenost, imamo SESTAVLJENA ŠTEVILA $\in$ NP. Dokaz, da imamo tudi PRAŠTEVILA $\in$ NP, ni tako enostaven [4, Izrek 9.1.4]. Vsaj od leta 1976 je večina matematikov domnevala, da mora veljati PRAŠTEVILA $\in$ P, torej da obstaja "dovolj hiter" deterministični algoritem, ki nam odloči, ali imamo opravka s praštevilom ali ne. Indijski matematiki M. Agrawal, N. Kayal in N. Saxena so leta 2004 v [1] objavili tak algoritem, s časovno zahtevnostjo $\ll_\varepsilon (\log n)^{6+\varepsilon}$. Njihov rezultat (glej knjigo [8] za zelo dostopno študijo) predstavlja zgodovinski napredek na področju (algoritmične) teorije števil, vendar se redko uporablja v praksi. Za potrebe RSA kriptografije so bolj prikladni stohastični algoritmi.

4 Stohastični algoritmi

Stohastični (randomiziran) algoritem je tak algoritem, ki sloni na naključnih spremenljivkah in tako lahko poda različne odgovore pri enakem vhodu. To je očitno v nasprotju z determinističnimi algoritmi. Pomemben podrazred stohastičnih algoritmov se imenuje *Monte Carlo algoritmi*: izhod je lahko "da" ali "verjetno ne", in velja naslednje:

1. če algoritem vrne "da", potem je vhod pozitiven primerek;
2. obstaja realno število $p \in (0, 1]$, da za vsak pozitiven primerek algoritem poda (pravilen) "da" odgovor z verjetnostjo vsaj p.

Poglejmo si naslednji algoritem `fermat_test`, napisan v programskem jeziku *Python*.

```python
from sympy.core.random import _randint
from sympy import gcd
def fermat_test(n):
    # n>2 je naravno stevilo
    if n%2 == 0:
        return f"{n} je sestavljeno stevilo"
    else:
        a = _randint()(1,n-1)
        if gcd(a,n) != 1:
            return f"{n} je sestavljeno stevilo"
        else:
            if pow(a,n-1,n) == 1:
                return f"{n} je verjetno prastevilo"
            else:
                return f"{n} je sestavljeno stevilo"
```

Algoritem 1: Fermatov test praštevilskosti.

Predno ga analiziramo, navedimo naslednje:

1. Uporabljamo knjižnico *SymPy* za simbolno matematiko, iz katere smo si naložili metodi `_randint` in `gcd`.

2. V vrstici 5 izraz `n%2 == 0` pomeni, da je ostanek pri deljenju n z 2 enak 0, tj. $2 \mid n$.

3. V vrstici 8 je parameter `a` iz množice $\{1, 2, \ldots, n-1\}$ izbran z metodo `_randint()(1,n-1)` *(psevdo)naključno.*

4. V vrstici 9 izraz `gcd(a,n) != 1` pomeni $(a, n) \neq 1$.

5. V vrstici 12 izraz `pow(a,n-1,n) == 1` pomeni $a^{n-1} \bmod n = 1$. Na tem mestu algoritem preko modularnega potenciranja preveri, ali velja $a^{n-1} \equiv 1 \pmod{n}$.

Če je $n \geq 3$ praštevilo, potem algoritem `fermat_test(n)` vrne `'n je verjetno prastevilo'`, kar je posledica *malega Fermatovega izreka:* $a^{p-1} \equiv 1 \pmod{p}$ *za praštevilo* p *in naravno število* a*, pri čemer moramo imeti* $p \nmid a$, glej [9, Izrek 6.3]. Od tod tudi ime algoritmu. Če pa algoritem vrne `'n je sestavljeno stevilo'`, potem imamo $(a, n) \neq 1$ ali $a^{n-1} \not\equiv 1 \pmod{n}$ za neki $a \in \{1, \ldots, n-1\}$. V tem primeru je n res sestavljeno število. Torej, `fermat_test` je stohastični algoritem, kjer "da" pomeni `'n je sestavljeno stevilo'` in pozitiven primerek je sestavljeno število. S tem je algoritem kandidat za Monte Carlo algoritem za odločitveni problem SESTAVLJENA ŠTEVILA. Na žalost pa ne izpolnjuje drugega pogoja. Z uporabo *teorije grup* se da pokazati naslednje [8, Lema 3.3.3].

Trditev 4.1. *Če za dano sestavljeno število* n *obstaja* $a \in \mathbb{Z}_n^* := \{k \in \{1, \ldots, n-1\} \colon (k, n) = 1\}$ *tako da velja* $a^{n-1} \not\equiv 1 \pmod{n}$*, potem je verjetnost da najdemo tak* a *v množici* $\mathbb{Z}_n^*$ *vsaj* $1/2$.

Kot primer navedimo, da so za $n = 15$ ustrezne vrednosti $a \in \{2, 7, 8, 13\} \subset \mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$. Torej, če a iz trditve 4.1 vedno obstaja, bo `fermat_test` učinkovit Monte Carlo algoritem (s $p = 1/2$) za odločitveni problem SESTAVLJENA ŠTEVILA. Toda tak a ne obstaja vedno. Sestavljenim številom n, za katera velja $a^{n-1} \equiv 1 \pmod{n}$ *za vsak* $a \in \mathbb{Z}_n^*$, pravimo *Carmichaelova števila.* Najmanjše tako število je $561 = 3 \cdot 11 \cdot 17$, Alford, Granville in Pomerance pa so leta 1994 v [2] celo dokazali, da jih je neskončno.

5 Miller–Rabinov test

Fermatov test ni Monte Carlo algoritem, saj obstaja (neskončna) množica pozitivnih primerkov (Carmichaelova števila), kjer algoritem *vedno* poda napačen odgovor. S tem bi si mislili, da je algoritem obsojen na propad. Toda, ali se bi ga dalo nekako "popraviti" v smislu, da se izognemo Carmichaelovim številom? Gary L. Miller je leta 1976 v [5] to storil z uporabo ustrezne različice malega Fermatovega izreka.

Izrek 5.1 (Miller, 1976)**.** *Naj bo* p *liho praštevilo. Pišimo* $p - 1 = d \cdot 2^l$*, kjer je* $d \in \mathbb{N}$*,* $l \in \mathbb{N}$ *in* $2 \nmid d$*. Če je* a *tako naravno število, da velja* $p \nmid a$*, potem:*

1. $a^d \equiv 1 \pmod{p}$*, ali*

2. $a^{d \cdot 2^i} \equiv -1 \pmod{p}$ *za neki* $i \in \{0, 1, \ldots, l-1\}$.

Miller je na podlagi izreka 5.1 konstruiral učinkovit deterministični algoritem za problem PRAŠTEVILA, vendar pod predpostavko o pravilnosti še vedno nerešene *posplošene Riemannove domneve* (za poseben neskončen podrazred Dirichletovih L-funkcij). Originalno Riemannovo domnevo lahko ekvivalentno formuliramo [6, Izrek 13.1] z enačbo

$$\pi(x) = \int_2^x \frac{\mathrm{d}u}{\log u} + O\left(\sqrt{x} \log x\right).$$

Najti dokaz te na videz preproste ocene spada med najpomembnejše odprte probleme v matematiki.

Michael O. Rabin je leta 1980 v [7] pokazal, da se da Millerjev algoritem brezpogojno preoblikovati v učinkovit Monte Carlo algoritem s $p = 3/4$. Različica takega algoritma, znana kot *Miller–Rabinov test praštevilskosti*, je zapisana spodaj.

```python
from sympy.core.random import _randint
from sympy import gcd
def miller_rabin_test(n):
    # n>2 je naravno stevilo
    if n%2 == 0:
        return f"{n} je sestavljeno stevilo"
    else:
        d = n-1
        l = 0
        while d%2 == 0:
            l = l+1
            d = d//2
        a = _randint()(1,n-1)
        if gcd(a,n) != 1:
            return f"{n} je sestavljeno stevilo"
        else:
            b = pow(a,d,n)
            if b == 1:
                return f"{n} je verjetno prastevilo"
            else:
                for i in range(l):
                    if (b+1)%n == 0:
                        return f"{n} je verjetno prastevilo"
                    else:
                        b = pow(b,2,n)
                return f"{n} je sestavljeno stevilo"
```

Algoritem 2: Miller–Rabinov test praštevilskosti.

Algoritem 2 lahko analiziramo podobno kot algoritem 1, pri čemer namesto malega Fermatovega izreka uporabimo izrek 5.1. Najtežja naloga je seveda dokaz, da imamo $p = 3/4$. Pri tem moramo trditev 4.1 nadomestiti s podobnim, toda težje dokazljivim rezultatom.

Izrek 5.2 (Rabin, 1980)**.** *Naj bo n liho sestavljeno naravno število. Pišimo $n-1 = d \cdot 2^l$, kjer je $d \in \mathbb{N}$, $l \in \mathbb{N}$ in $2 \nmid d$. Potem imamo*

$$\left|\left\{a \in \{1,\dots,n-1\} \colon a^d \not\equiv 1 \pmod{n} \wedge \forall i \in \{0,\dots,l-1\}.\ a^{d\cdot 2^i} \not\equiv -1 \pmod{n}\right\}\right| \geq \frac{3}{4}(n-1).$$

Časovna zahtevnost Miller–Rabinovega testa je $\ll (\log n)^3$. Ta test pa ni prvi učinkovit Monte Carlo algoritem: leta 1977 sta takega (s $p = 1/2$) objavila R. M. Solovay in V. Strassen v [11]. Njun algoritem temelji na Eulerjevem kriteriju za kvadratne ostanke [9, Izrek 11.3] in zakonu kvadratne recipročnosti za Jacobijev simbol [9, Poglavje 11.3], ter ima enako časovno zahtevnost kot algoritem 2. Vseeno pa v praksi deluje počasneje od Miller–Rabinovega testa, zato se slednji uporablja bolj pogosto.

6 Uporaba Miller–Rabinovega testa

V zaključnem razdelku se bomo soočili z zadnjim vprašanjem iz uvoda. Recimo, da želimo poiskati n-bitno praštevilo, torej, iščemo praštevila na intervalu $\left(2^{n-1}, 2^n\right)$. Spomnimo, da trenutni standard RSA kriptografije zahteva vsaj 2048-bitne ključe, torej $n \geq 1024$. Kako bi si pri tem pomagali z algoritmom 2? Poglejmo si naslednji postopek.

```
1  def iskalnik_prastevil(n,k,j=1):
2      # n>2 je naravno stevilo
3      # k>0 je naravno stevilo
4      num = _randint()(2**(n-1)+1,2**n-1)
5      a = miller_rabin_test(num)
6      if a == f"{num} je verjetno prastevilo":
7          i = 1
8          while i <= k-1:
9              a = miller_rabin_test(num)
10             if a == f"{num} je verjetno prastevilo":
11                 i = i + 1
12             else:
13                 return f"{num} je sestavljeno stevilo"
14         return [j, f"{num} je verjetno prastevilo"]
15     else:
16         j = j + 1
17         return iskalnik_prastevil(n,k,j)
```

Algoritem 3: Iskalnik praštevil na intervalu $\left(2^{n-1}, 2^n\right)$.

Algoritem `iskalnik_prastevil(n,k,j=1)` ima tri argumente. Argument `n` predstavlja bitno dolžino iskanega praštevila. Argument `j` je na začetku postavljen na vrednost 1 in nam šteje število poskusov, pri katerih je bil algoritem 3 neuspešen pri iskanju morebitnih praštevil (preko Miller–Rabinovega testa – algoritem 2), pri čemer štejemo uspeh `'n je verjetno prastevilo'` za zadnji poskus. Če se to zgodi, nam potem `k` predstavlja maksimalno možno število dodatnih sklicev (vključno s tistim pri zadnjem poskusu) na algoritem 2, glej vrstice 6–14 algoritma 3. Razjasnimo to s primerom uporabe.

```
In [1]: iskalnik_prastevil(1024,10)
Out[1]: [839,
 '164354620815488838961782026512943224046987541132720923309647418310268 1
  887706846458703258452211148377675802677456429921553201994500367975803 6
  456429908187830610484441024071654126583615621617057143652792368623948 5
  125551002075889233522137926336631026528078591699264489277128201390154
  346074524724635789483327177 81 je verjetno prastevilo']
```

V tem primeru je algoritem 3 v 839. poskusu na intervalu $\left(2^{1023}, 2^{1024}\right)$ našel 309-mestnega kandidata za praštevilo. To število je potem opravilo Miller–Rabinov test v vseh devetih ponovitvah. Kako bi interpretirali to ugotovitev v jeziku verjetnosti? Za natančno obravnavo potrebujemo definiciji:

1. Naj bo $\mathcal{P}$ dogodek, da je naključno izbrano število N (ki ga testiramo) iz množice $\left(2^{n-1}, 2^n\right) \cap \mathbb{N}$, $n \geq 3$, praštevilo.
2. Naj bo $\mathcal{MR}_k$ dogodek, da N opravi Miller–Rabinov test k-krat. V tem primeru lahko predpostavimo, da je ta k enak tistemu iz algoritma 3.

Skladno s prejšnjim vemo naslednje:

1. $0 < P\left(\mathcal{P}\right) < 1$: vsa števila v množici zagotovo niso praštevila, po Bertrandovem postulatu [6, str. 49] pa praštevilo tam vedno obstaja.
2. $P\left(\mathcal{MR}_k \mid \mathcal{P}\right) = 1$ za vsak $k \in \mathbb{N}$.
3. $P\left(\overline{\mathcal{MR}_1} \mid \overline{\mathcal{P}}\right) \geq 3/4$ po izreku 5.2. S tem je $P\left(\mathcal{MR}_1 \mid \overline{\mathcal{P}}\right) \leq 1/4$, torej $P\left(\mathcal{MR}_k \mid \overline{\mathcal{P}}\right) \leq 4^{-k}$.

Zanima nas $P(\mathcal{P}|\mathcal{MR}_k)$, tj. verjetnost, da je testirano število N praštevilo, ko je Miller–Rabinov test že vrnil `'N je verjetno prastevilo'` k-krat. Uporabimo *Bayesovo formulo*:

$$P\left(\mathcal{P}|\mathcal{MR}_k\right) = 1 - P\left(\overline{\mathcal{P}}|\mathcal{MR}_k\right) = 1 - \frac{1}{1 + \frac{P(\mathcal{MR}_k|\overline{\mathcal{P}})P(\overline{\mathcal{P}})}{P\left(\mathcal{MR}_k|\mathcal{P}\right)P\left(\mathcal{P}\right)}} \geq 1 - \frac{4^{-k}}{P\left(\mathcal{P}\right)} = 1 - \frac{2^{n-1}-1}{\pi\left(2^n\right) - \pi\left(2^{n-1}\right)} 4^{-k}.$$

Praštevilski izrek zagotavlja $\pi(2x) - \pi(x) \sim x/\log x$, *eksplicitna* različica [10] pa

$$\pi(2x) - \pi(x) \geq \left(1 - \frac{2}{\log(2x)}\right) \frac{x}{\log x}$$

za vse $x \geq 4$. Seveda obstajajo boljše ocene, vendar je zapisana za naše potrebe dovolj ostra, pa še enostavno si jo je zapomniti. S tem imamo naslednji rezultat.

Trditev 6.1. *Za vse $n \geq 3$ in $k \geq 1$ velja*

$$P(\mathcal{P}|\mathcal{MR}_k) \geq 1 - \left(1 - \frac{2}{n \log 2}\right)^{-1} \left(1 - \frac{1}{2^{n-1}}\right) 4^{-k}(n-1)\log 2.$$

Trditev 6.1 nam teoretično upravičuje pričakovano hevristično načelo: v primeru, da nam algoritem 3 za *dovolj velik* k obljubi "n je verjetno praštevilo", je število n *skoraj zagotovo* res praštevilo. V našem primeru imamo $n = 1024$ in $k = 10$. Po trditvi 6.1 imamo $P(\mathcal{P}|\mathcal{MR}_k) \geq 0.99932$, torej lahko rečemo naslednje: *Verjetnost, da je po algoritmu 3 izbrano število* $1643546 \ldots 781$ *res praštevilo, je vsaj* 99.932%. Z večanjem števila k lahko še izboljšamo to verjetnost, seveda na račun hitrosti algoritma 3. Zgornja neenakost nam natančno pove, kako to storiti.

Pri algoritmu 3 nimamo "deterministčnega" zagotovila, da se bo res ustavil, torej da bomo naleteli na uspešen poskus. Vseeno lahko podamo zgornjo mejo za *pričakovano* število poskusov, tj. vrednost parametra j. Naj bo $n \geq 3$, $p = \mathcal{P}(\mathcal{MR}_1)$ in $X \sim$ število poskusov. Potem imamo

$$p = P(\mathcal{MR}_1 \mid \mathcal{P})\, P(\mathcal{P}) + P\left(\mathcal{MR}_1 \mid \overline{\mathcal{P}}\right) P\left(\overline{\mathcal{P}}\right) \geq P(\mathcal{P}) = \frac{\pi(2^n) - \pi\left(2^{n-1}\right)}{2^{n-1} - 1}$$

in s tem

$$\mathbb{E}[X] = p \sum_{m=1}^{\infty} m(1-p)^{m-1} = \frac{1}{p} \leq \left(1 - \frac{2}{n \log 2}\right)^{-1} \left(1 - \frac{1}{2^{n-1}}\right)(n-1)\log 2.$$

Torej, za $n = 1024$ imamo $\mathbb{E}[X] \leq 712$, kar ni tako daleč od števila poskusov pri našem primeru. Podobno lahko pokažemo tudi, da je pričakovana časovna zahtevnost algoritma 3 enaka $O\left(kn^3\right)$.

Literatura

[1] M. Agrawal, N. Kayal, N. Saxena, *PRIMES is in P*, Ann. of Math. (2) **160** (2004), no. 2, 781–793.

[2] W. R. Alford, A. Granville, C. Pomerance, *There are infinitely many Carmichael numbers*, Ann. of Math. (2) **139** (1994), no. 3, 703–722.

[3] S. Arora, B. Barak, *Computational complexity: A modern approach*, Cambridge University Press, New York, 2009.

[4] E. Bach, J. Shallit, *Algorithmic number theory. Vol. 1: Efficient algorithms*, Foundations of Computing Series, MIT Press, Cambridge, MA, 1996.

[5] G. L. Miller, *Riemann's hypothesis and tests for primality*, J. Comput. System Sci. **13** (1976), no. 3, 300–317.

[6] H. L. Montgomery, R. C. Vaughan, *Multiplicative number theory. I. Classical theory*, Cambridge Studies in Advanced Mathematics 97, Cambridge University Press, Cambridge, 2007.

[7] M. O. Rabin, *Probabilistic algorithm for testing primality*, J. Number Theory **12** (1980), no. 1, 128–138.

[8] L. Rempe-Gillen, R. Waldecker, *Primality testing for beginners*, Student Mathematical Library 70, AMS, Providence, RI, 2014.

[9] K. H. Rosen, *Elementary number theory and its applications*, 6th ed., Addison-Wesley, USA, 2011.

[10] J. B. Rosser, L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64–94.

[11] R. Solovay, V. Strassen, *A fast Monte-Carlo test for primality*, SIAM J. Comput. **6** (1977), no. 1, 84–85.

[12] D. R. Stinson, M. B. Paterson, *Cryptography: theory and practice*, 4th. ed., Textbooks in Mathematics, CRC Press, Boca Raton, FL, 2019.

A ali B: to je tu vprašanje

Jasna Urbančič

Teads

1 Uvod: kaj je A/B testiranje?

Pogosto imamo na voljo dve možnosti, **A** in **B**, in želimo razumeti, katera je boljša. *A/B testiranje* je okrajšava za preprost randomiziran kontroliran eksperiment, v katerem primerjamo več vzorcev (npr. A in B) ene same (vektorske) spremenljivke.

Ključni sestavni deli so: (i) vzorce naključno razdelimo v skupine, s čimer zagotovimo primerljivost; (ii) med skupinama spremenimo eno samo stvar; in (iii) opazujemo eno merljivo spremenljivko — na primer oceno na lestvici od 1 do 10. Odgovoriti želimo na dve vprašanji:

1. Ali je povprečna ocena višja za A ali za B?
2. Ali je razlika med njima **pomembna** (ali pa je le posledica naključja)?

Prvo vprašanje je preprosto: primerjamo povprečji. Pravo delo se skriva v drugem vprašanju, saj vsaka meritev nosi negotovost.

2 Vzorci in porazdelitve

Vsakemu vzorcu pripišemo skupino (A ali B) in izmerjeno oceno. Ocene izhajajo iz neke *verjetnostne porazdelitve*. Če narišemo histogram ocen za obe skupini, običajno dobimo dva prekrivajoča se zvonasta kupa. Kadar se kupa močno prekrivata, je razlika med A in B negotova; kadar sta jasno ločena, je razlika verjetno resnična. Prav to negotovost formalno opišemo z intervalom zaupanja.

3 Intervali zaupanja

Povprečje iz vzorca je le *ocena* oziroma približek pravega povprečja: če bi poskus ponovili, bi dobili nekoliko drugačno vrednost. Kako zelo povprečje niha, meri standardna napaka

$$SE = \frac{s}{\sqrt{n}}, \qquad s = \sqrt{\frac{1}{n-1}\sum_{i=1}^{n}(x_i - \bar{x})^2},$$

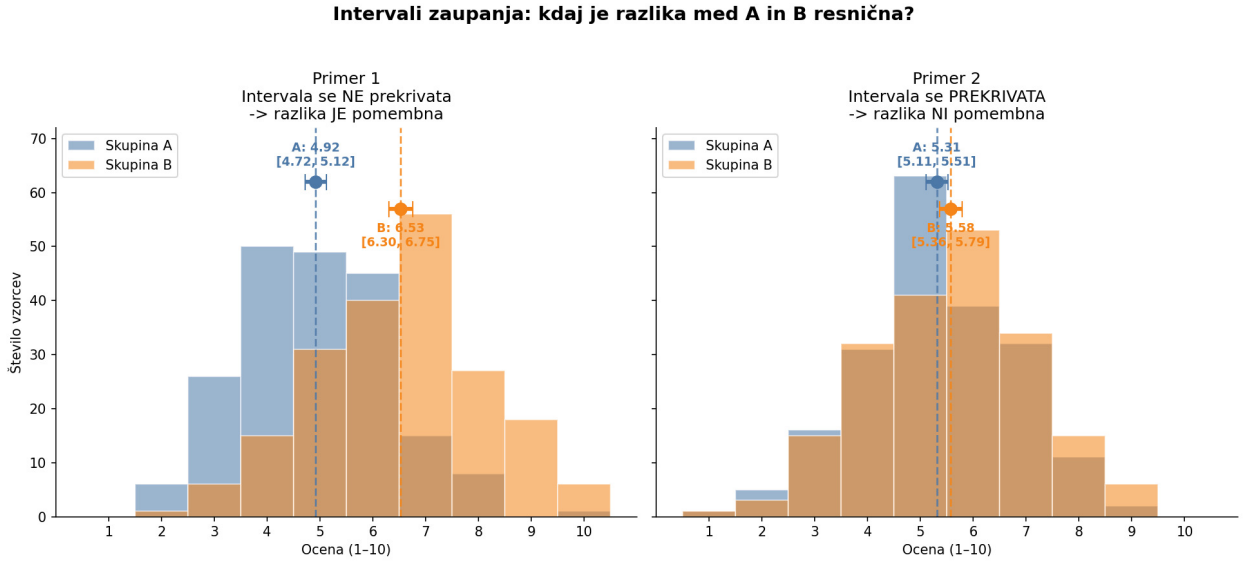
kjer je s standardni odklon ocen in n velikost vzorca. Večji vzorec pomeni manjšo standardno napako in s tem natančnejšo oceno.

Za velik vzorec iz približno normalne porazdelitve 95 % interval zaupanja za povprečje izračunamo kot

$$IZ_{95\%} = \bar{x} \pm 1{,}96 \cdot \frac{s}{\sqrt{n}}.$$

Faktor 1,96 izhaja iz normalne porazdelitve – 95 % vrednosti leži znotraj ±1,96 standardnega odklona od sredine. Interval razumemo takole: če bi poskus velikokrat ponovili, bi pravo povprečje padlo v ta razpon v približno 95 % primerov.

Uporaba pri A/B testu. Narišemo interval zaupanja za povprečje A in za povprečje B. Če se intervala *ne prekrivata*, je razlika pomembna; če se *prekrivata*, razlike ne moremo zanesljivo potrditi. Primer je prikazan na sliki 1. (Opomba: Strožja različica gleda interval zaupanja *razlike* verjetnostnih porazdelitev $B - A$ in preveri, ali vsebuje ničlo.)

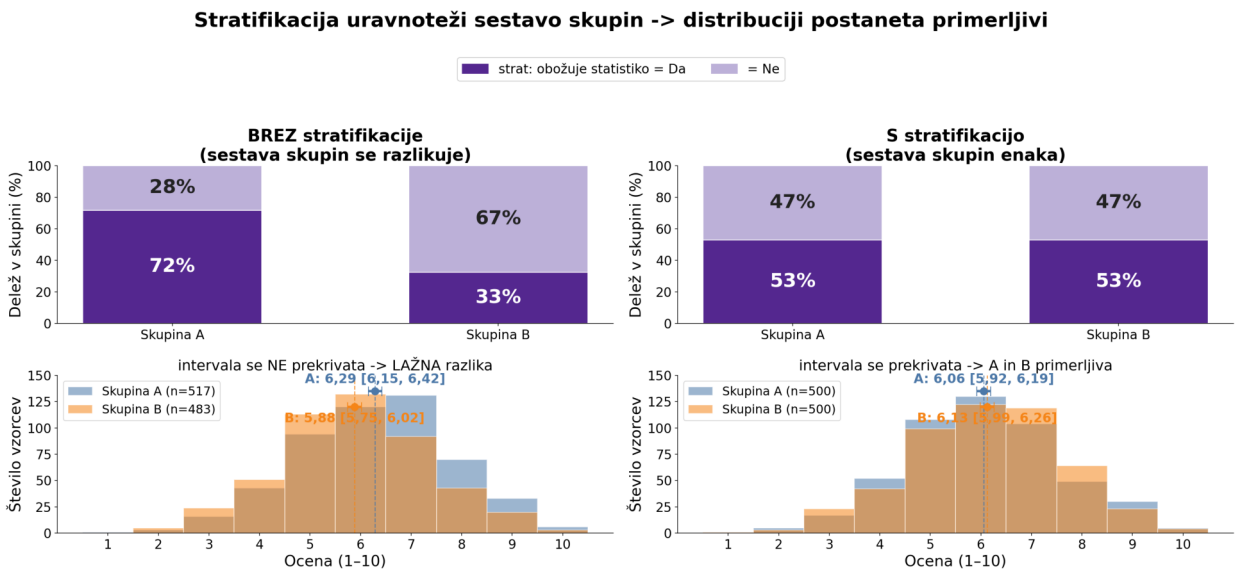


Slika 1: Dva primera A/B testa. *Levo:* povprečji sta jasno ločeni in intervala zaupanja se ne prekrivata – razlika je pomembna. *Desno:* povprečji sta blizu, intervala se prekrivata – čeprav ima B višje povprečje, razlike ne moremo potrditi.

4 Stratificirano vzorčenje

Naključna razdelitev v skupini je poštena le v povprečju. Pri manjših vzorcih (ali ob nesrečnem naključju) lahko ena skupina po sestavi močno odstopa od druge, na primer, če v skupino A pade veliko več ljudi z določeno lastnostjo, ki vpliva na oceno. Tedaj razlika v oceni ni posledica A proti B, temveč *različne sestave* skupin.

Rešitev je **stratificirano vzorčenje**: vzorce najprej razdelimo v *strate* – podskupine s podobnimi lastnostmi – in šele znotraj vsakega strata naključno razporedimo polovico v A in polovico v B. Tako sta skupini po sestavi skoraj enaki in primerjava postane poštena. Primer je prikazan na sliki 2.



Slika 2: Brez stratifikacije (levo) se sestavi skupin razlikujeta, kar ustvari lažno razliko v ocenah in ločena intervala zaupanja. S stratifikacijo (desno) sta sestavi enaki, distribuciji sovpadeta, intervala zaupanja pa se prekrivata in razlike med A in B ni.

5 A/B testiranje v spletnem oglaševanju

Na spletnih straneh del prostora ni namenjen vsebini, temveč **oglasom**; tako so strani za uporabnika brezplačne. Kateri oglas se prikaže, skoraj vedno določi **dražba v realnem času** (angl. *real-time bidding*, RTB): ko uporabnik odpre stran, nastane oglasni prostor, za katerega v delčku sekunde tekmuje več oglaševalcev. Najvišja ponudba zmaga, celoten postopek pa traja okrog 100 milisekund, saj morajo biti oglasi naloženi skupaj s spletno stranjo. Cene ne ponujajo ljudje, temveč **algoritmi**, ki ocenijo vrednost vsakega posameznega prikaza.

Ravno zato je A/B testiranje v tem okolju osrednje orodje: algoritme lahko nenehno izboljšujemo in med seboj primerjamo. A/B testiramo lahko:

- **oglase** – primerjamo razlike v sliki, barvah, naslovu ali pisavi; glavna opazovana metrika je delež klikov;
- **algoritme** – primerjamo razlike v značilkah, arhitekturi ali parametrih modela; opazovana metrika je odvisna od cilja (delež klikov, konverzij, zmag).

Izzivi so tu večji kot v učbeniškem primeru: kako sploh definirati vzorec (uporabnik, seja, prikaz, piškotek?), kako obvladati mešanje med skupinami, kako se spopasti z velikim oziroma prevelikim številom značilk za stratificirano vzorčenje in z dejstvom, da enako število zahtev še ne pomeni enakega proračuna. Poleg tega si pogosto želimo, da je testna skupina boljša iz *vseh* perspektiv hkrati, zato ene same metrike ni vedno mogoče izbrati.

6 Zaključek

A/B testiranje je preprosto v ideji, a zahtevno v podrobnostih. Intervali zaupanja nam povedo, kdaj je opažena razlika resnična in ne le naključje; stratificirano vzorčenje pa poskrbi, da primerjamo poštene, po sestavi primerljive skupine. Skupaj tvorita zanesljiv temelj za odločanje tako v učilnici kot v resničnem svetu spletnega oglaševanja.

ČLANKI UDELEŽENCEV

Apolonijev problem

Luka Krofl, Pija Pisar, Maja Vivod
Mentorica: *Manca Ernst*

Povzetek

V članku obravnavamo problem konstrukcije krožnice, tangentne trem danim krožnicam. Problem rešimo s pomočjo potence točke na krožnico in inverzije.

1 Potenca točke na krožnico

Definicija 1.1. *Naj bo ω krožnica s središčem v O in polmerom r ter naj bo X poljubna točka v ravnini. Število*

$$|XO|^2 - r^2$$

imenujemo ***potenca točke*** *X* ***na krožnico*** *ω. Označimo ga s $P(X, \omega)$.*

Iz definicije sledi, da je potenca točke na krožnico pozitivna, kadar točka leži zunaj krožnice, in negativna, kadar leži znotraj krožnice.

V nadaljevanju bomo v primerih, ko gre očitno za razdalje med točkami in ne za imena daljic, namesto z $|XO|$ dolžino daljice XO označili kar z XO. Oglejmo si naslednja izreka, ki povezujeta koncikličnost točk z razdaljami med njimi.

Izrek 1.1. *Naj bodo A, B, C in D točke v ravnini, med katerimi nobene tri niso kolinearne. Naj bo točka X presečišče premic AB in CD. Točke A, B, C in D so konciklične natanko tedaj ko velja*

$$XA \cdot XB = XC \cdot XD.$$

Če so točke A, B, C in D konciklične, je zgornja vrednost enaka potenci točke X na krožnico, ki poteka skozi točke A, B, C in D.

Dokaz. Denimo, da so točke A, B, C in D konciklične. Naj bo O središče krožnice, ki poteka skozi te točke. Presečišči premice XO s krožnico označimo z X_1 in X_2. Velja

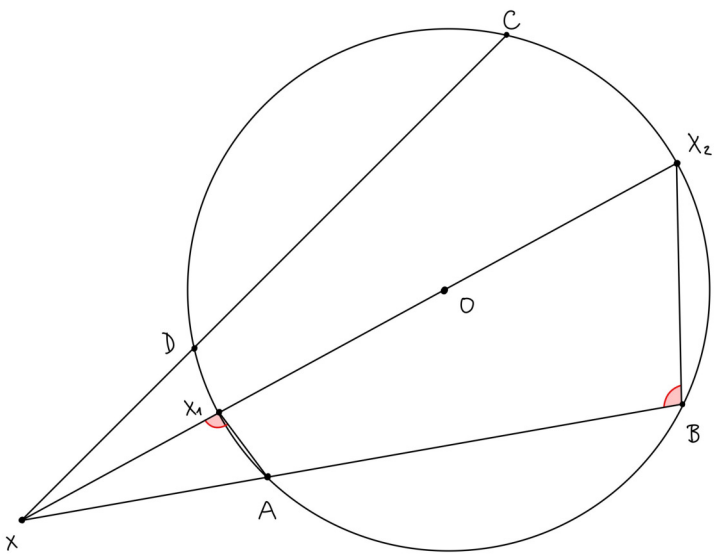
$$\angle XX_1A = 180^\circ - \angle AX_1X_2.$$

Iz koncikličnosti točk A, B, X_1 ter X_2 potem sledi

$$\angle XX_1A = \angle X_2BA.$$

Opazimo, da sta trikotnika $\triangle XAX_1$ in $\triangle XX_2B$ podobna, torej je

$$\frac{XA}{XX_1} = \frac{XX_2}{XB}$$



Slika 1: Točke A, B, C in D so konciklične natanko tedaj ko velja $XA \cdot XB = XC \cdot XD$.

in

$$XA \cdot XB = XX_1 \cdot XX_2.$$

Če ponovimo postopek še za točki C in D, dobimo $XC \cdot XD = XX_1 \cdot XX_2$, torej velja

$$XA \cdot XB = XC \cdot XD.$$

Pokažimo še, da je ta vrednost enaka potenci točke X na krožnico, ki poteka skozi točke A, B, C in D. Naj bo r polmer te krožnice. Ker točki X_1 in X_2 določata njen premer, lahko zapišemo

$$XX_1 \cdot XX_2 = (XO - r)(XO + r) = XO^2 - r^2 = P(X, \omega),$$

torej je res $XA \cdot XB = P(X, \omega)$.

Dokažimo še implikacijo v drugo smer. Predpostavimo, da velja $XA \cdot XB = XC \cdot XD$. Potem je

$$\frac{XA}{XC} = \frac{XD}{XB}.$$

Sledi, da sta $\triangle XAC$ in $\triangle XDB$ podobna. Velja

$$\angle BAC = 180^\circ - \angle CAX = 180^\circ - \angle XDB = \angle BDC,$$

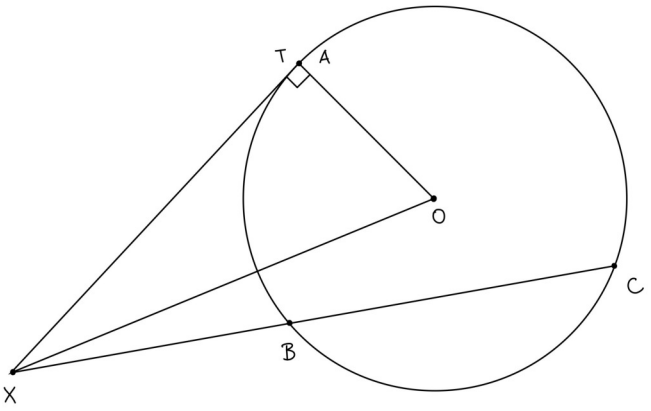
torej so točke A, B, C in D res konciklične. □

Pokažimo še poseben primer izreka 1.1.

Izrek 1.2. *Naj bodo A, B in C nekolinearne točke in naj točka X leži na premici BC. Naj bo ω krožnica, ki poteka skozi te točke. Potem velja*

$$XA^2 = XB \cdot XC$$

natanko tedaj ko je premica XA tangentna na to krožnico.



Slika 2: Premica XA je tangentna na krožnico, očrtano $\triangle ABC$, natanko tedaj ko velja $XA^2 = XC \cdot XD$.

Dokaz. Predpostavimo, da velja $XA^2 = XB \cdot XC$. Po izreku 1.1 velja, da je $XB \cdot XC = P(X, \omega)$. Ker je $XA^2 > 0$, je tudi $P(X, \omega) > 0$, torej točka X leži zunaj krožnice. Potem zagotovo obstaja tangenta na krožnico ω, ki poteka skozi točko X. Naj bo točka T dotikališče te tangente. Po Pitagorovem izreku velja

$$XT^2 = XO^2 - OT^2 = XO^2 - r^2 = P(X, \omega) = XA^2.$$

Iz tega sledi, da je $|XT| = |XA|$. Sedaj imamo dve možnosti; ali je $A = T$ in je XA tangenta na krožnico ω, ali pa je T dotikališče druge tangente iz točke X na to krožnico. Ker je $|XT| = |XA|$, je v tem primeru premica XA tudi tangentna na krožnico ω.

Dokažimo še drugo stran ekvivalence. Denimo, da je premica XA tangentna na očrtano krožnico trikotnika $\triangle ABC$. Potem velja

$$XA^2 = XO^2 - OA^2 = XO^2 - r^2 = P(X, \omega) = XB \cdot XC,$$

od koder sledi

$$XA^2 = XB \cdot XC.$$

□

1.1 Potenčna premica in potenčno središče

Poglejmo si, kako je videti množica točk, ki imajo na dve dani krožnici enako potenco.

Izrek 1.3 (Potenčna premica)**.** *Naj bosta Γ_1 in Γ_2 krožnici v ravnini s središči v točkah O_1 in O_2. Množica točk, za katere velja*

$$P(X, \Gamma_1) = P(X, \Gamma_2),$$

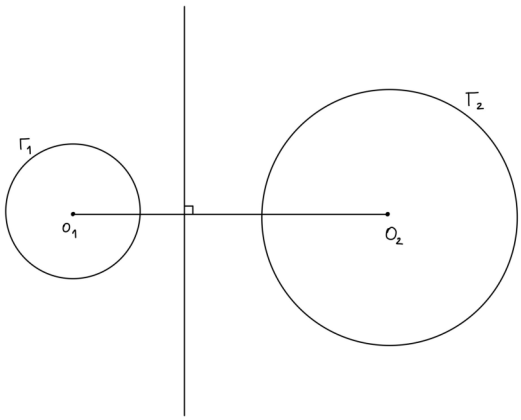
je premica, pravokotna na zveznico med točkama O_1 in O_2. Imenujemo jo ***potenčna premica*** *krožnic Γ_1 in Γ_2. Če se Γ_1 in Γ_2 sekata v točkah A in B, je njuna potenčna premica premica, ki poteka skozi točki A in B.*

Dokaz. Izrek bomo dokazali z uvedbo koordinatnega sistema. Recimo, da ima krožnica Γ_1 polmer r_1 in se njeno središče nahaja v točki $(a, 0)$, krožnica Γ_2 pa ima polmer r_2 in središče v točki $(b, 0)$, kjer $a \neq b$. Naj bo X točka s koordinatami (x, y). Za potenco X na krožnico Γ_1 velja

$$P(X, \Gamma_1) = (x - a)^2 + y^2 - r_1^2,$$

za potenco X na Γ_2 pa

$$P(X, \Gamma_2) = (x - b)^2 + y^2 - r_2^2.$$



Slika 3: Potenčna premica.

Ker sta potenci enaki, velja

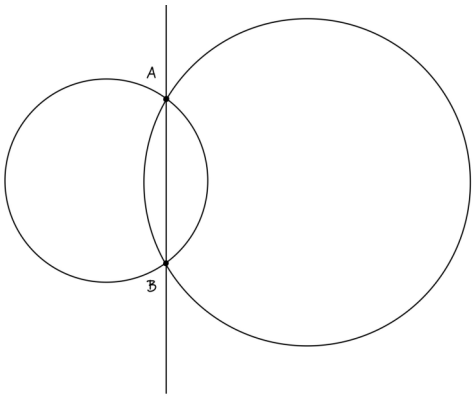
$$(x-a)^2 + y^2 - r_1^2 = (x-b)^2 + y^2 - r_2^2,$$
$$-2xa + a^2 - r_1^2 = -2xb + b^2 - r_2^2,$$
$$x = \frac{r_1^2 - r_2^2 + b^2 - a^2}{2b - 2a}.$$

Ker vemo, da $a \neq b$, smo v zgornjem računu smeli deliti z izrazom $2b - 2a$. Opazimo, da je x konstanten, y pa je poljuben. Točke oblike (x, y), ki imajo enako potenco na obe krožnici, torej opišejo premico z enačbo $x = c$, ki je pravokotna na x-os.

Poglejmo si še primer, ko se krožnici Γ_1 in Γ_2 sekata v točkah A in B. Ker ti točki ležita na obeh krožnicah, je

$$P(A, \Gamma_1) = P(A, \Gamma_2) = P(B, \Gamma_2) = P(B, \Gamma_1) = 0,$$

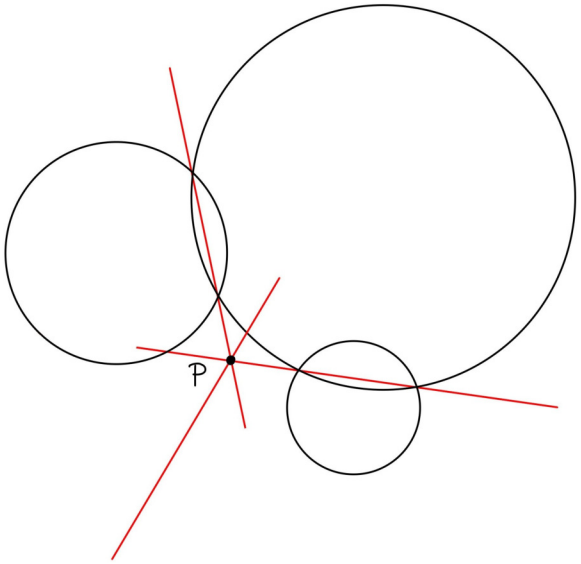
kar pomeni, da je njuna potenčna premica res premica, ki poteka skozi točki A in B. □



Slika 4: Potenčna premica krožnic, ki se sekata v točkah A in B.

Izrek 1.4 (Potenčno središče)**.** *Naj bodo Γ_1, Γ_2 in Γ_3 krožnice v ravnini in naj bodo O_1, O_2 in O_3 zaporedoma njihova središča.*

1. *Če so točke O_1, O_2 in O_3 kolinearne, so potenčne premice krožnic Γ_1, Γ_2 in Γ_3 vzporedne.*
2. *Če točke O_1, O_2 in O_3 niso kolinearne, se njihove potenčne premice sekajo v eni točki. To točko imenujemo* ***potenčno središče.***



Slika 5: Potenčno središče treh krožnic.

Dokaz. Poglejmo si najprej primer, ko so točke O_1, O_2 in O_3 kolinearne. Ker je potenčna premica dveh krožnic pravokotna na zveznico med njunimi središči, so potenčne premice Γ_1 in Γ_2, Γ_1 in Γ_3 ter Γ_2 in Γ_3 vzporedne.

Denimo sedaj, da točke O_1, O_2 in O_3 ne ležijo na isti premici. Naj bo p_{ij} potenčna premica krožnic s središčema v O_i in O_j, pri čemer sta $i, j \in \{1, 2, 3\}$, in naj bo X presečišče premic p_{12} in p_{23}. Vemo, da je

$$P(X, \Gamma_1) = P(X, \Gamma_2) \text{ in } P(X, \Gamma_2) = P(X, \Gamma_3),$$

iz česar sledi

$$P(X, \Gamma_1) = P(X, \Gamma_3).$$

Pokazali smo torej, da se potenčne premice p_{12}, p_{23} in p_{13} res sekajo v eni točki. □

2 Inverzija

Definicija 2.1. ***Inverzijska ravnina*** *je evklidska ravnina z dodano točko P_∞ v neskončnosti. Točka P_∞ leži na vsaki premici v ravnini.*

Poglejmo si, kaj smo dosegli s tem, ko smo ravnini dodali točko v neskončnosti. Premice si zdaj lahko predstavljamo kot krožnice z neskončnim polmerom. Opazimo, da se vsaki dve premici sekata natanko v dveh točkah, razen, če sta vzporedni – v tem primeru se sekata v eni.

Definicija 2.2. *Naj bo ω krožnica s središčem v O in polmerom r.* ***Inverzija preko*** *ω je preslikava, ki*

- *točko O preslika v točko P_∞,*
- *točko P_∞ preslika v točko O,*
- *vsako drugo točko X preslika v točko X', ki leži na poltraku OX, tako da velja $OX \cdot OX' = r^2$.*

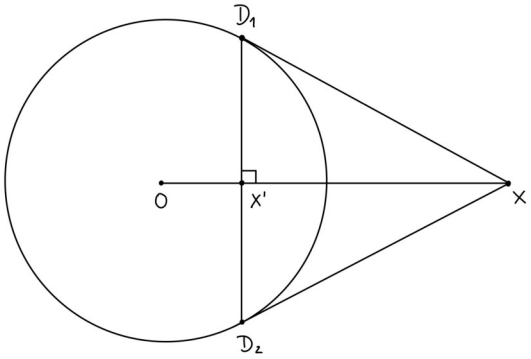
Inverzijo lahko razložimo tudi geometrijsko. Naj bo ω krožnica s središčem v O in X točka v ravnini, ki leži izven krožnice ω. Narišimo obe tangenti na krožnico, ki potekata skozi točko X. Naj bosta točki D_1 in D_2 točki, v katerih se tangenti dotikata krožnice. Točka X' naj bo presečišče premic D_1D_2 in XO. Ker sta kota $\angle D_1XO$ in $\angle OD_1X'$ enako velika, sta trikotnika $\triangle OXD_1$ in $\triangle OD_1X'$ podobna. Od tod sledi

$$\frac{OX}{OD_1} = \frac{OD_1}{OX'}$$

in

$$OX \cdot OX' = OD_1^2 = r^2,$$

kjer r označuje polmer krožnice ω. Vsaka točka X v zunanjosti krožnice ω se torej slika v razpolovišče daljice D_1D_2, kjer sta D_1 in D_2 dotikališči tangent skozi X na krožnico ω.



Slika 6: Geometrijska interpretacija inverzije.

Zdaj si lahko še pogledamo, kam inverzija slika različne objekte. Zanima nas, kam se slika premica, ki poteka skozi središče O krožnice ω. Opazimo, da se točki A in B, v katerih premica seka krožnico, ohranita. Po definiciji vemo, da se vse točke z inverzijo preslikajo na zveznico med središčem krožnice in med točko, ki jo invertiramo. Tako vemo, da se premica, ki poteka skozi središče krožnice, preslika sama vase. Za ostale primere si bomo pomagali z naslednjo lemo.

Lema 2.1. *Naj inverzija s središčem v O slika točki A in B zaporedoma v točki A' in B'. Potem velja*

$$\angle OAB = \angle A'B'O.$$

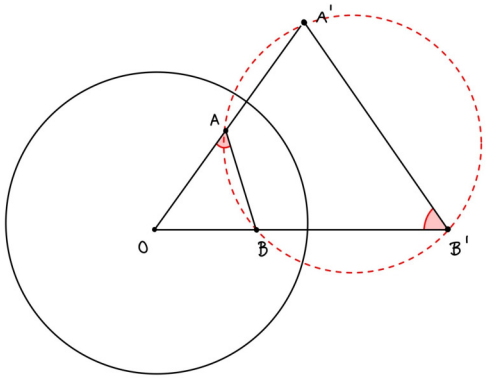
Dokaz. Ker sta točki A' in B' sliki točk A in B pod inverzijo, velja

$$OA \cdot OA' = r^2 = OB \cdot OB',$$

kjer je r polmer krožnice ω. Iz tega po potenci točke na krožnico sledi, da so točke $A,\ A',\ B$ in B' konciklične. Potem je

$$\angle OAB = 180^\circ - \angle BAA' = \angle A'B'B = \angle A'B'O,$$

kar zaključuje dokaz. □

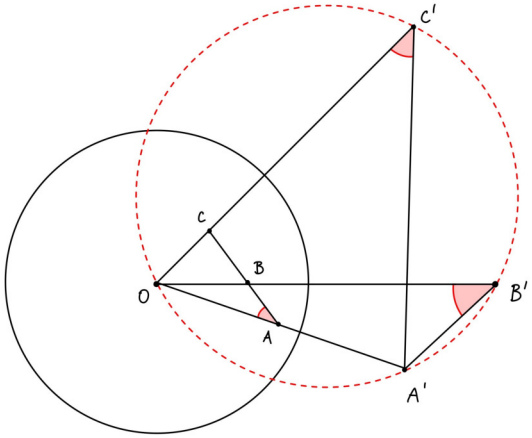


Slika 7: Ohranitev kota pri preslikavi dveh točk z inverzijo.

Poglejmo si še, kam inverzija slika premice, ki ne potekajo skozi središče krožnice ω, preko katere slikamo. Naj bodo točke $A,\ B$ in C kolinearne in naj bodo A', B' in C' slike teh točk pod inverzijo. Po lemi 2.1 velja

$$\angle OB'A' = \angle BAO = \angle CAO = \angle OC'A'.$$

Od tod sledi, da so točke O, A', B' in C' konciklične. Tako se premica AB slika v krožnico, očrtano trikotniku $\triangle OA'B'$.



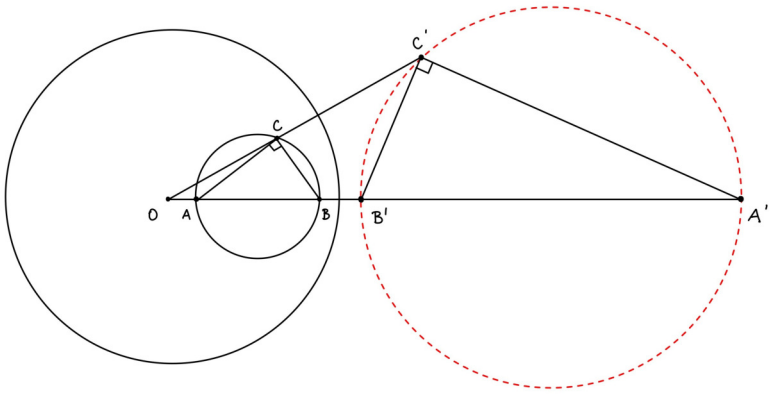
Slika 8: Inverzija premice, ki ne poteka skozi središče inverzije.

Poglejmo si še, kako inverzija slika krožnico, ki jo določajo točke A, B in C ter leži znotraj krožnice ω, preko katere jo slikamo. Naj bosta A in B taki točki, da je AB premer krožnice in točka O leži na premici AB. Naj bodo točke A', B' in C' zaporedoma inverzi točk A, B in C. Dovolj je, da pokažemo, da je daljica $A'B'$ premer inverza krožnice.

Vemo, da je $\angle ACB = \angle OCB - \angle OCA$. Po lemi 2.1 velja

$$90^\circ = \angle C'B'O - \angle C'A'O = 180^\circ - \angle A'B'C' - \angle C'A'B' = \angle B'C'A'.$$

S tem smo pokazali, da točka C' leži na krožnici s premerom $A'B'$.

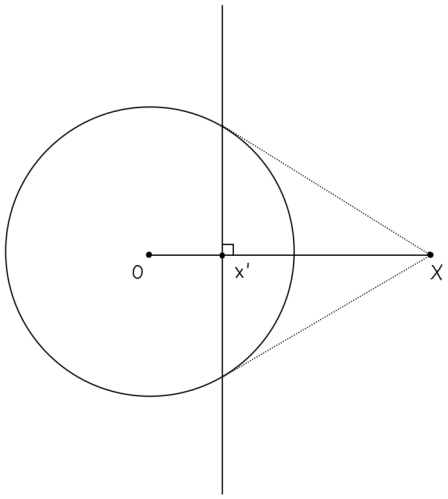


Slika 9: Inverzija krožnice.

2.1 Pol in polara

Pri konstrukciji si bomo pomagali tudi s polom in polaro.

Definicija 2.3. *Naj bo ω krožnica s središčem v O in naj bo X točka v ravnini. Naj bo X' njen inverz glede na ω.* ***Polara*** *je premica, ki poteka skozi točko X' in je pravokotna na premico, ki poteka skozi točki O in X. Točko X potem imenujemo* ***pol*** *premice.*



Slika 10: Pol in polara.

Izrek 2.1. *Točka X leži na polari točke Y natanko tedaj ko točka Y leži na polari točke X.*

Dokaz. Naj bo ω krožnica s središčem v O in polmerom r in naj bo X točka v ravnini. Naj bosta točka X' inverz točke X glede na ω in premica p polara točke X. Naj bo Y točka, ki leži na premici p. Vemo, da je premica p pravokotna na premico OX, saj je polara pravokotna na zveznico med središčem in polom, torej je daljica YX' pravokotna na premico OX.

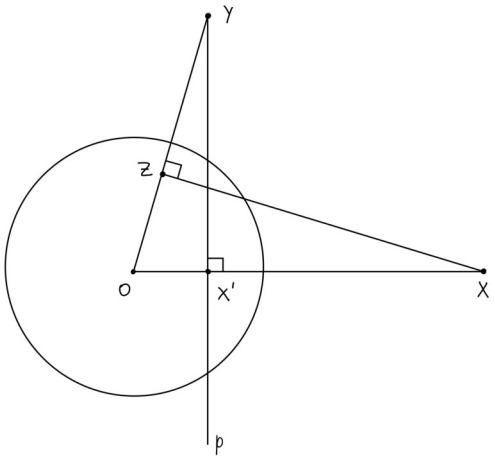
Naj bo Z taka točka na premici OY, da je premica XZ pravokotna na premico OY. Opazimo, da sta trikotnika $\triangle OXZ$ in $\triangle OYX'$ podobna, saj imata skupen kot $\angle XOY$ in sta oba pravokotna. Od tod sledi

$$\frac{OY}{OX} = \frac{OX'}{OZ}.$$

Ker je točka X' inverz točke X glede na ω, lahko zapišemo $OX \cdot OX' = r^2$, iz česar potem sledi

$$OY \cdot OZ = OX' \cdot OX = r^2.$$

To pomeni, da je točka Z inverz točke Y glede na ω, torej leži na polari točke Y. Ker je premica XZ pravokotna na premico OY, tudi točka X leži na polari točke Y, kar zaključuje dokaz. □



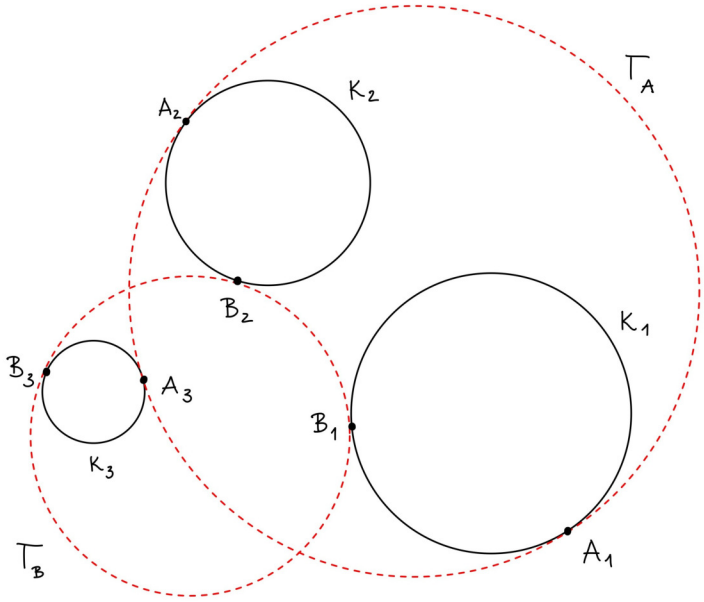
Slika 11: Točka X leži na polari točke Y natanko tedaj ko točka Y leži na polari točke X.

3 Rešitev problema

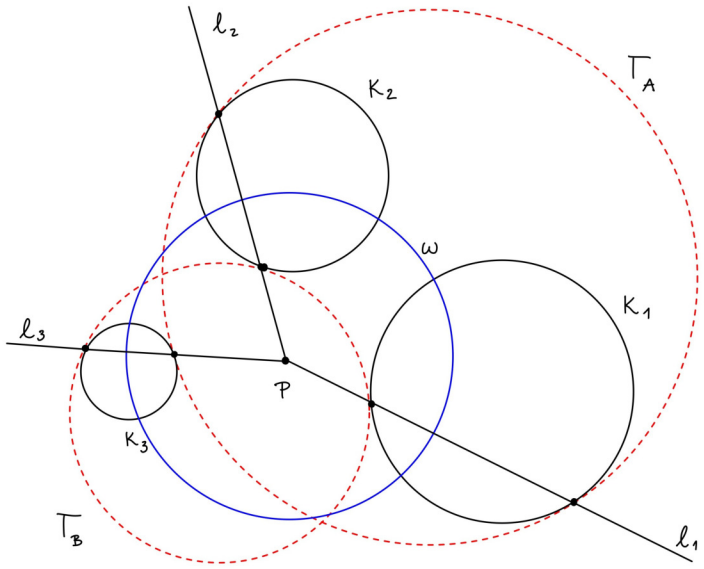
Sedaj lahko pokažemo konstrukcijo krožnic, tangentnih trem danim krožnicam. Rešitve bomo poiskali v parih.

Naj bodo K_1, K_2 in K_3 krožnice v ravnini in naj bosta Γ_A ter Γ_B iskan par krožnic, tangentnih krožnicam K_1, K_2 in K_3. Z A_i in B_i, kjer je $i \in \{1, 2, 3\}$, označimo točke, v katerih sta krožnici Γ_A ter Γ_B tangentni danim trem krožnicam. Krožnici Γ_A in Γ_B bomo konstruirali tako, da bomo za vsak i poiskali premico l_i, na kateri ležita točki A_i in B_i.

Naj bo P potenčno središče krožnic K_1, K_2 in K_3 in naj bo ω krožnica s središčem v P, ki pravokotno seka dane krožnice. Opazimo, da se z inverzijo glede na krožnico ω krožnica K_i ohrani, krožnici Γ_A in Γ_B, ki ju želimo konstruirati, pa se preslikata druga v drugo. Prav tako se druga v drugo preslikata točki A_i in B_i. Ker je središče opisane inverzije potenčno središče P, ta točka zagotovo leži na iskani premici l_i.

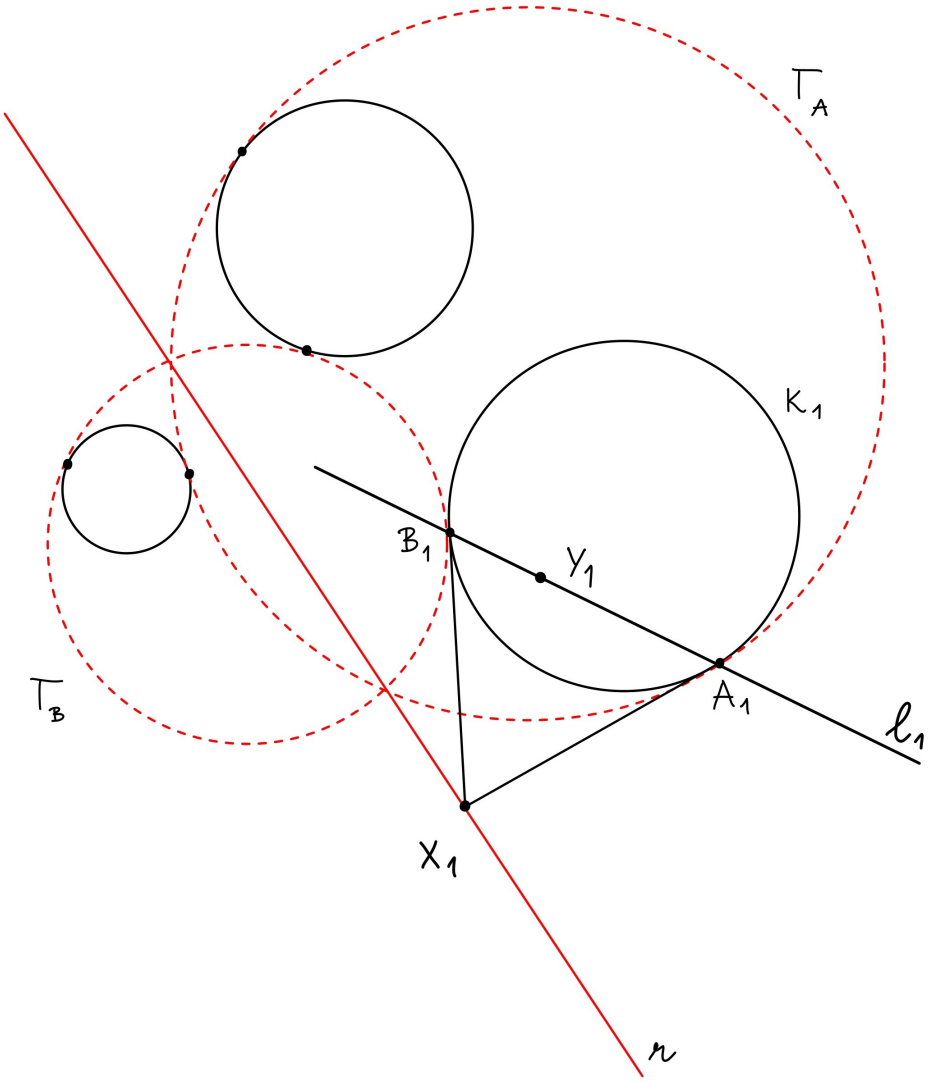


Slika 12: Krožnice K_1, K_2 in K_3 ter njim tangentni krožnici Γ_A in Γ_B.



Slika 13: Krožnica ω ter premice l_1, l_2 in l_3.

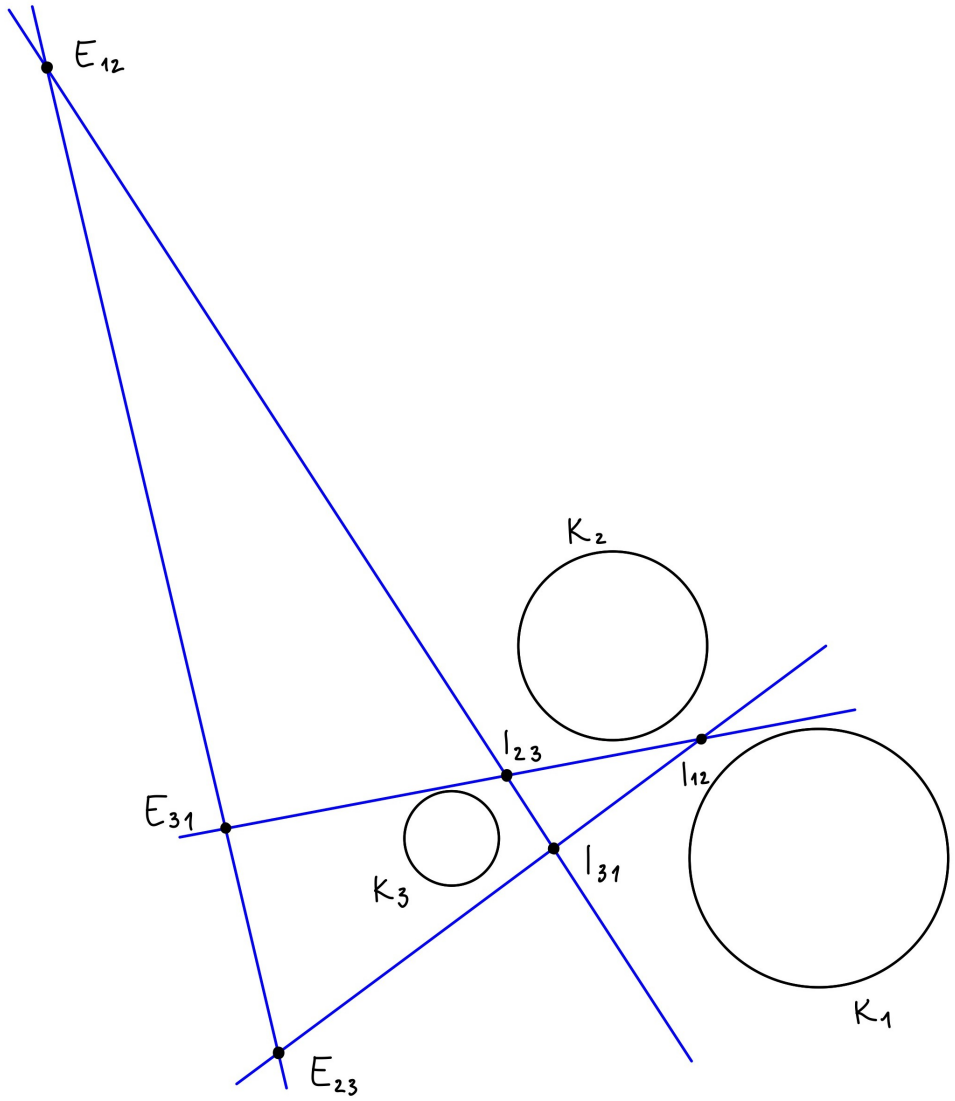
Za konstrukcijo druge točke, ki leži na premici l_i, si poglejmo tangenti na krožnico K_i, ki potekata skozi točki A_i in B_i. Naj bo X_i presečišče teh tangent. Točka X_i je potem pol premice l_i. Ker sta razdalji med točkama A_i in B_i ter polom enaki, je $P(X_i, \Gamma_A) = P(X_i, \Gamma_B)$, torej točka X_i leži na potenčni premici r krožnic Γ_A in Γ_B. Po izreku 2.1 potem pol Y_i premice r leži na premici l_i. To je torej druga točka, ki jo potrebujemo za konstrukcijo premice l_i.



Slika 14: Pol Y_i premice r je druga iskana točka, ki leži na premici l_i.

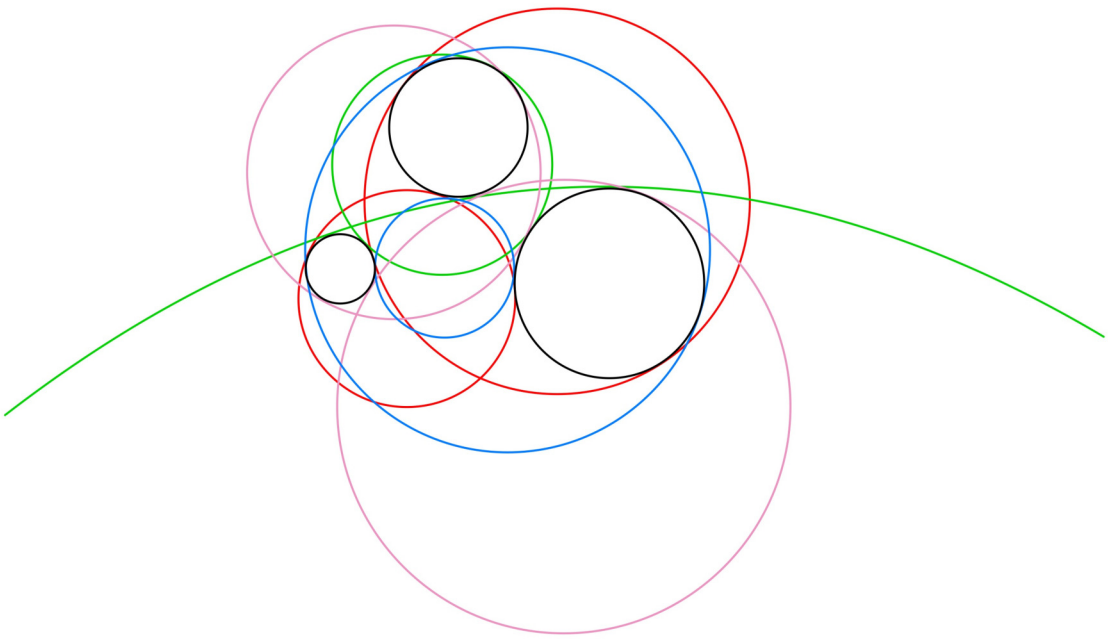
Poglejmo si krožnici K_1 in K_2. Zanju konstruirajmo notranje središče homotetije I_{12} in zunanje središče homotetije E_{12} tako, da poiščemo presečišči njunih skupnih tangent. Enako naredimo še za preostala para danih krožnic, da dobimo točke I_{23}, E_{23}, I_{31} in E_{31}. Po Mongeevem izreku te točke ležijo na natanko štirih premicah, prikazanih na sliki 15. Izkaže se, da je vsaka od teh premic ravno potenčna premica enega od parov krožnic Γ_A in Γ_B, ki jih želimo konstruirati[1]. Ker so take premice štiri, obstaja osem krožnic, ki rešijo naš problem.

[1] Dokaz lahko bralec najde v [1].



Slika 15: Premice, ki jih določajo središča homotetije.

Problem torej rešimo tako, da za vsak $i \in \{1, 2, 3\}$ konstruiramo premico l_i, ki poteka skozi točki A_i in B_i, v katerih sta krožnici Γ_A in Γ_B tangentni na eno od danih krožnic K_i. Premico l_i določimo z dvema točkama. Prva je potenčno središče P krožnic K_1, K_2 in K_3, druga pa pol Y_i ene od premic, ki jih določajo središča homotetije, glede na krožnico K_i. Če postopek ponovimo z vsemi štirimi premicami, dobimo vseh osem rešitev Apolonijevega problema, prikazanih na sliki 16.



Slika 16: Krožnice, tangentne trem danim krožnicam.

Literatura

[1] Dörrie, H. (1965). 100 Great Problems of Elementary Mathematics : Their History and Solution. Dover Publications.

[2] Chen, E. (2016). Euclidean Geometry in Mathematical Olympiads. The Mathematical Association of America.

Jožefov problem

Klara Jug, Stela Petrinić, Brina Umek
Mentor*: Jan Genc*

Povzetek

V članku je obravnavan Jožefov problem. Najprej je rešena poenostavljena različica problema. Končna formula je izpeljana s principom indukcije in je interpretirana v binarnem sistemu.

1 Uvod

Jožefov problem je problem v informatiki in matematiki, ki je zelo podoben izštevanki. Udeleženci stojijo v krogu in čakajo na usmrtitev. Štetje se začne pri prvi osebi v krogu in se nadaljuje v določeni smeri tako, da večkrat preskočimo enako število ljudi in potem usmrtimo naslednjega, dokler ne ostane samo še poslednji. Cilj udeleženca izštevanke je, da se postavi na tisto mesto, kjer bo najdlje preživel.

2 Indukcija

Indukcija je način dokazovanja matematičnih trditev. Poteka na naslednji način. Recimo, da dokazujemo neko lastnost P za vsa naravna števila. Naj $P(n)$ označuje trditev, da lastnost P velja za naravno število n. Vsak dokaz z indukcijo vključuje naslednje korake.
Baza indukcije. Dokažemo $P(1)$.
Indukcijska predpostavka. Naj bo k poljubno naravno število, predpostavimo, da velja $P(k)$.
Indukcijski korak. Z indukcijsko predpostavko dokažemo, da velja tudi $P(k+1)$.

S tem dokažemo, da velja $P(n)$ za vsako naravno število n. Sedaj pokažimo dva zgleda uporabe indukcije.

Zgled 2.1. *Dokažimo, da za vsako naravno število k velja $6 \mid 5^{2k-1}+1$. Najprej dokažemo bazni primer $k = 1$. To preverimo z računom $5^{2\cdot 1-1} + 1 = 5 + 1 = 6$, kar je deljivo s 6, torej bazni primer drži. Sledi indukcijski korak. Indukcijska predpostavka je, da trditev velja za nek $k \in \mathbb{N}$, torej da $6 \mid 5^{2k-1} + 1$. Število $5^{2k-1} + 1$ je deljivo s 6, zato je oblike $5^{2k-1} + 1 = 6l$ za neko naravno število l. Iz tega lahko izrazimo $5^{2k-1} = 6l - 1$. Dokazati je treba, da je $6 \mid 5^{2(k+1)-1} + 1$. Sledi*

$$5^{2(k+1)-1} + 1 = 5^{2k+1} + 1 = 5^{2k-1} \cdot 5^2 + 1 = (6l-1) \cdot 5^2 + 1 = 6l \cdot 25 - 24 = 6 \cdot (25l - 4),$$

kar pomeni, da $6 \mid 5^{2k-1} + 1$ in zaključi indukcijski korak.

Zgled 2.2. *Društvo DMFA Slovenije gospoda profesorja Jana obdari z neskončno mnogo kovanci za 2 € in neskončno mnogo bankovci za 5 €. Jan želi kupiti malico za tekmovalce na državnem tekmovanju iz matematike, ki stane n €. Dokažimo, da za $n \geqslant 4$ profesor Jan na blagajni lahko plača točno ceno.*

Ločeno obravnavamo soda in liha števila n. Pri dokazovanju uporabimo princip indukcije. Najprej dokažimo bazo indukcije $n = 4$ za sode n. Z dvema kovancema za 2 € lahko dobimo 4 €. Nadaljujemo z indukcijskim korakom za soda števila. Recimo, da lahko za neko sodo število n izvedemo želeno plačilo. Iz

tega sledi, da lahko izvedemo plačilo tudi za naslednje sodo število, saj lahko le doplačamo $2\,€$*. Prvotno trditev smo tako dokazali za soda števila* n*.*

Oglejmo si še bazni primer $n = 5$ *za liha števila* n*. Plačilo za najmanjši* $n = 5$ *lahko storimo z enim samim bankovcem po* $5\,€$*. Izvedimo še indukcijski korak. Če je plačilo mogoče plačati za neko liho število, lahko doplačamo* $2\,€$ *in dobimo ustrezno plačilo za naslednje liho število. Tezo smo dokazali za liha števila* n *in tako za vsa naravna števila* $n \geqslant 4$*.*

2.1 Močna indukcija

Denimo, da dokazujemo neko lastnost P za vsa naravna števila. Naj $P(n)$ označuje trditev, da lastnost P velja za naravno število n.
Baza indukcije. Dokažemo $P(1)$.
Indukcijska predpostavka. Naj bo k poljubno naravno število. Predpostavimo, da veljajo lastnosti za vse $P(1), P(2), \ldots, P(k)$.
Indukcijski korak. Z indukcijsko predpostavko dokažemo, da velja tudi $P(k+1)$.

S tem dokažemo, da velja $P(n)$ za vsako naravno število n. Hitro se da razmisliti, da sta indukcija in močna indukcija ekvivalentni metodi. Oglejmo si primer dokazovanja s slednjo.

Zgled 2.3. *Triangulacija je vsaka razdelitev* n*-kotnika brez samopresečišč, kjer je* n *naravno število, za katerega velja* $n \geqslant 3$*, na trikotnike z oglišči v* n*-kotniku, ki nimajo skupnih notranjosti. Dokažimo z močno indukcijo, da je vsaka triangulacija* n*-kotnika sestavljena iz* $n-2$ *trikotnikov.*

Najprej dokažimo bazo $n = 3$*. V tem primeru dobimo trikotnik, ki je razdeljen po edini možni razdelitvi, kar dokaže tezo za* $n = 3$*. Za indukcijski korak uporabimo močno indukcijo in tako predpostavimo, da trditev velja za vsa števila manjša ali enaka* n*. Želimo dokazati, da je* $(n+1)$*-kotnik sestavljen iz* $(n+1)-2 = n-1$ *trikotnikov. Vemo, da triangulacija vsebuje eno diagonalo, ki jo označimo z* D*. Diagonala* D *razdeli naš* $(n+1)$*-kotnik na* a*-kotnik in* b*-kotnik. Prvotni* $(n+1)$*-kotnik ima* $a+b-2$ *oglišč (odštejemo dve, ker sta dve oglišči (stičišči* a*-kotnika z* b*-kotnikom) šteti dvakrat). Lahko zapišemo* $a+b-2 = n+1$ *oz.* $a+b = n+3$*. Po indukcijski predpostavki ima* a*-kotnik* $a-2$ *trikotnikov in* b*-kotnik* $b-2$ *trikotnikov, celotna triangulacija našega* $(n+1)$*-kotnika pa* $(a-2)+(b-2)$ *oz.* $a+b-4$ *trikotnikov, kar je enako*

$$a+b-4 = (n+3)-4 = n-1,$$

in dokaže, da je $(n+1)$*-kotnik po triangulaciji sestavljen iz* $n-1$ *trikotnikov. To zaključi indukcijski korak.*

Sedaj imamo vse znanje, da se lahko lotimo našega osrednjega problema.

3 Jožefov problem

3.1 Zgodovinsko ozadje

Problem je poimenovan po vojskovodji in judovskem zgodovinarju Flaviju Jožefu, ki je živel v 1. stoletju. S svojimi štiridesetimi vojaki se je znašel ujet v jami, ki jo je obkolila rimska vojska. Odločili so se za medsebojni poboj, da jih Rimljani ne bi ubili, saj bi jim to bilo preveč pod častjo. Poboj je potekal na sledeči način. Postavili so se v krog. Vojak številka 1 je ubil vojaka za dva živa v levo - preskočil je sebe in še enega živega. Naslednji vojak po predhodno ubitem je storil enako in postopek se je nadaljeval, dokler naj bi ostal le še en vojak, ki bi moral ubiti samega sebe. Izkazalo se je, da je Jožef s še enim sojetnikom ostal zadnji živ. Iz neznanega razloga sta se raje, kot da bi se ubila, predala Rimljanom.

3.2 Poenostavitev problema

Za lažje reševanje poenostavimo problem. Spremenimo število vojakov, ki jih pri vsakem koraku preskočimo, tako da število preskočenih vojakov ni 2, kot pri izvornem Jožefovem problemu, ampak preskočimo samo

enega – tistega, ki ubije naslednjega. Zanima nas, kam se moramo postaviti, da bomo ostali zadnji živi. Naj bo število vseh vojakov v krogu enako n in $f(n)$ številka mesta, kamor se moramo postaviti, da ostanemo zadnji živi.

Najprej si skiciramo kroge z $n = 1, 2, \ldots, 16$ vojaki in pričnemo s simulacijo izštevanke. Rešitve prikažemo s tabelo, nato iz nje sklepamo odgovor in ga potem dokažemo.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$f(n)$	1	1	3	1	3	5	7	1	3	5	7	9	11	13	15	1

Najprej opazimo naslednjo lastnost. Pri n, ki je potenca naravnega ali ničelnega eksponenta števila dva, je zmagovalno mesto tisto, pri katerem začnemo simulacijo izštevanke.

Trditev 3.1. *Če je $n = 2^k$, kjer je $k \in \mathbb{N}_0$, je $f(n) = 1$.*

Dokaz. Trditev dokažimo z indukcijo, bazni primer je $k = 0$. Pri indukcijskem koraku predpostavimo, da za $n = 2^k$ velja $f(n) = 1$ in dokažemo trditev za $n = 2^{k+1}$. Vemo, da je $n = 2^{k+1} = 2 \cdot 2^k$. V prvem krogu umrejo vse sode številke, kar pomeni, da ostane $\frac{1}{2} \cdot 2^{k+1} = 2^k$ ljudi. Po tem ko so vse sode številke mrtve je na potezi vojak številka 1. V igri je takrat 2^k ljudi in vemo po indukcijski predpostavki, da bo vojak, ki začne zmagal. □

Sedaj dokažimo še dve formuli, s pomočjo katerih poiščemo končno rešitev. Začnimo pri sodih številkah vojakov.

Trditev 3.2. *Če je $n = 2k$ sodo število, velja $f(2k) = 2f(k) - 1$.*

Dokaz. V prvem krogu umrejo vsi vojaki s sodimi številkami in po njem je na potezi spet vojak številka 1. Število živih vojakov je tedaj $\frac{n}{2} = \frac{2k}{2} = k$. Preimenujmo preživele vojake po vrsti z oznakami $1, 2, 3, \ldots, k$. Po definiciji funkcije f zmaga vojak $f(k)$, saj je ostalo k vojakov, poimenovani so s prvimi k naravnimi števili ter je na potezi vojak številka 1. Opazimo, da če ima vojak po preimenovanju številko x, je imel pred poimenovanjem številko $2x - 1$. Sledi, da celotno igro zmaga vojak $2f(k) - 1$. Po definiciji funkcije f zmaga vojak $f(2k)$. V obeh primerih ima zmagovalec enako številko, zato lahko enačimo $2f(k) - 1 = f(2k)$. □

Podobno dokažemo tudi za liha števila.

Trditev 3.3. *Če je $n = 2k + 1$ liho število, velja $f(2k + 1) = 2f(k) + 1$.*

Dokaz. V prvem krogu umrejo vsi vojaki s sodimi številkami in vojak 1. Nato preimenujemo preživele vojake po vrsti z oznakami $1, 2, 3, \ldots, k$. Živih je k vojakov, zato je po definiciji funkcije f zmagovalec igre vojak $f(k)$. Celotno igro pa zmaga $f(2k + 1)$, torej lahko podobno kot prej enačimo $f(2k + 1) = 2f(k) + 1$. □

Trditev 3.4. *Če je $n = 2^k + l$, kjer velja $0 \leqslant l < 2^k$, je $f(n) = 1 + 2l$.*

Dokaz. Trditev dokažimo z močno indukcijo na n. Baza je dokazana v zgornji tabeli. Izvedimo indukcijski korak. Najprej obravnavajmo primer, ko je n sodo število. Tedaj je $n = 2^k + l$, pri čemer je l sod. Predpostavljamo, da je trditev resnična za vsa manjša števila od n. Število l lahko zapišemo kot $2t$. Ker je po indukcijski predpostavki $l < 2^k$, zapišemo $2 \cdot t < 2^k$ oz. $t < 2^{k-1}$. Računamo

$$\begin{aligned} f(n) &= f\left(2^k + l\right) = \\ &= f\left(2^k + 2t\right) = \\ &= f\left(2 \cdot \left(2^{k-1} + t\right)\right) = \\ &\overset{(1)}{=} 2 \cdot f\left(2^{k-1} + t\right) - 1 = \\ &\overset{(2)}{=} 2 \cdot (2 \cdot t + 1) - 1 = \\ &= 2 \cdot (l + 1) - 1 = \\ &= 2 \cdot l + 1. \end{aligned}$$

V koraku 1 smo uporabili trditev 3.2. V koraku 2 smo uporabili indukcijsko predpostavko. Izvedimo še indukcijski korak za liha števila n, torej ko je $n = 2^k + l$, pri čemer je l lih. Število l lahko zapišemo kot $2 \cdot t + 1$. Po indukcijski predpostavki velja $l < 2^k$, lahko zapišemo $2 \cdot t + 1 < 2^k$, zato velja tudi $2 \cdot t < 2^k$ oz. $t < 2^{k-1}$. Računamo

$$\begin{aligned} f(n) &= f\left(2^k + l\right) = \\ &= f\left(2^k + 2t + 1\right) = \\ &= f\left(2 \cdot \left(2^{k-1} + t\right) + 1\right) = \\ &\overset{(1)}{=} 2 \cdot f\left(2^{k-1} + t\right) + 1 = \\ &\overset{(2)}{=} 2 \cdot (2 \cdot t + 1) + 1 = \\ &= 2 \cdot l + 1. \end{aligned}$$

V koraku 1 smo uporabili trditev 3.3. V koraku 2 smo uporabili indukcijsko predpostavko. S tem je indukcija zaključena. □

Zanima nas še splošna formula za $f(n)$ v odvisnosti od n (brez zapisa $2l + 1$), zato ponovimo osnove logaritemske funkcije.

Definicija 3.1. *Naj bo a pozitivno realno število, ki ni enako 1, ter c pozitivno realno število. Potem definirajmo $\log_a c$ kot takšno realno število b, za katerega velja enakost $a^b = c$.*

Zgled 3.1. *Iz $2^5 = 32$ sledi $\log_2 32 = 5$.*

Vemo, da za $n = 2^k + l$, kjer je $0 \leqslant l < 2^k$, velja $f(n) = 2l + 1$ po trditvi 3.4. Iz enačbe $n = 2^k + l$ sledi $\log_2 n = \log_2(2^k + l)$, temu izrazu ocenimo spodnjo in zgornjo mejo. Pri tem upoštevamo, da je funkcija $g(x) = \log_2 x$ naraščajoča. Ugotovimo, da velja

$$\log_2(2^k + l) \geqslant \log_2(2^k + 0) = \log_2 2^k = k.$$

Zgornja meja je

$$\log_2(2^k + l) < \log_2(2^k + 2^k) = \log_2 n(2^{k+1}) = k + 1.$$

Sledi $\log_2 n \in [k, k + 1)$. To pomeni, da je $\lfloor \log_2 n \rfloor = k$. Tukaj smo uporabili naslednjo funkcijo, ki nam število zaokroži navzdol na najbližje celo število.

Definicija 3.2. *Realnemu številu a lahko s* ***funkcijo celi del*** *priredimo število $\lfloor a \rfloor$, ki je največje celo število b, za katerega velja $b \leqslant a$.*

Posledično je

$$n = 2^k + l = 2^{\lfloor \log_2 n \rfloor} + l.$$

Iz tega izrazimo $l = n - 2^{\lfloor \log_2 n \rfloor}$ in končno sledi

$$f(n) = 2l + 1 = 2\left(n - 2^{\lfloor \log_2 n \rfloor}\right) + 1.$$

S tem smo dokazali naslednjo trditev.

Trditev 3.5. *Naj bo v krogu n vojakov. Potem se moramo postaviti na mesto $2\left(n - 2^{\lfloor \log_2 n \rfloor}\right) + 1$, da v poenostavljenem Jožefovem problemu ostanemo zadnji živi.*

Poglejmo si primer uporabe.

Zgled 3.2. *Če je na taboru MaRS 28 astronavtov, izračunajmo, na katero mesto se moramo postaviti, da ostanemo zadnji živi. Izračunamo*

$$f(28) = 2l + 1 = 2\left(28 - 2^{\lfloor \log_2 28 \rfloor}\right) + 1 = 2\left(28 - 2^4\right) + 1 = 2(28 - 16) + 1 = 25,$$

kar pomeni, da 25. mesto zadošča, da ostanemo zadnji živi.

Glavno ugotovitev sedaj predstavimo z enostavnejšim zapisom.

Trditev 3.6. *Vrednost $f(n)$ v binarnem sistemu dobimo tako, da v binarnem zapisu števila n vodilno enico na levi strani premaknemo na zadnje mesto.*

Dokaz. Poljubno število lahko enolično zapišemo v binarnem sistemu kot $n = 2^k + l = \overline{1a_{k-1}\ldots a_1 a_0}_{(2)}$, kjer so števila a_i za $i = 1, 2, \ldots n-1$ iz množice $\{0, 1\}$, ter zmagovalno mesto kot $f(n) = 2l + 1$. Zapis 2^k predstavlja najvišjo potenco z osnovo 2, ki je manjša ali enaka n. Vemo tudi, da je l oblike

$$l = 2^{k-1} \cdot a_{k-1} + 2^{k-2} \cdot a_{k-2} + \cdots + 2^1 \cdot a_1 + 2^0 \cdot a_0.$$

Sledi

$$\begin{aligned} f(n) = 2l + 1 &= \\ &= 2 \cdot \left(2^{k-1} \cdot a_{k-1} + 2^{k-2} \cdot a_{k-2} + \cdots + 2^1 \cdot a_1 + 2^0 \cdot a_0\right) + 1 = \\ &= 2^k \cdot a_{k-1} + 2^{k-1} \cdot a_{k-2} + \cdots + 2^2 \cdot a_1 + 2^1 \cdot a_0 + 2^0 \cdot 1 = \\ &= \overline{a_{k-1}a_{k-2}\ldots a_1 a_0 1}_{(2)}, \end{aligned}$$

kar dokaže tezo. □

Zgled 3.3. *Na taboru MaRS je 28 astronavtov, kar lahko zapišemo kot $11100_{(2)}$. Ko izvedemo premik skrajno leve števke na skrajno desno stran, dobimo*

$$f(n) = 11001_{(2)} = 2^4 \cdot 1 + 2^3 \cdot 1 + 2^2 \cdot 0 + 2^1 \cdot 0 + 2^0 \cdot 1 = 25.$$

Opazimo, da se rezultat ujema z rezultatom, dobljenim s formulo za $f(n)$.

3.3 Vrnitev k osnovnemu problemu

S pomočjo metode indukcije smo torej izpeljali formulo za preskakovanje dveh oseb v krogu. V osnovi sicer Jožefov problem vključuje preskakovanje treh oseb, vendar za tako obliko problema trenutno še ni znano, kako bi zapisali splošno formulo za izračun, kdo preživi, znan je le algoritem. S predznanjem in na novo pridobljenim znanjem za zdaj tudi mi še nismo uspeli priti do splošne formule. Zato smo se odločili, da rešitev problema zapišemo še v binarnem sistemu.

4 Zaključek

Premeteni Jožef je očitno poznal način kako rešiti problem s preskakovanjem po dva vojaka, saj je ostal med zadnjima dvema preživelima. Njegova formula ostaja zapleten matematični problem, ki za zdaj še ni napisan v splošni formuli.

Literatura

[1] Wikipedija. Jožef Flavij. Pridobljeno 30. 7. 2026 s spletne strani: `https://sl.wikipedia.org/wiki/Jo%C5%BEef_Flavij`.

[2] Wikipedija. Josephus problem. Pridobljeno 31. 7. 2026 s spletne strani:`https://en.wikipedia.org/wiki/Josephus_problem`.

[3] Jakob Jurij Snoj. Indukcija. Pridobljeno 30. 7. 2026 s spletne strani: `https://http.rezultati.dmfa.si/Tekmovanja/MaSSA/Dokumenti/indukcija_predavanje.pdf`.

Kockarjev propad

Brin Osojnik, Naj Strmšek
Mentorica: *Nives Gošnjak*

Povzetek

V članku so predstavljene osnove verjetnostne teorije, s pomočjo katere smo rešili osnovni problem Kockarjevega propada (angleško *Gambler's ruin*). Za lažje razumevanje postopka reševanja so predstavljene tudi rekurzivne zveze s poudarkom na reševanju nekaterih enostavnejših zvez.

1 Uvod

Osrednji problem, ki ga v tem članku rešimo, se imenuje Kockarjev propad (angleško *Gambler's ruin*). V njem kockar igra igro na srečo, ki jo začne z nekim začetnim zneskom, vsako potezo pa se mu znesek poviša ali zniža za en kovanec – glede na to, ali ga zmaga ali zgubi. Verjetnost zmage je za vsako potezo enaka, prav tako so izidi potez med seboj neodvisni. Kockar igro igra, dokler ne doseže nekega končnega želenega zneska, ki je seveda višji od začetnega in je določen pred začetkom igre, ali pa mu zmanjka kovancev in bankrotira. Nas zanima, kolikšna je verjetnost, da kockarju uspe zaslužiti želen dobiček pred bankrotom in kako je ta vrednost odvisna od začetnega in končnega zneska ter same pravičnosti igre. Preden lahko rešimo ta problem, moramo najprej ugotoviti, kaj sploh je verjetnost, za lažje razumevanje nekaterih rezultatov pa bomo spoznali osnove rekurzivnih zvez.

2 Verjetnost

2.1 Osnovne definicije

Teorija verjetnosti se je razvila ravno zaradi iger na srečo, kjer so matematiki želeli ugotoviti, katere igre se jim najbolj splača igrati. Veda se je od takrat močno razširila, glavna ideja pa ostaja, da opazujemo kaj se dogaja pri nekem naključnem poizkusu, kot sta na primer met kovanca ali navadne kocke. Vsakemu možnemu rezultatu poizkusa pravimo izid, množicam izidov pa dogodki. Pri metu kocke so tako možni izidi, da pade število $1, 2, 3, 4, 5$ ali 6, medtem ko je en možen dogodek lahko to, da pade 6, lahko pa je dogodek tudi to, da pade sodo število, kar je unija izidov, ko pade $2, 4$ ali 6. Verjetnost definiramo kot funkcijo, ki vsakemu dogodku priredi vrednost, ki nam pove kako verjetno je, da se dogodek zgodi. Izkaže se, da so vse te vrednosti med 0 in 1, kjer 1 priredimo gotovim dogodkom, 0 pa nemogočim.

Definicija 2.1. *Verjetnostni prostor je trojica $(\Omega, \mathcal{A}, P)$, kjer je Ω množica vseh možnih izidov, $\mathcal{A}$ množica vseh dogodkov in $P : \mathcal{A} \to [0, 1]$ verjetnost.*

Definicija 2.2. *Nasprotni dogodek oz. komplement dogodka A se označi z A^c ali $\bar{A}$ in zajema vse izide v Ω, ki ne spadajo pod dogodek A.*

Definicija 2.3. *Presek dogodkov A_1 in A_2 se označi z $A_1 \cap A_2$ in predstavlja vse izide, ki se pojavijo tako v A_1 kot v A_2.*

Definicija 2.4. *Dogodek je vsebovan v drugem, če se vsak izid, ki se pojavi v prvem, pojavi tudi v drugem. Matematično to označimo kot $A \subseteq B$.*

Da je verjetnost smiselno definirana, mora kot funkcija zadoščevati nekaterim aksiomom.

Aksiom 1. *Za vsak dogodek $A \in \mathcal{A}$ velja $P(A) \geq 0$.*

Aksiom 2. $P(\Omega) = 1$.

Aksiom 3. *Za množico paroma disjunktnih dogodkov $A_1, A_2, ..., A_n$ velja*

$$P(A_1 + A_2 + ... + A_n) = P(A_1) + P(A_2) + ... + P(A_n).$$

Na podlagi teh aksiomov lahko izpeljemo še nekaj osnovnih posledic, ki nam pomagajo tako pri razumevanju kot tudi pri samem računanju verjetnosti.

Posledica 2.1. $P(\emptyset) = 0$.

Dokaz. V aksiom 3 vstavimo za vse disjunktne množice prazno množico n-krat in m-krat, kjer sta m in n različni naravni števili. Tako dobimo enačbo $nP(\emptyset) = mP(\emptyset)$, kar je mogoče le, če je $P(\emptyset) = 0$. □

Posledica 2.2. *Naj bosta A_1 in A_2 disjunktna dogodka, potem velja $P(A_1 \cup A_2) = P(A_1) + P(A_2)$.*

Dokaz. V aksiom 3 vstavimo za vse disjunktne množice, razen prvih dveh, prazne množice. □

Posledica 2.3. $P(\bar{A}) = 1 - P(A)$.

Dokaz. V posledico 2.2 vstavimo $A_1 = A^c$ in $A_2 = A$. □

Posledica 2.4. $0 \leq P(A) \leq 1$.

Dokaz. Ker je $P(\bar{A}) \geq 0$ in zaradi prejšnje posledice, sledi $1 - P(A) \geq 0$ oziroma $P(A) \leq 1$, po prvem aksiomu pa je tudi $P(A) \geq 0$.

□

Posledica 2.5. *Če je A vsebovan v B, potem velja $P(B) = P(A) + P(B \setminus A) \geq P(A)$.*

Dokaz. Množici A in $B \setminus A$ sta disjunktni in velja $B = A \cup (B \setminus A)$. Po prejšnji posledici dobimo verjetnost $P(B) = P(A) + P(B \setminus A)$. Ker je po prvem aksiomu $P(B \setminus A) \geq 0$, sledi $P(B) \geq P(A)$.

□

Posledica 2.6. *Za poljubni množici A in B velja $P(A \cup B) = P(A) + P(B) - P(A \cap B)$.*

Dokaz. Velja $A \cup B = A \cup (B \setminus A)$, pri čemer sta množici A in $B \setminus A$ disjunktni, zato velja enakost $P(A \cup B) = P(A) + P(B \setminus A)$. Nadalje velja $B = (B \setminus A) \cup (A \cap B)$, kjer sta množici ponovno disjunktni, zato dobimo $P(B) = P(B \setminus A) + P(A \cap B)$. Od tod izpeljemo

$$P(B \setminus A) = P(B) - P(A \cap B),$$

kar vstavimo v prvo enačbo in dobimo

$$P(A \cup B) = P(A) + P(B) - P(A \cap B).$$

□

2.2 Pogojna verjetnost

Pogojno verjetnost si najprej oglejmo na primeru, ko imamo v vreči 13 kroglic, od katerih je 7 črnih in 6 belih. Če vemo samo to in iz vreče na slepo povlečemo eno od kroglic, bo ta z verjetnostjo $\frac{7}{13}$ črne barve. Sedaj pa dodajmo še podatek, da je 5 črnih kroglic tudi mehkih, ena mehka pa je tudi bela. Če sedaj izvlečemo eno od kroglic, ki je na otip mehka, se verjetnost, da bo črne barve spremeni. Vseh mehkih kroglic je le 6, od tega je 5 črnih, torej je verjetnost, da je kroglica črna, pri pogoju, da je mehka, enaka $\frac{5}{6}$. Ideja kako izračunamo spremembo izhaja iz tega, da se je število vseh možnih izidov zmanjšalo le na tiste, ki so zadostovali našemu pogoju, v tem primeru, da je kroglica bila mehka. Prav tako smo za uspešne izide upoštevali le tiste, ki zadoščajo obema pogojema, v tem primeru, da je kroglica mehka in črna.

Definicija 2.5. *Naj bosta A in B dva možna dogodka in naj bo $P(B) \neq 0$. Verjetnost dogodka A pri pogoju, da se je zgodil dogodek B označujemo s $P(A|B)$ in izračunamo po formuli*

$$P(A|B) = \frac{P(A \cap B)}{P(B)}.$$

Izrek 2.1 (Izrek o popolni verjetnosti)**.** *Naj bodo $A_1, A_2, \ldots, A_n$ paroma disjunktni dogodki, za katere velja $\bigcup_{i=1}^{n} A_i = \Omega$ in $P(A_i) > 0$ za vsak i. Tedaj za poljuben dogodek B velja*

$$P(B) = \sum_{i=1}^{n} P(B|A_i)\, P(A_i).$$

Dokaz. Iz pogoja, da je unija vseh dogodkov A_i enaka Ω, sledi

$$B = B \cap \Omega = B \cap \left(\bigcup_{i=1}^{n} A_i \right) = \bigcup_{i=1}^{n} (B \cap A_i).$$

Ker so dogodki A_i paroma disjunktni, so paroma disjunktni tudi dogodki $B \cap A_i$, saj za $i \neq j$ velja

$$(B \cap A_i) \cap (B \cap A_j) = B \cap (A_i \cap A_j) = B \cap \emptyset = \emptyset.$$

Od tod po aksiomu 3 dobimo

$$P(B) = P\left(\bigcup_{i=1}^{n} (B \cap A_i) \right) = \sum_{i=1}^{n} P(B \cap A_i).$$

Po definiciji pogojne verjetnosti je $P(B|A_i) = \frac{P(B \cap A_i)}{P(A_i)}$. Zato velja $P(B \cap A_i) = P(B|A_i)\, P(A_i)$. Če to enakost vstavimo v zgornjo vsoto, dobimo izrek o popolni verjetnosti

$$P(B) = \sum_{i=1}^{n} P(B|A_i)\, P(A_i).$$

□

Poseben primer izreka je, ko za paroma disjunktne dogodke uporabimo kar dogodka A in $\bar{A}$, katerih unija je po definiciji enaka Ω. Najpogosteje nam to olajša računanje, ko lahko verjetnost dogodka B razdelimo na neke začetne pogoje in v tem primeru dobimo

$$P(B) = P(A)P(B|A) + P(\bar{A})P(B|\bar{A}).$$

Računanje pogojne verjetnosti po definiciji lahko zaradi potrebe po izračunu verjetnosti presekov dveh dogodkov hitro postane zahtevno, zato poznamo še eno formulo, ki nam delo občasno olajša.

Izrek 2.2 (Bayesov izrek)**.** *Naj bosta A in B dogodka in naj $P(A) \neq 0$ ter $P(B) \neq 0$. Potem velja*

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)}.$$

Dokaz. Iz definicije pogojne verjetnosti dobimo enačbi $P(A|B) = \frac{P(A\cap B)}{P(B)}$ in $P(B|A) = \frac{P(A\cap B)}{P(A)}$. Prvo enačbo pomnožimo s $P(A)$ in drugo s $P(B)$ ter dobimo $P(A|B)P(B) = P(A \cap B) = P(B|A)P(A)$. Skrajni strani enakosti delimo z $P(A)$ in dobimo želen rezultat. □

3 Rekurzija

Med reševanjem problema Kockarjevega propada bomo ugotovili, da njegovo rešitev najlažje najdemo s pomočjo rekurzije oz. rekurzivnih zvez. V nadaljevanju si bomo pogledali kako te najlažje in najhitreje rešimo.

3.1 Osnovne definicije

Definicija 3.1. *Zaporedje realnih števil je preslikava a iz $\mathbb{N}_0$ v $\mathbb{R}$. Pri tem pa n-ti člen zaporedja označimo z a_n.*

Definicija 3.2. *Rekurzivna zveza je matematično pravilo, ki vsak člen zaporedja definira s pomočjo enega ali več prejšnjih členov.*

Definicija 3.3. *Linearna homogena rekurzivna zveza k-tega reda s konstantnimi koeficienti je enačba oblike*

$$a_n = c_1a_{n-1} + c_2a_{n-2} + \cdots + c_ka_{n-k},$$

kjer so $c_1, c_2, \ldots, c_k$ realne konstante, ne vse enake 0. Za natančno določenost zaporedja moramo podati tudi k robnih pogojev – to so natančne vrednosti za k členov zaporedja.

Zgled 3.1. *Fibonaccijevo zaporedje je lep primer rekurzivne zveze, saj je vsak nov člen definiran s pomočjo prejšnjih dveh. Pravilo za izračun poljubnega (n-tega) člena je povsem preprosto, sešteti moramo le njegova dva neposredna predhodnika. S formulo to rekurzivno pravilo zapišemo kot*

$$F_n = F_{n-1} + F_{n-2}.$$

Začetni vrednosti zaporedja sta določeni s $F_0 = 0$ in $F_1 = 1$. Z upoštevanjem tega pravila zaporedje gradimo korak za korakom, tako za drugi člen seštejemo 0 in 1 ter dobimo 1. Za tretji člen seštejemo 1 in 1 ter dobimo 2 in za četrtega seštejemo 1 in 2 ter dobimo 3. Če ta postopek nadaljujemo, dobimo znano zaporedje števil $0, 1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots$

Problem tako podanega zaporedja je, da za izračun poznejših členov zaporedja potrebujemo tudi veliko predhodnih členov. Že na primeru Fibonaccijevega zaporedja hitro opazimo, da če želimo izvedeti 50. Fibonaccijevo število, bi postopoma morali izračunati vse predhodne člene. Takšen način reševanja problema je seveda zamuden, zato si bomo pri reševanju našega problema pomagali s karakterističnimi enačbami.

Definicija 3.4. *Karakteristična enačba za linearno homogeno rekurzivno zvezo s konstantnimi koeficienti je algebraična enačba, ki jo dobimo z vstavljanjem nastavka $a_n = r^n$ (kjer je $r \neq 0$) v rekurzivno zvezo.*

Reševanje rekurzivnih zvez je v splošnem lahko zahtevno, kar pa ne velja za linearne homogene rekurzije s konstantnimi koeficienti. Pri njihovem reševanju uporabimo dve ključni ideji. Iščemo rešitve eksponentne oblike $a_n = r^n$, kjer je r konstanta, hkrati pa je poljubna linearna kombinacija dveh rešitev linearne homogene rekurzije je prav tako rešitev.

Ko vstavimo $a_n = r^n$ v rekurzivno zvezo $a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$, dobimo

$$r^n = c_1 r^{n-1} + c_2 r^{n-2} + \cdots + c_k r^{n-k}.$$

Če celotno enačbo delimo z r^{n-k} in vse člene prenesemo na levo stran, dobimo karakteristično enačbo

$$r^k - c_1 r^{k-1} - c_2 r^{k-2} - \cdots - c_k = 0.$$

Rešitve r te enačbe se imenujejo karakteristični koreni in nam omogočajo zapis eksplicitne formule za n-ti člen.

3.2 Rekurzivne zveze drugega reda

Posvetimo se rekurzivnim zvezam drugega reda, saj se pojavljajo pri reševanju našega glavnega vprašanja. Slednje imajo obliko $a_n = c_1 a_{n-1} + c_2 a_{n-2}$, njihova karakteristična enačba pa je kvadratna enačba oblike $r^2 - c_1 r - c_2 = 0$.

Definicija 3.5. *Zaporedje je rešitev rekurzivne zveze, če vsak člen zaporedja zadošča dani enačbi in zanj veljajo dani robni pogoji.*

Zgled 3.2. *Vrnimo se znova na Fibonaccijevo zaporedje. Zanj velja rekurzivna zveza $F_n = F_{n-1} + F_{n-2}$, z začetnimi pogoji $F_0 = 0$ in $F_1 = 1$. Fibonaccijevo zaporedje je torej rešitev te rekurzivne zveze. Po drugi strani lahko spremenimo začetne pogoje, na primer $F_0 = 2$ in $F_1 = 3$. V tem primeru Fibonaccijevo zaporedje ni rešitev te zveze, saj ne zadošča njenim začetnim pogojem.*

Kot že omenjeno, lahko s pomočjo rešitev karakterističnih enačb najdemo eksplicitno formulo za člene zaporedja, ki je rešitev njej pripadajoči rekurzivni zvezi. Izkaže se tudi, da je rešitev enolična in natančno določena s karakterističnimi koreni in začetnimi pogoji. V našem primeru ima enačba natanko dve rešitvi, ki jih znamo izračunati s pomočjo formule za kvadratno enačbo. Glede na to, ali sta rešitvi različni ali enaki, ločimo ekspliciten zapis rešitve rekurzivne zveze na dva primera.

Izrek 3.1. *Naj bosta c_1, c_2 realni konstanti in predpostavimo, da ima enačba $r^2 - c_1 r - c_2 = 0$ dve različni ničli r_1 in r_2. Zaporedje $\{a_n\}$ je rešitev rekurzivne zveze $a_n = c_1 a_{n-1} + c_2 a_{n-2}$ natanko tedaj, ko velja*

$$a_n = \alpha_1 r_1^n + \alpha_2 r_2^n$$

za vse $n \geq 0$, kjer sta α_1, α_2 konstanti, ki jih določimo iz začetnih pogojev.

Dokaz. Najprej dokažimo, da je zaporedje oblike $a_n = \alpha_1 r_1^n + \alpha_2 r_2^n$ res rešitev rekurzivne zveze. Ker sta r_1 in r_2 ničli karakteristične enačbe, velja $r_1^2 = c_1 r_1 + c_2$ in $r_2^2 = c_1 r_2 + c_2$. Z vstavljanjem nastavka v desno stran rekurzivne zveze dobimo

$$\begin{aligned} c_1 a_{n-1} + c_2 a_{n-2} &= c_1(\alpha_1 r_1^{n-1} + \alpha_2 r_2^{n-1}) + c_2(\alpha_1 r_1^{n-2} + \alpha_2 r_2^{n-2}) \\ &= \alpha_1 r_1^{n-2}(c_1 r_1 + c_2) + \alpha_2 r_2^{n-2}(c_1 r_2 + c_2) \\ &= \alpha_1 r_1^{n-2} r_1^2 + \alpha_2 r_2^{n-2} r_2^2 \\ &= \alpha_1 r_1^n + \alpha_2 r_2^n \\ &= a_n, \end{aligned}$$

pri čemer smo za tretjo enakost uporabili zgoraj omenjeni enakosti za r_1 in r_2.

Dokažimo še obratno in sicer, naj bo $\{a_n\}$ zaporedje, ki reši dano rekurzivno zvezo. Definirajmo tudi zaporedje $\{b_n\}$, da velja $b_n = \alpha_1 r_1^n + \alpha_2 r_2^n$, pri čemer sta α_1 in α_2 konstanti. Če želimo, da zaporedje zadošča

rekurzivni zvezi, mora zadostiti začetnim pogojem, te pa lahko izpeljemo iz že danega zaporedja $\{a_n\}$ in sicer $a_0 = b_0$ in $a_1 = b_1$. S pomočjo tega dobimo sistem enačb za α_1 in α_2

$$a_0 = b_0 = \alpha_1 + \alpha_2,$$
$$a_1 = b_1 = \alpha_1 r_1 + \alpha_2 r_2.$$

Iz prve enačbe izrazimo $\alpha_2 = C_0 - \alpha_1$ in vstavimo v drugo

$$b_1 = \alpha_1 r_1 + (b_0 - \alpha_1) r_2 = \alpha_1 (r_1 - r_2) + b_0 r_2.$$

Od tod poračunamo

$$\alpha_1 = \frac{b_1 - b_0 r_2}{r_1 - r_2} \quad \text{in} \quad \alpha_2 = \frac{b_0 r_1 - b_1}{r_1 - r_2}$$

Ker sta korena r_1 in r_2 različna, sta konstanti α_1 in α_2 dobro definirani in enolično določeni z začetnima pogojema $a_0 = b_0$ in $a_1 = b_1$. S tem dobimo zaporedje $b_n = \alpha_1 r_1^n + \alpha_2 r_2^n$, ki se z danim zaporedjem a_n ujema v prvih dveh členih ter po prvem delu dokaza zadošča isti rekurzivni zvezi. Ker je vsak nadaljnji člen obeh zaporedij enolično določen z isto rekurzivno formulo iz predhodnih dveh členov, sta zaporedji a_n in b_n identični za vsak $n \geq 0$, s čimer je dokaz končan.

□

Zgled 3.3 (Izpeljava Binetove formule za Fibonaccijeva števila)**.** *Fibonaccijevo zaporedje zadošča rekurzivni zvezi $F_n = F_{n-1} + F_{n-2}$ z začetnima členoma $F_0 = 0$ in $F_1 = 1$. Njena karakteristična enačba je $r^2 - r - 1 = 0$. Rešitvi enačbe sta*

$$r_1 = \frac{1 + \sqrt{5}}{2} \quad \textit{in} \quad r_2 = \frac{1 - \sqrt{5}}{2},$$

kar nam za poljuben člen da $F_n = \alpha_1 \left(\frac{1+\sqrt{5}}{2}\right)^n + \alpha_2 \left(\frac{1-\sqrt{5}}{2}\right)^n$. Z vstavljanjem začetnih pogojev $F_0 = 0$ in $F_1 = 1$ dobimo sistem enačb

$$\alpha_1 + \alpha_2 = 0$$
$$\alpha_1 \left(\frac{1 + \sqrt{5}}{2}\right) + \alpha_2 \left(\frac{1 - \sqrt{5}}{2}\right) = 1.$$

Rešitev tega sistema je $\alpha_1 = \frac{1}{\sqrt{5}}$ in $\alpha_2 = -\frac{1}{\sqrt{5}}$, kar nam da znano eksplicitno ***Binetovo formulo***

$$F_n = \frac{1}{\sqrt{5}} \left(\frac{1 + \sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}} \left(\frac{1 - \sqrt{5}}{2}\right)^n.$$

Izrek 3.2. *Naj bosta c_1, c_2 realni konstanti ter $c_2 \neq 0$. Če ima enačba $r^2 - c_1 r - c_2 = 0$ le en koren r_0 z večkratnostjo 2, je zaporedje $\{a_n\}$ rešitev rekurzije $a_n = c_1 a_{n-1} + c_2 a_{n-2}$ natanko tedaj, ko velja:*

$$a_n = \alpha_1 r_0^n + \alpha_2 n r_0^n$$

za vse $n \geq 0$, kjer sta α_1, α_2 konstanti.

Izrek bomo pustili brez dokaza, ideja pa je enaka kot v izreku 3.1.

Zgled 3.4. *Rešimo rekurzivno zvezo $a_n = 6a_{n-1} - 9a_{n-2}$ pri začetnih pogojih $a_0 = 1$ in $a_1 = 6$. Karakteristična enačba je $r^2 - 6r + 9 = (r-3)^2 = 0$ ki ima eno samo dvojno rešitev $r_0 = 3$. Splošna rešitev je torej*

$$a_n = \alpha_1 3^n + \alpha_2 n 3^n.$$

Iz začetnih pogojev $a_0 = 1$ in $a_1 = 6$ dobimo sistem dveh enačb

$$a_0 = \alpha_1 = 1$$
$$a_1 = 3\alpha_1 + 3\alpha_2 = 6.$$

Od tod sledi $\alpha_1 = 1$ in $\alpha_2 = 1$. Končna rešitev rekurzivne zveze je tako $a_n = 3^n + n3^n = (1+n)3^n$.

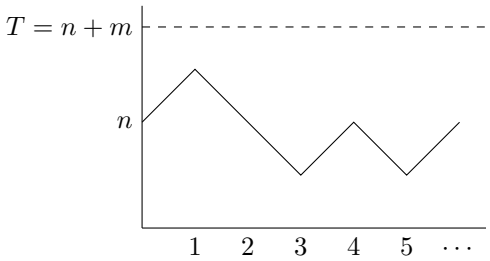
4 Kockarjev propad

Vrnimo se na naš osrednji problem, kjer kockar igra igro na srečo in se postavimo v vlogo kockarja. Za začetek reševanja tega problema je dobro naše podatke o igri natančneje matematično opisat in si jih označiti.

Definicija 4.1. *Naj bo $p \in [0,1]$ verjetnost zmage v vsaki potezi igre na srečo. Naj bosta n in m naravni števili, pri čemer z n označujemo svoj začetni znesek in z m želen dobiček. Naj bo $T = n+m$ končna vsota denarja, ki jo želimo osvojiti. Potem pravimo, da igro zmagamo, če nam uspe priti do želenega zneska T kovancev, preden bankrotiramo. Če se prej zgodi slednje, pravimo, da igro izgubimo. Dogodek zmage igre označujemo z Z.*

Zgled 4.1. *Poglejmo si takšno igro na primeru ameriške rulete, kjer je na kolesu 38 polj, od tega 18 črnih in 18 rdečih, 2 pa sta zeleni. Verjetnost zmage v posamezni potezi pri stavi na črna ali rdeča polja je enaka $p = \frac{18}{38} = \frac{9}{19} \approx 0,473$. Če vzamemo $n = 100$ € in $m = 100$ €, potem je $T = 200$ €. Zanima nas kolikšna je verjetnost, da si priigramo 100 € dobička, preden izgubimo začetnih 100 €.*

Potek igre si lahko za lažjo predstavo narišemo kot graf, kjer spremljamo količino denarja po posamezni potezi. Po pravilih igre vemo, da si pri vsaki potezi z verjetnostjo p priigramo en kovanec, z verjetnostjo $1-p$ pa ga izgubimo. Igro zmagamo, če na grafu zadanemo zgornjo mejo označeno z $T = n+m$ in izgubimo, če zadanemo spodnjo mejo 0 kovancev. Pri tem je vredno omeniti, da to nista edina možna izida igre, saj bi se lahko zgodilo, da nobene od mej ne zadanemo in igramo igro v neskončnost, čemur se bomo posvetili kasneje.



Skladno s tem definirajmo oznako D_i, ki označuje količino denarja po i-ti potezi. Pri tem je začetna količina denarja označena z D_0.

Izkaže se, da bomo problem najhitreje rešili, če pri fiksnem T opazujemo verjetnost zmage, glede na začetno količino denarja. To najlažje označimo kot $P_n = P(Z|D_0 = n)$ verjetnost, da dosežemo T kovancev, pri čemer začnemo z n kovanci. Dobimo zaporedje, katerega člene bi radi izračunali v splošnem, saj imamo potem rešitev našega problema za poljubne n in m.

Trditev 4.1. *Za zaporedje $\{P_n\}$ velja rekurzivna zveza $P_n = pP_{n+1} + (1-p)P_{n-1}$, z robnima pogojema $P_0 = 0$ in $P_T = 1$. Pri tem je p verjetnost zmage v posamezni potezi.*

Dokaz. Najprej preverimo smiselnost robnih pogojev. S P_0 označujemo verjetnost zmage, pri čemer smo začeli brez denarja. Po pravilih naše igre to pomeni, da smo že bankrotirali in igro končali, torej je verjetnost zmage res enaka 0. Podobno razmislimo, da P_T označuje verjetnost zmage, pri čemer smo začeli s T kovanci. Ker igro zmagamo takoj, ko dosežemo T kovancev, smo tokrat zmagali že pred samim začetkom, torej je verjetnost res enaka 1.

Težji del je dokazati rekurzivno zvezo, ki velja za ostale člene zaporedja. Pri tem je vredno omeniti, da nas členi poznejši od P_T v resnici ne zanimajo, saj igro vedno začnemo z manj kovanci, kot jih želimo osvojiti za zmago. Pri dokazu rekurzivne zveze si bomo pomagali z razdelitvijo prve poteze igre na dva možna izida in sicer na dogodek A, ki označuje zmago v prvi potezi, ki se zgodi z verjetnostjo p, in seveda $\bar{A}$, ki označuje poraz v prvi potezi in se posledično zgodi z verjetnostjo $1-p$. Ko sedaj razpišemo definicijo našega zaporedja,

dobimo

$$\begin{aligned} P_n &= P(Z|D_0 = n) \\ &= P(Z \cap A|D_0 = n) + P(Z \cap \bar{A}|D_0 = n) \\ &= P(A)P(Z|A \cap D_0 = n) + P(\bar{A})P(Z|\bar{A} \cap D_0 = n), \end{aligned}$$

pri čemer smo upoštevali definicijo pogojne verjetnosti in izrek 2.1. Enačbo lahko še poenostavimo s tem, da poznamo vrednosti $P(A)$ in $P(\bar{A})$. Poleg tega lahko pomislimo, da nam zmaga v prvi potezi in začetna vrednost n kovancev pove, da se bo naša količina denarja povečala na $D_1 = n + 1$. Podobno iz poraza v prvi potezi in enake začetne količine denarja izpeljemo $D_1 = n - 1$ in vse skupaj zapišemo kot

$$P_n = pP(Z|D_1 = n + 1) + (1 - p)P(Z|D_1 = n - 1).$$

Sedaj se spomnimo, da so poteze med seboj neodvisne, kar pomeni, da na verjetnost zmage v resnici ne vpliva, koliko denarja smo imeli v preteklosti, temveč le koliko ga imamo ta trenutek. To pomeni, da je verjetnost zmage ob pogoju, da smo imeli n denarja na začetku ali da smo imeli n denarja po prvi potezi, enaka in dobimo

$$\begin{aligned} P_n &= pP(Z|D_0 = n + 1) + (1 - p)P(Z|D_0 = n - 1) \\ &= pP_{n+1} + (1 - p)P_{n-1}. \end{aligned}$$

□

Od tukaj naprej moramo le še rešiti rekurzivno zvezo, ki jo prepišemo v $pP_{n+1} - P_n + (1 - p)P_{n-1} = 0$ in izpeljemo karakteristično enačbo

$$pr^2 - r + 1 - p = 0.$$

Dobimo rešitvi $r_1 = \frac{1-p}{p}$ in $r_2 = 1$ ter opazimo, da sta enaki le za primer $p = \frac{1}{2}$, ki ga bomo obravnavali posebej.

V primeru, ko igra ni pravična, torej $p \neq \frac{1}{2}$ po izreku 3.1 dobimo formulo

$$P_n = A\left(\frac{1-p}{p}\right)^n + B \cdot 1^n = A\left(\frac{1-p}{p}\right)^n + B.$$

S pomočjo začetnih pogojev dobimo sistem enačb

$$\begin{aligned} P_0 = 0 &= A + B, \\ P_T = 1 &= A\left(\frac{1-p}{p}\right)^T + B. \end{aligned}$$

Iz prve enačbe dobimo $A = -B$, kar nam z vstavljanjem v drugo enačbo da

$$\begin{aligned} A &= \frac{1}{\left(\frac{1-p}{p}\right)^T - 1} \quad \text{in} \\ B &= \frac{-1}{\left(\frac{1-p}{p}\right)^T - 1}. \end{aligned}$$

Enačbo za splošni člen zaporedja lahko potem preoblikujemo v

$$P_n = \frac{\left(\frac{1-p}{p}\right)^n - 1}{\left(\frac{1-p}{p}\right)^T - 1}.$$

S tem lahko natančno izračunamo verjetnost zmage v vsaki nepravični igri v odvisnosti od začetnega člena in želene končne vrednosti. Vseeno pa ta enačba ni najlepša, zaradi česar si je težko predstavljati, kako zelo se vrednosti spreminjajo v odvisnosti od posameznih spremenljivk. Enačbo bi zato radi olepšali in verjetnost zmage le omejili navzgor, najraje v primeru nepravične igre, ko verjetnost ni na naši strani. V tem primeru velja poenostavitev

$$\begin{aligned} P_n &= \frac{\left(\frac{1-p}{p}\right)^n - 1}{\left(\frac{1-p}{p}\right)^T - 1} \\ &\leq \frac{\left(\frac{1-p}{p}\right)^n}{\left(\frac{1-p}{p}\right)^T} \\ &= \frac{1}{\left(\frac{1-p}{p}\right)^m} \\ &= \left(\frac{p}{1-p}\right)^m. \end{aligned}$$

Za $p < \frac{1}{2}$ je $\frac{p}{1-p} < 1$, kar pomeni, da se verjetnost hitro manjša, ko povečujemo želen dobiček. Poleg tega je ta omejitev popolnoma neodvisna od začetnega zneska, kar pomeni, da je verjetnost za zmago velikih dobičkov majhna ne glede na to, kako bogati igro začnemo.

Zgled 4.2. *Vrnimo se na primer ameriške rulete. Ugotovili smo, da zanjo velja $p = \frac{9}{19}$, zanima pa nas verjetnost, da si priigramo dodatnih 100 €. Z vstavljanjem v dobljeno enačbo dobimo*

$$P(Z) \leq \left(\frac{9}{10}\right)^{100} \leq \frac{1}{37648},$$

pri čemer je verjetnost neodvisna od našega začetnega zneska. Rezultat se nam lahko zdi precej presenetljiv, saj imamo občutek, da je igra skoraj pravična, verjetnost za zmago pa vseeno izjemno hitro pada.

Poglejmo si še primer, ko je igra pravična, torej $p = \frac{1}{2}$. Kot smo že prej izračunali, imamo dvojno rešitev $r = r_{1,2} = 1$ in dobimo enačbo za splošni člen

$$P_n = An \cdot 1^n + B \cdot 1^n = An + B.$$

S pomočjo robnih pogojev $P_0 = 0 = B$ in $P_T = 1 = AT + B$ hitro izpeljemo $B = 0$ in $A = \frac{1}{T}$, kar nam da natančen rezultat

$$P_n = \frac{n}{T}.$$

Kot lahko vidimo je pri pravični igri verjetnost zmage veliko bolj odvisna od razmerja med začetnim in končnim zneskom, kot samo od želenega dobička.

Zgled 4.3. *Spomnimo se na igro Ameriške rulete, kjer si želimo priigrati 100 €. Kot smo že izračunali v zgledu 4.2, je verjetnost naše zmage, ne glede na našo začetno količino denarja, izredno majhna. Po drugi strani bi v primeru pravične igre, ki jo začnemo z 100 €, verjetnost zmage bila kar $\frac{100}{200} = \frac{1}{2}$. Če bi želeli verjetnost, da si prislužimo 100 €še povečati, bi lahko igro začeli z na primer 900 €, in bi verjetnost bila kar $\frac{900}{1000} = 0,9$.*

Pri reševanju tega problema smo ugotovili, da se glede na konstrukcijo igre lahko zgodi, da igre nikoli ne bi končali – ne bi dosegli končnega zneska, prav tako pa nikoli ne bi izgubili vsega svojega denarja. To je zelo nezaželen rezultat igre, saj bi si želeli, da sta zmaga in poraz drug drugemu nasprotna dogodka, kar bi se zgodilo, če igra v neskončnost ni mogoča.

Trditev 4.2. *Verjetnost, da bomo igro igrali v neskončnost, je za vsak p enaka 0.*

Dokaz. Za začetek si oglejmo robna primera. Če je $p = 0$, bomo v vsaki potezi denar izgubili, torej se bo igra očitno končala, podobno bomo pri $p = 1$ v vsaki potezi denar dobili, kar nas tudi vodi do konca igre. V nadaljevanju lahko zato predpostavimo, da velja $0 < p < 1$.

Označimo s F dogodek igranja igre v neskončnost in definirajmo novo zaporedje $\{Q_n\}$, kjer predstavlja $Q_n = P(F|D_0 = n)$ verjetnost igre v neskončnost, če smo igro začeli z n kovanci, pri fiksnem T. Podobno kot v trditvi 4.1 lahko enostavno izračunamo robna pogoja $Q_0 = 0$ in $Q_T = 0$. Tako v primeru, ko začnemo igro brez denarja, kot v primeru, ko jo začnemo z zmagovalno količino, je igra takoj končana, torej je verjetnost, da jo bomo igrali v neskončnost res enaka 0. Za vse vmesne člene lahko s podobno razlago kot v dokazu trditve 4.1 izpeljemo rekurzivno zvezo

$$Q_n = pQ_{n+1} + (1 - p)Q_{n-1}.$$

Opazimo, da ima enako karakteristično enačbo kot zaporedje $\{P_n\}$, razlikuje se le v robnih pogojih. Rešitve te karakteristične enačbe že poznamo, zato moramo zopet problem, ko je $p = \frac{1}{2}$ ločiti od primera $p \neq \frac{1}{2}$.

V primeru $p \neq \frac{1}{2}$ imamo enačbo za splošni člen

$$Q_n = A\left(\frac{1-p}{p}\right)^n + B.$$

Iz začetnega pogoja $Q_0 = 0 = A + B$ dobimo $A = -B$, kar lahko vstavimo v drug robni pogoj in dobimo

$$\begin{aligned} Q_T = 0 &= A\left(\frac{1-p}{p}\right)^T - A \\ &= A\left(\left(\frac{1-p}{p}\right)^T - 1\right). \end{aligned}$$

Ker vemo, da $p \neq \frac{1}{2}$, mora za enakost enačbe veljati $A = 0$, kar pomeni da je tudi poljuben člen zaporedja $Q_n = 0$.

Ko je igra pravična in je $p = \frac{1}{2}$, je enačba za splošni člen enaka

$$Q_n = An + B.$$

Iz robnih pogojev $Q_0 = 0 = B$ in $Q_T = 0 = An + B$ dobimo $A = B = 0$, kar pomeni, da je igra v neskončnost tudi pri pravični igri skoraj nemogoča. □

Za konec si poglejmo še, kaj se zgodi, če igro igramo brez zgornje omejitve. Za igro, kjer sreča ni na naši strani, se nam zdi, da bomo po dolgem igranju vedno izgubili denar, saj bomo po velikem številu potez več denarja izgubili, kot dobili. Nam mogoče zanimivejši primer se pojavi pri igranju pravične igre, saj gotovega bankrota ne moremo utemeljiti kot pri nepravični igri.

Trditev 4.3. *Če igramo pravično igro ($p = \frac{1}{2}$) in igramo brez zgornje meje – igra se konča le v primeru, ko ves denar izgubimo, potem je verjetnost, da se to zgodi enaka 1 ne glede na začetno vrednost denarja.*

Dokaz. Pomagali si bomo tako, da bomo najprej verjetnost omejili s pomočjo verjetnosti, ko imamo zgornjo mejo T, nato pa bomo pogledali kako se vrednost spremeni, če T pošljemo proti neskončnosti.

Označimo z B dogodek našega bankrota. Očitno lahko to verjetnost omejimo z

$$P(B) \geq P(B \text{ preden dosežemo T}).$$

Ker vemo, da igra, kjer imamo zgornjo mejo ne more iti v neskončnost, je nasprotni dogodek od bankrota preden dosežemo T kar enak temu, da dosežemo T preden bankrotiramo. V preteklih dokazih smo temu

dogodku rekli zmaga in ga označili z Z. Poleg tega, smo $P(Z)$ pri $p = \frac{1}{2}$ tudi izračunali in sicer je $P(Z) = \frac{n}{T}$. Zgornjo neenakost lahko zato zapišemo kot

$$\begin{aligned} P(B) &\geq 1 - P(Z) \\ &\geq 1 - \frac{n}{T}. \end{aligned}$$

V tem primeru je seveda n fiksen, kot obljubljeno pa T pošljemo proti neskončnosti in velja, da je

$$\lim_{T \to \infty} \left(1 - \frac{n}{T}\right) = 1,$$

kar pomeni, da je tudi $P(B) = 1$. □

Literatura

[1] K. H. Rosen, **Discrete mathematics & applications**, McGraw-Hill, 1999.

[2] T. Leighton, R. Rubinfeld, **Random walks**, Zapiski s predavanj, dostopno na `http://web.MIT.edu/neboat/Public/6.042/randomwalks.pdf`, 2006.

[3] J. Gravner, **Lecture notes for introductory probability**, Oddelek za matematiko, Univerza Kalifornije, 2010.

Tropski polkolobar in problem najkrajše poti

Val Čokl, Teja Zabukovec
Mentor*: Juš Kocutar*

Povzetek

Definirani so tropski polkolobar in tropski polinomi. Kot primer uporabe tropskih operacij je dokazano, da je mogoče izračunati dolžino najkrajše poti med dvema vozliščema v usmerjenem grafu z nenegativnimi utežmi kot element dovolj visoke tropske potence matrike sosednosti tega grafa.

1 Uvod

Na množici realnih števil definiramo nenavadni operaciji, poimenovani tropsko seštevanje in tropsko množenje, označeni z $\oplus$ in $\odot$. Ugotovimo, da imata podobne lastnosti kot običajno seštevanje in množenje, če množici $\mathbb{R}$ dodamo še element ∞, zato si tudi zaslužita takšni imeni. Kot primer uporabe teh definicij obravnavamo problem iz teorije grafov, ki je druga veja matematike. Ugotovimo namreč, da se tropski operaciji naravno pojavita pri problemu iskanja dolžine najkrajše poti med vozlišči v uteženem usmerjenem grafu.

2 Tropsko seštevanje in tropsko množenje

Definirajmo novo množico, ki bo ob vseh realnih številih vsebovala še en element, ki ga označimo s simbolom ∞, in jo bomo uporabljali v nadaljevanju. Element ∞ ima lastnost, da je večji od vseh realnih števil.

Definicija 2.1. *Definirajmo $\overline{\mathbb{R}} = \mathbb{R} \cup \{\infty\}$ in naj velja $x < \infty$ za vsak $x \in \mathbb{R}$.*

Za $x, y \in \overline{\mathbb{R}}$ naj $\min(x, y)$ označuje manjše izmed njiju. Velja torej $\min(x, y) = y$, če je $x \geq y$, drugače je $\min(x, y) = x$.

Definicija 2.2. *Tropsko seštevanje je operacija na množici $\overline{\mathbb{R}}$, definirana s predpisom $x \oplus y = \min(x, y)$.*

Lema 2.1. *Za operacijo tropskega seštevanja veljata asociativnost in komutativnost, obstaja tudi nevtralni element.*

Dokaz. Preverimo, da velja asociativnost

$$(x \oplus y) \oplus z = \min(\min(x, y), z) = \min(x, y, z) = \min(x, \min(y, z)) = x \oplus (y \oplus z).$$

Drži tudi komutativnost $x \oplus y = \min(x, y) = \min(y, x) = y \oplus x$. Za nevtralni element $y \in \overline{\mathbb{R}}$ mora veljati, da za vsak $x \in \overline{\mathbb{R}}$ drži, da $x \oplus y = \min(x, y) = x$. Zlahka preverimo, da ∞ zadošča tej lastnosti in je zato nevtralni element za operacijo $\oplus$. □

Omenimo še, da je ∞ edini element v $\overline{\mathbb{R}}$, ki ima inverz za operacijo $\oplus$, namreč ∞. Za poljuben $x \in \overline{\mathbb{R}} \backslash \{\infty\}$ in $y \in \overline{\mathbb{R}}$ velja $x \oplus y \leq x$. Njuna vsota zato ne more biti enaka nevtralnemu elementu ∞.

Definicija 2.3. *Definirajmo operacijo na množici $\overline{\mathbb{R}}$, imenovano tropsko množenje, s predpisom $x \odot y = x + y$, če sta $x, y \in \mathbb{R}$. Definiramo tudi $x \odot \infty = \infty \odot x = \infty$ za vsak $x \in \overline{\mathbb{R}}$.*

Tropsko množenje je na množici realnih števil definirano enako kot običajno seštevanje, zato si na $\mathbb{R}$ deli tudi njegove lastnosti.

Lema 2.2. *Tropsko množenje je asociativno in komutativno, obstaja nevtralen element. Vsak element $x \in \overline{\mathbb{R}}\backslash\{\infty\}$ ima inverz.*

Dokaz. Tropsko množenje je komutativno, saj velja $x \odot y = x + y = y + x = y \odot x$, tudi kadar je kateri izmed členov enak ∞. Preveriti moramo, ali za vse $x, y, z \in \overline{\mathbb{R}}$ velja asociativnost

$$(x \odot y) \odot z = (x + y) + z = x + (y + z) = x \odot (y \odot z).$$

To očitno velja, kadar so $x, y, z \in \mathbb{R}$. Kadar je vsaj eden izmed x, y ali z enak ∞, bo njegova vsota s poljubnim realnim številom enaka ∞, zato bosta obe strani zgornjega izraza enaki ∞, torej enaki. Nevtralni element je enak kot pri navadnem seštevanju, torej 0, za vsak $x \in \overline{\mathbb{R}}$ velja namreč $x \odot 0 = x$. Inverz imajo vsa števila razen ∞, torej razen nevtralnega elementa za seštevanje $\oplus$. □

Izrek 2.1. *Za operaciji tropskega seštevanja in množenja velja distributivnost.*

Dokaz. Naj bodo $x, y, z \in \overline{\mathbb{R}}$. Sledi

$$x \odot (y \oplus z) = x + \min(y, z) = \min(x + y, x + z) = (x \odot y) \oplus (x \odot z).$$

Tako preverimo veljavnost leve distributivnosti. Desna sledi iz komutativnosti tropskega množenja. □

Množici $\overline{\mathbb{R}}$ skupaj z operacijama $\oplus$ in $\odot$ pravimo tropski polkolobar. Z uporabo tropskih operacij namesto običajnih različic lahko še vedno računamo kot običajno zaradi vseh zgornjih pravil. Edina bistvena razlika je, da v splošnem ni inverzov za tropsko seštevanje.

Definicija 2.4. *Za $x \in \overline{\mathbb{R}}$ in $n \in \mathbb{N}_0$ označimo tropsko n-to potenco na sledeči način*

$$x^{\odot n} := \overbrace{x \odot x \odot \cdots \odot x}^{n\text{-krat}} = \overbrace{x + x + \cdots + x}^{n\text{-krat}} = nx.$$

Če je $n = 0$, naj bo $x^{\odot 0} := 0$.

Poljubno tropsko potenco dvočlenika lahko izračunamo na enostaven način.

Izrek 2.2. *Za $x, y \in \overline{\mathbb{R}}$ in $n \in \mathbb{N}$ velja $(x \oplus y)^{\odot n} = x^{\odot n} \oplus y^{\odot n}$.*

Dokaz. Predpostavimo najprej, da velja $x, y \in \mathbb{R}$. Prevedimo izraz z običajnimi operacijami,

$$(x \oplus y)^{\odot n} = n \cdot \min(x, y) = \min(nx, ny) = x^{\odot n} \oplus y^{\odot n}.$$

Izraz tudi velja, kadar je kateri izmed x in y enak ∞. □

2.1 Tropski kvadratni polinomi

Tropski polinom je funkcija iz $\overline{\mathbb{R}}$ v $\overline{\mathbb{R}}$ definirana enako kot običajni polinom, samo da klasični operaciji seštevanja in množenja zamenjamo s tropskima različicama.

Definicija 2.5. *Tropski polinom je funkcija $f : \overline{\mathbb{R}} \to \overline{\mathbb{R}}$ s predpisom $f(x) = \bigoplus_{i=0}^{n}(a_i \odot x^{\odot i})$ za $n \in \mathbb{N}_0$, $a_i \in \overline{\mathbb{R}}$ in $a_n \neq \infty$.*

Osredotočimo se na tropske kvadratne polinome. Z običajnimi operacijami lahko poljubni tropski kvadratni polinom zapišemo kot

$$(a \odot x^{\odot 2}) \oplus (b \odot x) \oplus c = \min(a + 2x, b + x, c),$$

kjer $a \neq \infty$. Gre torej za funkcijo, ki najde minimum treh linearnih funkcij. Linearne funkcije v izrazu imajo različne smerne koeficiente, zato se zagotovo sekajo.

Definicija 2.6. *Ničla tropskega polinoma* $f(x) = \bigoplus_{i=0}^{n}(a_i \odot x^{\odot i})$ *je točka* $x_0 \in \overline{\mathbb{R}}$*, za katero obstajata* $0 \leq j < k \leq n$ *tako, da* $f(x_0) = a_j \odot x_0^{\odot j} = a_k \odot x_0^{\odot k}$.

Ničla tropskega polinoma je torej točka, v kateri je minimum dosežen vsaj dvakrat. Je tudi točka, v kateri se graf odsekoma linearne funkcije »prelomi«.

Osredotočimo se na ničle tropskega kvadratnega polinoma. Opazimo, da je ∞ ničla, če in samo če je $c = \infty$. V tem primeru, če je tudi $b = \infty$, je ∞ edina ničla, če pa $b \neq \infty$ je druga ničla enaka presečišču $a + 2x$ in $b + x$, ki je enako $b - a$, torej ima polinom dve ničli.

Predpostavimo, da $c \neq \infty$, torej ∞ ni ničla. Izračunajmo ostale potencialne ničle, to so:

- $a + 2x = b + x$, kar velja, ko $x_1 = b - a$,
- $b + x = c$, kar velja, ko $x_2 = c - b$ in
- $a + 2x = c$, kar velja, ko $x_3 = \frac{c-a}{2}$.

Če je $b = \infty$ je x_3 edina ničla, zato predpostavimo, da velja $b \neq \infty$. Izračunajmo $b + x_3 = b + \frac{c-a}{2}$. S tem dobimo vrednost izraza $b + x$ pri presečišču $a + 2x$ in c. Če je $b + \frac{c-a}{2} \geq c$, potem ima polinom eno ničlo x_3. Če pa je $b + \frac{c-a}{2} < c$, potem ima polinom dve ničli x_1 in x_2.

Predpostavimo, da noben izmed koeficientov a, b ali c ni enak ∞. Vrednosti $a + c - 2b$ pravimo tropska diskriminanta, saj ima enake lastnosti kot navadna diskriminanta. Če velja $a + c - 2b > 0$, ima kvadratni polinom dve različni ničli. Če pa je izraz $a + c - 2b \leq 0$ pa ima kvadratni polinom eno ničlo.

Kot zanimivost omenimo »tropski osnovni izrek algebre«, ki pravi, da ima tropski polinom stopnje n natanko n ničel, štetih s primerno definicijo večkratnosti.

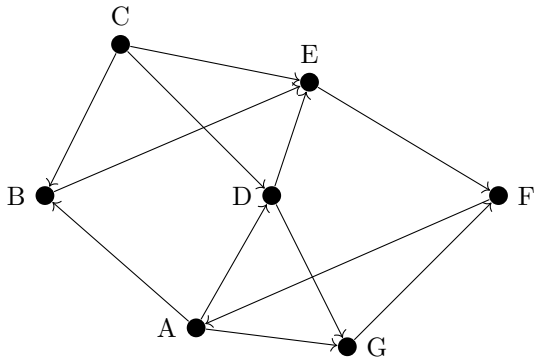
3 Problem najkrajše poti v usmerjenem grafu

V nadaljevanju predstavimo uporabo tropskih operacij na problemu iz teorije grafov. Vseskozi uporabljamo usmerjene grafe.

Definicija 3.1. *Usmerjen graf* $G = (V, E)$ *je urejen par, kjer je* $V = \{u_1, \ldots, u_n\}$ *neprazna končna množica vozlišč in* $E \subset V \times V$ *množica povezav med njimi.*

Grafe lahko ponazorimo z diagrami, tako da je vsako vozlišče točka. Vsaka povezava je urejen par (u, v), kar v diagramu predstavimo s puščico, ki poteka od vozlišča u do vozlišča v.

Primer 3.1. *Naj bo* $G = (V, E)$ *usmerjen graf, kjer je* $V = \{A, B, C, D, E, F, G\}$ *in s povezavami označenimi na naslednji sliki.*

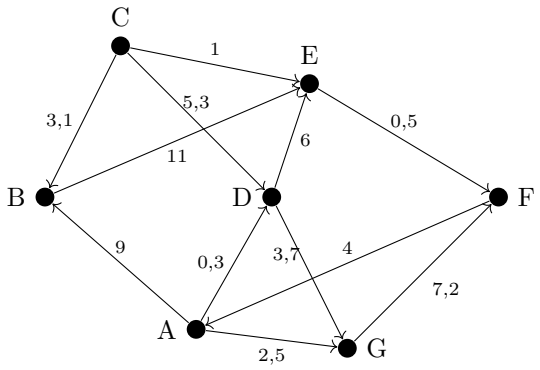


Slika 1: Usmerjen graf.

Povezavam lahko dodamo uteži in tako dobimo utežen graf. Vse uteži lahko predstavimo s preslikavo c iz množice povezav v $\overline{\mathbb{R}}_{\geq 0}$.

Definicija 3.2. *Naj bo G usmerjen graf in $c : E \to \overline{\mathbb{R}}_{\geq 0}$ preslikava. Paru (G, c) pravimo utežen graf.*

Primer 3.2. *Povezavam grafa iz primera 3.1 dodelimo uteži, tako da dobimo utežen graf.*



Slika 2: Utežen usmerjen graf.

Definicija 3.3. *Pot P med vozliščema v in w je zaporedje $v = u_0, u_1, \ldots, u_m = w$, kjer je $(u_i, u_{i+1}) \in E$ za vse $0 \leq i \leq m-1$.*

Dolžino poti P definiramo kot vsoto uteži vseh povezav, ki se pojavijo v poti, kar zapišemo kot

$$c(P) = \sum_{i=0}^{m-1} c(u_i, u_{i+1}).$$

Zanima nas kolikšna je najmanjša dolžina poti med poljubnima vozliščema i in j grafa G. Takšni poti pravimo najkrajša pot med i in j. Za enostavnejše računanje bomo grafe predstavili s kvadratnimi matrikami velikosti $n \times n$, kjer je n število vozlišč grafa.

Definicija 3.4. *Matrika A velikosti $p \times q$ je tabela s p vrsticami in q stolpci, kjer za vsak element $a_{ij} = [A]_{ij}$ velja $a_{ij} \in \overline{\mathbb{R}}$. Element a_{ij} se v matriki nahaja v i-ti vrstici in v j-tem stolpcu. Matrika je kvadratna, kadar velja $p = q$. Množico vseh matrik velikosti $p \times q$ označimo z $\overline{\mathbb{R}}^{p \times q}$.*

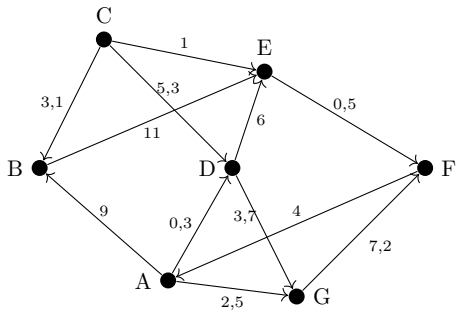
Primer 3.3. *Primer matrike $A \in \overline{\mathbb{R}}^{3\times 3}$ je*

$$A = \begin{bmatrix} 2 & 4 & 0{,}5 \\ \pi & \frac{1}{3} & 1 \\ -1 & 0 & \infty \end{bmatrix}.$$

Ta matrika je kvadratna, saj ima enako število vrstic in stolpcev.

Definicija 3.5. *Naj bo (G, c) utežen usmerjen graf in $n = |V|$. Definirajmo matriko $A(G) \in \overline{\mathbb{R}}_{\geq 0}^{n\times n}$ s predpisom $[A]_{ij} = c(i, j)$ če velja $i \neq j$ in $(i, j) \in E$ ter $[A]_{ij} = \infty$, če velja $i \neq j$ in $(i, j) \notin E$. Določimo tudi $[A(G)]_{ii} = 0$ za vsak i. Matriki $A(G)$ pravimo utežena matrika sosednosti uteženega grafa (G, c).*

Primer 3.4. *Naj bo G graf iz primera 3.2. Matriko sosednosti $A(G)$ tega grafa dobimo tako, da za vsak par vozlišč i, j v ustrezno mesto matrike vpišemo težo povezave (i, j), če ta obstaja. Če povezava ne obstaja, vpišemo ∞.*



$$A(G) = \begin{bmatrix} 0 & 9 & \infty & 0{,}3 & \infty & \infty & 2{,}5 \\ \infty & 0 & \infty & \infty & 11 & \infty & \infty \\ \infty & 3{,}1 & 0 & 5{,}3 & 1 & \infty & \infty \\ \infty & \infty & \infty & 0 & 6 & \infty & 3{,}7 \\ \infty & \infty & \infty & \infty & 0 & 0{,}5 & \infty \\ 4 & \infty & \infty & \infty & \infty & 0 & \infty \\ \infty & \infty & \infty & \infty & \infty & 7{,}2 & 0 \end{bmatrix}.$$

Slika 3: Utežen graf in njegova utežena matrika sosednosti.

Naj velja $A, B \in \overline{\mathbb{R}}^{n\times n}$.

Definicija 3.6. *Vsota matrik A in B je matrika $A + B \in \overline{\mathbb{R}}^{n\times n}$, za katero velja*

$$[A + B]_{ij} = [A]_{ij} + [B]_{ij}.$$

Definicija 3.7. *Produkt matrik A in B je matrika $AB \in \mathbb{R}^{n\times n}$, za katero velja*

$$[AB]_{ij} = \sum_{m=1}^{n} [A]_{im}[B]_{mj}.$$

Definicija 3.8. *Tropska vsota matrik A in B, sta $A, B \in \overline{\mathbb{R}}^{n\times n}$, je matrika $A \oplus B \in \overline{\mathbb{R}}^{n\times n}$, za katero velja*

$$[A \oplus B]_{ij} = [A]_{ij} \oplus [B]_{ij}.$$

Primer 3.5. *Naj bosta $A, B \in \overline{\mathbb{R}}^{2\times 2}$ naslednji matriki*

$$A = \begin{bmatrix} 2 & 5 \\ \infty & -4{,}3 \end{bmatrix}, \qquad B = \begin{bmatrix} 0 & \sqrt{2} \\ 4 & 7 \end{bmatrix}.$$

Njuna tropska vsota je matrika

$$A \oplus B = \begin{bmatrix} \min(2,0) & \min(5,\sqrt{2}) \\ \min(\infty,4) & \min(-4.3,7) \end{bmatrix} = \begin{bmatrix} 0 & \sqrt{2} \\ 4 & -4{,}3 \end{bmatrix}.$$

Opazimo, da pri tropskem seštevanju matrik v vsakem polju izberemo manjše izmed števil v pripadajočih poljih obeh matrik.

Definicija 3.9. *Naj bosta $A, B \in \overline{\mathbb{R}}^{n\times n}$ matriki. Tropski produkt matrik A in B je matrika $A \odot B \in \overline{\mathbb{R}}^{n\times n}$, za katero velja*

$$[A \odot B]_{ij} = \bigoplus_{m=1}^{n} ([A]_{im} \odot [B]_{mj}).$$

Primer 3.6. *Naj bosta A, B matriki iz primera 3.5. Njun tropski produkt $A \odot B \in \overline{\mathbb{R}}^{2\times 2}$ izračunamo po definiciji, na primer elementa $[A \odot B]_{11}$ in $[A \odot B]_{21}$*

$$[A \odot B]_{11} = \min([A]_{11} \odot [B]_{11},\ [A]_{12} \odot [B]_{21}) = \min(2+0,\ 5+4) = \min(2,9) = 2,$$

$$[A \odot B]_{21} = \min([A]_{21} \odot [B]_{11},\ [A]_{22} \odot [B]_{21}) = \min(\infty+0,\ -4.3+4) = \min(\infty,\ -0.3) = -0,3.$$

Na enak način izračunamo še preostale elemente in dobimo

$$A \odot B = \begin{bmatrix} 2 & 2+\sqrt{2} \\ -0{,}3 & 2{,}7 \end{bmatrix}.$$

Tropsko množenje matrik je asociativno in distributivno nad tropskim seštevanjem matrik.

Izkaže se, da problem najkrajše poti rešimo ravno s tropskim množenjem. To storimo tako, da matriko večkrat tropsko pomnožimo samo s sabo. Matriko, ki smo jo k-krat tropsko pomnožili, zapišemo tudi z $A^{\odot k}$.

Izrek 3.1. *Naj bo (G, c) utežen usmerjen graf z n vozlišči in naj bo $A(G) \in \overline{\mathbb{R}}_{\geq 0}^{n\times n}$ njegova utežena matrika sosednosti. Za $k \geq 1$, drži, da za vsaka $i, j \in V$ element $[A(G)]_{ij}^{\odot k}$ predstavlja dolžino najkrajše pot od vozlišča i do vozlišča j, ki vključuje največ k povezav. Iz tega sledi, da je $[A(G)]_{ij}^{\odot(n-1)}$ enako dolžini najkrajše poti od i do j.*

Dokaz. Za $i, j \in V$ in $k \geq 1$ naj $d_{ij}^{(k)} \in \overline{\mathbb{R}}$ označuje dolžino najkrajše poti od i do j z največ k povezavami. Ker so uteži zmeraj nenegativna realna števila ali ∞ velja $d_{ij}^{(1)} = c(i, j)$. Trdimo, da za vsak $k \geq 1$ in $i, j \in V$ velja rekurzivna zveza

$$d_{ij}^{(k+1)} = \min\{d_{im}^{(k)} + c(m, j) \mid m \in V\}.$$

Naj bo $i = u_0, \ldots, u_{l+1} = j$ najkrajša pot od i do j z največ $k + 1$ povezavami (torej $l \leq k$), ki ne ponavlja vozlišč. Opazimo, da je $i = u_0, \ldots u_l$ najkrajša pot od i do u_l z največ k povezavami. Zato velja

$$d_{ij}^{(k+1)} = \sum_{r=0}^{l} c(u_r, u_{r+1}) = d_{iu_l}^{(k)} + c(u_l, j) \geq \min\{d_{im}^{(k)} + c(m, j) \mid m \in V\}.$$

Dokažimo še drugo stran neenakosti. Recimo, da $\{d_{im}^{(k)} + c(m, j) \mid m \in V\}$ doseže minimum v $d_{ip}^{(k)} + c(p, j)$. Naj bo $i = w_0, \ldots, w_{q+1} = p$ pot od i do p dolžine največ k, za katero drži $\sum_{r=0}^{q} c(u_r, u_{r+1}) = d_{ip}^{(k)}$. Potem je $i = w_0, \ldots, w_{q+1}, j$ pot od i do j dolžine največ $k + 1$ zato po definiciji sledi

$$\min\{d_{im}^{(k)} + c(m, j) \mid m \in V\} = d_{ip}^{(k)} + c(p, j) = \sum_{r=0}^{q} c(w_r, w_{r+1}) \geq d_{ij}^{(k+1)}.$$

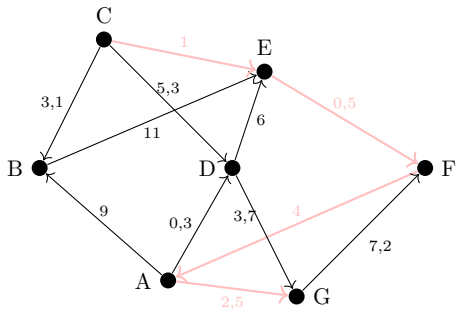
Rekurzivna zveza je dokazana. Za konec pokažimo še, da za vsak $k \geq 1$ velja $\left[A(G)^{\odot k}\right]_{ij} = d_{ij}^{(k)}$. Trditev lahko dokažemo z indukcijo, kot smo omenili na začetku dokaza, je res za $k = 1$. Recimo, da velja za nek $k \geq 1$. Potem imamo naslednjo verigo enakosti

$$\begin{aligned}
\left[A(G)^{\odot(k+1)}\right]_{ij} &= \left[A(G)^{\odot k} \odot A(G)\right]_{ij} \\
&= \oplus_{l=1}^{n} \left(\left[A(G)^{\odot k}\right]_{il} \odot [A(G)]_{lj}\right) \\
&= \min_{l=1,\ldots,n} \left(\left[A(G)^{\odot k}\right]_{il} + [A(G)]_{lj}\right) \\
&= \min_{l=1,\ldots,n} (d_{il}^{(k)} + c(l, j)) \\
&= d_{ij}^{(k+1)},
\end{aligned}$$

kar zaključi indukcijski korak in prvi del izreka.

Uteži v grafu G so nenegativne, zato lahko vsako najkrajšo pot spremenimo v najkrajšo pot, ki obišče vsako vozlišče največ enkrat. To je zato, ker mora vsak cikel, ki se pojavi v najkrajši poti, imeti težo 0. Zato med poljubnima vozliščema $i, j \in V$ obstaja najkrajša pot, ki vključuje največ n vozlišč oziroma $n - 1$ povezav. □

Ponazorimo izrek 3.1 na primeru 3.2. Najkrajša pot od vozlišča C do G je označena z roza barvo. Sestavlja jo zaporedje vozlišč C, E, F, A, G dolžine 8. To se sklada s poljem v tretji vrstici in sedmem stolpcu matrike $[A(G)]^{\odot 6}$, ki je prav tako enaka 8.



$$A(G)^{\odot 6} = \begin{bmatrix} 0 & 9 & \infty & 0{,}3 & 6{,}3 & 6{,}8 & 2{,}5 \\ 15{,}5 & 0 & \infty & 15{,}8 & 11 & 11{,}5 & 18 \\ 5{,}5 & 3{,}1 & 0 & 5{,}3 & 1 & 1{,}5 & 8 \\ 10{,}5 & 19{,}5 & \infty & 0 & 6 & 6{,}5 & 3{,}7 \\ 4{,}5 & 13{,}5 & \infty & 4{,}8 & 0 & 0{,}5 & 7 \\ 4 & 13 & \infty & 4{,}3 & 10{,}3 & 0 & 6{,}5 \\ 11{,}2 & 20{,}2 & \infty & 11{,}5 & 17{,}5 & 7{,}2 & 0 \end{bmatrix}.$$

Slika 4: Utežen graf in šesta tropska potenca njegove matrike sosednosti.

Literatura

[1] B. Sturmfels, M. Michałek, *Invitation to Nonlinear Algebra*, Graduate Studies in Mathematics Volume: 211; 2021; dostopno na `https://math.berkeley.edu/~bernd/gsm211.pdf`

Simetrični polinomi

Katja Anzeljc, Lovro Kastelic, Živa Lenarčič
Mentor*: Jure Kreže*

Povzetek

V članku so obravnavani simetrični polinomi. Razložene so njihove lastnosti ter računske operacije. Definiran je pojem leksikografske urejenosti. Dokazan je osnovni izrek o simetričnih polinomih, ki pravi, da se vsak simetrični polinom lahko zapiše kot polinom v elementarnih simetričnih polinomih.

1 Uvod

Neverjetni svet števil in krivulj odpirajo polinomi v več spremenljivkah. Da ne prehitimo lastnih misli, obnovimo znanje polinomov v eni spremenljivki. Zapišemo jih kot formalno vsoto členov, ki so sestavljeni iz realnih koeficientov $a_0, a_1, a_2, \ldots, a_n$ in formalne spremenljivke X, pri čemer velja $a_n \neq 0$. Definicija polinoma v eni spremenljivki z realnimi koeficienti f je

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0.$$

Množico polinomov v eni spremenljivki označimo z $\mathbb{R}[X]$. Oglejmo si polinome z več spremenljivkami. V njih poleg običajne X spremenljivke nastopajo tudi druge. Najprej definiramo polinome, ki imajo ob spremenljivki X še spremenljivko Y, potem pa posplošimo to definicijo na n spremenljivk. Množico polinomov z realnimi koeficienti v dveh spremenljivkah označimo z $\mathbb{R}[X, Y]$. Polinom z realnimi koeficienti v dveh spremenljivkah X in Y gledamo kot polinom v eni spremenljivki Y, ki ima za koeficiente polinome v spremenljivki X. Torej polinom $f \in \mathbb{R}[X, Y]$ lahko zapišemo kot

$$f(X, Y) = a_n(X) Y^n + \cdots + a_1(X) Y + a_0,$$

pri čemer so koeficienti a_i polinomi z realnimi koeficienti v spremenljivki X. Podobno velja tudi za polinome z več spremenljivkami, namreč polinom f v spremenljivkah $X_1, \ldots, X_n$ obravnavamo kot polinom v spremenljivki X_n, ki ima za koeficiente polinome v spremenljivkah $X_1, \ldots, X_{n-1}$. Množico polinomov v n spremenljivkah označimo z $\mathbb{R}[X_1, \ldots, X_n]$.

V članku definiramo leksikografsko urejenost, ki nam pomaga pri definiranju multistopenj in vodilnih koeficientov polinomov več spremenljivk, ter se seznanimo z računskimi operacijami polinomov. Spoznamo simetrične polinome, ki so posebna vrsta polinomov z več spremenljivkami. Definiramo elementarne simetrične polinome, ki so v določenem smislu osnovne gradbene enote simetričnih polinomov. Dokažemo osnovni izrek o simetričnih polinomih, ki pravi, da se lahko vsak simetrični polinom zapiše kot polinom v elementarnih simetričnih polinomih.

2 Leksikografska urejenost

2.1 Definicija

Označimo z $\mathbb{N}_0 = \mathbb{N} \cup \{0\} = \{0, 1, \ldots\}$ množico nenegativnih celih števil. Z $\mathbb{N}_0^n$ označimo množico n-teric nenegativnih celih števil.

Primerjali bi radi dve n-terici nenegativnih celih števil $\mathbf{i} = (i_1, i_2, \ldots, i_n)$ in $\mathbf{j} = (j_1, j_2, \ldots, j_n)$, kjer so člani $i_t,\ j_t \in \mathbb{N}_0$. Pogost način urejanja n-teric[1] je leksikografska urejenost. Ta ureja števila podobno kot so urejene besede v slovarjih. Besede najprej razdelimo po prvih črkah glede na njihovo mesto v abecedi. Besede, ki se začnejo na isto črko, potem dalje razvrstimo glede na drugo črko, potem glede na tretjo in tako dalje, dokler se beseda ne konča. Leksikografsko urejanje enako poteka tudi pri n-tericah nenegativnih celih števil z razliko, da imamo namesto črk številke. Začnemo tako, da pogledamo števili na prvi koordinati obeh n-teric. Če se razlikujeta, n-terici primerjamo kot bi primerjali ti dve števili, torej če je število i_1 večje od števila j_1, je tudi $\mathbf{i}$ večji od $\mathbf{j}$ in obratno. V primeru, da je število enako, pogledamo drugo koordinato, če velja $i_2 > j_2$, določimo $\mathbf{i} > \mathbf{j}$ in obratno. Ti dve števili potem že spet primerjamo, kot smo to storili za prvo koordinato. Če se tudi tukaj ne razlikujeta, se ponovno premaknemo na naslednje mesto. Postopek ponavljamo, dokler se števili ne razlikujeta oziroma dokler nam ne zmanjka mest. Če ugotovimo, da je $\mathbf{i}$ manjši od $\mathbf{j}$, to zapišemo kot $\mathbf{i} \prec \mathbf{j}$ oziroma $\mathbf{i} \succ \mathbf{j}$, če ugotovimo, da je $\mathbf{i}$ večji od $\mathbf{j}$. V nasprotnem primeru se zgodi, da so vse koordinate enake, potem sta tudi n-terici enaki, torej velja $\mathbf{i} = \mathbf{j}$. Če velja bodisi $\mathbf{i} \prec \mathbf{j}$ bodisi $\mathbf{i} = \mathbf{j}$, pišemo $\mathbf{i} \preceq \mathbf{j}$.

Za primer vzemimo 5-terici $\mathbf{i} = (1, 7, 3, 10, 5)$ in $\mathbf{j} = (1, 7, 6, 0, 2)$. Najprej pogledamo prvo koordinato, ta je pri obeh enaka številu 1. Števili na prvi koordinati sta enaki, zato pogledamo drugo koordinato, ki je v obeh 5-tericah enaka številu 7. Ker imamo dve enaki števili, pogledamo naslednjo koordinato. Na tretji koordinati ima $\mathbf{i}$ število 3, $\mathbf{j}$ pa število 6. Velja $3 < 6$, iz česar sledi $\mathbf{i} \prec \mathbf{j}$.

2.2 Lastnosti leksikografske urejenosti

Za nas so pomembne naslednje tri lastnosti leksikografske urejenosti, pri čemer velja $n \in \mathbb{N}$ in $\mathbf{i}, \mathbf{j}, \mathbf{k}, \mathbf{i}', \mathbf{j}' \in \mathbb{N}_0^n$:

1. (Tranzitivnost) Iz $\mathbf{i} \preceq \mathbf{j}$ in $\mathbf{j} \preceq \mathbf{k}$ sledi $\mathbf{i} \preceq \mathbf{k}$.
2. (Monotonost seštevanja) Naj velja $\mathbf{i} \preceq \mathbf{i}'$ in $\mathbf{j} \preceq \mathbf{j}'$. Sledi, da je $\mathbf{i} + \mathbf{j} \preceq \mathbf{i}' + \mathbf{j}'$. V primeru, da je $\mathbf{i} \prec \mathbf{i}'$ ali $\mathbf{j} \prec \mathbf{j}'$, velja $\mathbf{i} + \mathbf{j} \prec \mathbf{i}' + \mathbf{j}'$.
3. (Totalnost) Za vsaki dve n-terici $\mathbf{i}$ in $\mathbf{j}$ velja natanko eden izmed sledečih izrazov

$$\mathbf{i} \prec \mathbf{j}, \qquad \mathbf{i} \succ \mathbf{j}, \qquad \mathbf{i} = \mathbf{j}.$$

Dokaz. Najprej dokažimo tranzitivnost. Naj $\mathbf{i} = (i_1, i_2, \ldots, i_n)$, $\mathbf{j} = (j_1, j_2, \ldots, j_n), \mathbf{k} = (k_1, k_2, \ldots, k_n) \in \mathbb{N}_0^n$, kjer so člani $i_t, j_t, k_t \in \mathbb{N}_0$. Brez škode za splošnost naj velja $\mathbf{i} \prec \mathbf{j}$ in $\mathbf{j} \prec \mathbf{k}$. Prvi različni člen med $\mathbf{j}$ in $\mathbf{i}$ je večji pri $\mathbf{j}$ oziroma $i_m < j_m$, kjer je $m \in \mathbb{N}$ zaporedno število prvega različnega člena. Ker so vsi člani pred m-tima členoma enaki, velja zapis

$$\mathbf{j} = (i_1, i_2, \ldots, i_{m-1}, j_m, j_{m+1}, j_{m+2}, \ldots, j_n).$$

Enak razmislek ponovimo z neenakostjo $\mathbf{j} \prec \mathbf{k}$. Označimo s $p \in \mathbb{N}$ zaporedno število prvega različnega člena n-teric $\mathbf{j}$ in $\mathbf{k}$ ter ločimo dva primera.
Najprej predpostavimo, da je $m \leq p$. V tem primeru zapišemo

$$\mathbf{k} = (i_1, \ldots, i_{m-1}, j_m, j_{m+1}, \ldots, j_{p-1}, k_p, k_{p+1}, \ldots, k_n),$$

in opazimo, da se prvih $m-1$ mest n-terice $\mathbf{k}$ ujema s prvimi $m-1$ mesti n-terice $\mathbf{i}$, za naslednje mesto pa že velja $i_m < k_m$, iz česar sledi $\mathbf{i} \prec \mathbf{k}$.
Zdaj pa predpostavimo, da je $p < m$. V tem primeru zapišemo

$$\mathbf{k} = (i_1, \ldots, i_{p-1}, k_p, k_{p+1}, \ldots, k_n),$$

[1] Mi primerjamo n-terice nenegativnih celih števil, enaka metoda pa deluje za primerjanje n-teric, ki vsebujejo druge matematične objekte, ki jih znamo med sabo primerjati.

in opazimo, da se prvih $p-1$ členov n-teric $\mathbf{i}$ in $\mathbf{k}$ ujema, za naslednji člen pa že velja $j_p < k_p$ in $i_p = j_p$, torej $i_p < k_p$, iz česar sledi $\mathbf{i} \prec \mathbf{k}$.

Dokažimo še totalnost. Vzemimo n-terici $\mathbf{i} = (i_1, i_2, \ldots, i_n)$ in $\mathbf{j} = (j_1, j_2, \ldots, j_n)$. Predpostavimo najprej, da se n-terici ne razlikujeta v nobenem členu, potem velja $\mathbf{i} = \mathbf{j}$. V nasprotnem primeru naj bo p zaporedno število prvega člena z različnim številom. Člena j_p in i_p primerjamo. Primerjamo dve naravni števili, zato lahko velja samo $i_p < j_p$, iz česar sledi $\mathbf{i} \prec \mathbf{j}$, ali pa $i_p > j_p$, iz česar sledi $\mathbf{i} \succ \mathbf{j}$. □

Dokaz monotonosti seštevanja prepuščamo bralcu. Za dokaz osnovnega izreka o simetričnih polinomih potrebujemo še naslednji izrek.

Izrek 2.1. *Vsako strogo padajoče zaporedje n-teric $\mathbf{d}_1 \succ \mathbf{d}_2 \succ \cdots$ je končno.*

Pri dokazu izreka nam bo pomagala naslednja lema, v kateri za n-terico $\mathbf{b} \in \mathbb{N}_0^n$ in $a \in \mathbb{N}_0$ uvedemo zapis

$$\mathbf{b} = (b_1, \ldots, b_n),$$
$$(a, \mathbf{b}) = (a, b_1, \ldots, b_n) \in \mathbb{N}_0^{n+1}.$$

Lema 2.1. *Vsaka neprazna podmnožica $\mathbb{N}_0^n$ ima najmanjši element.*

Dokaz. Trditev dokažimo z indukcijo.

Brez dokaza uporabimo, da lema velja v primeru $n = 1$, saj je to znano dejstvo. Ta lastnost se imenuje načelo dobre urejenosti, njen dokaz je dostopen na spletu.

Predpostavimo, da trditev velja za poljubno neprazno podmnožico $\mathbb{N}_0^n$. Trdimo, da velja tudi za vse neprazne podmnožice $\mathbb{N}_0^{n+1}$. Naj bo S neprazna podmnožica $\mathbb{N}_0^{n+1}$. Naj bo $S_0 \subseteq \mathbb{N}_0$ množica prvih koordinat elementov množice S. Po indukcijski predpostavki obstaja najmanjši element v S_0, saj je neprazna podmnožica naravnih števil. Označimo ga z a. Definirajmo še množico $T \subseteq \mathbb{N}_0^n$, za katero velja $\mathbf{k} \in T$, če velja $(a, \mathbf{k}) \in S$. Po definiciji množice S_0 je T neprazna, zato ima po indukcijski predpostavki T najmanjši element, ki ga poimenujemo $\mathbf{b}$. Trdimo, da je $(a, \mathbf{b})$ najmanjši element množice S. Naj bo $\mathbf{j} = (j_0, j_1, \ldots, j_n) \in S$. Po definiciji velja $j_0 \in S_0$, zato vemo, da je $a \leq j_0$. Iz $a < j_0$ sledi, da je $(a, \mathbf{b}) \prec \mathbf{j}$, zato predpostavimo, da je $a = j_0$. Posledično je $(j_1, \ldots, j_n) \in T$ in velja $(j_1, \ldots, j_n) \leq \mathbf{b}$, kar pomeni, da velja neenakost $\mathbf{j} \preceq (a, \mathbf{b})$. Element $(a, \mathbf{b})$ je torej najmanjši element množice S, kar zaključi indukcijski korak. □

Dokaz izreka. Predpostavimo, da obstaja neskončno strogo padajoče zaporedje elementov $\mathbf{d}_1 \succ \mathbf{d}_2 \succ \cdots$ v $\mathbb{N}_0^n$. Množica vseh n-teric v zaporedju je neprazna podmnožica $\mathbb{N}_0^n$, ki nima najmanjšega elementa. Z uporabo zgornje leme to vodi v protislovje. Zato drži nasprotno, in sicer da je vsako strogo padajoče zaporedje $\mathbf{d}_1 \succ \mathbf{d}_2 \succ \cdots$ končno. □

3 Polinomi

3.1 Zapis z vsoto

Polinom z več spremenljivkami lahko zapišemo tako, da vsak člen izrazimo kot $C_{\mathbf{d}} X^{\mathbf{d}} = C_{\mathbf{d}} X_1^{d_1} X_2^{d_2} \cdots X_n^{d_n}$, pri čemer je $\mathbf{d} \in \mathbb{N}_0^n$ in $C_{\mathbf{d}} \in \mathbb{R}$.

Če uporabimo takšen zapis za vse člene, lahko zapišemo polinom f v obliki

$$f = \sum_{\mathbf{a} \in \mathbb{N}_0^n} C_{\mathbf{a}} \mathbf{X}^{\mathbf{a}},$$

pri čemer so $C_{\mathbf{a}} \in \mathbb{R}$, med katerimi je končno mnogo neničelnih.

3.2 Osnovne definicije

V uvodu so definirani polinomi, definirajmo nekaj osnovnih pojmov, ki opisujejo polinome. Stopnja neničelnega polinoma v eni spremenljivki je najvišja potenca neničelnih členov polinoma in jo označimo z $\deg(f)$. Stopnja ničelnega polinoma ni definirana.[2] Za neničelni polinom stopnje n je vodilni člen $a_n x^n$. Koeficient pri vodilnem členu imenujemo vodilni koeficient in ga označimo z $\operatorname{lead}(f)$.

Zgled 3.1. *Naj bo $f \in \mathbb{R}[X]$ polinom, dan s predpisom*

$$f(X) = 3X^4 + 2X^3 + 5X - 7,$$

potem velja, da je $\deg(f) = 4, \operatorname{lead}(f) = 3$.

Tako kot imamo pri polinomih z eno spremenljivko vodilni člen, ki določa stopnjo polinoma, imamo pri polinomih z več spremenljivkami vodilni člen, ki določa tako imenovano multistopnjo.

Definicija 3.1. *Naj bo $f \in \mathbb{R}[X_1, \ldots, X_n]$ neničelni polinom, zapišimo $f = \sum_{\mathbf{a} \in \mathbb{N}_0^n} c_{\mathbf{a}} \mathbf{X}^{\mathbf{a}}$. Multistopnja polinoma f je leksikografsko največja n-terica $\mathbf{d}$, pri kateri je koeficient $c_{\mathbf{d}}$ neničeln in se označi z* $\operatorname{mdeg}(f)$. *Pri tem imenujemo $c_{\mathbf{d}} X^{\mathbf{d}}$ vodilni člen. Multistopnja ničelnega polinoma ni definirana.*

Zgled 3.2. *Pri polinomu $f(X_1, X_2, X_3, X_4) = 5X_1^3 + 3X_1X_2X_3X_4^6 + 7X_2^5$ so 4-terice potenc pri členih $5X_1^3, 3X_1X_2X_3X_4^6$ ter $7X_2^5$ zaporedoma enake $(3,0,0,0), (1,1,1,6)$ ter $(0,5,0,0)$, multistopnja polinoma je torej* $\operatorname{mdeg}(f) = (3,0,0,0)$.

Tudi polinomom z več spremenljivkami lahko določimo vodilni koeficient.

Definicija 3.2. *Vodilni koeficient neničelnega polinoma f v več spremenljivkah je koeficient pred vodilnim členom. Označimo ga z* $\operatorname{lead}(f)$. *Vodilni koeficient ničelnega polinoma ni definiran.*

Pri prejšnjem zgledu je $\operatorname{lead}(f) = 5$.

Zgled 3.3. *Naj bo $f \in \mathbb{R}[X, Y, Z]$ polinom, podan s predpisom*

$$f(X, Y, Z) = 3X^4 + 2XYZ + 5Y^2 + Z.$$

Velja $\operatorname{mdeg}(f) = (4,0,0)$ *in* $\operatorname{lead}(f) = 3$. *Pri tem privzamemo naravno leksikografsko urejenost, ki je po vrstnem redu navedbe spremenljivk, torej $X \succ Y \succ Z$.*

Definirajmo podmnožico polinomov z več spremenljivkami imenovani simetrični polinomi. Označimo z $[n] = \{1, 2, \ldots, n\}$. Bijekcijo $\pi : [n] \to [n]$ imenujemo permutacija. Polinom $f \in \mathbb{R}[X_1, \ldots, X_n]$ je simetrični, če za vsako permutacijo $\pi : [n] \to [n]$ velja $f(X_{\pi(1)}, X_{\pi(2)}, \ldots, X_{\pi(n)}) = f(X_1, X_2, \ldots, X_n)$. To pomeni, da lahko zamenjamo spremenljivke na poljuben način in zmeraj dobimo enak polinom. Na primer polinom $p(x, y) = x + y$ je simetrični polinom, saj velja $p(x, y) = x + y = y + x = p(y, x)$. Kasneje bomo dokazali, da lahko vsak simetrični polinom zapišemo kot polinom v tako imenovanih elementarnih simetričnih polinomih.

Definicija 3.3. *Polinom $S_{n,k} \in \mathbb{R}[X_1, \ldots, X_n]$, ki ga imenujemo k-ti elementarni simetrični polinom v n spremenljivkah, je vsota vseh možnih produktov k spremenljivk izmed $X_1, \ldots, X_n$. Predpis je dan s*

$$S_{n,k} = \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} X_{i_1} X_{i_2} \cdots X_{i_k}.$$

Zgled 3.4. *Za $n = 3$ so elementarni simetrični polinomi*

$$\begin{aligned} S_{3,0}(X, Y, Z) &= 1, \\ S_{3,1}(X, Y, Z) &= X + Y + Z, \\ S_{3,2}(X, Y, Z) &= XY + YZ + XZ, \\ S_{3,3}(X, Y, Z) &= XYZ. \end{aligned}$$

[2] Pogosto se definira $\deg 0 = -\infty$.

3.3 Vietove formule

Primer uporabe simetričnih polinomov so Vietove formule. Če kubični polinom $f(X) = aX^3 + bX^2 + cX + d$ z ničlami $X_1, X_2, X_3 \in \mathbb{R}$ zapišemo v ničelni obliki kot $f(X) = a(X - X_1)(X - X_2)(X - X_3)$ in zmnožimo vse faktorje ničelne oblike, dobimo

$$\begin{aligned} f(X) &= a(X - X_1)(X - X_2)(X - X_3) = \\ &= aX^3 - a(X_1 + X_2 + X_3)X^2 + a(X_1X_2 + X_1X_3 + X_2X_3)X - aX_1X_2X_3. \end{aligned}$$

Opazimo, da lahko enačimo koeficiente pri istoležnih členih, da dobimo dobro znane Vietove formule

$$\begin{aligned} 1 &= \frac{a}{a}, \\ X_1 + X_2 + X_3 &= -\frac{b}{a}, \\ X_1X_2 + X_3X_2 + X_1X_3 &= \frac{c}{a}, \\ X_1X_2X_3 &= -\frac{d}{a}. \end{aligned}$$

Zapišemo vse elementarne simetrične polinome v treh spremenljivkah in opazimo, da se pojavijo v Vietovih formulah.

$$\begin{aligned} S_{3,0}(X_1, X_2, X_3) &= 1, \\ S_{3,1}(X_1, X_2, X_3) &= X_1 + X_2 + X_3, \\ S_{3,2}(X_1, X_2, X_3) &= X_1X_2 + X_1X_3 + X_2X_3, \\ S_{3,3}(X_1, X_2, X_3) &= X_1X_2X_3. \end{aligned}$$

Multistopnja polinoma $S_{n,k}$ je enaka $(\underbrace{1, \ldots, 1}_{k}, 0, \ldots, 0)$, pri čemer je na prvih k mestih število 1, na vseh ostalih pa 0.

3.4 Trditve o polinomih

V tem poglavju predstavimo tri trditve o polinomih v več spremenljivkah, ki jih uporabljamo pri računanju. Za množenje neničelnih polinomov več spremenljivk veljata trditvi $\operatorname{mdeg}(f \cdot g) = \operatorname{mdeg}(f) + \operatorname{mdeg}(g)$ in $\operatorname{lead}(f \cdot g) = \operatorname{lead}(f) \cdot \operatorname{lead}(g)$, pri čemer prva razloži, kako izračunamo multistopnjo pri množenju, druga pa pri istem postopku opisuje nastanek vodilnega koeficienta. Za seštevanje polinomov v več spremenljivkah velja bodisi $f + g = 0$ bodisi $\operatorname{mdeg}(f + g) \preceq \max\{\operatorname{mdeg}(f), \operatorname{mdeg}(g)\}$.

Dokaz prvih dveh trditev. Označimo $\operatorname{mdeg}(f) = \mathbf{n}$ in $\operatorname{mdeg}(g) = \mathbf{m}$. Oglejmo si njun produkt v strnjenem zapisu, torej polinoma f in g zaporedoma zapišemo kot

$$f = c_{\mathbf{n}}\mathbf{X}^{\mathbf{n}} + \sum_{\mathbf{a} \prec \mathbf{n}} c_{\mathbf{a}}\mathbf{X}^{\mathbf{a}} \text{ in } g = b_{\mathbf{m}}\mathbf{X}^{\mathbf{m}} + \sum_{\mathbf{a} \prec \mathbf{m}} b_{\mathbf{a}}\mathbf{X}^{\mathbf{a}}.$$

Množenje polinomov poteka po členih. Velja

$$f \cdot g = c_{\mathbf{n}}b_{\mathbf{m}}\mathbf{X}^{\mathbf{n}}\mathbf{X}^{\mathbf{m}} + \text{členi nižje multistopnje},$$

kar argumentiramo v nadaljevanju. Po definiciji velja enakost $c_{\mathbf{a}}\mathbf{X}^{\mathbf{a}}c_{\mathbf{b}}\mathbf{X}^{\mathbf{b}} = c_{\mathbf{a}}c_{\mathbf{b}}\mathbf{X}^{\mathbf{a}+\mathbf{b}}$. Spomnimo se na monotonost leksikografske urejenosti. Iz te sledi, da je vsota multistopenj dveh členov, med katerima vsaj

eden ni vodilni, strogo manjša kot vsota multistopenj vodilnih členov. Sledi, da je vodilni člen produkta produkt vodilnih členov faktorjev. S tem smo pokazali, da je $\operatorname{mdeg}(f \cdot g) = \operatorname{mdeg}(f) + \operatorname{mdeg}(g)$ in, da je

$$\operatorname{lead}(f \cdot g) = \operatorname{lead}(f) \cdot \operatorname{lead}(g).$$

□

Dokaz trditve o multistopnji polinoma pri seštevanju prepustimo bralcu.

4 Osnovni izrek o simetričnih polinomih

Trdimo, da je vsak simetrični polinom mogoče zapisati kot polinom v elementarnih simetričnih polinomih.

Izrek 4.1. *Naj bo f simetrični polinom v n spremenljivkah. Potem velja*

$$f \in \mathbb{R}[S_{n,1}, S_{n,2} \ldots, S_{n,n}].$$

To pomeni, da obstajajo takšna realna števila $c_{\mathbf{a}} \in \mathbb{R}$, med katerimi je največ končno mnogo neničelnih, da lahko z uporabo zapisa $\mathbf{S} = (S_{n,1}, S_{n,2}, \ldots, S_{n,n})$ in $\mathbf{S}^{(a_1,a_2,\ldots,a_n)} = S_{n,1}^{a_1} S_{n,2}^{a_2} \cdots S_{n,n}^{a_n}$ zapišemo

$$f = \sum_{\mathbf{a} \in \mathbb{N}_0^n} c_{\mathbf{a}} \mathbf{S}^{\mathbf{a}}.$$

Dokaz. Naj bo $f \in \mathbb{R}[X_1, \ldots X_n]$ poljuben simetrični polinom z multistopnjo $\mathbf{d} = (d_1, d_2, \ldots, d_n)$. Dokaza se lotimo tako, da postopoma iščemo polinome elementarnih simetričnih polinomov, ki vsoto v določenem smislu približujejo polinomu f. Najprej odštejemo tak polinom iz elementarnih simetričnih polinomov, ki ima enak vodilni člen kot f, in razliko poimenujemo f_1. S tem je multistopnja novega polinoma manjša kot multistopnja prejšnjega in postopek ponavljamo, dokler ne pridemo do ničelnega polinoma. Uporabimo že znano lastnost multistopnje produkta simetričnih polinomov $\operatorname{mdeg}(fg) = \operatorname{mdeg}(f) + \operatorname{mdeg}(g)$ ter zapišemo

$$\operatorname{mdeg}(S_{n,1}^{a_1} S_{n,2}^{a_2} \cdots S_{n,n}^{a_n}) = a_1 \operatorname{mdeg}(S_{n,1}) + \cdots + a_n \operatorname{mdeg}(S_{n,n}).$$

Multistopnja je tako enaka $(a_1 + a_2 + \cdots + a_n, a_2 + a_3 + \cdots + a_n, \ldots, a_n)$. Želimo, da je multistopnja enaka $\mathbf{d}$, torej $(d_1, d_2, \ldots, d_n)$. Iz tega sledi, da je $d_n = a_n$ ter

$$\begin{aligned} d_{n-1} &= a_{n-1} + a_n, \\ a_{n-1} &= d_{n-1} - d_n. \\ d_{n-2} &= a_{n-2} + a_{n-1} + a_n, \\ a_{n-2} &= d_{n-2} - d_{n-1} + d_n - d_n = d_{n-2} - d_{n-1}. \end{aligned}$$

Enako lahko izrazimo vse ostale a-je z d-ji. Če $k \neq n$, nastavimo $a_k = d_k - d_{k+1}$. Če so te razlike negativne, pride do problema, zato moramo zagotoviti, da velja

$$d_1 \geq d_2 \geq d_3 \geq \cdots \geq d_n \geq 0.$$

Hitro opazimo, da je problem le v nesimetričnih polinomih. Pri polinomu $f(X_1, X_2, X_3) = X_1 X_3^5 + X_2$ sta multistopnji posameznih členov (1,0,5) in (0,1,0), kjer za multistopnjo polinoma (1,0,5) zgornji pogoj ni izpolnjen. Pri simetričnih polinomih, kot je $f(X_1, X_2) = X_1^2 X_2 + X_1 X_2^2$, z multistopnjama členov (2, 1) in (1, 2), opazimo, da za multistopnjo polinoma (2,1) zgornji pogoj velja. Zaradi simetričnosti so koordinate multistopnje vedno v padajočem vrstnem redu. Če to ne bi držalo, bi lahko zamenjali spremenljivke polinoma in dobili polinom z večjo multistopnjo, kar je protislovje.

V nadaljevanju dokaza določimo vse a_i in produkt $S_{n,1}^{a_1} S_{n,2}^{a_2} \cdots S_{n,n}^{a_n}$ pomnožimo z $\operatorname{lead}(f)$, da dobimo g_1, ki ga odštejemo od f. Tako se odštejeta vodilna člena, kar je tudi naš cilj. Za lažje razumevanje poglejmo primer odštevanja dveh polinomov z eno spremenljivko.

Zgled 4.1. *Podana imamo polinoma*

$$f(X) = 5X^6 + 7X^5 + 3X,$$
$$g(X) = X^6 + X.$$

Če ju odštejemo takoj, se člani s stopnjo polinoma ne odštejejo, saj ostane še $4X^6$. Zato g pomnožimo z vodilnim koeficientom f, pri odštevanju dobimo polinom $h(X) = 7X^5 - 2X$, torej znižamo stopnjo polinoma f.

Nadaljujemo dokaz izreka 2. Ko odštejemo polinom $\text{lead}(f)g_1$ od f, se vodilna člena odštejeta in dobimo polinom f_1 s strogo nižjo multistopnjo od f.

Polinom f_1 je simetrični. Iz tega sledi, da lahko postopek ponovimo s f_1 namesto f. To dokažimo z računom

$$\begin{aligned} f_1(X_{\pi(1)}, \ldots, X_{\pi(n)}) &= f(X_{\pi(1)}, \ldots, X_{\pi(n)}) - g_1(X_{\pi(1)}, \ldots, X_{\pi(n)}) = \\ &= f(X_1, \ldots, X_n) - g_1(X_1, \ldots, X_n) = f_1(X_1, \ldots, X_n). \end{aligned}$$

Nadaljujemo tako, da po enakem postopku kot za iskanje g_1 poiščemo polinom g_2 z enako multistopnjo kot f_1, tega pomnožimo z vodilnim koeficientom f_1 in razliko vzamemo za f_2.

Ponovno velja $\text{mdeg}(f_1) \succ \text{mdeg}(f_2)$ in f_2 je simetrični polinom. Prikazan proces ponavljamo, dokler sčasoma ne dobimo $f_r = 0$. Zaporedje se mora zaključiti z ničelnim polinomom zaradi izreka (2.1). To lahko zapišemo tudi kot

$$\begin{aligned} 0 &= f_{r-1} - g_r = \\ &= f_{r-2} - g_{r-1} - g_r = \\ &\vdots \\ &= f - g_1 - g_2 - \cdots - g_r, \end{aligned}$$

iz česar sledi

$$f = g_1 + g_2 + \cdots + g_r.$$

Ker so polinomi $g_1, \ldots, g_r$ produkti elementarnih simetričnih polinomov, smo s tem dokazali, da je vsak simetrični polinom vsota produktov elementarnih simetričnih polinomov. □

4.1 Primer osnovnega izreka o simetričnih polinomih

Za primer uporabe osnovnega izreka o simetričnih polinomih izpeljimo postopek, opisan v dokazu, na konkretnem simetričnem polinomu. Obravnavajmo primer s tremi spremenljivkami X, Y, Z, ki so urejene s pravilom $X \succ Y \succ Z$. Vzamemo simetrični polinom $f(X, Y, Z) = X^2 + Y^2 + Z^2$, ki ga želimo izraziti kot polinom v elementarnih simetričnih polinomih.

Za začetek vzemimo $S_{3,1}^2 = (X + Y + Z)^2$, ki ga lahko zapišemo tudi kot

$$S_{3,1}^2 = X^2 + 2XY + Y^2 + 2XZ + 2YZ + Z^2$$

in ga odštejemo od polinoma f. Dobimo polinom f_1 s predpisom

$$\begin{aligned} f_1 &= (X^2 + Y^2 + Z^2) - (X^2 + 2XY + Y^2 + 2XZ + 2YZ + Z^2), \\ f_1 &= -2XY - 2XZ - 2YZ. \end{aligned}$$

Opazimo, da lahko polinomu f_1 preprosto prištejemo dvakratnik oblike $S_{3,2} = XY + YZ + XZ$, torej zapišemo izraz $f_2 = f_1 + 2S_{3,2}$. Če bi bila multistopnja simetričnega polinoma večja kot v tem primeru, bi postopek lahko trajal dlje in na enak način naprej, v tem primeru pa se konča pri $f_2 = 0$, kar pomeni, da smo bili uspešni.

Združimo te izraze in dobimo zapis polinoma f kot polinom v elementarnih simetričnih polinomih

$$\begin{aligned} f_1 &= f - S_{3,1}^2, \\ f_2 &= f_1 + 2S_{3,2} = 0, \\ 0 &= f - S_{3,1}^2 + 2S_{3,2}, \\ f &= S_{3,1}^2 - 2S_{3,2}. \end{aligned}$$

Literatura

[1] K. Conrad, *Symmetric polynomials*, spletni zapiski, University of Connecticut. Dostopno na: `https://kconrad.math.uconn.edu/blurbs/galoistheory/symmfunction.pdf`

Reed-Solomonov kod

Samo Jan, Eva Šolinc
Mentor*: Matija Likar*

Povzetek

V članku opredelimo osnovni problem ter predstavimo ključne izreke teorije kodiranja. Definiramo Singletonovo mejo, ki opredeljuje teoretsko mejo učinkovitosti koda. Vpeljemo polinome nad končnimi polji in pokažemo temeljne izreke o njihovih ničlah. Predstavimo še kodiranje z uporabo Reed-Solomonovega koda in dokažemo, da izpolnjuje Singletonovo mejo.

1 Uvod

Dne 26. julija leta FF26 po marsovskem štetju so Zemljani želeli vzpostaviti stik z Marsovci kot najbližjimi zunajzemskimi bitji. Poslali so torej sporočilo: „Pozdravljeni!“.

Mlada Marsovca Eva in Samo sta sporočilo polna navdušenja prestregla. A navdušenju je sledilo razočaranje. Pisalo je: „gozdrarljeni!“ „Kakšni gozdarji neki?“ je zavzdihnila Eva, obupavajoča nad neumnostjo sporočila. Tedaj pa je Samo doživel preblisk: „Najbrž so želeli napisati kaj bolj smiselnega, pa se je sporočilo na poti uničilo! Pomagajva jim.“

Tako sta 1. avgusta FF26 Eva in Samo planetu Zemlji poslala sporočilo, kodirano po Reed-Solomonovem kodu. Obenem sta v medgalaktično medmrežje pripela pričujoči članek, v posebni Zemljin predalček pa položila izvirno sporočilo, da ga bodo znali razvozlati. Vse seveda v upanju, da Zemljani sploh imajo dostop do galaktičnega medmrežja.

2 Osnove teorije kodiranja

Za začetek si oglejmo nekaj osnovnih definicij, ki nam bodo pomagale opredeliti problem kodiranja in dekodiranja sporočil.

Definicija 2.1. ***Abeceda*** Σ *je množica znakov (npr.* $\Sigma = \{0, 1\}$*).* ***Niz*** *je* n*-terica znakov iz* Σ*, množico vseh takih* n*-teric označimo z* Σ^n*.* ***Kod*** C *je podmnožica* Σ^n*. Številu* n *pravimo tudi dolžina bloka koda.*

Za vsak kod lahko definiramo tudi **dimenzijo koda**, ki je definirana s $k = \log_q |C|$, kjer je $q = |\Sigma|$ velikost abecede. **Hitrost koda** definirano s $R = k/n$, ki nam pove gostoto informacij, ki jih pošiljamo z nekim kodom. Poznamo tudi **redudanco koda** $(n - k)$, kjer je $n \geq k$. Pojme bomo uporabljali v nadaljevanju kot metrike, ki bodo opisovale kvaliteto koda.

2.1 Pot sporočila

Začnemo s svojim sporočilom $m \in \Sigma^k$, ki ga s **kodirno funkcijo** E spremenimo v **kodirno besedo** $c \in C$. Ta gre nato skozi **kanal**, kjer se lahko zamenjajo nekateri znaki osnovnega sporočila. S tem dobimo nov niz $\mathrm{Ch}(c) \in \Sigma^n$, ki sestoji iz kodirne besede, kateri so bili nekateri znaki morda spremenjeni. Nato ta niz pošljemo skozi **dekodirno funkcijo** D, ki prejemniku rekonstruira osnovno sporočilo. Eden izmed temeljnih problemov

teorije kodiranja je najti kod C ter funkciji E in D, ki omogočata rekonstrukcijo izvirnega sporočila pri čim večjem številu napak, ki se lahko pojavijo med prenosom.

$$\Sigma^k \xrightarrow{E} C \subseteq \Sigma^n \xrightarrow{\text{Ch}} \Sigma^n \xrightarrow{D} \Sigma^k$$

Zgled 2.1. *Vzemimo $\Sigma = \{0,1\}$, $k = 3$ in $n = 9$. Sporočilo $m = (1,0,1)$ kodirna funkcija E zakodira tako, da ga trikrat ponovi.*

$$E(m) = (1,0,1,1,0,1,1,0,1) \in C \subseteq \Sigma^n$$

Recimo, da kanal spremeni znak na tretjem mestu (torej namesto 1 pošlje 0).

$$Ch(E(m)) = (1,0,0,1,0,1,1,0,1)$$

Dekodirna funkcija D za vsako od treh mest prvotnega sporočila izbere znak, ki se med tremi ponovitvami pojavi večkrat (večinsko odločanje), in tako pravilno rekonstruira

$$D(Ch(E(m))) = (1,0,1) = m.$$

Rekli smo, da se lahko med prenosom nekateri znaki v našem sporočilu spremenijo. Podrobneje si oglejmo, kako lahko te napake štejemo in kako z njimi opredelimo kvaliteto kanala.

2.2 Hammingova razdalja

Definicija 2.2. *Naj bosta $u, v \in \Sigma^n$. Izraz $\Delta(u,v)$ predstavlja število znakov, kjer se u in v razlikujeta, čemur pravimo Hammingova razdalja.*

Izrek 2.1. *Hammingova razdalja je metrika.*

Dokaz. Razdalja $\Delta(u,v)$ je po definiciji večja ali enaka nič. Hkrati je razdalja enaka nič, natanko tedaj, ko je $u = v$. Iz definicije sledi tudi simetričnost, torej $\Delta(u,v) = \Delta(v,u)$.

Velja tudi trikotniška neenakost, ki pravi,

$$\Delta(u,w) \leq \Delta(u,v) + \Delta(v,w).$$

To drži, saj če spremenimo niz u v niz v potrebujemo $\Delta(u,v)$ korakov. Če nato še nastali niz spremenimo v w pa še $\Delta(v,w)$ korakov. Torej se u in w razlikujeta kvečjemu v $\Delta(u,v) + \Delta(v,w)$ znakih. □

Dokaz trikotniške neenakosti še podkrepimo s primerom. $x = (0,0,1)$, $y = (1,0,1)$ in $z = (0,1,0)$, kjer če x prevedemo v z prek y opravimo štiri spremembe, medtem ko se niza x in z razlikujeta v dveh znakih.

2.3 Kanal s t napakami

Spomnimo se, da je kanal Ch funkcija iz Σ^n v Σ^n. Torej slika nize dolžine n v nize iste dolžine, kjer nekatere znake morebiti spremeni. Za kanal Ch pravimo, da ima t **napak**, če velja, da za vsak $v \in \Sigma^n$ velja $\Delta(v, \text{Ch}(v)) \leq t$. Povedano drugače, posameznemu nizu spremeni kvečjemu t znakov. Pravimo, da kod C zaznava t napak, če obstaja dekodirna funkcija $D : \Sigma^n \to \{0,1\}$, kjer 0 pomeni, da je v kanalu prišlo do spremembe vsaj enega znaka, 1 pa, da so znaki prišli skozi brez napake. Pravimo tudi, da kod C popravi t napak, če obstaja dekodirna funkcija D, tako da za vsak $m \in \Sigma^k$ velja $D(\text{Ch}(E(m))) = m$.

Zgled 2.2. *Za primer koda si bomo pogledali **ponovitveni kod**. S ponovitvenim kodom nekajkrat ponovimo naše osnovno sporočilo. Vzemimo $\Sigma = \{0,1\}$ in $n = 9$. Nato lahko zakodiramo sporočilo (x_1, x_2, x_3) na naslednji način.*

$$C_{3,rep}(x_1,x_2,x_3) = (x_1,x_2,x_3,x_1,x_2,x_3,x_1,x_2,x_3)$$

Našo dimenzijo koda k dobimo s preprostim računom $k = \log_2 2^3 = 3$. Zdaj lahko še izračunamo hitrost koda

$$R = \frac{k}{n} = \frac{3}{9} = \frac{1}{3},$$

kar pomeni, da naša kodirna beseda nosi trikrat več podatkov, kot bi jih bilo minimalno potrebnih za uprizoritev sporočila.

2.4 Minimalna razdalja

Kot bomo videli, nam pri izbiri koda pomaga dejstvo, da se posamezni nizi v kodu med seboj razlikujejo v čim več znakih. To raznolikost bomo izrazili z minimalno razdaljo koda.

Definicija 2.3. ***Minimalna razdalja*** *koda je minimalna Hammingova razdalja med poljubnima različnima kodirnima besedama.*

$$\Delta(C) = \min_{\substack{c_1, c_2 \in C \\ c_1 \neq c_2}} \Delta(c_1, c_2)$$

Na primer, bralec se lahko prepriča, da pri ponovitvenem kodu velja $\Delta(C_{3,\text{rep}}) = 3$.

Naslednji izrek je ključen, saj nam pove, da večja kot je razdalja med kodi, več napak lahko zaznamo oz. popravimo.

Izrek 2.2. *Naj bo C kod. Naslednje trditve so ekvivalentne.*

1. *Minimalna razdalja C je $d \geq 2$.*
2. *Kod C zazna $d - 1$ napak.*
3. *Kod C popravi $\lfloor \frac{d-1}{2} \rfloor$ napak.*

Dokaz tega izreka je na voljo v [1, Trditev 1.4.2]. Na tej točki se nam poraja vprašanje, kolikšna je največja minimalna razdalja, ki jo lahko doseže nek kod z dolžino bloka n in dimenzijo k.

Izrek 2.3 (Singletonova meja)**.** *Naj bo C kod z dolžino bloka n in dimenzijo k. Tedaj za njegovo minimalno razdaljo d velja*

$$d \leq n - k + 1.$$

Dokaz tega izreka je na voljo v [1, Izrek 4.3.1].

Če je za nek kod ta meja dosežena, pravimo, da ima kod **minimalno separabilno razdaljo**. Zdaj lahko znanje o minimalni razdalji uporabimo pri poljih. V nadaljevanju bomo videli, da je prav Reed-Solomonov kod primer koda z minimalno separabilno razdaljo.

3 Polinomi nad končnim poljem

Preden se lotimo opisa Reed-Solomonovega koda, se moramo seznaniti z nekaj definicijami in rezultati iz teorije grup in polinomov nad končnimi polji.

Definicija 3.1. ***Grupa*** *je par $(G, +)$, kjer je G množica, $+ \colon G \times G \to G$ pa binarna operacija, za katero velja*

- *asociativnost: za vsake $g_1, g_2, g_3 \in G$ velja $(g_1 + g_2) + g_3 = g_1 + (g_2 + g_3)$,*
- *enota: obstaja tak $e \in G$, da za vsak $g \in G$ velja $e + g = g + e = g$,*
- *inverz: za vsak $g \in G$ obstaja $g^{-1} \in G$, da velja $g + g^{-1} = e = g^{-1} + g$.*

Primer grupe je denimo množica celih števil z operacijo seštevanja, množica racionalnih števil z operacijo množenja pa ni grupa, ker število 0 nima inverza.

Definicija 3.2. *Če je operacija + komutativna, torej velja $a + b = b + a$ za vsak par $a, b \in G$, pravimo grupi* ***Abelova grupa****.*

Definicija 3.3. *Polje je trojica $(F, +, \cdot)$, kjer je F množica, $+$ in $\cdot$ pa binarni operaciji, za katere velja*

- *$(F, +)$ je Abelova grupa,*
- *$(F \setminus \{0\}, \cdot)$ je Abelova grupa,*
- *distributivnost: za vsake $a, b, c \in F$ velja $a \cdot (b + c) = a \cdot b + a \cdot c$.*

Primer polja je množica racionalnih števil z operacijama seštevanja in množenja. Polja pa ne rabijo biti nujno končna. Za nas bodo prav koristna končna polja, primer katerih je naslednji. Naj bo p praštevilo. Množica $\mathbb{F}_p$ je množica $\{0, 1, 2, ..., p-1\}$ z operacijama seštevanja po $\bmod p$ in množenja po $\bmod p$ tvori polje. Dokaz, da gre res za polje, je na voljo v [1, Lema 2.1.4].

Definicija 3.4. ***Polinom*** *$f(x)$ nad poljem F je izraz*

$$f(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0,$$

kjer sta $d \in \mathbb{N}_0$ in $a_i \in F$ za vsak $0 \leq i \leq d$ ter $a_d \neq 0$. Stopnja polinoma f je $\deg f = d$. Množico vseh polinomov nad poljem F označimo s $F[x]$.

Polinome lahko med seboj seštevamo in množimo. Za polinoma f in g naj velja $\deg f \leq \deg g = n$. Zapišimo ju kot $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ in $g(x) = b_n x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0$. Njuna vsota znaša

$$f(x) + g(x) = (a_n + b_n) x^n + (a_{n-1} + b_{n-1}) x^{n-1} + ... + (a_1 + b_1) x + a_0 + b_0.$$

Produkt f in g je h, čigar koeficienti so

$$c_k = \sum_{0 \leq i \leq k} a_i b_{k-i}.$$

Zgled 3.1. *Seštevanje in množenje polinomov nad poljem bomo pokazali na primeru. Vzemimo za polje $\mathbb{F}_3 = \{0, 1, 2\}$ in si izberimo polinoma $x^2 + 2x + 2$ in $x^2 + 2$, ki sta oba stopnje 2. Izračunajmo njuno vsoto in produkt.*

$$(x^2 + 2x + 2) + (x^2 + 2) = 2x^2 + 2x + 4 = 2x^2 + 2x + 1$$

$$(x^2 + 2x + 2) \cdot (x^2 + 2) = x^4 + 2x^2 + 2x^3 + 4x + 2x^2 + 4 = x^4 + 2x^3 + x^2 + x + 1$$

Spomnimo se, da smo računali po $\bmod 3$.

Opazimo lahko, da je produkt izbranih polinomov stopnje 4, vsota pa stopnje 2. V splošnem velja

$$\deg fg = \deg f + \deg g \quad \text{in} \quad \deg(f + g) \leq \max(\deg f, \deg g),$$

pri čemer enakost velja, kadar vsota vodilnih koeficientov f in g ni enaka nič.

Definicija 3.5. *Vrednost $a \in F$ je ničla polinoma f, če velja $f(a) = 0$.*

Bralec verjetno že ve, da je število ničel realnega polinoma omejeno z njegovo stopnjo. Podobno velja tudi za polinome nad poljubnim poljem.

Izrek 3.1. *Neničelni polinom $f \in F[x]$ stopnje d ima kvečjemu d različnih ničel.*

Izreka v tem članku ne bomo dokazali, lahko ga pa bralec najde v [1, Trditev 5.1.5].

Izrek 3.2. *Naj bodo $x_1, x_2, ..., x_k \in F$ paroma različni in naj bodo $y_1, y_2, ..., y_k$ poljubni. Obstaja enoličen polinom $f \in F[x]$ s stopnjo $\deg(f) \leq k-1$, za katerega velja $f(x_i) = y_i$ za vsak $1 \leq i \leq k$.*

Dokaz.

Posebej bomo dokazali obstoj in enoličnost takega polinoma f.

i) Enoličnost bomo dokazali s protislovjem. Predpostavimo, da obstajata različna polinoma f in g, ki ustrezata pogojem, torej zanju velja $\deg f \leq k-1$, $\deg g \leq k-1$ in $f(x_i) = g(x_i) = y_i$ za vsak $1 \leq i \leq k$. Potem velja tudi $\deg(f-g) \leq k-1$. Posledično ima po izreku 3.1 polinom $f-g$ največ $k-1$ ničel.

A poglejmo še drugače. Za vsak x_j, kjer je $1 \leq j \leq k$ velja

$$(f-g)(x_j) = f(x_j) - g(x_j) = y_j - y_j = 0.$$

Polinom $f-g$ ima tako vsaj k ničel, kar je v protislovju s prejšnjo ugotovitvijo. Polinom je torej enolično določen.

ii) S konstrukcijo še dokažimo obstoj tega polinoma. Za ta namen bomo vpeljali Lagrangeev bazni polinom

$$L_i(x) = \prod_{\substack{1 \leq j \leq k \\ i \neq j}} \frac{x - x_j}{x_i - x_j}.$$

Lagrangeev bazni polinom $L_i(x_j)$ zavzame vrednost 1, če $i = j$, in 0, če $i \neq j$, o čemer naj se bralec prepriča sam.

Definirajmo polinom $f(x)$ kot

$$f(x) = \sum_{i=1}^{k} y_i L_i(x).$$

V točki x_j je tako vrednost polinoma enaka

$$f(x_j) = \sum_{i=1}^{k} y_i L_i(x_j) = y_j L_j(x_j) = y_j.$$

Dokazali smo torej, da obstaja polinom, za katerega velja $f(x_i) = y_i$ za vsak $1 \leq i \leq k$. Iz konstrukcije Lagrangeevih baznih polinomov pa tudi vidimo, da ima stopnjo največ $k-1$.

□

4 Reed-Solomonov kod

Naj bo $m = (a_0, a_1, ..., a_{k-1}) \in \mathbb{F}_p^k$ naše sporočilo, ki ga želimo poslati. Definirajmo polinom

$$f(x) = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \cdots + a_1 x + a_0.$$

Vrednosti p in k sta med pošiljateljem in prejemnikom vnaprej dogovorjeni. Prav tako je določena vrednost $n \leq p$, ki predstavlja dolžino bloka v kodu, in različne evalvacijske točke $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_p$. Kodirna beseda je niz vrednosti polinoma $f(x)$ nad poljem $\mathbb{F}_p$ v izbranih evalvacijskih točkah. Natančneje

$$(a_0, a_1, \ldots, a_{k-1}) \overset{E}{\mapsto} (f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_{n-1})).$$

Reed-Solomonov kod je množica vseh možnih kodirnih besed. V primeru, da na kanalu ne pride do napak, lahko prejemnik s poznavanjem evalvacijskih točk na podlagi izreka 3.2 rekonstruira polinom in s tem prvotno sporočilo.

Definicija 4.1. *Reed-Solomonov kod s parametroma n in k (krajše RS) je množica*

$$RS[n,k] = \{(f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)) : f \in \mathbb{F}_p[x],\ \deg f < k\} \subseteq \mathbb{F}_p^n.$$

Zgled 4.1. *Oglejmo si še primer kodiranja sporočila po Reed-Solomonovem kodu. Sporočevalec želi poslati niz (1, 0, 1) dolžine $k = 3$. Izbere $p = 7$, torej računa v $\mathbb{F}_7$. Določi še $n = 5$ in za evalvacijske točke izbere*

$$\alpha_1 = 1, \alpha_2 = 2, \ldots, \alpha_5 = 5.$$

Pripadajoči polinom je

$$f(x) = 1 \cdot x^2 + 0 \cdot x + 1 = x^2 + 1.$$

Zdaj si ogleda vrednosti polinoma $f(x)$ v izbranih evalvacijskih točkah: $f(\alpha_1) = f(1) = 2$, $f(\alpha_2) = f(2) = 5$, $f(\alpha_3) = f(3) = 10 = 3$, $f(\alpha_4) = f(4) = 17 = 3$ in $f(\alpha_5) = f(5) = 26 = 5$. Sporočevalec tako pošlje kodirno besedo (2, 5, 3, 3, 5).

Naštejmo še nekaj lastnosti Reed-Solomonovega koda.

1. Dimenzija RS je k.
2. RS je linearen kod, kar pomeni, da velja $E(m_1 + m_2) = E(m_1) + E(m_2)$ in $E(m_1\lambda) = \lambda E(m_1)$, kjer je $\lambda \in \mathbb{F}_p$ in sta m_1 in m_2 poljubni sporočili.
3. RS ima minimalno separabilno razdaljo $\Delta(RS) = n - k + 1$, zato lahko popravi $\lfloor \frac{n-k}{2} \rfloor$ napak in zazna $n - k$ napak.

V dokazu tretje lastnosti RS bomo uporabili naslednjo lemo.

Lema 4.1. *Naj bo C linearen kod. **Hammingovo težo** $\mathrm{wt}(c)$ definirajmo kot število neničelnih členov v kodirni besedi. Minimalna Hammingova teža neničelnih elementov v kodu C je enaka minimalni razdalji v C, torej*

$$\Delta(C) = \min_{\substack{c \in C \\ c \neq 0}} \mathrm{wt}(c).$$

Iskanje minimalne razdalje koda C smo tako prevedli na iskanje neničelne kodirne besede z minimalno Hammingovo težo. Ker mora biti kodirna beseda $(f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_{n-1}))$ neničelna f pa ima stopnjo kvečjemu $k-1 < n$, mora po izreku 3.1 biti f neničeln polinom. Sledi torej, da je izmed $f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_{n-1})$ največ $k - 1$ enakih nič, torej je

$$\min_{\substack{c \in C \\ c \neq 0}} \mathrm{wt}(c) \geq n - (k-1) = n - k + 1.$$

Takšen c, ki doseže mejo pa prav tako obstaja, saj lahko izberemo

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_{n-1}).$$

Sledi, da je $\Delta(C) = n - k + 1$. Po izreku 2.2 vidimo, da torej Reed-Solomonov kod popravi $\lfloor \frac{n-k}{2} \rfloor$ napak.

Preostalo nam je le še opisati, kako lahko prejemnik iz kodirne besede pridobi prvotno sporočilo z napakami. Eden bolj znanih načinov, kako to storiti, je t.i. Welch-Berlekampov algoritem, ki je opisan v [3].

Literatura

[1] V. Guruswami, A. Rudra, M. Sudan, **Essential Coding Theory**, osnutek, avgust 2025. Brezplačno dostopno na `https://cse.buffalo.edu/faculty/atri/courses/coding-theory/book`.

[2] I. S. Reed, G. Solomon, **Polynomial Codes over Certain Finite Fields**, Journal of the Society for Industrial and Applied Mathematics, 8(2):300–304, 1960. Ustanovni štiristranski članek.

[3] CS 70 Course Staff, **Note 9: Error Correcting Codes**, Discrete Mathematics and Probability Theory, UC Berkeley, pomlad 2017. Berlekamp–Welchev algoritem razloži kot sistem linearnih enačb z uvedbo polinoma napak $E(x)$. Dostopno na `https://sp17.eecs70.org/static/notes/n9.pdf`.

Diskretni račun

Zarja Čibej, Ana Helbl
Mentor*: Tim Milanez*

Povzetek

Z uvedbo pojmov diference in antidiference funkcije kot diskretnih analogov odvoda in nedoločenega integrala raziščemo metode računanja končnih vsot, ki jih interpretiramo kot diskretni analog določenega integrala.

1 Uvod

Diskretni račun je matematično področje, ki se ukvarja z računanjem vsot s končno mnogo členi. Razumemo ga lahko kot diskretni analog diferencialnega in integralnega računa, v katerem pojem odvoda zamenja razlika zaporednih členov, določeni integral pa vsota s končnim številom členov. Takim vsotam bomo rekli *končne vsote*.

Med najbolj znanimi končnimi vsotami je vsota prvih n naravnih števil, za katero velja znana formula

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}.$$

Do te formule lahko pridemo na več različnih načinov, na primer algebraično ali geometrijsko, najpogosteje pa se jo dokaže z indukcijo. Težava z indukcijo je, da moramo formulo vnaprej poznati. Kako bi na primer uganili formulo za vsoto prvih n kvadratov

$$1^2 + 2^2 + 3^2 + \cdots + n^2,$$

ki nima tako lepe formule kot prejšnja vsota? Pri tovrstnih vprašanjih nam diskretni račun ponudi sistematično orodje reševanja.

Preden se potopimo v svet diskretnega računa, uvedimo še primerno notacijo. Vsoto členov zaporedja $a_1, a_2, a_3 \ldots, a_n$ bomo označevali z

$$\sum_{k=1}^{n} a_k = a_1 + a_2 + a_3 + \cdots + a_n,$$

kjer grška Σ (sigma) ponazarja besedo "vsota" (lat. *summa*). Indeks k, po katerem seštevamo, imenujemo *sumacijski indeks*. Izbira oznake sumacijskega indeksa je poljubna:

$$\sum_{k=1}^{n} a_k = \sum_{i=1}^{n} a_i = \sum_{x=1}^{n} a_x.$$

Formulo za vsoto prvih n naravnih števil lahko sedaj kompaktno zapišemo kot

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}.$$

V diskretnem računu se člene vsote pogosto obravnava kot vrednosti funkcije, tj. $a_k = f(k)$. Vsota prvih n členov zaporedja potem postane

$$\sum_{x=1}^{n} f(x) = f(1) + f(2) + f(3) + \cdots + f(n).$$

Na primer, pri vsoti prvih n naravnih števil seštevamo vrednosti funkcije $f(x) = x$, pri vsoti prvih n kvadratov pa vrednosti funkcije $f(x) = x^2$.

Ker bomo funkcije skozi celotni članek obravnavali kot člene neke vsote, bo njihovo definicijsko območje vedno vsebovano v množici celih števil $\mathbb{Z}$.

2 Diferenca funkcije

Definicija 2.1. ***Diferenca*** *funkcije $f(x)$ je izraz*

$$\Delta f(x) = f(x+1) - f(x).$$

Simbolu Δ pravimo ***diferenčni operator****.*

Diferenca funkcije šteje, za koliko se v naslednjem koraku spremeni vrednost funkcije. To lahko predstavimo tudi z enačbo

$$f(x+1) = f(x) + \Delta f(x). \tag{1}$$

Drugače povedano, da pridemo do naslednje vrednosti funkcije, moramo prejšnji vrednosti prišteti diferenco.

Zgled 2.1. *Poračunajmo diference osnovnih funkcij.*

(1) *Ker se vrednost konstantne funkcije ne spreminja, je njena diferenca enaka* 0*. To bi lahko preverili tudi z računom*

$$\Delta c = c - c = 0.$$

(2) *Vrednost funkcije $f(x) = x$ se v vsakem koraku poveča za natanko eno enoto, kot pokaže račun*

$$\Delta x = x + 1 - x = 1.$$

(3) *V primeru kvadratne funkcije $f(x) = x^2$ je diferenco že malce težje ugotoviti. Račun pokaže*

$$\Delta x^2 = (x+1)^2 - x^2 = x^2 + 2x + 1 - x^2 = 2x + 1.$$

Na enak način poračunamo diferenco funkcije $f(x) = x^3$, ki je enaka

$$\Delta x^3 = 3x^2 + 3x + 1.$$

(4) *Diferenca eksponentne funkcije z osnovo $a \geq 0$ je enaka*

$$\Delta a^x = a^{x+1} - a^x = (a-1)a^x.$$

Ista formula velja tudi, kadar je $a < 0$ (eksponentna funkcija z negativno osnovo je v našem primeru dobro definirana, saj smo predpostavili, da je definicijsko območje vseh obravnavanih funkcij vsebovano v množici celih števil).

Pri $a = 2$ dobimo

$$\Delta 2^x = 2^x.$$

(5) *V primeru logaritemske funkcije z osnovo $a > 0$ velja*

$$\Delta \log_a(x) = \log_a(x+1) - \log_a(x) = \log_a\left(\frac{x+1}{x}\right) = \log_a\left(1 + \frac{1}{x}\right).$$

(6) *Iz formul za faktorizacijo kotnih funkcij sledita zvezi*

$$\Delta \sin(ax+b) = 2\sin\left(\frac{a}{2}\right)\cos\left(ax+b+\frac{a}{2}\right),$$
$$\Delta \cos(ax+b) = -2\sin\left(\frac{a}{2}\right)\sin\left(ax+b+\frac{a}{2}\right).$$

Ker diference funkcije ne želimo vsakič računati po definiciji, si oglejmo nekaj lastnosti, ki jim zadošča diferenčni operator.

Trditev 2.1 (**Linearnost diferenčnega operatorja**)**.** *Diferenčni operator Δ je **linearen**, tj. zadošča lastnostma*

(*i*) $\Delta[f(x) + g(x)] = \Delta f(x) + \Delta g(x)$,

(*ii*) $\Delta[c \cdot f(x)] = c \cdot \Delta f(x)$.

Dokaz. Lastnosti preprosto sledita iz definicije diference:

(*i*)

$$\begin{aligned}\Delta[f(x) + g(x)] &= f(x+1) + g(x+1) - (f(x) + g(x)) \\ &= f(x+1) - f(x) + g(x+1) - g(x) \\ &= \Delta f(x) + \Delta g(x),\end{aligned}$$

(*ii*)

$$\begin{aligned}\Delta[c \cdot f(x)] &= c \cdot f(x+1) - c \cdot f(x) \\ &= c \cdot (f(x+1) - f(x)) \\ &= c \cdot \Delta f(x).\end{aligned}$$

□

Trditev 2.2 (**Pravilo produkta**)**.** *Diferenca produkta dveh funkcij zadošča pravilu*

$$\Delta[f(x) \cdot g(x)] = \Delta f(x) \cdot g(x+1) + f(x) \cdot \Delta g(x).$$

Dokaz. Upoštevajoč formulo (1) in definicijo diference, velja račun

$$\begin{aligned}\Delta[f(x) \cdot g(x)] &= f(x+1) \cdot g(x+1) - f(x) \cdot g(x) \\ &= (f(x) + \Delta f(x)) \cdot g(x+1) - f(x) \cdot g(x) \\ &= \Delta f(x) \cdot g(x+1) + f(x) \cdot g(x+1) - f(x) \cdot g(x) \\ &= \Delta f(x) \cdot g(x+1) + f(x) \cdot \Delta g(x).\end{aligned}$$

□

Opomba 2.1. *Imamo tudi naslednjo formulo za diferenco kvocienta dveh funkcij*

$$\Delta\left[\frac{f(x)}{g(x)}\right] = \frac{\Delta f(x) g(x) - f(x) \Delta g(x)}{g(x) g(x+1)},$$

ki pa je v tem članku ne bomo potrebovali.

2.1 Padajoče potence

Pri računanju diferenc znanih funkcij smo opazili, da diference potenčnih funkcij $f(x) = x^m$ nimajo prav lepe oblike, ko je $m \geq 2$. Oglejmo si še enkrat formulo, ko je $m = 2$:

$$\Delta x^2 = 2x + 1.$$

Vemo, da je $\Delta x = 1$, torej lahko zgornjo formulo zapišemo kot

$$\Delta x^2 - \Delta x = 2x.$$

Po linearnosti lahko razliko diferenc na levi strani zapišemo kot diferenco razlike, kar pokaže

$$\Delta[x^2 - x] = 2x,$$

oziroma

$$\Delta[x(x-1)] = 2x. \tag{2}$$

Diferenca izraza $x(x-1)(x-2)$ ima tudi lepo obliko, in sicer

$$\Delta[x(x-1)(x-2)] = 3x(x-1). \tag{3}$$

To nas motivira vpeljati naslednjo definicijo.

Definicija 2.2. ***Padajoča potenca*** *števila x je izraz*

$$x^{\underline{m}} = \overbrace{x(x-1)(x-2)\cdots(x-m+1)}^{m \text{ členov}},$$

kjer je $m \in \mathbb{N}$. Oznako $x^{\underline{m}}$ preberemo kot "x na m padajoče". Po dogovoru je $x^{\underline{0}} = 1$.

V novih oznakah imata formuli (2) in (3) sedaj obliko

$$\Delta x^{\underline{2}} = 2x^{\underline{1}},$$

$$\Delta x^{\underline{3}} = 3x^{\underline{2}}.$$

To nas vodi do naslednjega sklepa.

Izrek 2.1. *Za vsako naravno število m velja*

$$\Delta x^{\underline{m}} = m \cdot x^{\underline{m-1}}.$$

Dokaz. Ker je $\Delta x = 1$ in $x^{\underline{0}} = 1$, formula drži za $m = 1$. Za $m \geq 2$ velja račun

$$\begin{aligned}
\Delta x^{\underline{m}} &= (x+1)^{\underline{m}} - x^{\underline{m}} \\
&= (x+1)x(x-1)\cdots(x-m+2) - x(x-1)(x-2)\cdots(x-m+2)(x-m+1) \\
&= x(x-1)(x-2)\cdots(x-m+2)((x+1) - (x-m+1) \\
&= m \cdot x^{\underline{m-1}}.
\end{aligned}$$

□

2.2 Negativne padajoče potence

Padajočo potenco lahko razširimo na negativne potence, in sicer preko formule

$$x^{\underline{m}} = (x - m + 1)x^{\underline{m-1}}. \tag{4}$$

Zgornja formula podaja induktivno zvezo, ki ji padajoča potenca zadošča. Za definicijo padajoče potence bi lahko uporabili tudi to formulo, le podati bi morali še začetni člen $x^{\underline{0}}$, ki smo mu po dogovoru dali vrednost 1. Vse višje padajoče potence se potem da poračunati z uporabo (4). Če v (4) izrazimo $x^{\underline{m-1}}$ in zamaknemo potenco, dobimo zvezo

$$x^{\underline{m}} = \frac{x^{\underline{m+1}}}{x - m}.$$

Ta nam pove, kako izračunati $x^{\underline{m}}$, če poznamo $x^{\underline{m+1}}$. To nas vodi do definicije **negativne padajoče potence**

$$x^{\underline{-m}} = \frac{1}{(x+1)(x+2)\cdots(x+m)},$$

kjer je $m \in \mathbb{N}$.

Pokažimo, da za diferenco negativne padajoče potence velja ista formula kot za pozitivne padajoče potence.

Trditev 2.3. *Za vsak $m \in \mathbb{N} \cup \{0\}$ velja*

$$\Delta x^{\underline{-m}} = -m \cdot x^{\underline{-m-1}}.$$

Dokaz. Dokaz je zelo podoben dokazu izreka 2.1, le da tukaj sedaj nastopijo ulomki. Za $m = 0$ formula očitno drži, za $m \geq 1$ pa velja račun

$$\begin{aligned}
\Delta x^{\underline{-m}} &= (x+1)^{\underline{-m}} - x^{\underline{-m}} \\
&= \frac{1}{(x+2)(x+3)\cdots(x+m)(x+m+1)} - \frac{1}{(x+1)(x+2)\cdots(x+m)} \\
&= \frac{x+1-(x+m+1)}{(x+1)(x+2)\cdots(x+m+1)} \\
&= -m \cdot x^{\underline{-m-1}}.
\end{aligned}$$

□

V tabeli 1 so zbrane diference funkcij, ki jih bomo uporabili v nadaljevanju članka.

$f(x)$	$\Delta f(x)$
c	0
x	1
$x^{\underline{m}}, m \in \mathbb{Z}$	$m \cdot x^{\underline{m-1}}$
a^x	$a^x(a-1)$
2^x	2^x
$\sin(ax+b)$	$2\sin\left(\frac{a}{2}\right)\cos\left(ax+b+\frac{a}{2}\right)$
$\cos(ax+b)$	$-2\sin\left(\frac{a}{2}\right)\sin\left(ax+b+\frac{a}{2}\right)$

Tabela 1: Diference osnovnih funkcij.

3 Antidiferenca

Bralcem, ki poznajo pojem odvoda in integrala, naslednja definicija ne bi smela biti preveč tuja.

Definicija 3.1. *Funkciji $F(x)$, za katero velja*

$$\Delta F(x) = f(x)$$

pravimo ***antidiferenca*** *funkcije $f(x)$.*

Antidiferenca služi kot neke vrste inverz diferenčnega operatorja. Razlog, zakaj je pojem antidiference tako pomemben, bomo spoznali v naslednjem poglavju, v tem poglavju pa bomo razvili metode računanja antidiferenc funkcij.

Preden začnemo s primeri, povejmo besedo še o enoličnosti antidiference. Recimo, da je poleg $F(x)$ tudi $G(x)$ antidiferenca funkcije $f(x)$. Potem velja

$$\Delta F(x) = f(x) = \Delta G(x).$$

Po linearnosti diferenčnega operatorja lahko zgornjo enakost zapišemo kot

$$\Delta(G(x) - F(x)) = 0.$$

Definirajmo novo funkcijo $C(x) = G(x) - F(x)$. Po zgornji enačbi zanjo velja

$$\Delta C(x) = 0.$$

Ta enačba pove, da se vrednosti funkcije $C(x)$ ne spreminjajo, torej je $C(x)$ konstantna funkcija. Pišimo $C(x) = C$. Po definiciji funkcije $C(x)$ velja

$$G(x) - F(x) = C,$$

oziroma

$$G(x) = F(x) + C.$$

Pokazali smo, da če poznamo eno antidiferenco $F(x)$ funkcije $f(x)$, so vse ostale antidiference oblike $F(x) + C$ za poljubno konstanto C.

Definicija 3.2. *Družino vseh antidiferenc označimo z*

$$\sum_x f(x) = F(x) + C$$

in ji pravimo ***nedoločena vsota*** *funkcije $f(x)$.*

Da izračunamo antidiferenco neke funkcije $f(x)$, moramo poiskati takšno funkcijo $F(x)$, katere diferenca se ujema s funkcijo $f(x)$. Diference pomembnih funkcij imamo zbrane v tabeli 1. Iz nje lahko na primer razberemo, da je $\Delta x = 1$, kar nam pove, da je antidiferenca konstantne funkcije $f(x) = 1$ enaka identični funkciji, tj.

$$\sum_x 1 = x + C.$$

Podobno lahko sklepamo, da je antidiferenca funkcije 2^x kar funkcija sama, saj velja $\Delta 2^x = 2^x$. Za padajoče potence velja zveza

$$\Delta x^{\underline{m}} = m \cdot x^{\underline{m-1}}.$$

Po linearnosti diferenčnega operatorja torej velja

$$\Delta \left[\frac{x^{\underline{m}}}{m} \right] = x^{\underline{m-1}},$$

kar pokaže

$$\sum_x x^{\underline{m-1}} = \frac{x^{\underline{m}}}{m} + C.$$

Ta formula velja za $m \neq 0$. V primeru, ko je $m = 0$ in računamo antidiferenco funkcije $x^{\underline{-1}} = \frac{1}{x+1}$, je težje izračunati antidiferenco. Da pridemo do nje, moramo malo goljufati in preskočiti do izreka 4.1, ki nam izraža antidiferenco funkcije s končno vsoto. V našem primeru je to vsota

$$H_x = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{x}.$$

Enostavno je preveriti, da je diferenca zgornje vsote res enaka $\frac{1}{x+1}$. Števila H_x, kjer je $x \in \mathbb{N}$, imenujemo **harmonična števila**.

Če upoštevamo še druge vrstice v tabeli 1, lahko zapišemo tabelo antidiferenc pripadajočih funkcij (glej tabelo 2).

$f(x)$	Antidiferenca $f(x)$
1	x
$x^{\underline{m}}, m \neq -1$	$\frac{x^{\underline{m+1}}}{m+1}$
$a^x, a \neq 1$	$\frac{a^x}{a-1}$
2^x	2^x
$\sin(ax+b), a \neq 2\pi k$	$-\frac{1}{2\sin\left(\frac{a}{2}\right)} \cos\left(ax+b-\frac{a}{2}\right)$
$\cos(ax+b), a \neq 2\pi k$	$\frac{1}{2\sin\left(\frac{a}{2}\right)} \sin\left(ax+b-\frac{a}{2}\right)$

Tabela 2: Antidiference osnovnih funkcij.

V tabeli 2 moramo paziti, da ni dovoljeno vstaviti vseh vrednosti parametrov m, a in b. Primer padajoče potence pri $m = -1$ smo že razrešili. Prav tako je jasno, kaj je antidiferenca eksponentne funkcije z osnovo $a = 1$. Pri računanju antidiference kotnih funkcij za $a = 2\pi k$, kjer je $k \in \mathbb{Z}$, si pomagamo z naslednjo trditvijo.

Trditev 3.1. *Naj bo $f(x)$ funkcija s periodo T, tj. $f(x+T) = f(x)$ za vsak x. Potem velja*

$$\sum_x f(Tx+b) = x \cdot f(Tx+b) + C.$$

Dokaz. Velja račun

$$\begin{aligned}
\Delta[x \cdot f(Tx+b)] &= (x+1) \cdot f(T(x+1)+b) - x \cdot f(Tx+b) \\
&= (x+1) \cdot f(Tx+b+T) - x \cdot f(Tx+b) \\
&= (x+1) \cdot f(Tx+b) - x \cdot f(Tx+b) \\
&= f(Tx+b)(x+1-x) \\
&= f(Tx+b).
\end{aligned}$$

□

Zgled 3.1. *Z uporabo tabele 2 in trditve 3.1 lahko poračunamo*

$$\sum_x \cos x = \frac{1}{2\sin\frac{1}{2}} \sin\left(x - \frac{1}{2}\right) + C,$$

$$\sum_x \cos(2\pi x) = x \cos(2\pi x) + C.$$

Kot smo že omenili, nam antidiferenca, in s tem tudi nedoločena vsota, podajata nekakšen inverz diference. Linearnost, ki ji zadošča diferenčni operator Δ, se zato prenese tudi na nedoločeno vsoto.

Trditev 3.2 (**Linearnost nedoločene vsote**). *Nedoločena vsota je linearna, tj. velja*

(*i*) $\sum_x [f(x) + g(x)] = \sum_x f(x) + \sum_x g(x)$,

(*ii*) $\sum_x [c \cdot f(x)] = c \cdot \sum_x f(x)$.

Čeprav je dokaz te trditve lahek, je precej tehničen, zato ga bomo izpustili.
Še ena metoda za računanje nedoločenih vsot pride iz pravila produkta

$$\Delta[f(x) \cdot g(x)] = \Delta f(x) \cdot g(x+1) + f(x) \cdot \Delta g(x).$$

Če uporabimo nedoločeno vsoto Σ_x na obeh straneh zgornje enačbe, se na levi strani Σ_x izniči z Δ, saj sta si drug drugemu inverzna, in dobimo

$$f(x) \cdot g(x) = \sum_x \Delta f(x) \cdot g(x+1) + \sum_x f(x) \cdot \Delta g(x).$$

Od tod sledi formula za seštevanje po delih, ki je diskretni analog metode per partes.

Izrek 3.1 (**Seštevanje po delih**). *Velja*

$$\sum_x f(x) \cdot \Delta g(x) = f(x) \cdot g(x) - \sum_x \Delta f(x) \cdot g(x+1).$$

Zgled 3.2. *Oglejmo si uporabo metode seštevanja po delih na nedoločeni vsoti*

$$\sum_x (x-1) \sin\left(\frac{\pi x}{2}\right).$$

Glavna ideja metode je, da za $f(x)$ in $\Delta g(x)$ izberemo takšni funkciji, da bosta izraza $\Delta f(x)$ in $g(x)$ enostavnejša. V našem primeru lahko vzamemo

$$f(x) = x - 1, \qquad \Delta g(x) = \sin\left(\frac{\pi x}{2}\right).$$

Potem je

$$\Delta f(x) = 1$$

in

$$g(x) = -\frac{1}{2\sin\left(\frac{\pi}{4}\right)} \cos\left(\frac{\pi x}{2} - \frac{\pi}{4}\right) = -\frac{1}{\sqrt{2}} \cos\left(\frac{\pi x}{2} - \frac{\pi}{4}\right).$$

Po seštevanju po delih je iskana nedoločena vsota enaka

$$\begin{aligned}
&(x-1) \cdot \left(-\frac{1}{\sqrt{2}} \cos\left(\frac{\pi x}{2} - \frac{\pi}{4}\right)\right) - \sum_x 1 \cdot \left(-\frac{1}{\sqrt{2}} \cos\left(\frac{\pi(x+1)}{2} - \frac{\pi}{4}\right)\right) = \\
&= \frac{1}{\sqrt{2}}(1-x) \cos\left(\frac{\pi x}{2} - \frac{\pi}{4}\right) + \frac{1}{\sqrt{2}} \sum_x \cos\left(\frac{\pi x}{2} + \frac{\pi}{4}\right) \\
&= \frac{1}{\sqrt{2}}(1-x) \cos\left(\frac{\pi x}{2} - \frac{\pi}{4}\right) + \frac{1}{2} \sin\left(\frac{\pi x}{2}\right).
\end{aligned}$$

4 Računanje končnih vsot

Povezavo med končno vsoto in nedoločeno vsoto podaja naslednji izrek.

Izrek 4.1 (**Osnovni izrek diskretnega računa**). *Naj bo $F(x)$ antidiferenca $f(x)$ in $b > a$ celi števili. Potem velja*

$$\sum_{x=a}^{b} f(x) = F(b+1) - F(a).$$

Če vpeljemo oznako $F(x)\Big|_a^b = F(b) - F(a)$, lahko zgornji izrek zapišemo kot

$$\sum_{x=a}^{b} f(x) = F(x)\Big|_a^{b+1},$$

kjer je

$$\sum_x f(x) = F(x) + C.$$

Dokaz. Po definiciji antidiference je $\Delta F(x) = f(x)$, zato velja

$$\begin{aligned}
\sum_{x=a}^{b} f(x) &= \sum_{x=a}^{b} \Delta F(x) \\
&= \sum_{x=a}^{b} [F(x+1) - F(x)] \\
&= F(a+1) - F(a) + F(a+2) - F(a+1) + F(a+3) - F(a+2) + \cdots + \\
&\qquad + F(b) - F(b-1) + F(b+1) - F(b) \\
&= F(b+1) - F(a),
\end{aligned}$$

kjer smo v zadnjem koraku upoštevali, da se odštejejo vsi členi, razen dveh. □

Zgled 4.1. (1) *Poiščimo formulo za vsoto*

$$1^2 + 2^2 + 3^2 + \cdots + n^2.$$

Če želimo uporabiti izrek 4.1, moramo izračunati nedoločeno vsoto funkcije x^2. Poznane so nam že nedoločene vsote padajočih potenc, zato si pomagajmo z njimi:

$$\begin{aligned}
\sum_{x=1}^{n} x^2 = \sum_{x=1}^{n} \left[x^2 - x + x\right] = \sum_{x=1}^{n} [x(x-1) + x] = \sum_{x=1}^{n} x^{\underline{2}} + \sum_{x=1}^{n} x^{\underline{1}} = \frac{x^{\underline{3}}}{3}\Big|_1^{n+1} + \frac{x^{\underline{2}}}{2}\Big|_1^{n+1} = \\
= \frac{x(x-1)(x-2)}{3}\Big|_1^{n+1} + \frac{x(x-1)}{2}\Big|_1^{n+1} = \frac{n(n+1)(n-1)}{3} - 0 + \left(\frac{n(n+1)}{2} - 0\right) = \\
= \frac{n(n+1)(2n+1)}{6}.
\end{aligned}$$

(2) *Izračunajmo vsoto prvih n členov vrste*

$$\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \cdots.$$

Ta vsota ima v sumacijski notaciji obliko

$$\sum_{x=0}^{n} \frac{1}{(x+1)(x+2)}.$$

Iščemo torej nedoločeno vsoto izraza $\frac{1}{(x+1)(x+2)}$. *To pa je ravno definicija padajoče potence* $x^{\underline{-2}}$. *Iskana vsota je enaka*

$$\sum_{x=0}^{n} x^{\underline{-2}} = \frac{x^{\underline{-1}}}{-1}\bigg|_0^{n+1} = -\frac{1}{x+1}\bigg|_0^{n+1} = -\left(\frac{1}{n+2} - 1\right) = 1 - \frac{1}{n+2}.$$

(3) *Izračunajmo vsoto prvih n kubov, tj. vsoto*

$$\sum_{x=1}^{n} x^3.$$

Ker poznamo antidiference padajočih potenc, se nam splača izraz x^3 *zapisati kot linearno kombinacijo padajočih potenc nižje ali enake stopnje. Iščemo torej takšne konstante* a, b, c *in* d, *da velja*

$$x^3 = ax^{\underline{3}} + bx^{\underline{2}} + cx^{\underline{1}} + d.$$

Če v zgornji enačbi upoštevamo definicijo padajočih potenc in razstavimo ulomke, dobimo

$$x^3 = ax^3 - 3ax^2 + 2ax + bx^2 - bx + cx + d.$$

Zgornjo enakost lahko sedaj gledamo kot enakost polinomov v spremenljivki x. *Ker sta dva polinoma enaka natanko tedaj, ko imata enake koeficiente, lahko koeficiente pred istimi stopnjami enačimo, kar nas privede do sistema linearnih enačb*

$$\begin{aligned} 1 &= a, \\ 0 &= -3a + b, \\ 0 &= 2a - b + c, \\ 0 &= d. \end{aligned}$$

Dobimo $a = 1$, $b = 3$, $c = 1$ *in* $d = 0$. *Polinom* x^3 *lahko torej zapišemo kot*

$$x^3 = x^{\underline{3}} + 3x^{\underline{2}} + x^{\underline{1}}.$$

Po linearnosti nedoločene vsote velja

$$\sum_x \left[x^{\underline{3}} + 3x^{\underline{2}} + x^{\underline{1}}\right] = \frac{x^{\underline{4}}}{4} + 3\frac{x^{\underline{3}}}{3} + \frac{x^{\underline{2}}}{2} + C.$$

Začetna vsota je torej enaka

$$\begin{aligned} \left(\frac{x^{\underline{4}}}{4} + x^{\underline{3}} + \frac{x^{\underline{2}}}{2}\right)\bigg|_1^{n+1} &= \left(\frac{x(x-1)(x-2)(x-3)}{4} + x(x-1)(x-2) + \frac{x(x-1)}{2}\right)\bigg|_1^{n+1} \\ &= \frac{(n+1)n(n-1)(n-2)}{4} + (n+1)n(n-1) + \frac{(n+1)n}{2} - (0+0+0). \end{aligned}$$

Zadnja vrstica se poenostavi do izraza

$$\left(\frac{n(n+1)}{2}\right)^2.$$

Če upoštevamo formulo za izračun vsote prvih n naravnih števil, pridemo do zanimivega spoznanja: vsota prvih n kubov je enaka kvadratu vsote prvih n naravnih števil

$$1^3 + 2^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2.$$

(4) *Dajmo še s pomočjo diskretnega računa izračunati prvih n členov geometrijske vrste*

$$1 + a + a^2 + \cdots .$$

Ta vsota je enaka

$$\sum_{x=0}^{n} a^x = \frac{a^x}{a-1}\Big|_0^{n+1} = \frac{a^{n+1}}{a-1} - \frac{1}{a-1} = \frac{a^{n+1}-1}{a-1}.$$

Če želimo pri računanju končne vsote uporabiti seštevanje po delih, moramo paziti, da meje porazdelimo na oba člena.

Zgled 4.2. *Oglejmo si vsoto*

$$\sum_{x=1}^{n} (x+1)(x+2) \cdot 2^x.$$

Opazimo, da je izraz $(x+1)(x+2)$ ravno enak zamaknjeni padajoči potenci $(x+2)^{\underline{2}}$. Enostavno je preveriti, da tudi za zamaknjene padajoče potence veljajo iste formule kot za padajoče potence, in sicer imamo

$$\sum_x (x+a)^{\underline{m}} = \frac{(x+a)^{\underline{m+1}}}{m+1}.$$

Uporabimo seštevanje po delih za funkciji

$$\begin{aligned} f(x) &= (x+2)^{\underline{2}}, & \Delta g(x) &= 2^x, \\ \Delta f(x) &= 2(x+2)^{\underline{1}}, & g(x) &= 2^x, \end{aligned}$$

po katerem je začetna vsota enaka

$$\begin{aligned} &(x+2)^{\underline{2}} \cdot 2^x\Big|_1^{n+1} - \sum_{x=1}^{n} 2(x+2)^{\underline{1}} \cdot 2^{x+1} = \\ &= (x+2)(x+1) \cdot 2^x\Big|_1^{n+1} - 4\sum_{x=1}^{n} (x+2) \cdot 2^x = \\ &= (n+3)(n+2) \cdot 2^{n+1} - 12 - 4\sum_{x=1}^{n} (x+2) \cdot 2^x. \end{aligned}$$

Vsoto v zadnji vrstici lahko ponovno poračunamo s pomočjo seštevanja po delih. Če za funkciji izberemo

$$\begin{aligned} u(x) &= x+2, & \Delta v(x) &= 2^x, \\ \Delta u(x) &= 1, & v(x) &= 2^x, \end{aligned}$$

dobimo

$$\begin{aligned} \sum_{x=1}^{n} (x+2) \cdot 2^x &= (x+2) \cdot 2^x\Big|_1^{n+1} - \sum_{x=1}^{n} 2^{x+1} = \\ &= (n+3) \cdot 2^{n+1} - 6 - 2 \cdot 2^x\Big|_1^{n+1} = \\ &= (n+3) \cdot 2^{n+1} - 6 - 2(2^{n+1} - 2) = \\ &= (n+1) \cdot 2^{n+1} - 2. \end{aligned}$$

Če to vstavimo v prejšnji izraz in poenostavimo, dobimo rezultat

$$\sum_{x=1}^{n}(x+1)(x+2)\cdot 2^x = (n+2)(n+1)\cdot 2^{n+1} - 4.$$

Za konec rešimo še eno težjo nalogo.

Naloga 4.1. *Poišči vsoto prvih n členov vrste*

$$\frac{1^2\cdot 4}{2\cdot 3} + \frac{2^2\cdot 4^2}{3\cdot 4} + \frac{3^2\cdot 4^3}{4\cdot 5} + \cdots$$

Rešitev. *Računamo vsoto*

$$\sum_{x=1}^{n}\frac{x^2\cdot 4^x}{(x+1)(x+2)}.$$

Na prvi pogled se zdi, da bi lahko uporabili seštevanje po delih. Vendar diferenca, kot tudi antidiferenca, izraza $\frac{x^2}{(x+1)(x+2)}$ *nima enostavne oblike in s seštevanjem po delih ne bi prevedli začetne vsote na lažjo vsoto. Tako nam ne preostane drugega. kot da antidiferenco izraza v vsoti poiščemo po definiciji. Iščemo torej takšno funkcijo* $F(x)$*, za katero velja*

$$F(x+1) - F(x) = \frac{x^2\cdot 4^x}{(x+1)(x+2)}. \tag{5}$$

Desna stran zgornje enačbe je produkt racionalne funkcije in eksponentne funkcije 4^x*, zato lahko sklepamo, da mora biti iste oblike tudi funkcija* $F(x)$*. Pišimo*

$$F(x) = 4^x\cdot Q(x),$$

kjer je $Q(x)$ *neka racionalna funkcija. Če to vstavimo nazaj v izraz (5), dobimo*

$$4^{x+1}\cdot Q(x+1) - 4^x\cdot Q(x) = \frac{x^2\cdot 4^x}{(x+1)(x+2)}.$$

Opazimo, da lahko na obeh straneh enačbe krajšamo z izrazom 4^x*, kar nas privede do enačbe*

$$4Q(x+1) - Q(x) = \frac{x^2}{(x+1)(x+2)}. \tag{6}$$

Funkcija na desni strani enačbe ima pola pri -1 *in* -2*, zato mora imeti ista pola tudi funkcija na levi strani enačbe. Opazimo, da če ima* $Q(x)$ *pol pri* a*, potem ima* $Q(x+1)$ *pol pri* $a-1$*. Če hočemo, da ima leva stran enačbe želena pola, je torej dovolj vzeti takšno racionalno funkcijo* $Q(x)$*, ki ima en pol pri* $a=-1$*. Funkcijo* $Q(x)$ *iščemo v obliki*

$$Q(x) = \frac{p(x)}{x+1},$$

kjer je $p(x)$ *nek polinom. Če ta izraz za* $Q(x)$ *vstavimo nazaj v (6), dobimo*

$$\frac{4p(x+1)}{x+2} - \frac{p(x)}{x+1} = \frac{x^2}{(x+1)(x+2)}.$$

Če se znebimo ulomkov, ostanemo s polinomsko funkcijsko enačbo

$$4p(x+1)(x+1) - p(x)(x+2) = x^2. \tag{7}$$

Dobljeni enačbi lahko zadošča le polinom stopnje manjše ali enake 1*, torej oblike*

$$p(x) = bx + c.$$

Če ta predpis vstavimo nazaj v (7), dobimo

$$4(b(x+1)+c)(x+1)-(bx+c)(x+2)=x^2.$$

Pokažimo še en postopek iskanja vrednosti parametrov v polinomski enačbi. Če v enačbo namesto x zaporedoma vstavimo vrednosti -1 in 0, dobimo enačbi

$$\begin{aligned}0-(-b+c)&=1,\\4(b+c)-2c&=0.\end{aligned}$$

Ta sistem rešita parametra $b=\frac{1}{3}$ in $c=-\frac{2}{3}$, ki nam dasta polinom

$$p(x)=\frac{1}{3}x-\frac{2}{3}.$$

Sedaj poznamo predpis racionalne funkcije

$$Q(x)=\frac{p(x)}{x+1}=\frac{x-2}{3(x+1)}.$$

in posredno še antidiference

$$F(x)=4^x\cdot Q(x)=\frac{4^x(x-2)}{3(x+1)}.$$

Vrednost iskane vsote je enaka

$$\sum_{x=1}^{n}\frac{x^2\cdot 4^x}{(x+1)(x+2)}=\frac{4^x(x-2)}{3(x+1)}\bigg|_1^{n+1}=\frac{4^{n+1}(n-1)}{3(n+2)}+\frac{2}{3}.$$

Literatura

[1] G. Boole, *Calculus of Finite Differences*, Chelsea Scientific Books **5**, Chelsea Publishing Company, New York, 1970.

[2] D. F. Gleich, *Finite Calculus: A tutorial for solving nasty sums*, dostopno na `https://www.cs.purdue.edu/homes/dgleich/publications/Gleich%202005%20-%20hierarchical%20directed%20spectral.pdf`.

Teorija grup in Rubikova kocka

Martin Flisar, Jaka Horvat, Naja Oblak
Mentor*: Jakob Žorž*

Povzetek

V članku definiramo pojme in dokažemo osnovne izreke iz teorije grup. S tem znanjem izračunamo število dosegljivih permutacij Rubikove kocke.

1 Uvod

Vsi smo že kdaj preizkusili svojo kapaciteto za prostorsko mišljenje z vrtenjem Rubikove kocke. Nekaterim nam jo je celo uspelo pospremiti iz kaotične zmešnjave v tisto najčistejše stanje, v katerem se vsaka barva zadržuje na svoji ploskvi. Večina nas je pri tem podvigu sledila enemu izmed splošno predpisanih postopkov, ki jih dandanes kar mrgoli na medmrežju.

Podmnožica teh nas je pomislila tudi na izvor takih receptov – le kako se je nekemu srečnežu uspelo dokopati do takšne modrosti?

Le redki pa so šli še dlje in se potopili v globlje skrivnosti. Katera stanja so dosegljiva in koliko jih sploh je?

Odgovor na ta in mnoga druga vprašanja o tej zloglasni igrači najdemo v teoriji grup.

2 Grupe

Definicija 2.1. *Naj bo G množica in $\cdot$ binarna operacija v G, torej $\cdot : G \times G \to G$. Vrednost operacije $\cdot(a, b)$ raje krajše zapišemo kot $a \cdot b$ in ji pravimo* produkt *elementov a in b. Par $(G, \cdot)$ je* grupa*, če:*

- *za vse $a, b, c \in G$ velja $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (asociativnost),*
- *v G obstaja tak e, da za vsak $a \in G$ velja $e \cdot a = a$ (enota),*
- *za vsak $a \in G$ obstaja $a^{-1} \in G$, da velja $a^{-1} \cdot a = e$ (inverz).*

Trditev 2.1. *Naj bo $(G, \cdot)$ grupa in naj bodo a, b in c elementi grupe G. Iz začetnih pogojev lahko dokažemo naslednje trditve.*

1. *Enota deluje tudi z desne, torej $a \cdot e = a$.*
2. *Velja $(a^{-1})^{-1} = a$.*
3. *Inverz deluje tudi z desne, torej $a \cdot a^{-1} = e$.*
4. *Enota je enoličnа.*
5. *Inverz je enoličen.*
6. *Če velja $a \cdot b = a \cdot c$, potem je $b = c$.*

Dokaz. V prvih treh točkah z a^{-1} označimo poljuben element, za katerega velja $a^{-1} \cdot a = e$; da je tak element enolično določen, pokažemo šele v peti točki.

1. Vemo, da je $a^{-1} \cdot a = e$. Če a zamenjamo z a^{-1}, dobimo
$$(a^{-1})^{-1} \cdot a^{-1} = e.$$
Če to enačbo z desne pomnožimo z a, dobimo
$$(a^{-1})^{-1} \cdot a^{-1} \cdot a = e \cdot a = a.$$
Ker pa je $a^{-1} \cdot a = e$, je leva stran enaka $(a^{-1})^{-1} \cdot e$, torej velja
$$(a^{-1})^{-1} \cdot e = a.$$
Če zadnjo enačbo z desne pomnožimo še z e in upoštevamo $e \cdot e = e$, dobimo
$$(a^{-1})^{-1} \cdot e = (a^{-1})^{-1} \cdot e \cdot e = a \cdot e.$$
Leva stran je po prejšnji enačbi enaka a, torej je $a \cdot e = a$ in enota res deluje tudi z desne.
2. Zdaj vemo, da enota deluje tudi z desne, zato je v enačbi $(a^{-1})^{-1} \cdot e = a \cdot e$ leva stran enaka $(a^{-1})^{-1}$, desna pa a. Dobimo torej še $(a^{-1})^{-1} = a$.
3. Sedaj pa lahko iz že izpeljane enačbe $(a^{-1})^{-1} \cdot a^{-1} = e$ z uporabo $(a^{-1})^{-1} = a$ dobimo še $a \cdot a^{-1} = e$.
4. Predpostavimo, da enota e ni enolična, torej da obstajata enoti e_1 in e_2, kjer $e_1 \neq e_2$. Potem velja $e_1 = e_1 \cdot e_2 = e_2$, kar pa je protislovje, torej je enota res enolična.
5. Predpostavimo, da obstajata inverza a_1^{-1} in a_2^{-1}, kjer $a_1^{-1} \neq a_2^{-1}$, da je $a \cdot a_1^{-1} = e$ in $a \cdot a_2^{-1} = e$. Potem je tudi $a_1^{-1} \cdot a \cdot a_2^{-1} = a_1^{-1} \cdot e = a_1^{-1}$. Ampak $a_1^{-1} \cdot a \cdot a_2^{-1} = e \cdot a_2^{-1} = a_2^{-1}$, torej je $a_1^{-1} = a_2^{-1}$, kar pa je protislovje. Inverz je torej res enoličen.
6. Enačbo $a \cdot b = a \cdot c$ pomnožimo z leve z a^{-1} in dobimo
$$\begin{aligned} a^{-1} \cdot a \cdot b &= a^{-1} \cdot a \cdot c, \\ e \cdot b &= e \cdot c, \\ b &= c. \end{aligned}$$
Temu pravilu rečemo krajšanje z leve. Po prvi in tretji lastnosti simetrično deluje tudi krajšanje z desne, saj iz $b \cdot a = c \cdot a$ sledi $b = c$.

□

Definicija 2.2. *Naj bo $(G, \cdot)$ grupa. Grupa $(H, \cdot)$ je* podgrupa *grupe $(G, \cdot)$, kar označimo s $H \leq G$, če je H podmnožica množice G in je grupa za isto operacijo, omejeno na $H \times H$. Velja $G \leq G$ in $\{e\} \leq G$. Samo grupo G imenujemo* neprava podgrupa, *$\{e\}$ pa* trivialna podgrupa.

Izrek 2.1. *Naj bo H neprazna podmnožica grupe G. Množica H je podgrupa grupe G natanko tedaj, ko je za vsak par elementov $a, b \in H$ tudi $a \cdot b^{-1}$ element H.*

Dokaz. Vsako smer ekvivalence dokažemo posebej.
($\Rightarrow$) Predpostavimo, da je H podgrupa. To je očitno, saj so v grupi inverzi vseh elementov in produkti vseh elementov.
($\Leftarrow$) Predpostavimo, da je $a \cdot b^{-1} \in H$ za vsaka $a, b \in H$, in dokažimo, da je H grupa.
Najprej dokažimo $e \in H$. Če v izrazu $a \cdot b^{-1}$ zamenjamo b z a, dobimo $a \cdot a^{-1} = e \in H$.

Želimo še, da če je $a \in H$, je tudi $a^{-1} \in H$. V izrazu $a \cdot b^{-1}$ zamenjamo najprej a z e in nato b z a in dobimo $e \cdot a^{-1} = a^{-1} \in H$.
Sedaj dokažimo še, da iz $a, b \in H$ sledi $a \cdot b \in H$. V izrazu $a \cdot b^{-1}$ pustimo a in zamenjamo b z b^{-1} in dobimo produkt $a \cdot b \in H$.
Dokazali smo torej, da ima H enoto ter vsebuje inverze in produkte, asociativnost pa podeduje od grupe G. Množica H je torej grupa, s čimer smo dokazali tudi izrek. □

Definicija 2.3. *Naj bosta $(G, \cdot_G)$ in $(H, \cdot_H)$ grupi ter $f : G \to H$ funkcija. Pravimo, da je f* homomorfizem, *če za vsaka $a, b \in G$ velja*

$$f(a \cdot_G b) = f(a) \cdot_H f(b).$$

Trditev 2.2. *Naj bo $f : G \to H$ homomorfizem, naj bo e_G enota grupe G in e_H enota grupe H. Potem veljata naslednji trditvi.*

1. *Enota se slika v enoto, torej $f(e_G) = e_H$.*
2. *Za vsak $a \in G$ velja $f(a^{-1}) = f(a)^{-1}$.*

Dokaz.

1. Če v enačbi $f(a \cdot_G b) = f(a) \cdot_H f(b)$ zamenjamo tako a kot b z e_G, dobimo

   $$f(e_G \cdot_G e_G) = f(e_G) = f(e_G) \cdot_H f(e_G),$$

   iz česar sledi $f(e_G) = e_H$.

2. Velja $e_H = f(e_G) = f(a \cdot_G a^{-1}) = f(a) \cdot_H f(a^{-1})$, iz česar vidimo, da je $f(a^{-1})$ inverz elementa $f(a)$. Prav tako mora seveda biti inverz $f(a)$ tudi $f(a)^{-1}$. Ker pa je inverz enoličen, velja $f(a^{-1}) = f(a)^{-1}$.

□

Definicija 2.4. *Naj bo $f : G \to H$ homomorfizem. Potem definiramo* sliko homomorfizma f *kot*

$$\operatorname{Im} f = \{f(g) \mid g \in G\}$$

in jedro homomorfizma f *kot*

$$\ker f = \{g \mid f(g) = e\}.$$

Izrek 2.2. *Naj bo $f : G \to H$ homomorfizem. Potem je slika $\operatorname{Im} f$ podgrupa H.*

Dokaz. Naj bosta $a, b \in \operatorname{Im} f$, da je $a = f(a')$ in $b = f(b')$. Velja $f(a' \cdot b'^{-1}) = f(a') \cdot f(b')^{-1} = a \cdot b^{-1} \in \operatorname{Im} f$, torej je po izreku 2.1 slika $\operatorname{Im} f$ podgrupa H. □

Izrek 2.3. *Naj bo $f : G \to H$ homomorfizem. Potem je jedro $\ker f$ podgrupa G.*

Dokaz. Naj bosta $a, b \in \ker f$, torej $f(a) = f(b) = e$. Potem je $f(a \cdot b^{-1}) = f(a) \cdot f(b)^{-1} = e \cdot e = e$, torej je $a \cdot b^{-1} \in \ker f$ in je po izreku 2.1 jedro $\ker f$ podgrupa G. □

Definicija 2.5. *Naj bo $H \leq G$ in $g \in G$. Množico $g \cdot H = \{g \cdot h \mid h \in H\}$ imenujemo* levi odsek, *množico $G/H = \{g \cdot H \mid g \in G\}$ pa* faktorski prostor.

Izrek 2.4. *Naj bo G grupa in H njena podgrupa. Unija vseh podmnožic faktorskega prostora je grupa G, torej*

$$\bigcup_{A \in G/H} A = G.$$

Dokaz. Ker so vse podmnožice faktorskega prostora v G, je unija vseh teh množic $\bigcup_{A\in G/H} A$ podmnožica G. Po definiciji faktorskega prostora je unija podmnožic faktorskega prostora unija levih odsekov za vse g v G, torej

$$\bigcup_{A\in G/H} A = \bigcup_{g\in G} g\cdot H.$$

Velja tudi

$$\bigcup_{g\in G}\{g\} \subseteq \bigcup_{g\in G} g\cdot H,$$

saj je $e\in H$ in je potem tudi $g\in g\cdot H$. Ampak $\bigcup_{g\in G}\{g\}$ pa je ravno grupa G. Velja torej

$$G \supseteq \bigcup_{A\in G/H} A = \bigcup_{g\in G} g\cdot H \supseteq \bigcup_{g\in G}\{g\} = G,$$

kar pomeni, da je $\bigcup_{A\in G/H} A = G$. □

Izrek 2.5 (Lagrangeev izrek)**.** *Naj bo G končna grupa in H njena podgrupa. Potem $|H|$ deli $|G|$.*

Dokaz. Najprej dokažimo, da če $a\cdot H \neq b\cdot H$, je potem $a\cdot H \cap b\cdot H = \emptyset$.

Predpostavimo, da presek ni prazen, in naj bo $p\in a\cdot H\cap b\cdot H$, $g\in a\cdot H$ in $g\notin b\cdot H$. Potem obstaja $h\in H$, da je $g = a\cdot h$. Ker presek ni prazen, naj bo $p = a\cdot h_1$ in $p = b\cdot h_2$. Iz tega sledi $a\cdot h_1 = b\cdot h_2$ in zato $a = b\cdot h_2\cdot h_1^{-1}$. Sledi, da je $g = b\cdot h_2\cdot h_1^{-1}\cdot h$. Ker je $h_2\cdot h_1^{-1}\cdot h$ element H, je $g = b\cdot h_2\cdot h_1^{-1}\cdot h\in b\cdot H$, kar je protislovje.
To pomeni, da za $a\cdot H\neq b\cdot H$ odseka $a\cdot H$ in $b\cdot H$ nimata skupnih elementov. Sedaj bomo dokazali še $|a\cdot H| = |b\cdot H|$.
Obstaja preslikava $a\cdot H\to b\cdot H$, ki slika $a\cdot h\mapsto b\cdot h$, in je bijektivna, saj je njen inverz preslikava $b\cdot h\mapsto a\cdot h$, torej enakost res drži. To pomeni, da za končno G velja $|G/H|\cdot|H| = |G|$, torej mora $|H|$ deliti $|G|$. □

Izrek 2.6. *Naj bo $g\in G$. Z g^n označimo produkt n kopij elementa g, z $\mathrm{ord}_G(g)$ pa najmanjše naravno število n, da velja $g^n = e$, ter naj $\langle g\rangle$ označuje najmanjšo podgrupo $H\leq G$, da je $g\in H$. Potem velja $\langle g\rangle = \{e, g, g^2, \ldots, g^{n-1}\}$, kjer je $n = \mathrm{ord}_G(g)$.*

Definicija 2.6. *Podgrupi $\langle g\rangle$ pravimo* ciklična podgrupa.

Iz tega izreka sledita tudi dve posledici.

Posledica 2.1. *Če je G končna grupa, obstaja ciklična podgrupa $H\leq G$.*

Posledica 2.2. *Število $\mathrm{ord}_G(g)$ deli $|G|$, kar velja po Lagrangeevem izreku (izrek 2.5).*

3 Delovanje grup

Definicija 3.1. Permutacija *množice S je bijektivna preslikava iz S v S.*

Definicija 3.2. *Naj bo G grupa in naj bo S množica. Pravimo, da grupa G* deluje *na množico S, če vsak element $g\in G$ inducira permutacijo na množici S, ki ustreza dvema pogojema.*

- *Enota grupe G deluje kot identična permutacija na množici S.*
- *Za elementa g in h v G je permutacija, ki jo inducira produkt $g\cdot h$, enaka kompoziciji permutacij, ki ju inducirata g in h.*

Sliko elementa $x\in S$ v permutaciji, ki jo inducira g, označimo z $g\cdot x$.

3.1 Orbita in stabilizator

Definicija 3.3. Orbita *elementa $x \in S$ pod delovanjem grupe G je podmnožica množice S, ki sestoji iz vseh tistih elementov, ki jih lahko dosežemo z delovanjem elementov grupe G na element x, in jo označimo z $G \cdot x$, natančneje*

$$G \cdot x = \{g \cdot x : g \in G\}.$$

Definicija 3.4. Stabilizator *elementa $x \in S$ v grupi G je podmnožica množice G, ki sestoji iz vseh elementov, ki pri delovanju ohranijo x, in ga označimo z G_x, natančneje*

$$G_x = \{g \in G : g \cdot x = x\}.$$

Izrek 3.1. *Stabilizator G_x je podgrupa grupe G.*

Dokaz. Pokazali bomo, da je za vsak element $h \in G_x$ tudi $h^{-1} \in G_x$. Velja namreč

$$h^{-1} \cdot x = h^{-1} \cdot (h \cdot x) = (h^{-1} \cdot h) \cdot x = x.$$

Posledično je $(g \cdot h^{-1}) \cdot x = g \cdot x = x$, torej je po izreku 2.1 stabilizator res podgrupa. □

Izrek 3.2 (Izrek o orbiti in stabilizatorju)**.** *Naj bo G končna grupa, ki deluje na množico S, in naj bo $x \in S$. Potem je moč faktorskega prostora G/G_x enaka moči orbite $G \cdot x$.*

Dokaz. Skonstruirali bomo bijekcijo med elementi faktorskega prostora in orbito. Natančneje, pokazali bomo, da je preslikava $g \cdot G_x \longmapsto g \cdot x$ bijekcija. Izberemo poljubna g_1 in g_2. Potem je

$$g_1 \cdot G_x = g_2 \cdot G_x \iff g_2^{-1} \cdot g_1 \cdot G_x = G_x \iff g_2^{-1} \cdot g_1 \in G_x \iff g_2^{-1} \cdot g_1 \cdot x = x \iff g_1 \cdot x = g_2 \cdot x.$$

Iz tega sledi, da sta preslikava in njen inverz dobro definirana in da je torej izbrana preslikava res bijekcija. □

4 Permutacije in simetrična grupa

Definicija 4.1. Simetrična grupa *S_n je grupa vseh permutacij množice $[n] = \{1, 2, ..., n\}$ z operacijo kompozicije.*

V prihodnje bomo poljubno permutacijo prvih n naravnih števil označevali z n-terico $a_1, a_2, ..., a_n$. Pri tem permutacija slika element i v a_i. Permutaciji, ki vsak element slika vase, pravimo *identična permutacija* in jo zapišemo kot $1, 2, ..., n$.

Definicija 4.2. Transpozicija *je permutacija, ki fiksira (ohrani na svojem mestu) vse razen dveh elementov.*

Definicija 4.3. Inverzija *je par indeksov $i < j$, za katera velja $a_i > a_j$.*

Definicija 4.4. *Permutaciji pravimo* soda *oz.* liha*, če jo lahko dosežemo začenši iz identične permutacije s sodim oz. lihim številom transpozicij.*

Izrek 4.1. *Vsaka permutacija je bodisi soda bodisi liha.*

Dokaz. Vsako permutacijo lahko očitno dosežemo z zaporedjem transpozicij, natančneje s transpozicijami sosednjih členov. Pri vsaki taki transpoziciji se spremeni sodost števila inverzij permutacije. Če namreč zamenjamo sosednja člena, se število inverzij zveča ali zmanjša za 1. Identična permutacija nima inverzij, zato lahko vsako permutacijo opredelimo za sodo ali liho glede na to, ali je število njenih inverzij sodo ali liho. □

5 Rubikova kocka

Rubikova kocka je mehanska uganka, na kateri lahko uporabimo teorijo grup.

Definicija 5.1. *Grupo Rubikove kocke $(G, \cdot)$ definiramo kot vsa stanja, ki jih lahko dosežemo s premiki ploskev. Rezultat množenja pa definiramo kot stanje, ki ga dosežemo, ko na prvem stanju uporabimo zaporedje potez, ki vodi iz rešenega stanja v drugo stanje.*

Definicija 5.2. *Poteze so premiki ploskev za* $90°$ *v smeri urinega kazalca, poimenovane po prvi črki ploskve v angleščini* ***U****p,* ***D****own,* ***L****eft,* ***R****ight,* ***F****ront in* ***B****ack. Z X' označimo potezo X v nasprotni smeri urinega kazalca, z X^2 pa dve zaporedni potezi X, torej premik ploskve za* $180°$.

Posamezne koščke označujemo na naslednji način.

- Centri so koščki, ki imajo natanko eno barvo. Označimo jih s črko ploskve, na kateri ležijo, na primer U.
- Robovi so koščki, ki imajo natanko dve različni barvi. Označimo jih z dvema črkama ploskev, na kateri mejita, na primer UF.
- Vogali so koščki, ki imajo natanko tri različne barve. Označimo jih s tremi črkami ploskev, na katere mejijo, na primer UFL.

Rubikova kocka ima 6 fiksnih centrov, 12 robov in 8 vogalov. Po dogovoru je bela ploskev zgoraj in rumena spodaj.

Definicija 5.3. *Naj bo X množica vseh permutacij Rubikove kocke. To so vsa stanja, ki jih lahko konstruiramo, ko razstavimo in ponovno sestavimo kocko.*

Permutiramo vseh dvanajst robov, kjer je vsak lahko vstavljen na 2 načina. Podobno lahko naredimo z osmimi vogali, ki so vstavljeni na enega izmed treh načinov.

$$|X| = 12! \cdot 2^{12} \cdot 8! \cdot 3^8 = 519024039293878272000.$$

Vsi stabilizatorji grupe G so trivialni oziroma $|G_x| = 1$, saj je vsako zaporedje potez, ki poljubno stanje premeša vase, enako *enoti* grupe. Zaradi izreka o orbiti in stabilizatorju sledi

$$|G| = |G_x| \cdot |G \cdot x|,$$
$$|G| = |G \cdot x|.$$

Iz tega sledi, da so vse orbite Rubikove kocke enako velike.

Izrek 5.1. *Vsako stanje, ki ga lahko dosežemo s potezami, ustreza sodi permutaciji koščkov.*

Dokaz. Če gledamo skupaj permutacije 12 robov in 8 vogalov, dobimo homomorfizem iz grupe G v grupo S_{20}. Vsaka poteza permutira natanko 4 robove in 4 vogale, torej 8 koščkov vse skupaj. Za primer premik zgornje ploskve za $90°$ v smeri urinega kazalca permutira robove UB $\to$ UR $\to$ UF $\to$ UL $\to$ UB in vogale UBR $\to$ UFR $\to$ UFL $\to$ UBL $\to$ UBR. Ker so si vse poteze enake po simetriji, naredijo dva cikla velikosti štiri. Posledično vsi grupni elementi slikajo v sode permutacije. To pomeni, da le s potezami na Rubikovi kocki ne moremo priti v liho permutacijo. □

Definicija 5.4. *Rob je* rešen*, kadar leži na mestu, kamor spada, in se njegovi barvi ujemata z barvama ploskev, na kateri meji. Rob je* dober*, če ga lahko rešimo le s potezami iz množice $\{F^2, B^2, R, L, U, D\}$, torej brez zasukov ploskev F in B za* $90°$*; pri tem ni pomembno, kam se medtem premaknejo drugi koščki. Rob, ki ni dober, je* slab.

Z naštetimi potezami lahko vsak rob premaknemo na katero koli mesto, zato je edino vprašanje, ali ga lahko na njegovo mesto premaknemo tudi pravilno obrnjenega. V rešenem stanju so torej vsi robovi dobri.

Izrek 5.2. *Pri vsaki potezi se ohrani sodost števila dobrih robov.*

Dokaz. Na začetku so vsi robovi dobri, tako da imamo 12 dobrih in 0 slabih robov. Vsaka poteza iz podmnožice $\{F^2, B^2, R, L, U, D\}$ po definiciji ne spremeni dejstva, ali je nek rob dober ali ni. Isto velja za njihove inverze R', L', U' in D', saj lahko vsako zaporedje teh potez izvedemo tudi v obratni smeri.
Po drugi strani potezi F in B obrneta dobre robove v slabe in obratno. Rob, ki smo ga prej lahko premaknili na pravo mesto brez F in B, se zdaj tja ne more več premakniti, in obratno. Poteza F premakne natanko 4 robove, zato spremeni dobrost natanko teh štirih robov. Če je bilo med njimi k dobrih, jih je po potezi $4 - k$, torej se število dobrih robov spremeni za $4 - 2k$, kar je sodo število. Sodost števila dobrih robov se torej ohrani. Enako velja za poteze B, F' in B', saj spremenijo dobrost istih štirih robov. □

Definicija 5.5. *Vsak vogal ima natanko en beli ali rumeni del. Za vsak vogal definiramo njegovo* pravilno *orientacijo kot orientacijo, kjer ta del gleda gor ali dol.* Rotacija *vogala je število zasukov za* 120° *v smeri urinega kazalca, ki so potrebni, da iz pravilne orientacije pridemo v dano orientacijo, torej število iz množice* $\{0, 1, 2\}$.

Izrek 5.3. *Vsota rotacij vogalov v smeri urinega kazalca se ohranja po modulu 3.*

Dokaz. Ker je vsaka poteza zasuk ene ploskve za 90°, je dovolj, da trditev preverimo za poteze U, D, F, B, R in L. Vsaka izmed njih premakne natanko štiri vogale, in sicer tiste na svoji ploskvi.

Pri potezah U in D beli ali rumeni del vsakega premaknjenega vogala ostane obrnjen navzgor oziroma navzdol, zato se rotacije sploh ne spremenijo.

Pri potezah F, B, R in L pa pogledamo spremenjene vogale in ugotovimo, da se v vsakem paru sosednjih vogalov eden obrne za 120° v smeri urinega kazalca, drugi pa v nasprotno smer. Rotacije štirih premaknjenih vogalov se torej po vrsti spremenijo za 1, -1, 1 in -1, njihova vsota pa ostane enaka.

Pri nobeni potezi se vsota rotacij torej ne spremeni po modulu 3. □

Pokažimo še, da je ta invarianta edina ovira za pravilno orientacijo vogalov.

Trditev 5.1. *Če je vsota rotacij vogalov deljiva s 3, lahko vse vogale z zaporedjem potez spravimo v pravilno orientacijo, ne da bi premaknili kateri koli košček.*

Dokaz. Zaporedje potez

$$Z = R'\,D'\,R\,D\,R'\,D'\,R\,D\,U\,D'\,R'\,D\,R\,D'\,R'\,D\,R\,U'$$

zasuka vogal na mestu UFR za 120° v nasprotni smeri urinega kazalca in vogal na mestu UBR za 120° v smeri urinega kazalca, vse druge koščke pa pusti na svojih mestih in v isti orientaciji. Zaporedje Z torej spremeni rotacijo prvega vogala za -1 in rotacijo drugega za 1, zaporedje Z^2 pa ravno obratno. Ker je vsota teh dveh sprememb enaka 0, je to v skladu z izrekom 5.3.

Naj bo A poljubno zaporedje potez. Zaporedje AZA' ima enak učinek kot Z, le da zasuka tista vogala, ki ju A premakne na mesti UFR in UBR. Ker lahko poljubna dva vogala s potezami premaknemo na ti dve mesti, imamo za vsak par vogalov zaporedje potez, ki enega zasuka v smeri urinega kazalca, drugega pa v nasprotno smer, vse ostalo pa pusti nespremenjeno.

Izberimo zdaj en vogal in ga označimo z v. Za vsakega izmed preostalih sedmih vogalov uporabimo tako zaporedje potez za par tega vogala in vogala v, in sicer tolikokrat, da pride obravnavani vogal v pravilno orientacijo. Ko to naredimo za vseh sedem, so vsi v pravilni orientaciji, rotacija vogala v pa se je povečala ravno za vsoto njihovih začetnih rotacij. Rotacija vogala v je zato enaka vsoti vseh začetnih rotacij, ki je po predpostavki deljiva s 3. Ker je rotacija število iz množice $\{0, 1, 2\}$, je torej enaka 0, kar pomeni, da je tudi vogal v v pravilni orientaciji. □

Izrek 5.4. *V množici X je dvanajst orbit.*

Dokaz. Po izrekih 5.1, 5.2 in 5.3 se pri potezah ohranijo tri invariante: sodost permutacije koščkov, sodost števila dobrih robov in vsota rotacij vogalov po modulu 3. Stanji, ki se razlikujeta v kateri koli izmed teh invariant, torej nista v isti orbiti, velja pa tudi obratno, da lahko stanje s potezami premešamo v vsako stanje z istimi invariantami; za rotacije vogalov to pokaže trditev 5.1. Invariante lahko zavzamejo $2 \cdot 2 \cdot 3 = 12$ različnih kombinacij, saj pri sestavljanju kocke lahko zamenjamo zadnja dva robova, obrnemo zadnji rob in zasukamo zadnji vogal. Orbit je torej dvanajst. □

Ker je orbit dvanajst in ker so vse enako velike, je legalnih stanj natanko dvanajstina vseh, torej po izreku o orbiti in stabilizatorju (izrek 3.2) velja

$$|G| = \frac{|X|}{2 \cdot 2 \cdot 3} = 12! \cdot 2^{10} \cdot 8! \cdot 3^7 = 43252003274489856000.$$

S tem dobimo število legalnih stanj, do katerih lahko pridemo s premiki na Rubikovi kocki. Za primerjavo je na Zemlji šestkrat manj zrn peska kot vseh legalnih stanj. Imamo algoritme, ki pa rešijo Rubikovo kocko v končnem številu potez, ki ustrezajo navedenim invariantam (npr. CFOP, začetniška metoda, 3-Style).

Literatura

[1] M. Brešar *Uvod v algebro*, DMFA – založništvo; 2018; dostopno na `https://users.fmf.uni-lj.si/bresar/documents/UvodVAlgebro2018.pdf`

DRUŽABNI PROGRAM

Estimathon

Jakob Žorž

1 Kaj je Estimathon?

Estimathon je ekipna igra, pri kateri imajo ekipe 30 minut časa, da pravilno odgovorijo na 13 vprašanj. Odgovor na vsako vprašanje je pozitivno realno število x. Ekipe morajo oceniti pravilni odgovor, tako da podajo interval $[a, b]$, kjer velja $0 < a < b$, za katerega upajo, da $x \in [a, b]$. Interval, ki ga ekipa odda je *dober*, če velja $x \in [a, b]$. Končno število točk ekipe se izračuna po formuli

$$\left(10 + \sum_{\substack{\text{dobri intervali} \\ [\min,\max]}} \left\lfloor \frac{\max}{\min} \right\rfloor\right) \cdot 2^{13-\#\text{ število dobrih intervalov}},$$

cilj pa je, da ekipa dobi čim nižji rezultat.

Poglobljena obravnava zgornje formule nam pove, da je začetno število točk, ki jih ima vsaka ekipa $10 \cdot 2^{13} = 81920$. Z vsakim dobrim intervalom se število točk ekipe približno razpolovi, torej je cilj doseči čim večje število dobrih intervalov. Hkrati pa je pomembno, da je za vsak dobri interval $[a, b]$ njegova 'relativna velikost' $\left\lfloor \frac{b}{a} \right\rfloor$ čim manjša. Zato so najboljši tisti intervali, ki dosežejo najmanjšo relativno velikost, ampak še vedno največjo verjetnost, da zadenejo odgovor, oblike $[a, 1.99a]$.

Igra Estimathon je bila ustvarjena leta 2013 v podjetju Jane Street, več o igri pa lahko izvemo na `https://estimathon.com/`.

Slika 1: Tekmovalci letošnjega Estimathona.

2 Podrobnosti

Vsaka ekipa ima 18 listkov, ki jih lahko uporabi za vnos odgovora. Ko ekipa vloži listek, sodniki preverijo odgovor in v živo na zaslonu označijo, če je odgovor pravilen ali napačen. Zato lahko ekipe ves čas vedo, kako dobro gre vsem ekipam. Izjema je zadnjih 5 minut, ko ekipe želijo porabiti vse listke in zato sodniki ne morejo dohajati. To ustvari tudi napetost pred svečano razglasitvijo končnih rezultatov.

Zgornja in spodnja meja intervala morata biti podani v desetiškem ali znanstvenem zapisu, tj. kot decimalno število, pomnoženo z 10^k za celo število k. Včasih bi namreč koristil zapis v obliki potenc števila 2, vendar to ni dovoljeno.

V naši izvedbi tekmovanja je sodelovalo 7 ekip, ki so bile sestavljene iz 19 udeležencev tabora, v vsaki ekipi pa je bil natanko en mentor. Ekipe so bile izžrebane naključno.

3 Vprašanja

1. Koliko čokoladic Mars bi potrebovali, da bi z njimi zapolnili skupno prostornino teles vseh trenutno aktivnih šahovskih velemojstrov?
2. Koliko besed vsebuje Deklaracija o neodvisnosti ZDA (z naslovom, brez podpisov)?
3. Koliko dolžin filma *The Martian* (kinematografska, ne podaljšana različica) je minilo od smrti Neila Armstronga do dneva Estimathona?
4. Koliko vrstic izvorne kode ima Linux?
5. Kolikšna je numerična vrednost izraza 2^{3^4}?
6. Koliko šahovskih partij je bilo na spletu in v živo odigranih na mednarodni dan šaha, 20. julija 2024?
7. Koliko minut skupaj traja celotna animirana serija *One Piece*?
8. Koliko območij svetovne dediščine UNESCO obstaja?
9. Koliko tranzistorjev vsebuje Applov čip M5?
10. Kolikšen je bil skupni trgovalni promet družbe Jane Street v ameriških dolarjih leta 2025?
11. Za koliko ljudi je bil Pentagon ob zgraditvi zasnovan?
12. Koliko publikacij je napisal Leonhard Euler?
13. Koliko moških košarkarskih žog bi po masi ustrezalo Mednarodni vesoljski postaji?

4 Odgovori

Vprašanje	8	9	10	11	12	13
Odgovor	1248	$2{,}9 \cdot 10^{10}$	$3{,}96 \cdot 10^{10}$	25 000	866	722 000

Vprašanje	1	2	3	4	5	6	7
Odgovor	$1{,}02 \cdot 10^6$	1337	52 000	$3{,}03 \cdot 10^7$	$2{,}41 \cdot 10^{24}$	$7{,}28 \cdot 10^6$	35 430

5 Rezultati

Ekipe	1	2	3	4	5	6	7	8	9	10	11	12	13	Rezultat
Žorž (tk ko storž, ampak z ž-jem)	x	9	3	1	1	9	1	100		7	3	10	40	776
ŽEJN STRIC	2	2	3		1		2	1			1	xx	xx	1.408
KLIMATIZATORJI	2	2	2	xx	x	x	x	2	x	x	4	xx	x	5.632
Tarokovci	xxxx	x	1	x	1		2	9		x	x	2	xx	6.400
Kiki bonboni		xx			1		1	5	x	x	xxxx	xx	4	10.752
8	x	x	xx	x	1		1	x	x	xxxxx	x	x	x	24.576
Ime ekipe	9	x	100	xx	x	x	x	xx	x	x	x	5	100	114.688

Slika 2: Končni rezultati – številka v vsakem polju je $\left\lfloor \frac{b}{a} \right\rfloor$ če je podani interval $[a, b]$ dober, ali toliko znakov `x`, kolikor listkov je ekipa porabila, če ni zadela dobrega intervala. Prazno polje pomeni, da ekipa vprašanja ni poskusila rešiti.

Po koncu igre je eno izmed trinajstih vprašanj ostalo nerešeno. To je vprašanje številka 9, ki sprašuje po številu tranzistorjev v Applovem čipu M5; teh je kar $2{,}9 \cdot 10^{10}$, torej 29 milijard. Poleg tega so bila najtežja vprašanja 4, 6 in 10 – o številu vrstic izvorne kode Linuxa, o številu šahovskih partij, odigranih na mednarodni dan šaha, in o letnem trgovalnem prometu družbe Jane Street – saj je vsako od njih rešila natanko ena ekipa.

Najbolje rešena vprašanja so bila 3, 5, 7 in 8, vsako je rešilo pet od sedmih ekip. Spraševala so zaporedoma o številu dolžin filma *The Martian*, ki je minilo od smrti Neila Armstronga, o vrednosti izraza 2^{3^4}, o skupnem trajanju serije *One Piece* in o številu območij svetovne dediščine UNESCO.

Povprečno število rešenih vprašanj je bilo 5,4, kar je nekoliko več kot v lanski različici, ko je znašalo 5,2. Zmago si je prislužila ekipa *Žorž (tk ko storž, ampak z ž-jem)*, ki je dosegla 776 točk kar z enajstimi dobrimi intervali – to je bila hkrati edina ekipa, ki je zadela dobri interval pri vprašanjih 4, 6 in 10.

Organizacijsko ekipo letošnjega Estimathona sva sestavljala Jakob Žorž in Jure Kreže.

IZKUŠNJE UDELEŽENCEV

Izkušnje udeležencev

Zarja Čibej, Naja Oblak, Stela Petrinić

Zarja

Poletni teden na MaRSu je prav posebno doživetje. Mentorji se zelo potrudijo pri tem, da tudi udeležencem, ki niso prvič na MaRSu, predstavijo čisto nove aktivnosti, predavanja in delavnice poleg ohranjanja tradicije z MaRSovskim piknikom, pustolovščino in Jane Street Estimathonom. Letos sem bila še posebej navdušena nad Hitradio Center Summerspin kvizom, saj smo se v skupinici v le eni uri povezali, si zaupali in odlično sodelovali ter na koncu celo sestavili svojo plesno koreografijo na izbrano pesem. Vsak večer smo tudi v večjih skupinah igrali Avalon in tarok. Izjemno zabavno je bilo igrati z ljudmi, ki se igrajo prvič in razvijati nove strategije. Uživala sem z ostalimi na nočnih obiskih plaže in na nezahtevni in zabavni vendar rekreativni jutranji telovadbi, ki nas je prijetno zbudila za nadaljnje aktivnosti. Letošnji projekt mi je bil zelo všeč in zanimiv ter lahko sem mu sledila.

Če česa nisva razumeli, nama je Tim razložil še enkrat malo drugače in tudi sproti preverjal najino razumevanje s primeri, ki sva jih rešili na tablo. Najbolj mi je pri projektih všeč to, da pokrijejo zanimive teme, s katerimi se v šoli ne srečamo in vzbudijo neko zanimanje za matematiko izven meja šolskega programa. Kljub natrpanemu urniku, se je vsakih pet minut pavze izkoristilo za delanje načrtov kaj se bo v učilnici igralo po kosilu, kdaj se gre na plažo ali v trgovino in kako ubiti naslednjo žrtev morilca. Zaradi majhnega števila udeležencev smo se bolj povezali in spletli številne prijateljske vezi, tudi z mentorji, ki bodo (upam) držale še dolgo po koncu poletja. Na žalost je bilo to moje zadnje leto na MaRSu, pridem pa seveda naslednje leto pozdravit vse na piknik.

Naja

MaRS je bil zame nepozabna izkušnja tako zaradi zanimivih novih matematičnih tem, ki sem jih spoznala, kot zabavnih trenutkov, dogodivščin in ljudi, ki so ga soustvarjali. Kljub temu da sem na tabor prišla z dvodnevno zamudo, me je pričakala topla dobrodošlica lanskih znancev in pa spoznavanje novih ljudi ter delo na projektu, letos iz teorije grup. Vsekakor me je ponovno fascinirala izvirnost posadke pri organizaciji aktivnosti, ki so bile zato še bolj zanimive in zaradi česar sem porabila veliko časa za razvozlavanje dnevnika, se spomnila verzov slovenske poezije, naučila prepričati turiste pozirati za sliko in spoznala, da nimam svetle prihodnosti v sestavljanju koreografij.

Najbolj se mi bo v spomin vtisnila zadnja noč, ki sem jo preživela v super družbi nekaterih soudeležencev, polnočnega kopanja, degustaciji vodene slane karamele in enega litra vrele vode, novih strategij Avalona in iskanja nesmiselnih povezav pri igri Codenames. Zapomnila si bom ure zabave, smeha, novih iger in dobrega druženja kljub večdnevnemu ponočevanju. S tabora sem se vrnila s hripavim glasom, z novimi spomini, znanjem in prijateljstvi ter izkušnjo, ki bi jo definitivno priporočila vsem, ki jih matematika zanima, saj je tabor veliko več kot le delo na projektih.

Stela

V nedeljo sem se po peturni vožnji s tremi različnimi avtobusi in dveh zgrešenih pešpoteh navkreber končno znašla pred CŠOD Breženka. Po sprejemu zelo prijaznih mentorjev so moje neobstoječe znanje preizkusili s serijo nalog, ob katerih sem se začela spraševati, če imam dovolj znanja za tabor. Srečoma sem imela najboljše cimre, ki so me prepričale, da to sploh ni tako pomembno. Pokazali so mi tudi renomirano igro Avalon, v kateri nisem ravno blestela. Presenetljivo je Avalon ena tistih iger, ki mi očitno bolje grejo med plavanjem, kot na suhem. Z izvrstnim mentorjem Gencem smo ugotovili, kateri sladoled v zaporedju je ta pravi, ga potem pojedli in si tem uspešno olajšali vpliv žgočih 90° Fahrenheit. Še zlasti dostikrat je zmagala lučka King. Zvečer smo z njim preizkusili tudi baristarske veščine in spili kavice s slano karamelo.

Vrhunec tabora je zame bila velika marsovska pustolovščina, pri kateri so nam odgovore prišepetale primorske in pozidne kuščarice, čeprav se je tudi njim že malo mešalo od piranske vročine. Kljub pomanjkanju spanja so me zanimivi projekti in predavanja povsem prevzeli in zanetili radovednost do statistike, barvanja kvadratkov in testov praštevilskosti. Tabor je bila zelo prijetna izkušnja in izjemno vesela sem, da sem se opogumila ter prijavila, čeprav morda nimam takšnih matematičnih sposobnosti kot preostali udeleženci. Poslušanje zgodb s tekmovanj in olimpijad me je zelo navdihnilo in res občudujem vse mentorje in udeležence. Kljub začetnim dvomom in vročini je bil tabor nepozabno doživetje, domov pa sem odšla s kupom lepih spominov in še lepših prijateljev.

PODPORNIKI

DMFA Slovenije

Društvo matematikov, fizikov in astronomov Slovenije je stanovska organizacija, ki združuje pedagoge, raziskovalce in študente. Ustanovljeno je bilo leta 1949. Društvo skrbi za popularizacijo matematike, fizike in astronomije med mladimi in v širši javnosti. Organizira tekmovanja iz znanja, ki se jih vsako leto udeleži več kot 100000 tekmovalcev. Organizira znanstvena srečanja in promovira znanstvene dosežke svojih članic in članov. Izdaja društveno glasilo Obzornik za matematiko in fiziko in Presek, list za mlade matematike, fizike, astronome in računalnikarje. Društvo aktivno deluje v mednarodnih združenjih na posameznih področjih in sodeluje z društvi, raziskovalnimi organizacijami in pedagoškimi inštitucijami v Sloveniji.

Zavarovalna skupina Sava

Zavarovalna skupina Sava je k strankam usmerjena, prilagodljiva in trajnostno naravnana zavarovalniška skupina s posli na več kot 110 zavarovalnih in pozavarovalnih trgih sveta. Skupina ponuja zavarovalne, pozavarovalne in pokojninske rešitve ter storitve upravljanja premoženja. Matična družba Sava Re, d.d., zagotavlja pozavarovalne storitve več kot 450 partnerjem po vsem svetu. Z družbami je prisotna v šestih državah regije Adria in je tako ena večjih zavarovalniških skupin s sedežem v jugovzhodni Evropi. Bonitetni agenciji S&P Global Ratings in AM Best sta v letu 2023 Savi Re obnovili bonitetno oceno kreditne sposobnosti in finančne moči »A« s stabilno napovedjo. V letu 2023 je obseg poslovanja skupine znašal več kot 910 milijonov EUR, dobiček pa 65 milijonov EUR.

UL FMF

Fakulteta za matematiko in fiziko (FMF) je nastala leta 1995 z razdružitvijo tedanje Fakultete za naravoslovje in tehnologijo, študija fizike in matematike na Univerzi v Ljubljani pa obstajata vse od njene ustanovitve leta 1919.

UM FNM

Oddelek za matematiko in računalništvo FNM UM je iskriv in zagnan kolektiv, ki ga vseskozi krasi skrb za strokovno in znanstveno odličnost, kot tudi poudarjeno skrben odnos do pedagoškega dela ter skrb za kakovosten prenos znanja in navdušenja nad našo stroko: na študente, pa tudi na naše ožje in širše okolje. Oddelek izvaja naslednje študijske programe:

- **Matematika 1. stopnje**: traja 3 leta in predstavlja vstopno točko v svet matematike. Namenjen je študentom, ki želijo podrobneje spoznati temeljne matematične vsebine.
- **Matematika 2. stopnje**: traja 2 leti in je zasnovan tako, da s specializacijo na tri module študentu omogoči, da pridobi poglobljena znanja matematike z enega izmed treh področij: splošna matematika, računalniška matematika in finančna matematika.
- **Izobraževalna matematika 2. stopnje**: traja dve leti in je v kombinaciji s programom Matematika na 1. stopnji namenjen izobraževanju učiteljev matematike, ki lahko poučujejo tudi na gimnazijah.
- **Matematika 3. stopnje**: je doktorski študijski program, ki je vključen v doktorsko šolo Univerze v Mariboru in traja 4 leta.
- **Predmetni učitelj**: je enovit magistrski študijski program, ki traja 5 let. Namenjen je izobraževanju dvopredmetnih učiteljev s pravico poučevanja na predmetni stopnji osnovne šole in večini srednjih šol.

Univerza v Mariboru

Fakulteta za naravoslovje in matematiko

Jane Street

Jane Street je kvantitativno trgovsko podjetje s pisarnami po vsem svetu. Zaposlujemo pametne, skromne ljudi, ki radi rešujejo probleme, gradijo sisteme in preizkušajo teorije. V naši pisarni se boste vsak dan naučili nekaj novega – naj bo to povezovanje s kolegom za izmenjavo pogledov ali sodelovanje v pogovoru, predavanju ali večeru igre. Naš uspeh poganjajo naši ljudje in nikoli se ne nehamo izboljševati.

Jane Street®

Teads

Teads je vodilna globalna oglaševalska platforma za odprti internet, specializirana za večkanalno oglaševanje na povezani televiziji (CTV), mobilnih napravah in spletu. Njihova napredna umetna inteligenca omogoča optimizacijo oglasov z obdelavo 8 milijonov zahtevkov in ustvarjanjem milijarde napovedi na sekundo, s čimer povezujejo več kot 20.000 oglaševalcev z globalno mrežo medijev. Podjetje, s skoraj 1.800 zaposlenimi v 36 državah, ima močno prisotnost in ekipo tudi v Sloveniji. Velik poudarek dajejo kulturi spoštovanja, zaupanja in dobrega počutja, kar podpirajo z možnostmi za razvoj, digitalnim nomadstvom in hišnim ljubljenčkom prijazno pisarno.

AFLabs

Smo mednarodno razvojno raziskovalno podjetje, ki se ukvarja z unikatnimi projekti, ki zahtevajo visoko raven tehničnega znanja, natančnosti, ekipnega dela, izkušenj in zanesljivosti.

Abelium

Abelium d.o.o. je visokotehnološko raziskovalno-razvojno podjetje, specializirano za reševanje zahtevnih poslovnih in industrijskih izzivov. To dosega z inovativno uporabo matematične optimizacije, umetne inteligence, velepodatkov, tehnologije bločnih verig in naprednih digitalnih preobrazb. S svojo ekipo strokovnjakov, večinoma matematikov, razvija programske rešitve po meri za naročnike na področjih logistike, financ, fintech industrije in javnega sektorja.

Akademija Panta Rei

Akademija Panta Rei je izobraževalna organizacija, ki že več kot dve desetletji organizira poslovna izobraževanja, seminarje in delavnice s področij podjetništva, marketinga, prodaje, vodenja in osebnih financ. Na svojih dogodkih gosti mednarodno priznane strokovnjake in vrhunska svetovna znanja prenaša v slovensko okolje, udeleženci njenih izobraževalnih programov pa prihajajo iz več kot 70 držav. Verjame, da je znanje ključ do uspeha in da se je smiselno učiti od najboljših, zato podpira radovedne in ambiciozne posameznike na njihovi poti.