MaRS 2023

Matematično raziskovalno srečanje 2023

Javorniški Rovt
30. julij – 5. avgust

DMFA Slovenije

Matematično raziskovalno srečanje 2023

Zbornik

Avtorji: *dr. Katja Berčič, Nino Cajnkar, Nejc Černe, dr. David Gajser, Jan Genc, Žan Hafner Petrovski, dr. Vesna Iršič, Izak Jenko, Juš Kocutar, dr. Boštjan Kuzman, Matija Likar, David Opalič, Petra Podlogar, Katarina Šipec, dr. Blaž Škrlj, dr. Russ Woodroofe, Nejc Zajc*

Uredili: *Žan Hafner Petrovski, Matija Likar, David Opalič*

Recenzenti: *Nino Cajnkar, Jan Genc, Žan Hafner Petrovski, Izak Jenko, Juš Kocutar, Matija Likar, David Opalič, Petra Podlogar, Katarina Šipec, Nejc Zajc*

Oblikoval: *Žan Hafner Petrovski*

Izdalo: *Društvo matematikov, fizikov in astronomov Slovenije*

Predstavnik: *prof. dr. Primož Potočnik*

Kraj in leto izida: Ljubljana, 2024

Prva elektronska izdaja objavljena na povezavi:
`http://mars.dmfa.si/clanki/zbornik-2023.pdf`

Kataložni zapis o publikaciji (CIP) pripravili v Narodni in univerzitetni knjižnici v Ljubljani

COBISS.SI-ID 185517315
ISBN 978-961-91896-8-9 (PDF)

Kazalo

UVOD

Uvodnik

Nejc Zajc

O taboru

Matematično raziskovalno srečanje, ali MaRS, je poletni matematični tabor za srednješolke in srednješolce. Pred vami je zbornik tabora MaRS 2023. Z njim bomo poskusili povzeti vsebine letošnje izvedbe in prikazati, kaj vse smo na taboru počeli.

Izvedba MaRS 2023 je bila že osemnajsta zapored. Tabor je potekal v tednu med nedeljo, 30. julijem, in soboto, 5. avgustom. Udeležilo se ga je 27 dijakinj in dijakov, ki so pod mentorstvom 10 študentov širili svoja matematična obzorja.

Strokovni del tabora je sestavljen iz treh sklopov. Skozi osrednjo delavnico tabora, ki je potekala v treh delih med ponedeljkom in sredo, so udeleženci spoznali osnove in nekaj zanimivih uporab teorije grafov. Drugi sklop matematičnih vsebin tabora so večerna predavanja gostujočih profesorjev slovenskih univerz in naših podpornikov – letos smo jih imeli kar pet. Prisluhnili smo lahko temam izračunljivosti, probabilističnih algoritmov in deljivosti binomskih koeficientov ter spoznali življenja aktuarjev in pomembnega slovenskega matematika Josipa Plemlja.

Glavna matematična vsebina so bili, kot na MaRSu vedno, projekti. Skupine treh udeležencev so pod mentorstvom študenta raziskale izbrane matematične teme. Delo na projektih je potekalo tekom celega tedna. Dijaki so se najprej s temo svojega projekta spoznali preko uvodnih primerov, jo raziskali in prišli do zaključkov. Pripravili so tako članke, ki podrobno opišejo njihovo delo in so del tega zbornika, kot kratke predstavitve za starše in ostale udeležence, ki so jih predstavili ob zaključku tabora.

Poleg vseh omenjenih matematičnih dejavnosti smo za udeležence pripravili tudi pester družabni program, ki je na preizkušnjo postavil spretnosti ocenjevanja, izvirnost in domišljijo udeležencev. Ob večerih pa so se dijaki in mentorji do poznih ur družili ob raznolikih družabnih igrah. Tradicionalni del programa, ki vsebuje pohod, Veliko MaRSovsko pustolovščino in MaRSovski piknik, tudi letos ni manjkal. Navkljub dežju v dneh pred njim, smo pohod uspeli izvesti. Velika MaRSovksa pustolovščina, ki je sicer orientacijski tek po naravi, pa je bila letos zaradi dežja organizirana v notranjih prostorih. Kratke in zabavne naloge na postajah pri mentorjih so bile tako razporejene kar po domu.

Tako je bil urnik tabora tudi letos zelo poln. S pomočjo naših podpornikov smo ga uspeli v celoti izvesti, udeleženci pa so z nami lahko preživeli zanimiv, poučen in nepozaben teden.

Beseda odgovorne osebe

Drage udeleženke, udeleženci in posadka, spoštovani predavatelji, podporniki in ostali bralci zbornika. Za nami je še en uspešen polet na MaRS. Letos sem prvič prevzel vlogo kapitana, oz. odgovorne osebe. Za zaupanje te vloge bi se rad zahvalil Žanu in ostali ekipi. Tudi sicer bi se rad zahvalil vsem članom posadke. Prav vsak predstavlja pomemben in nepogrešljiv del organizacije našega tabora. Vseeno pa nam ne uspeva samim. Tudi letos ste predavatelji in podporniki pokazali izjemno pripravljenost za sodelovanje. Zahvaljujem se vam za vse.

Glavni del tabora ste seveda udeleženci. Vsako leto me navduši vaša energija, radovednost in želja po spoznavanju novega. Tudi letos je bilo tako. Upam, da ste na taboru preživeli lep in zanimiv teden. Letošnjega tabora se je udeležilo veliko četrtih letnikov, želim vam veliko uspeha in naj vas MaRSovska zagnanost spremlja tudi pri študiju. Z ostalimi upam, da se vidimo na MaRSu tudi naslednje leto.

Lep MaaaaRSovki pozdrav, Nejc!

Word of the president of the committee

Dear participants, crew, sponsors and other readers. We have successfully returned from another mission to MaRS. This was my first year as a ship captain, i.e. committee president. I would like to thank Žan, the previous captain, and the rest of the team for entrusting me with this responsibility. I am also thankful for everything else you, my crew, have done for our camp. Each and every one of you contributed in an important and irreplaceable way to the success of the event. Furthermore, MaRS 2023 wouldn't be possible without our supporters. Some of you helped us financially, some in other ways, but you all showed honest readiness to help and it was always a pleasure to work with you. I am grateful for your help.

Participants, you are of course the soul of the camp. Each year I am enthralled by your energy, curiosity and your will to learn. This year was no different. I hope you spent an interesting and fun week at the camp. Lots of you are soon starting with your university days. I wish you a lot of success, face the new challenges with the same enthusiasm and determination you showed at MaRS. As for the others, a bit younger students, good luck to you all and I hope to see you at MaRS 2024.

Greetings from MaaaaRS, Nejc!

Posadka

Za uspešno izvedbo tabora je zaslužna celotna ekipa organizatorjev – posadka. Sestavljali smo jo:

- *Nejc Zajc* [kapitan], magistrski študent matematike, FMF, Univerza v Ljubljani ,
- *Petra Podlogar* [pilotka], magistrska študentka IŠRM, FMF in FRI, Univerza v Ljubljani,
- *Žan Hafner Petrovski* [starešina], magister inženir računalništva in matematike, FMF in FRI, Univerza v Ljubljani,
- *David Opalič* [kontrolor letenja], magister matematike, ETH Zürich,
- *Katarina Šipec* [višja častnica], magistrska študentka matematike, FMF, Univerza v Ljubljani,
- *Nino Cajnkar* [častnik], dodiplomski študent finančne matematike, FMF, Univerza v Ljubljani,
- *Izak Jenko* [častnik], magistrski študent matematike, FMF, Univerza v Ljubljani,
- *Jan Genc* [praporščak], dodiplomski študent matematike, FMF, Univerza v Ljubljani,
- *Juš Kocutar* [praporščak], dodiplomski študent matematike, Univerza v Groningenu,
- *Matija Likar* [praporščak], dodiplomski študent matematike, Tehnološki inštitut Massachusettsa.

Dnevnik

Žan Hafner Petrovski 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.

Nedelja, 30. julij 2023

Navkljub dežju in neznanemu (letečemu) predmetu na izvozu Jesenice – vzhod smo letošnjo opdravo lansirali z iztrelišča pod Golico ob Javorniškem jezeru skoraj brez zamude. Med potniki smo uspešno prebili led z letaljènjem. Vse, kar smo potrebovali, sta bili dve potici in en glaž. Po vzletu smo mrzke duhove s te strani Karavank pregnali z udarnim MaRSovskim pozdravom v slogu Maorske hake. Ta namreč človeka toliko izprazni, da si poželi kapljice rujnega ričeta. Njegova nobel, uporabna in povabljiva podoba je nosila jesenske odtenke – domnevamo, da bomo s trenutnim tempom morda jutri kosíli novoletno sarmo.

Za lahko noč smo šteli zajčke z obzirom na svoj čas in spomin. Jaz sem jih naštel osem (kolk?). Tu nam je prišel naproti dr. Blaž Škrlj iz podjetja Outbrain s salamoreznico probabilističnih algoritmov.

Konec današnjega vnosa še pospremimo z domnevnim citatom slovenskega pesnika Braneta B.:

Moj narod je že od nekdaj gojil borbenost.
In tut js, hočem it na Mars.

Ponedeljek, 31. julij 2023

Po zajtrku smo skrenili na prvo jutranjo telovadbo, nekateri tudi na jogo. Bilo je togo. Razcepili smo se v skupine za projekte in se spoznali s temo, ki nam bo za eno nedeljo dni vžgala stigmo v čelo. Sledili sta indoktrinacija v svet programiranja in košnja v jedilnici. Sarm ni bilo, so pa izbruh okusov docela nadoknadil vzorno termično obdelan pečen krompir in Pepini zrezki s Pohorja.

Padec krvnega tlaka nas je pregnal v postelje, kjer smo na višini odsmrčali gloso. Spočite nas je pozdravila dr. Vesna Iršič s Fakultete za matematiko in fiziko v Ljubljani. Menda množico vozlišč poljubnega grafa najbolje obogatimo tako, da vzamemo vse pare (v separé). Analogija nas pripelje do današnjega sponzorja Jane Street in es(ti)^{42}mathona. Ugibali smo število objav na Takojšnji enoti mase naše Barbike, a so nam načrte prekrižali hekerji, ki so subjekt preko noči opeharili za en kilopost, post-hoc.

Ob paranoičnem motanju po hodnikih CŠOD se je marsikateri dijak spraševal, kako izgleda življenje velikih slovenskih matematikov. To radovednost je potešil dr. Boštjan Kuzman s svojim predavanjem o življenju dr. Josipa Plemlja – soustanovitelja današnje Univerze v Ljubljani.

Intelektualno siti in konvencionalno lačni smo se že tretjič danes odpravili v jedilnico in pomazali krožnike prhkega golaža z našim vsakdanjim kruhom.

Na večernem predavanju smo z gostujočim Nejcem Černetom z Zavarovalnice Triglav ugotavljali, kako se najučinkoviteje ukrade zavarovan avtomobil izračuna donosna premija avtomobilskega zavarovanja.

Utrujeni smo legli na jogi. Bilo je togi.

Opomba. *Indoktrinacija je proces usađivanja ideja, stavova, kognitivnih strategija ili profesionalne metodologije (vidi doktrina).*

Torek, 1. avgust 2023

Ranega jutra dan: ko smo začeli z jogo, smo končali z jogo. Sprostili smo se šele na drugem delu delavnice o grafih. Doumeli smo, da matematika nikakor ne šepa za časom. Tehnologija je prodrla v vse pore sveta – staromodne paznike so namreč v galeriji nadomestili novodobni senzorji.

Nato smo se spoznali še s klasično metodo matematičnega tekstopisja in se iniciirali v Latežane.

Drugega resnega dneva dan: začetek zime. Napolnili so nas z belo vegetarijansko lazanjo brez zelenjave in rjavimi kosi milke v omaki. To je bil čas košnje.

Po odsmrčani gazeli smo se mladi mlečniki končno resneje spopadli s togotnimi mentorji. Po triurni histeriji so naše oplemenitene stenice nadalje bodrili štirje disciplinski postopki, ki naj bi nas popeljali do večerne krme. Po odmoru krikov groze nam je dr. Russ Woodroofe predstavil svoje vprašanje o binomskem koeficentu in praštevilih. Dejal je še, da $(x+1)^n$ deluje za $n = 3$ in $n = 6$. Da. Kaj? Sporočimo jutri.

Sečniki so šele pozno odšli počit.

Sreda, 2. avgust 2023

Dan smo otvorili ob polnoči s kratko rundo štetja do pet za piromane ali tarota za Jana G. Prav tako smo naredili en šnelkurs rimskih števil do 21 za potrebe taroka. Bralec se lahko tudi sam preizkusi v tej veščini, s tem da nam na marsovski mail odgovori, kateremu številu ustreza VIII.

Naredili smo kratek n-urni počitek, kjer je S_n grupa z več kot tremi normalnimi podgrupami. Zbudili smo se sveži in osveženi v ranih in rosnih urah sredinega jutra. Imenitno smo prikopitljali v jedilnico in se nasitili z delavsko porcijo svežega kruha in paštete z nalepko Kekca.

Nato smo se odpravili na Ojlerjev obhod grafa, ki ga sestavljajo natanko tiste povezave, ki smo jih prehodili. Na svoji poti smo zmedeno obstali pri domu Pristava, kjer smo se starosti primerno okrepčali s cedevito in vožnjo po toboganu, juhej! Medtem smo mentorji imeli kratek sestanek, na katerem smo kolektivno opazili svojo organiziranost in profesionalnost. Sledil je ogled znamenitih Javorniških slapov, ki spadajo po mnenju nekaterih strokovnjakov med ene izmed slapov v Sloveniji.

Seveda pa pohod ne mine brez ustreznega razvedrila, ki bodri burne ume naših mladih matematikov. Med potjo smo se spraševali o treh ključnih spрašanjih:

- Kdo ima kapo? (Juš ma kapo. Ne, ti maš kapo.)
- Kam grem lahko na morje? (Na Jesènice? Ne, tam ni morja.)
- Ali imajo vse netrivialne ničle Riemannove funkcije realni del enak $\frac{1}{2}$?

Trava pred CŠOD se je ob prihodu že pošteno zarasla, tako da je sledila košnja. Svoje brbončice smo opojili z vegetarijansko zajčjo juho ter sferičnimi polnjenimi paprikami brez paprik.

Konvencionalno siti in intelektualno lačni smo se podali na zadnji del delavnice o grafih, kjer smo spoznali sodobne priprave za preprečevanje utaplanja otrok v bazenih (ali morju, če lahko gre tja, seveda). V tem času smo prav tako dobili še najbolj praktičen doprinos letošnjega tabora. Vključno s Katarino imamo zdaj kar tri grilje.

Preostanek popoldneva smo namenili delu na projektih, ki ga je za kakšno uro prekinilo spontano zborovanje v kletnem prostoru, ko smo se nahranili z različno oblikovanimi izdelki iz gnetenega testa ter gostljatim dodatkom jedi iz Bologne (njam njam, dva njama, več je več).

Upam, da bomo nocoj morda že prej bili ležečki, danes je sreda moji dečki.

Četrtek, 3. avgust 2023

Vjutro smo se s polnimi prebavili zakadili navzdol po klancu in potem še nazaj v grič. Ostali so igrali krompir, vendar niso imeli sreče, vseeno so bili primorani k svojim mentorjem pod nož. Osupnili smo jih s svojo predanostjo, izkazali smo nenaravne veščine lateksa.

Tehnično spodkovani in tuitivno lačni smo šila in kopita premaknili do obednice, kjer je sledil drugi osrednji centralni dogodek dneva – paša. Ta je bila navdihnjena z lokalnimi nizozemskimi mlinci, pripravljenimi v morju in začinjenimi z avtohtono javorniško perutnino.

Sledil je prvi tradicionalni marsovski piknik. Najdelj smo dušili oglje in pripravljali mentorjem osebno ukrojene marinade. Ni sledil boj, temveč vegeterijansko klanje. Kot bi baba rekla: *"Ananas na pici – metek v hrbtenici."*

Točno popoldne smo izpopolnjevali članski kaospis, saj osebo poteši izključno rigorozni čistopis. Prècej je trajalo, da smo na tretjem osrednjem dogotku dneva dobili dva kosa večernega sera in ju delili med 5 ljudi – $\frac{\text{(Marko, 6:41)}}{1000}$.

Natanko zvečeraj smo čakajoč pričakali dr. Davida Gajserja – Gaserja, ki nam je pristavil še poslednje davanje preje tega leta Gospodovega. V obzir Barbiki, smo se na začetku posvetili problemu Postov. Nato pa smo se spoznali, v nebiblijskem pomenu, s stroji naključnega dostopa, ki jih céneni bralec lahko smatra kot računala, ki imajo neskončno trdega (diska).

Obljubili smo vam razlago torkove šale.

Opomba. *V bibliji so se spoznavali hitreje kot dandanašnjega dneva dan – (Mojzes, 4:1).*

Petek, 4. avgust 2023

Oke smo odprli, da bi si s čudovitim jutrom iz oči v uče zrli. Pogled smo umaknili. Deš, deš, deš … A bejš!

Ko smo se zmočili izmakniti iz romantičnega cikličnega trikotnika tekača, plavolaske in kralja živali, smo si na prste naložili delo na žarkovniku. Ti so, nič hudega sluteč, sredi črnega dne naleteli na šibo, saj, razen izjem, niso prepričali neprilagodljivega Davida. Zgledniki so jih zato naučili strežbe, nato pa smo vsi z odprtimi senčniki nad beticami odšli po gobe na ovekovečenje. Naleteli smo na zasedo Gaserjev, ki so brezsramno bliskali in šklopotali – ujeli so nas v lečo.

Ampak resno in namestno vprašanje je, kaj smo obedovali. Ne vemò. In nikoli ne boste. Računamo, da je izkušnja z razlago šale še sveža.

Vemo pa, da za Dežjem ne posije Sonce, zato smo se kljub vztrajnemu prigovarjanju in naivnosti izključno slednjega odločili lovljenje pusta izvesti po notranjosti doma za zaprtimi Vrati, namesto na opolzki travi in Kotalečem kamenju. Dijaki so se šesti dan tabora znali po Javorniškem mastodontu zadostno in zanesljivo orientirati ter so se lahko mirnodušno predali izzivom, kot sta maziljenje z Genčevimi posplošenimi kremicami v inverzijski ravnini ter Susovo podoživljanje košarkarskega tabora.

Iztrošeni od hoje po stopnicah smo s podolgovatimi mesninami delno potešili dela željna prebavila. Sledilo je tekmovanje v seštevanju seštevancev velikih magnitud, razglasitev zmagovalcev, ki so pometli z zavidljivo dvoletno dinastijo Palič. Sledil je še naključni razcep umetniškohišne strjene kakavove mase, ki je dodatno razdražila našo peristaltiko.

Kmalu so se pričeli vrstiti hodi z žara, sprva le mlečni derivati in vegetacija kot pozdrav iz kuhinje, kasneje pa tudi različni mesni pridelki podolgovatih razmerij. Stanje pred žarom je hitro alarmantno eskaliralo, ko je začel uhajati dimeljski dim. *"Gre plin"*, je ob dogodku domnevno izustil gostujoči župan D. G.

"Sledeča vzporedna zaporedja dogodkov so le še povestnica."

Opomba. *Župan – der Bürgermeister.*

Sobota, 5. avgust 2023

Poslednje jutro smo radostno vstali in skočili na zajtrk, tam nas je namreč čakala tuna. Z obedom smo pohiteli, da smo lahko potem čim dlje čakali na slavnostni pristanek pred roditelji. Izmenjevali smo tugotne misli in se spraševali, če smo še dovolj prisebni, da izpeljemo, kar nam je bilo zadano s strani mentorjev.

Vedeli smo, da stojimo na tankem ledu, zato smo ga prebili s samozavestnim pozdravom, nato pa se posedli nazaj na sedišča daleč stran od pogledov. Da smo res padli v mrzlo morje, je bilo očitno ob koncu naspičenega povzetka tedna. S kamnom na ledvici smo pričakovali svoj trematični nastop. Pred steno so nas klicali v trojicah po tri.

Ob sedečih ovacijah se nam je vsakemu posebej s prečiščevalnega organa odvalil velik kos peska. Končno smo si segli v roke in si zaželeli srečno pot skozi povodenj na domači grudi.

OSREDNJA DELAVNICA

Teorija grafov

dr. Vesna Iršič

Fakulteta za matematiko in fiziko, Univerza v Ljubljani, Slovenija
Inštitut za matematiko, fiziko in mehaniko, Ljubljana, Slovenija

Povzetek

Ali lahko zemljevid pobarvamo s štirimi barvami tako, da sosednje države niso istih barv? Kako naj v galerijo namestimo čim manjše število senzorjev, da bomo varovali celotno galerijo? Najmanj koliko radijskih oddajnikov moramo postaviti v mestu, da bodo vsi prebivalci lahko sprejemali signal? Najmanj koliko policijskih vozil potrebujemo, da lahko ujamemo pobeglega roparja v mestu?

Naštete probleme (in še mnoge druge) lahko rešimo s pomočjo teorije grafov, ki je del diskretne matematike in preučuje lastnosti grafov oziroma omrežji. V okviru delavnice bomo spoznali, kaj so grafi in kako opišemo njihove osnovne lastnosti. Raziskali bomo nekaj klasičnih tem (npr. ravninski grafi, barvanja, dominacija) in spoznali igre na grafih.

1 Uvod

Za motivacijo si oglejmo nekaj primerov, kjer nam pri razumevanju ali reševanju problema pomagajo grafi.

1. Zemljevid cestnega, železniškega ali avtobusnega omrežja. S pomočjo metod iz teorije grafov lahko poiščemo najkrajšo pot.

2. Kemijske molekule lahko predstavimo kot graf (vozlišča so atomi, povezave so kemijske vezi med atomi). Izkaže se, da so kemijske lastnosti molekul povezane z lastnostmi dobljenih grafov.

3. Prehode med prostori v stavbi lahko ponazorimo z grafom. Analiza dobljenega grafa nam pomaga razumeti gibanje ljudi v večji stavbi.

4. Podjetje zaposluje n delavcev in mora opraviti m različnih nalog, vendar niso vsi delavci primerni za vsako nalogo. Problem lahko predstavimo kot graf katerega vozlišča so delavci in naloge, med delavcem in nalogo pa dodamo povezavo, če je delavec usposobljen za opravljanje te naloge. S pomočjo prirejanj v dvodelnih grafih lahko poiščemo ustrezno razporeditev dela.

5. Problem sestavljanja urnika izpitnih rokov za študente FMF, če noben študent ne sme imeti dveh izpitov na isti dan, lahko modeliramo kot problem barvanja grafov. Izpitne roke predstavimo kot vozlišča grafa in dve vozlišči povežemo, če obstaja študent, ki bo opravljal oba izpita. Iščemo barvanje vozlišč s čim manj barvami, tako da nobeni sosednji vozlišči nista iste barve.

6. Družabna omrežja lahko predstavimo kot grafe (vozlišča so osebe, povezave pa prijateljstva ali sledenje med njimi). S pomočjo analize dobljenega grafa lahko analiziramo tudi družabno omrežje.

Teorija grafov je zelo bogato področje, ki se povezuje s številnimi drugimi vejami matematike. V okviru delavnice bomo imeli čas spoznati le nekatere teme, dodatne naloge so označene z *. Vsebina poglavji 2–9 je

povzeta po [1, 4, 5, 7], poglavje 7 tudi po [3], vsebina poglavja 10 pa po [1, 2].[1] Ker gre za klasične rezultate iz obravnavanih tem, viri sproti niso dodatno citirani.

2 Osnovni pojmi

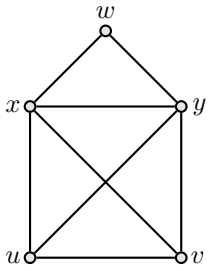
2.1 Kaj je graf?

Graf $G = (V(G), E(G))$, kjer je $V(G)$ *množica vozlišč* grafa G in $E(G)$ množica neurejenih parov vozlišč. ki jim pravimo *povezave* grafa G. Mi se bomo ukvarjali le s končnimi grafi ($V(G)$ je končna množica) z neusmerjenimi povezavami (povezave so neurejeni pari) brez zank in brez vzporednih povezav.

Če je $\{u, v\}$ povezava grafa G, pravimo, da sta vozlišči u in v sosednji, kar označimo kot $u \sim v$ ali $u \sim_G v$. Namesto $\{u, v\}$ lahko pišemo kar uv ali vu. Vozlišči u in v sta krajišči povezave uv. Če imata dve povezavi skupno krajišče, pravimo, da sta incidenčni. Soseščina vozlišča v je množica njegovih sosedov: $N_G(v) = \{u \colon vu \in E(G)\}$. Zaprta soseščina v je $N_G[v] = N_G(v) \cup \{v\}$. Stopnja vozlišča v je $\deg_G(v) = |N_G(v)|$. Najmanjšo stopnjo vozlišč v grafu G označimo z $\delta(G)$, največjo pa z $\Delta(G)$.

Sliko grafa dobimo tako, da vozlišča narišemo kot točke v ravnini (vsako vozlišče predstavimo s svojo točko), povezave pa kot loke med ustreznimi točkami. Isti graf lahko narišemo na več na videz različnih načinov.

Naloga 1. Za graf G na sliki 1 določi $V(G)$, $E(G)$, $N_G(u)$, $N_G[u]$ in stopnje vseh vozlišč. Poišči še $\delta(G)$ in $\Delta(G)$.



Slika 1: Graf za nalogo 1.

Naloga 2 (*)**.** Naj bo $G = (V, E)$ enostaven graf in $|V| \geq 2$. Pokažite, da G vsebuje vsaj dve vozlišči, ki imata isto stopnjo.

Opomba 2.1 (Dirichletov princip)**.** *Če n predmetov razvrstimo v k škatel, bo zagotovo v vsaj eni škatli vsaj $\lceil \frac{n}{k} \rceil$ predmetov.*

Naloga 3 (*, iz revije Presek)**.** V cirkuški predstavi nastopajo štirje pari klovnov: dva rdeča, dva modra, dva zelena in dva rumena. Med predstavo se zaletavajo med seboj, a nikoli se ne zaletita dva klovna iste barve. Nekega dne je 1. rdeči klovn vprašal ostalih 7, v koliko drugih klovnov so se zaleteli. Dobil je same različne odgovore. V koliko klovnov se je med predstavo zaletel drugi rdeči klovn?

Nalogo zapišite v jeziku teorije grafov in rešite.

Naloga 4 (*)**.** (a) Zaporedje $(d_1, d_2, \ldots, d_n)$ je *grafovsko*, če obstaja graf z n vozlišči, ki imajo stopnje $d_1, d_2, \ldots, d_n$. Pokažite naslednjo trditev.

Naj bo $n \geq 2$, $d_1 \geq 1$ in $d_1 \geq d_2 \geq \cdots \geq d_n$. Potem je zaporedje $(d_1, d_2, \ldots, d_n)$ grafovsko natanko tedaj, ko je grafovsko zaporedje $(d_2 - 1, d_3 - 1, \ldots, d_{d_1+1} - 1, d_{d_1+2}, \ldots, d_n)$.

[1] V kolikor vas bo delavnica pritegnila, se lahko natančneje poglobite v vsebino omenjenih knjig. Za morebitna vprašanja ali nasvet sem na voljo preko elektronske pošte tudi po MaRSu.

(b) Katera od naslednjih zaporedij so grafovska? Za vsako zaporedje, ki je grafovsko, poiščite tudi graf s takšnim zaporedjem stopenj.

(i) $(6, 5, 5, 4, 3, 3, 2, 2, 2)$

(ii) $(5, 5, 4, 3, 3, 3, 2)$

(iii) $(3, 3, 2, 2, 2, 2, 1, 1)$

(iv) $(7, 4, 3, 3, 2, 2, 2, 1, 1, 1)$

(v) $(4, 3, 2, 1)$

(c) Poišči neizomorfna grafa z zaporedjem stopenj vozlišč $(3, 3, 2, 2, 2, 2)$.

Lema 2.1. *Za vsak graf G velja*

$$\sum_{v \in V(G)} \deg_G(v) = 2 \cdot |E(G)|.$$

Dokaz. Lemo dokažemo s pomočjo dvojnega štetja. Naj bo M množica vseh urejenih parov $(v, e) \in V(G) \times E(G)$, za katere je v krajišče povezave e. Število elementov množice M lahko preštejemo na dva načina. Če združimo tiste urejene pare, ki se ujemajo na prvi komponenti, dobimo

$$|M| = \sum_{v \in V(G)} |\{e \mid v \text{ je krajišče povezave } e \in E(G)\}| = \sum_{v \in V(G)} \deg(v).$$

Če združimo pare, ki se ujemajo na drugi komponenti, pa dobimo

$$|M| = \sum_{e \in E(G)} |\{v \mid v \text{ je krajišče povezave } e \in E(G)\}| = \sum_{e \in E(G)} 2 = 2 \cdot |E(G)|.$$

Od tod sledi

$$\sum_{v \in V(G)} \deg(v) = |M| = 2 \cdot |E(G)|,$$

torej je trditev dokazana. □

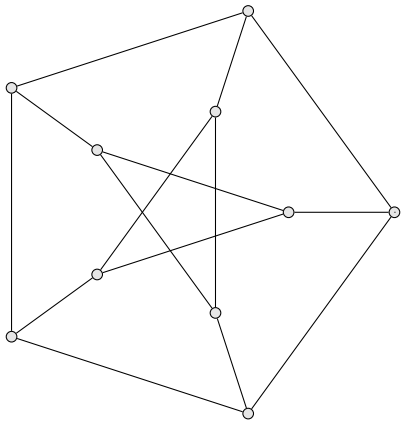
Naloga 5. Dokaži, da ima vsak graf sodo mnogo vozlišč lihe stopnje.

Naloga 6 (*)**.** Na zabavi se je zbralo 13 ljudi. Vsak je s seboj prinesel 3 darila, ki bi jih rad izmenjal s tremi drugimi udeleženci zabave. Ali je to izvedljivo? Predstavite kot problem iz teorije grafov in ga rešite.

2.2 Družine grafov

Oglejmo si nekaj pomembnih družin grafov:

- K_n, $n \geq 1$: *polni graf* na n vozliščih; graf, v katerem je vsak par vozlišč povezan.
- P_n, $n \geq 1$: *pot* na n vozliščih; graf z vozlišči $\{1, 2, \ldots, n\}$ in povezavami $\{i(i+1) \mid i \in \{1, 2, \ldots, n-1\}\}$.
- C_n, $n \geq 3$: *cikel* na n vozliščih; graf, ki ga dobimo iz poti na n vozliščih, tako da dodamo povezavo med začetkom in koncem poti.
- $K_{m,n}$, $m, n \geq 1$: *polni dvodelni graf*; graf z množico vozlišč $\{u_1, \ldots, u_m\} \cup \{v_1, \ldots, v_n\}$ in povezavami $\{u_i v_j \mid i \in \{1, \ldots, m\}, j \in \{1, \ldots, n\}\}$.
- Q_n, $n \geq 0$: *hiperkocka*; graf, katerega vozlišča so vse urejene n-terice sestavljene iz 0 in 1, dve vozlišči pa sta sosednji, če se razlikujeta v natanko eni koordinati.



Slika 2: Petersenov graf.

- P: *Petersenov graf* je graf na sliki 2.

Naloga 7. (a) Nariši grafe K_1, K_2, K_3, K_4, K_5. Koliko vozlišč in koliko povezav ima graf K_n?

(b) Nariši grafe P_1, P_2, P_3, P_4. Koliko vozlišč in koliko povezav ima graf P_n?

(c) Nariši grafe C_3, C_4, C_5, C_6. Koliko vozlišč in koliko povezav ima graf C_n?

(d) Nariši grafe $K_{1,6}$, $K_{2,2}$, $K_{3,3}$, $K_{2,4}$. Koliko vozlišč in koliko povezav ima graf $K_{m,n}$?

(e) Nariši grafe Q_0, Q_1, Q_2, Q_3. Koliko vozlišč in koliko povezav ima graf Q_n?

Komplement $\overline{G}$ grafa G je graf z isto množico vozlišč kot G in z dvema vozliščema sosednjima v $\overline{G}$ natanko tedaj, ko vozlišči nista sosednji v G.

Naloga 8 (*)**.** Poišči komplement grafa $G = (V, E)$, kjer je $V = \{1, 2, 3, 4, 5\}$ in $E = \{\{1, 2\}, \{2, 3\}, \{2, 4\}, \{2, 5\}, \{3, 4\}, \{4, 5\}\}$.

2.3 Izomorfizem grafov

Naj bosta G in H grafa. Preslikava $f\colon V(G) \to V(H)$ je *izomorfizem*, če je bijekcija in zanjo velja: $uv \in E(G) \iff f(u)f(v) \in E(H)$. Grafa G in H sta *izomorfna*, če obstaja izomorfizem med njima. Preprosto povedano, izomorfna grafa se razlikujeta le v poimenovanju vozlišč. Izomorfna grafa imata enake grafovske lastnosti, na primer enako število vozlišč in povezav, število podgrafov, zaporedje stopenj vozlišč ipd.

Naloga 9 (*)**.** Poiščite vse neizomorfne grafe na treh ali štirih vozliščih.

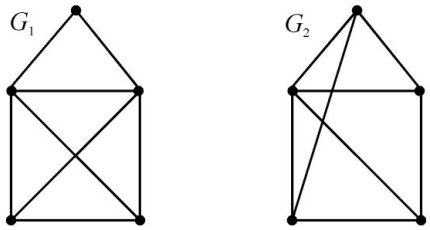
Naloga 10 (*)**.** (a) Ali sta grafa na sliki 3 izomorfna?

(b) Ali sta grafa na sliki 4 izomorfna?

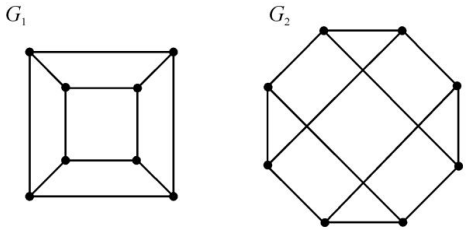
(c) Ali sta grafa na sliki 5 izomorfna? Nasvet: v vsakem od grafov preštejte cikle dolžine 4.

Naloga 11 (*)**.** Naj bo G graf z n vozlišči in m povezavami. Koliko povezav ima njegov komplement?
Ali je graf na šestih vozliščih lahko izomorfen svojemu komplementu?

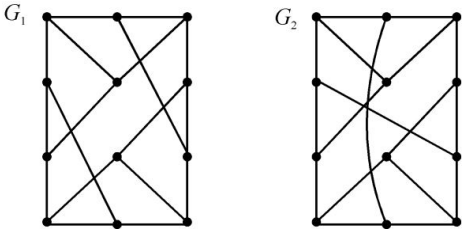
Naloga 12 (*)**.** Naj bo G graf, katerega vozlišča so vsi možni pari števil $\{k, \ell\}$, kjer sta $k, \ell \in \{1, 2, 3, 4, 5\}$ in $k \neq \ell$. Vozlišči $\{k_1, \ell_1\}$ in $\{k_2, \ell_2\}$ sta sosednji, če je $\{k_1, \ell_1\} \cap \{k_2, \ell_2\} = \emptyset$. Dokaži, da je G izomorfen Petersenovemu grafu.



Slika 3: Slika za nalogo 10(a).



Slika 4: Slika za nalogo 10(b).



Slika 5: Slika za nalogo 10(c).

2.4 Podgrafi

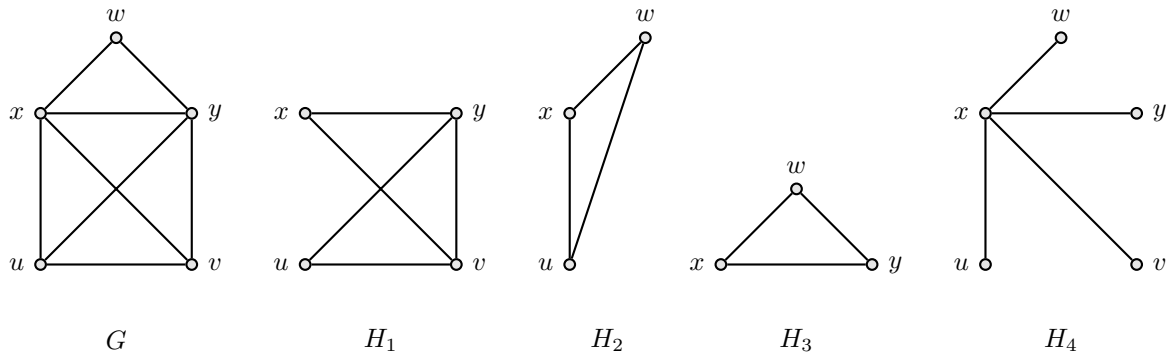
Graf H je *podgraf* grafa G, če je $V(H) \subseteq V(G)$ in $E(H) \subseteq E(G)$. To označimo kot $H \subseteq G$. Če za podgraf H grafa G velja $V(H) = V(G)$, je H *vpet podgraf* G. Podgraf H grafa G je *induciran podgraf*, če velja $E(H) = \{uv \in E(G) \mid u, v \in V(H)\}$. Induciran podgraf H grafa G je enolično določen s svojo množico vozlišč U, zato ga označimo kot $G[U]$.

Naloga 13 (*)**.** Kateri izmed grafov H_1, H_2, H_3 in H_4 so podgrafi grafa G (glej sliko 6)? Utemelji. Če je $H_i \subseteq G$, razmisli, ali je morda vpet ali induciran podgraf.

Naloga 14 (*)**.** Naj bo G graf z n vozlišči in m povezavami. Koliko vpetih in koliko induciranih podgrafov ima graf G?

2.5 Sprehodi, poti in povezanost

Zaporedje vozlišč $v_0v_1 \dots v_k$ grafa G je *sprehod* dolžine k, če velja $v_i \sim v_{i+1}$ za vse $i \in \{0, \dots, k-1\}$ (vozlišča v sprehodu niso nujno različna). Sprehod je enostaven, če vsako povezavo grafa prehodi največ enkrat. Sprehod je sklenjen, če je $v_0 = v_k$. Sprehod, na katerem so vsa vozlišča med seboj različna, je *pot v grafu*. Enostaven sklenjen sprehod dolžine vsaj 3, na katerem sta enaki le prvo in zadnje vozlišče, je *cikel grafa*.



Slika 6: Graf za nalogo 13.

Lema 2.2. *Če med dvema vozliščema obstaja sprehod dolžine k, potem med njima obstaja tudi pot dolžine kvečjemu k.*

Naloga 15. Dokaži Lemo 2.2.

Lema 2.3. *Če med vozliščema u in v v grafu G obstajata dve različni poti, potem G vsebuje cikel.*

Dokaz. Naj bosta $P = u_0u_1 \dots u_k$ in $Q = v_0v_1 \dots v_m$ različni poti v G med $u = u_0 = v_0$ in $v = u_k = v_m$. Naj bo ℓ najmanjši indeks, za katerega velja $u_\ell = v_\ell$ in hkrati $u_{\ell+1} \neq v_{\ell+1}$. Ker $P \neq Q$, tak indeks $\ell \geq 0$ obstaja.

Naj bo $j \geq 1$ najmanjši tak, da $u_{\ell+j}$ leži na poti Q (obstaja, ker je $u_k = v$ na Q). Naj bo t takšen, da je $u_{\ell+j} = v_{\ell+t}$.

Oglejmo si sklenjeni sprehod

$$C = u_\ell u_{\ell+1} \dots u_{\ell+j-1} v_{\ell+t} v_{\ell+t-1} \dots v_{\ell+1} v_\ell.$$

Ker po definiciji nobeno od vozlišč $u_{\ell+1} \dots u_{\ell+j-1}$ ne želi na Q in ker sta P in Q poti, je C cikel. □

Lema 2.4. *Če ima graf sklenjen sprehod lihe dolžine, tedaj ima tudi cikel lihe dolžine.*

Naloga 16 (*)**.** Dokaži Lemo 2.4. Nasvet: dokazuj z indukcijo po dolžini sklenjenega sprehoda. Ali analogna trditev velja tudi za sode sprehode?

Za dve vozlišči u in v rečemo, da sta v isti *povezani komponenti*, če med njima obstaja sprehod. Graf je *povezan*, če ima eno samo povezano komponento. Vozlišče v grafa G je *prerezno vozlišče*, če ima $G - v$ več komponent za povezanost kot G. Povezava e grafa G je *prerezna povezava* ali *most*, če ima graf $G - e$ več komponent za povezanost kot G.

Naloga 17 (*)**.** Nariši povezan graf. Nariši graf z natanko tremi povezanimi komponentami. Nariši graf z natanko enim prereznim vozliščem. Nariši graf z natanko enim mostovom.

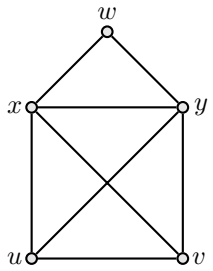
Naloga 18 (*)**.** Ali ima graf P_n kakšno prerezno vozlišče? Kaj pa most? Na enaki vprašanji odgovori tudi za družino $K_{m,n}$ (obravnavaj glede na m in n).

2.6 Razdalja v grafu

Razdaljo $d_G(u, v)$ med vozliščema u in v v grafu G definiramo kot dolžino najkrajše poti od u do v v G; če taka pot ne obstaja, za razdaljo vzamemo vrednost ∞. Dolžini najkrajšega cikla v grafu pravimo *ožina* grafa.

Največji razdalji med parom vozlišč grafa pravimo *premer* (ali *diameter*) grafa, $\operatorname{diam}(G) = \max\{d_G(u, v) \mid u, v \in V(G)\}$; za nepovezane grafe G je $\operatorname{diam}(G) = \infty$. *Ekscentričnost* vozlišča $v \in V(G)$ definiramo kot $\operatorname{ecc}(v) = \max\{d(v, x) \colon x \in V(G)\}$. Torej je premer grafa največja ekscentričnost vozlišča. *Polmer* (ali *radij*) grafa G je najmanjša ekscentričnost, torej $\operatorname{rad}(G) = \min\{\operatorname{ecc}(v) \colon v \in V(G)\}$.

Naloga 19 (*)**.** Za vsako vozlišče grafa na sliki spodaj določi ekscentričnost. Določi premer, polmer in ožino grafa.



Naloga 20 (*)**.** Kolikšna sta premer in ožina naslednjih grafov: Petersenov graf; hiperkocka Q_d, $d \geq 2$.

Naloga 21 (*)**.** Dokaži, da za vsak graf G velja $\mathrm{rad}(G) \leq \mathrm{diam}(G) \leq 2\,\mathrm{rad}(G)$. Poišči primer grafa, kjer je $\mathrm{diam}(G) = \mathrm{rad}(G)$ in primer grafa, kjer je $\mathrm{diam}(G) = 2\,\mathrm{rad}(G)$.

Naloga 22 (*)**.** Naj bo G graf z vsaj enim ciklom. Dokaži, da ožina grafa G ni večja od $2\,\mathrm{diam}(G) + 1$.

3 Drevesa

Drevo je povezan graf brez ciklov. *Gozd* je graf brez ciklov (torej je gozd disjunktna unija dreves). *List* je vozlišče stopnje 1.

Naloga 23 (*)**.** Poišči vsa drevesa na 6 vozliščih.

Trditev 3.1. *Vsako drevo na vsaj dveh vozliščih ima vsaj dva lista.*

Dokaz. Naj bo T drevo na vsaj dveh vozliščih. Naj bo $P = v_0v_1 \dots v_k$ najdaljša pot v drevesu T. Ker T vsebuje vsaj dve vozlišči, je $k \geq 1$ in $v_0 \neq v_k$. Ker je P najdaljša pot v T, je $N(v_k) \subseteq V(P)$. Ampak ker T ne vsebuje ciklov, je $N(v_k) = \{v_{k-1}\}$, torej je v_k list. Podoben razmislek pokaže, da je tudi v_0 list. □

Trditev 3.2. *Če je T drevo, potem je $|E(T)| = |V(T)| - 1$.*

Dokaz. Dokazujemo z indukcijo na število vozlišč. Edino drevo z enim samim vozliščem je K_1 in zanj enačba velja. Naj bo sedaj T drevo na $n \geq 2$ vozliščih. Po trditvi 3.1 ima T list, recimo mu v. Graf $T - v$ je povezan in brez ciklov, torej drevo, zato po indukcijski predpostavki velja $|E(G - v)| = |V(T - v)| - 1$. Iz tega sledi $|E(T)| = |E(T - v)| + 1 = |V(T - v)| = |V(T)| - 1$. □

Opomba 3.1 (Princip popolne matematične indukcije)**.** *Naj bo $S \subseteq \mathbb{N}$. Če je $1 \in S$ in je za vsako število $n \in \mathbb{N}$ pravilen sklep: $n \in S \implies (n+1) \in S$, je $S = \mathbb{N}$.*

Dokazovanje s pomočjo indukcije – dokazujemo, da neka lastnost velja za vsa naravna števila.

1. *Dokažemo, da lastnost velja za 1 (*baza indukcije*).*
2. *Predpostavimo, da lastnost velja za n (*indukcijska predpostavka*), in dokažemo, da potem velja tudi za $n + 1$ (*indukcijski korak*).*

Trditev 3.3. *Za graf G so ekvivalentne naslednje trditve:*

(1) G je drevo;

(2) med poljubnima vozliščema v G obstaja natanko ena pot;

(3) G je povezan in vsaka njegova povezava je most;

(4) G je povezan in velja $|E(G)| = |V(G)| - 1$.

Naloga 24 (*). Dokaži trditev 3.3.

Naloga 25 (*). Naj bo T drevo s 17 vozlišči, ki so vsa stopnje 1 ali 4. Koliko vozlišč stopnje 4 ima T? Nariši kakšno takšno drevo.

Naloga 26 (*). Dokaži, da ima vsako drevo T vsaj $\Delta(T)$ listov.

Naloga 27 (*). Naj bo T drevo v katerem imajo vsa vozlišča, ki so sosednja s kakšnim listom, stopnjo vsaj 3. Dokaži, da T vsebuje par listov s skupnim sosedom.

Naloga 28 (*). Poišči vsa drevesa, ki so izomorfna svojemu komplementu.

Naloga 29 (*). Dokaži, da v vsakem drevesu obstaja vozlišče, ki leži na vseh najdaljših poteh drevesa.

Naloga 30 (*). Dokaži, da je graf G povezan natanko tedaj, ko premore vpeto drevo.

Naloga 31 (*). *Center* $C(G)$ grafa G je množica vozlišč, katerih ekscentričnost je enaka $\mathrm{rad}(G)$. Dokaži, da center drevesa T sestavlja bodisi eno vozlišče bodisi dve sosednji vozlišči. Poišči primer grafa (ki ni drevo), za katerega to ne velja.

4 Dvodelni grafi

Graf G je *dvodelen*, če lahko množico vozlišč $V(G)$ zapišemo kot disjunktno unijo dveh neprazniih podmnožic $A, B \subseteq V(G)$ tako, da je za vsako povezavo $uv \in E(G)$ eno od vozlišč u, v vsebovano v množici A, drugo pa v množici B. Par $\{A, B\}$ imenujemo *dvodelna razdelitev* ali *biparticija*.

Naloga 32 (*). Sorojenci Ana, Bine, Cene, Črt in Dora so mami obljubili pomoč pri pospravljanju hiše. Mama je pripravila seznam petih nalog (ki jih bomo okrajšali kot 1–5), sorojenci pa so se odločili, da poskusijo najti razporeditev nalog, tako da bo vsak opravil natanko eno, in sicer takšno, ki mu je vsaj malo v veselje. Ana z veseljem opravi 1, 2 ali 4, Bine bi najraje postoril 1 ali 3, Cene se ne brani 1 ali 5, Črt je pripravljen narediti le 5, Dori pa je v veselje karkoli razen 4.

Ali lahko najdejo ustrezno razporeditev? Problem predstavi v jeziku teorije grafov.

Naloga 33 (*). Dokaži, da je Q_n, $n \geq 1$, dvodelen graf.

Izrek 4.1. *Graf je dvodelen natanko tedaj, ko ne vsebuje cikla lihe dolžine.*

Dokaz. Graf je dvodelen natanko tedaj, ko je dvodelna vsaka njegova povezana komponenta. Zato je izrek dovolj dokazati za povezane grafe.

Denimo, da je G dvodelen z razdelitvijo $\{A, B\}$, in da vsebuje lih cikel $C = v_0v_1 \dots v_{2k+1}$, $v_{2k+1} = v_0$. Brez škode za splošnost je $v_0 \in A$. Tedaj je $v_1 \in B$, $v_2 \in A$, …, $v_{2k} \in A$. Vendar je v_{2k} sosednje vozlišču $v_{2k+1} = v_0$, ki je v A, kar je protislovje.

Denimo, da G ni dvodelen. Poiskati želimo cikel lihe dolžine. Naj bo $v_0 \in V(G)$ neko izbrano vozlišče. Definiramo:

$$L = \{v \in V(G) \colon d(v_0, v) \text{ je liho}\} \quad \text{in}$$
$$S = \{v \in V(G) \colon d(v_0, v) \text{ je sodo}\}.$$

Ker G ni dvodelen, $\{L, S\}$ ni dvodelna razdelitev, torej za nek $A \in \{L, S\}$ obstajata $u, v \in A$, da je $uv \in E(G)$. Naj bo $v_0u_1 \dots u_{m-1}u$ najkrajša pot od v_0 do u in $v_0v_1 \dots v_{k-1}v$ najkrajša pot od v_0 do v. Tedaj sta $m = d(v_0, u)$ in $k = d(v_0, v)$ iste parnosti. Sklenjeni sprehod $v_0u_1 \dots uv \dots v_1v_0$ je dolžine $m + 1 + k$, kar je liho število. Po lemi 2.4 sledi obstoj lihega cikla v G. □

Naloga 34 (*). Naj bo G dvodelen graf z vsaj eno povezavo, v katerem imajo vsa vozlišča isto stopnjo. Dokaži, da sta množici dvodelnega razbitja grafa G enako močni.

5 Ravninski grafi

Graf G je *ravninski*, če ga lahko narišemo v ravnini tako, da se nobeni povezavi ne sekata. *Graf vložen v ravnino* je graf skupaj z ravninsko risbo.

Naloga 35. Za naslednje grafe ugotovi, ali so ravninski ali ne: K_4, K_5, $K_{2,3}$, $K_{3,3}$.

Ravninska risba grafa G razdeli ravnino v sklenjena območja, ki jim pravimo *lica*. Množico vseh lic G označimo z $F(G)$. Neomejenemu licu rečemo *zunanje lice*. Vsako lice $f \in F(G)$ je omejeno s sklenjenim sprehodom v grafu G, ki mu rečemo rob lica f, njegovo dolžino (tj. število povezav na robu lica) pa označimo z $\ell(f)$.

Trditev 5.1. *Če je G ravninski graf z neko svojo risbo v ravnini, potem je*

$$\sum_{f \in F(G)} \ell(f) = 2|E(G)|.$$

Naloga 36. Dokaži trditev 5.1.

Izrek 5.1 (Eulerjeva formula)**.** *Če je G povezan graf vložen v ravnino z n vozlišči, m povezavami in f lici, potem je*

$$n - m + f = 2.$$

Dokaz. Naj bo n število vozlišč grafa. Dokazujemo s pomočjo indukcije na število povezav m. Ker ima povezan graf na n vozliščih vsaj $n-1$ povezav (drevo), za bazo indukcije pogledamo primer $m = n-1$. Ker je v tem primeru graf drevo, je lice le eno (zunanje), torej je res $n - m + f = n - (n-1) + 1 = 2$.

Naj bo sedaj $m > n-1$. Tedaj graf G vsebuje cikel in ima torej vsaj dve lici. Naj bo $e \in E(G)$ neka povezava G, ki leži na meji med dvema cikloma. Oglejmo si graf $G - e$: ima n vozlišč, $m-1$ povezav in $f-1$ lic (z odstranitvijo e smo dve lici družili v eno). Ker ima ta graf manj povezav, zanj velja indukcijska predpostavka. Torej je $n - (m-1) + (f-1) = 2$. Če to poenostavimo, dobimo $n - m + f = 2$. □

Posledica 5.1. *Če je G ravninski graf, potem ima vsaka njegova vložitev v ravnino isto število lic.*

Posledica 5.2. *Če je G povezan ravninski graf z $n \geq 3$ vozlišči in m povezavami, potem je*

$$m \leq 3n - 6.$$

Če je G povezan ravninski graf brez trikotnikov z $n \geq 3$ vozlišči in m povezavami, potem je

$$m \leq 2n - 4.$$

Naloga 37. Dokaži posledico 5.2.

Naloga 38 (*)**.** Dokaži, da Petersenov graf ni ravninski

Naloga 39 (*)**.** Za katere $n \in \mathbb{N}$ je hiperkocka Q_n ravninska?

Naloga 40. Dokaži, da za vsak povezan ravninski graf G velja $\delta(G) \leq 5$.

Naloga 41 (*)**.** Pokažite, da ima povezan kubičen graf v ravnini, pri katerem so vsa lica petkotniki ali šestkotniki, natanko 12 petkotnikov.

Naloga 42 (*)**.** Naj bo G povezan regularen graf stopnje $p \geq 3$, vložen v ravnino tako, da imajo vsa lica enako število povezav $q \geq 3$ na robu. Kakšna sta lahko p in q?

Opomba 5.1. *Za preverjanje ravninskosti grafov običajno uporabljamo enega od naslednjih izrekov:*

- *Izrek Kuratowskega: Graf je ravninski natanko tedaj, ko ne vsebuje podgrafa, izomorfnega subdiviziji grafa K_5 ali subdiviziji grafa $K_{3,3}$.*
- *Wagnerjev izrek: Graf je ravninski natanko tedaj, ko nima minorja, izomorfnega K_5 ali $K_{3,3}$.*

Ravninski graf je *zunanje-ravninski*, če ga lahko narišemo v ravnini tako, da vsa njegova vozlišča ležijo na robu istega lica.

Naloga 43 (*)**.** Ali sta grafa na spodnji sliki zunanje-ravninska?

Naloga 44 (*)**.** Dokaži, da za zunanje-ravninski graf G velja $\delta(G) \leq 2$.

6 Barvanja grafov

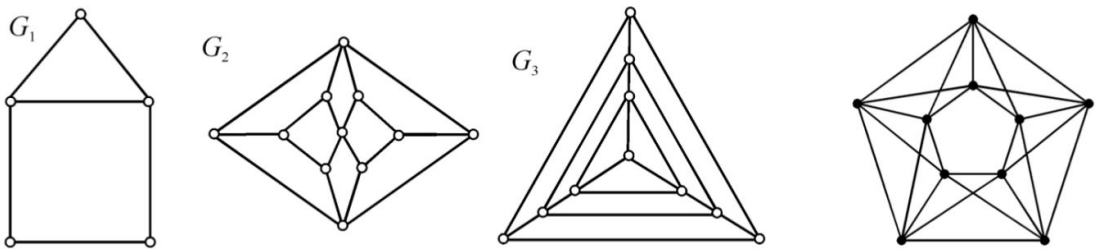
Preslikava $c\colon V(G) \to K$ je *barvanje vozlišč* grafa G z barvami iz množice K. Običajno nas zanima le število barv v K, zato takšnemu barvanju rečemo kar k-barvanje, kjer je $|K| = k$. Barvanje c je *dobro*, če so sosednja vozlišča pobarvana z različnimi barvami, tj. če za vsaka $u, v \in V(G)$ velja: $uv \in E(G) \Rightarrow c(u) \neq c(v)$. Najmanjši k za katerega obstaja dobro k-barvanje G, imenujemo *kromatično število* $\chi(G)$ grafa G. Če želimo dokazati, da je $\chi(G) = k$, moramo dokazati dvoje:

1. $\chi(G) \leq k$ (konstruiramo dobro k-barvanje);
2. $\chi(G) \geq k$ (dokažemo, da ne obstaja dobro $(k-1)$-barvanje).

Naloga 45. Določi kromatično število naslednjih grafov: K_n, P_n, C_n, Petersenov graf.

Naloga 46. Naj bo H podgraf grafa G. Dokaži, da je $\chi(H) \leq \chi(G)$.

Naloga 47 (*)**.** Za grafe na sliki 7 poiščite njihovo kromatično število.



Slika 7: Grafi za nalogo 47.

Naloga 48. Dokaži naslednji trditvi.

(a) Za graf G je $\chi(G) = 1$ natanko tedaj, ko je G brez povezav.

(b) Za graf G z vsaj eno povezavo je $\chi(G) = 2$ natanko tedaj, ko je G dvodelen.

V linearnem času lahko preverimo, ali za nek graf obstaja dobro 2-barvanje. Že za dobro 3-barvanje pa ne poznamo polinomskega algoritma.

Oglejmo si naslednji algoritem, ki vrne dobro barvanje c podanega grafa G. Imenuje se *požrešni algoritem barvanja*.

1. Izberi nek vrsti red vozlišč grafa G: $v_1, v_2, \ldots, v_n$.
2. $c(v_1) = 1$
3. Za $i = 2, \ldots, n$: $c(v_i) = r$, kjer je r najmanjša barva iz $\{1, \ldots, n\}$, ki ni v množici $\{c(v_j) \colon j < i \text{ in } v_iv_j \in E(G)\}$, tj. r je najmanjša barva, ki še ni uporabljena na že pobarvanih sosedih vozlišča v_i.

Naloga 49. Dokaži, da za vsak graf G obstaja tak vrstni red vozlišč, da požrešni algoritem G dobro pobarva z $\chi(G)$ barvami.

Naloga 50 (*)**.** Poišči graf G in takšen vrstni red vozlišč, da požrešni algoritem G pobarva s poljubno več barvami kot je $\chi(G)$.

Naloga 51 (*)**.** Imejmo tako (končno) množico premic v ravnini, da se nobene tri ne sekajo v isti točki. Konstruiraj graf G, katerega vozlišča so presečišča premic in dve vozlišči povezani, če sta zaporedni vozlišči na neki premici. Dokaži, da je $\chi(G) \leq 3$.

Naloga 52 (*, Hadwiger–Nelson problem)**.** Naj bo G neskončen graf, katerega vozlišča so točke v $\mathbb{R}^2$ in vozlišči sosednji, če sta na razdalji natanko ena. Dokaži, da je $4 \leq \chi(G) \leq 7$.

Trditev 6.1. *Za vsak graf G velja*

$$\chi(G) \leq \Delta(G) + 1.$$

Naloga 53. Dokaži trditev 6.1.

V resnici velja močnejši izrek.

Izrek 6.1 (Brooks)**.** *Naj bo G povezan graf, ki ni niti polni graf niti lih cikel. Potem je $\chi(G) \leq \Delta(G)$.*

Naloga 54 (*)**.** Graf je regularen, če imajo vsa vozlišča isto stopnjo. Dokaži, da za graf G, ki ni regularen, velja $\chi(G) \leq \Delta(G)$. Nasvet: uporabi požrešni algoritem na primerno izbranem vrstnem redu vozlišč.

Naloga 55. Dokaži, da če je $\chi(G) = r$, potem je $|E(G)| \geq \binom{r}{2} = \frac{r(r-1)}{2}$. Opiši grafe, za katere velja enakost.

Naloga 56. Opiši grafe, ki imajo med vsemi grafi G z n vozlišči in $\chi(G) = r$ največje število povezav.

Rešitev naloge so *Turanovi grafi* $T_{n,r}$, ki so polni r-multipartitni grafi z n vozlišči, v katerih se kosi particije po velikosti paroma razlikujejo kvečjemu za 1.

Naloga 57. Dokaži, da za vsak ravninski graf G velja $\chi(G) \leq 6$. Nasvet: naloga 40.

Naloga 58 (*)**.** Dokaži, da za vsak ravninski graf G velja $\chi(G) \leq 5$. Nasvet: naloga 40.

Naslednji izrek sta prva dokazala Appel in Haken v 70. letih prejšnjega stoletja, pri čemer je del dokaza naredil računalnik. Danes sicer poznamo krajši dokaz, še vedno pa ni znan dokaz izreka, ki bi ga bil sposoben v realnem času preveriti človek brez računalniške pomoči.

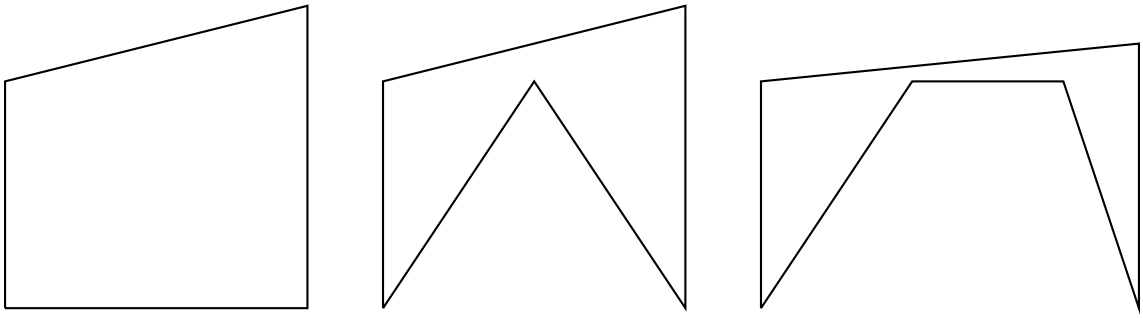
Izrek 6.2 (Izrek štirih barv)**.** *Za vsak ravninski graf G je $\chi(G) \leq 4$.*

Naloga 59. Dokaži, da lahko vsak zunanje-ravninski graf pobarvamo s 3 barvami.

7 Problem umetnostne galerije

Tloris umetnostne galerije ima obliko (ravninskega) mnogokotnika z n oglišči, ki nima notranjih dvorišč (torej je tloris galerije "brez lukenj"). V galerijo želimo namestiti senzorje tako, da bodo nadzirali celotno galerijo. Vsak senzor spremlja dogajanje poljubno daleč v vseh smeri, ne more pa se premikati in ne vidi skozi zidove. Ker so tovrstni senzorji precejšen strošek, jih želimo namestiti čim manj. Najmanj koliko senzorjev potrebujemo, da bo vsako točko v galeriji nadziral vsaj eden?

Naloga 60. Problem reši na konkretnih tlorisih galerij s slike 8.



Slika 8: Galerije za nalogo 60.

Naloga 61. Poišči tloris galerije s $3k$ oglišči, v katero moramo namestiti vsaj k senzorjev.

Izrek 7.1. *Dokaži, da za nadzor galerije (brez lukenj) z n oglišči vedno zadošča $\lfloor \frac{n}{3} \rfloor$ senzorjev.*

Naloga 62. Dokaži izrek 7.1.

Poglejmo si še nekoliko drugačen problem. Tloris umetnostne galerije ima obliko (ravninskega) mnogokotnika z n oglišči, ki nima notranjih dvorišč (torej je tloris galerije "brez lukenj"). Galerija ima lahko tudi ravne notranje stene, ki vedno povezujejo vogale galerije in se med seboj ne križajo (lahko pa se dotikajo). Vsaka notranja stena ima prehod. Če v prehod postavimo senzor, bo ta senzor lahko nadziral dogajanje v obeh sobah.

Naloga 63 (*)**.** Dokaži, da v zgornjem primeru $\lfloor \frac{2n-3}{3} \rfloor$ senzorjev zadostuje za nadzor celotne galerije.

8 Ramseyeva števila

Naloga 64 (*)**.** Ali lahko povezave grafa K_5 pobarvaš z dvema barvama tako, da ne ustvariš monokromatičnega trikotnika (tj. trikotnik, katerega povezave so vse iste barve)? Utemelji.

Naloga 65 (*)**.** Ali lahko povezave grafa K_6 pobarvaš z dvema barvama tako, da ne ustvariš monokromatičnega trikotnika (tj. trikotnik, katerega povezave so vse iste barve)? Utemelji.

Grafovsko Ramseyevo število $N(G_1, \ldots, G_k)$ je najmanjši N, tako da če povezave polnega grafa K_N poljubno pobarvamo z barvami $1, \ldots, k$, tedaj v tem K_N najdemo vsaj en podgraf G_i, ki ima vse povezave barve i.

Naloga 66 (*)**.** Dokaži, da je $N(K_2, K_k) = k$.

Naloga 67 (*)**.** Dokaži, da je $N(K_3, K_3, K_3) \leq 17$.

Naloga 68 (*)**.** Dokaži, da je $N(K_3, K_4) = 9$.

Naloga 69 (*)**.** Dokaži, da za $a \geq 3$ velja $N(K_a, K_a) \geq 2^{\frac{a}{2}}$.

9 Dominacija v grafih

Vozlišče $v \in V(G)$ *dominira* sebe in svoje sosede (torej $N[v]$). Množica $D \subseteq V(G)$ je *dominacijska množica* grafa G, če velja $V(G) = \bigcup_{x \in D} N[x]$, tj. vsako vozlišče v $V(G) - D$ ima soseda iz D. Moč najmanjše množice, ki dominira G, je *dominacijsko število* grafa G in ga označimo z $\gamma(G)$.

Naloga 70. Določi dominacijsko število grafov K_n, P_n, Petersenov graf.

Naloga 71. Koliko najmanj trdnjav je treba postaviti na šahovsko desko tako, da so napadena vsa polja šahovnice?

Naloga 72. Koliko kraljic je treba postaviti na šahovsko desko tako, da so napadena vsa polja šahovnice? Poišči rešitev s čim manj kraljicami.

Trditev 9.1. *Za vsak graf G velja*

$$\frac{|V(G)|}{\Delta(G)+1} \leq \gamma(G) \leq |V(G)| - \Delta(G).$$

Naloga 73 (*)**.** Dokaži trditev 9.1.

Izrek 9.1. *Za vsak graf G velja*

$$\gamma(G) \leq |V(G)| \cdot \frac{1+\ln(1+\delta(G))}{1+\delta(G)}.$$

Dokaz. Označimo $n = |V(G)|$ in $p = \frac{\ln(1+\delta(G))}{1+\delta(G)}$. Če je $\delta(G) = 0$ (G ima izolirana vozlišča), potem je $p = 1$ in trditev očitno drži. Zato od zdaj naprej predpostavljamo, da velja $\delta(G) \geq 1$ (G nima izoliranih vozlišč). Iz tega sledi, da je $p \in (0, 1)$.

Naj bo $X \subseteq V(G)$ množica, ki jo dobimo tako, da vsako vozlišče $x \in V(G)$ z verjetnostjo p vstavimo v množico X (neodvisno od preostalih vozlišč). Naj bo $Y = V(G) - \bigcup_{x \in X} N[x]$. Očitno je $X \cup Y$ dominacijska množica grafa G. Želeli bi določiti $|X \cup Y|$.

Po definiciji množice X je $E(|X|) = \sum_{x \in V(G)} P(x \in X) = np$. Če želimo določiti $E(|Y|)$, moramo najprej oceniti $P(y \in Y)$. Opazimo, da je $y \in Y$ natanko tedaj, ko noben $x \in N[y]$ ni v Y, torej natanko tedaj, ko za vsak $x \in N[y]$ velja $x \notin X$. Ker gre za neodvisne dogodke, velja $P(y \in Y) = (1-p)^{\deg(y)+1}$. Zdaj se spomnimo dveh lastnosti funkcij:

- Ker je $1 - p \in (0, 1)$ in $\deg(y) \geq \delta(G)$, velja $(1-p)^{\deg(y)+1} \leq (1-p)^{\delta(G)+1}$.
- Za vse $x \in (0, 1)$ je $1 - x \leq e^{-x}$. (Ogledamo si funkcijo $f(x) = e^{-x} - 1 + x$ na $[0, 1]$, ugotovimo, da je $f(0) = 0$ in $f'(x) \geq 0$ na $[0, 1]$, torej f na tem intervalu narašča, od koder sledi želena lastnost.)

Če ti dve lastnosti in definicijo p uporabimo za poenostavitev $P(y \in Y)$ dobimo $P(y \in Y) \leq \frac{1}{\delta(G)+1}$.

Ker sta X in Y disjunktni množici, sledi

$$E(|X \cup Y|) \leq n(p + \frac{1}{\delta(G)+1}) = n\frac{1+\ln(1+\delta(G))}{1+\delta(G)} = a.$$

Pričakovana velikost dominacijske množice $X \cup Y$ je torej navzgor omejena z a. Če bi bilo $\gamma(G) > a$, potem bi bile vse dominacijske množice velikosti več kot a, torej bi bila tudi pričakovana velikost $X \cup Y$ več kot a, kar je protislovje. Torej zagotovo obstaja neka dominacijska množica velikosti kvečjemu a, zato je $\gamma(G) \leq a$. □

Naloga 74 (*)**.** Najdi neskončno družino povezanih grafov na n vozliščih:

(a) Z minimalno stopnjo 1 in $\gamma(G) = \frac{n}{2}$.

(b) Z minimalno stopnjo 2 in $\gamma(G) = \frac{2}{5}n$.

(c) Z minimalno stopnjo 3 in $\gamma(G) = \frac{3}{8}n$ (dovolj je poiskati le en tak povezan graf).

Naloga 75 (*)**.** (a) Naj bo G graf brez izoliranih vozlišč in $S \subseteq V(G)$ dominacijska množica moči $\gamma(G)$. Dokaži, da je tudi $V(G) - S$ dominacijska množica.

(b) Dokaži, da za vsak povezan graf G na n vozliščih velja $\gamma(G) \leq \frac{n}{2}$.

10 Igra policajev in roparja na grafih

10.1 Osnove

Igra policajev in roparja na grafu je igra za dva igralca, eden upravlja k policajev, drugi pa roparja. Policaji in ropar se premikajo po vozliščih grafa, pri čemer se lahko na potezi premaknejo na sosednje vozlišče ali pa ostanejo na mestu. Cilj policajev je ujeti roparja, ki se želi temu izogniti. Igralca sta na vrsti izmenično, začne tisti, ki upravlja policaje. Najprej izbere začetna vozlišča za vseh k policajev, nato začetno vozlišče izbere še igralec, ki upravlja roparja. Na kratko bomo prvemu igralci rekli "policaji", drugemu pa "ropar". Sledi znova poteza policajev; vsak izmed njih se lahko premakne na sosednje vozlišče ali pa ostane pri miru. Ropar vidi njihove poteze in nato izbere svojo naslednjo potezo, tj. premik na sosednje vozlišče ali ostati na mestu. To se ponavlja, dokler se eden izmed policajev ne nahaja v istem vozlišču grafa kot ropar. Če se to zgodi, rečemo, da so policaji ujeli roparja in so zmagali igro. Če se to nikoli ne zgodi (tj. ropar se lahko izogiba ujetju v neskončnost) pravimo, da je zmagal ropar. Zmagovalna strategija policajev je množica pravil, za katere velja, da če jim policaji sledijo, zmagajo (ne glede na to, kako igra ropar). Analogno definiramo strategijo roparja.

Če v vsako vozlišče grafa postavimo policaja, bodo policaji zagotovo zmagali. Zato je najmanjše število policajev, ki so potrebni za zmago na danem grafu G, dobro definirano naravno število. Imenujemo ga *policijsko število* grafa G in označimo s $c(G)$.

Naloga 76. Določi $c(P_n)$, $c(C_n)$, $c(K_n)$ in $c(K_{1,n})$.

Naloga 77 (*)**.** Določi $c(Q_n)$ za $n \in \{2, 3, 4\}$. Postavi domnevo za $c(Q_n)$ v splošnem.

Lema 10.1. *Če je G graf, potem je $c(G) \leq \gamma(G)$.*

Dokaz. Naj bo D dominacijska množica G moči $\gamma(G)$. Strategija $\gamma(G)$ policajev je, da si za začetna vozlišča izberejo vozlišča iz množice D. Ne glede na to, v katerem vozlišču začne ropar, je to vozlišče bodisi v D ali pa ima soseda v D (ker je D dominacijska množica). Torej policaji zmagajo v prvi potezi. □

Naloga 78. Ali je za kakšno družino grafov dosežena enakost v lemi 10.1? Ali je razlika med $\gamma(G)$ in $c(G)$ lahko poljubno velika?

Lema 10.2. *Če je T (končno) drevo, potem je $c(T) = 1$.*

Dokaz. Opisati moramo zmagovalno strategijo za enega policaja. Začetni položaj policaja je poljubno izbrano vozlišče drevesa T. Policajeva strategija je, da se na vsaki potezi premakne proti roparju (po najkrajši poti med njunima trenutnima položajema). Ker je T drevo, je ta najkrajša pot enolična (glej trditev 3.3). S tem policaj zagotovi, da se razdalja med policajem in roparjem nikoli ne poveča. Velja še več, razdalja ostane enaka le, če se ropar premakne "stran" od policaja. Ker je drevo končno, je to mogoče v kvečjemu $\mathrm{diam}(T)$ zaporednih potezah. Iz tega sledi, da se vsaj na vsakih $\mathrm{diam}(T)$ potez razdalja med policajem in roparjem zmanjša za vsaj ena. Torej se bosta po končnem številu potez policaj in ropar nahajala na istem vozlišču, zato res velja $c(T) = 1$. □

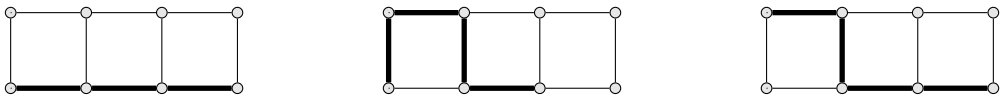
10.2 Izometrične poti

Induciran podgraf H grafa G je *k-varovan*, če se (po končnem številu začetnih potez) lahko k policajev premika zgolj po $V(H)$ tako, da če v neki potezi ropar stopi na vozlišče iz H, ga v naslednji potezi policaji ujamejo. Iz leme 10.1 sledi, da je vsak graf G $\gamma(G)$-varovan. Opazimo tudi, da je vsak polni podgraf grafa G 1-varovan in vsaka zaprta soseščina $N_G[v]$ v G 1-varovana.

Pot P v grafu G je *izometrična*, če za vsaki vozlišči $u, v \in V(P)$ velja

$$d_P(u, v) = d_G(u, v).$$

Naloga 79. Ali so označene poti na spodnji sliki izometrične? Utemelji.



Izrek 10.1. *Izometrična pot je 1-varovana.*

Dokaz. Naj bo P izometrična pot v grafu G in $V(P) = \{v_0, v_1, \ldots, v_k\}$. Naj bo

$$D_i = \{x \in V(G) \colon d_G(x, v_0) = i\}.$$

Opazimo, da je $v_i \in D_i$ za vsak $i \in \{0, 1, \ldots, k\}$.

Strategijo enega policaja, ki varuje pot P, opišemo tako, da definiramo *senco* $\sigma(r)$ trenutnega položaja roparja r:

$$\sigma(r) = \begin{cases} v_i, \text{ če } r \in D_i; \\ v_k, \text{ če } d_G(v_0, r) \geq k. \end{cases}$$

Če $r \in D_i$, potem se lahko ropar v naslednji potezi nahaja na vozlišču iz D_{i-1}, D_i ali D_{i+1}, torej se senca roparja iz v_i premakne v vozlišče v_{i-1}, v_i ali v_{i+1}. Če se torej ropar premakne iz r v r', velja $d_P(\sigma(r), \sigma(r')) \leq d_G(r, r')$.

Ker je P pot in je $c(P) = 1$, se bo policaj po končnem številu potez nahajal v $\sigma(r)$. Iz zgornjega sledi, da se od tega trenutka dalje policaj lahko ves čas nahaja v $\sigma(r)$. Od tod sledi, da če ropar stopi na vozlišče iz P, bo najkasneje v naslednjem koraku ujet. □

Varovanje izometričnih poti z enim policajem se je izkazalo kot ključno orodje pri naslednjem dokazu (ki ga bomo izpustili).

Izrek 10.2. *Če je G ravninski graf, potem je $c(G) \leq 3$.*

Naloga 80 (*)**.** Naj bo G zunanje-ravninski graf, ki nima prereznih vozlišč. Dokaži, da je $c(G) \leq 2$.

Določanje zgornje meje za policijsko število grafov je še danes aktivno področje raziskav. Še vedno je na primer odprta Meynielova domneva iz leta 1985, ki pravi, da za dovolj velike n obstaja konstanta $d > 0$, da je $c(G) \leq d\sqrt{n}$. Podobna vprašanja zanimajo raziskovalce tudi glede zgornje meje za grafe, ki jih lahko vložimo na ploskev roda g.

10.3 Retrakti

Homomorfizem f iz grafa G v graf H je preslikava $f \colon V(G) \to V(H)$, ki ohranja povezave, tj. če je $xy \in E(G)$, potem je $f(x)f(y) \in E(H)$. Na kratko pišemo kar $f \colon G \to H$.

Naloga 81. Poišči kakšen homomorfizem iz grafa C_6 v graf K_2.

Naloga 82. Naj bo G dvodelni graf. Dokaži, da obstaja homomorfizem $f\colon G \to K_2$.

Naloga 83. Naj bo $f\colon G \to H$ homomorfizem. Dokaži, da za vsaki vozlišči $x, y \in V(G)$ velja $d_G(x,y) \geq d_H(f(x), f(y))$.

Naj bo H induciran podgraf grafa G. Pravimo, da je H *retrakt* grafa G, če obstaja homomorfizem $f\colon G \to H$, za katerega velja $f(x) = x$ za vse $x \in V(H)$. Takšni preslikavi f pravimo *retrakcija*.

Naloga 84. Naj bodo vozlišča grafa C_6 zaporedoma označena z $v_1, \ldots, v_6$. Dokaži, da je $C_6[\{v_1, v_2\}]$ retrakt C_6.

Naloga 85. Naj bo P izometrična pot v G. Ali je P retrakt G? Dokaži ali ovrzi.

Naloga 86. Poišči primer grafa G in njegovega induciranega podgrafa H, ki ni retrakt. Primerjaj $c(G)$ in $c(H)$. Lahko najdeš tak primer, da bo $c(H) > c(G)$?

Izrek 10.3. *Če je H retrakt G, potem je $c(H) \leq c(G)$.*

Dokaz. Predpostavimo, da ima k policajev zmagovalno strategijo na grafu G. Poiskati moramo zmagovalno strategijo za k policajev na grafu H. Naj bo $f\colon G \to H$ retrakcija.

Strategija policajev na grafu H je, da si predstavljajo, da hkrati poteka igra na G (ker je H induciran podgraf G, lahko položaj in premik roparja v H enolično razumemo kot enak položaj in premik v G). Policaji igrajo optimalno na G (kjer imajo zmagovalno strategijo), svoje položaje in premike na grafu H pa določajo s pomočjo retrakcije f. Natančneje, če je premik iz vozlišča u v v optimalna poteza nekega policaja na grafu G, potem je optimalna poteza istega policaja na grafu H premik iz $f(u)$ v $f(v)$. Tovrstni strategiji rečemo *strategija sence* in $f(c)$, kjer je c položaj nekega policaja, imenujemo *senca* policaja c.

Trdimo, da je strategija sence zmagovalna strategija za k policajev na grafu H. Ker ima k policajev zmagovalno strategijo na G, se za nek položaj roparja r zgodi, da je vsako vozlišče iz $N_G[r]$ sosednje nekemu policaju (torej bo ropar v naslednji potezi gotovo ujet). Naj bodo $c_1, \ldots, c_k$ položaji policajev v G v tem trenutku. V G torej velja, da za vsako vozlišče $v \in N_G[r]$ obstaja policaj c_i, da je $vc_i \in E(G)$. Ker je f retrakcija, od tod sledi, da je $f(v)f(c_i) \in E(H)$. Ropar igra igro na H, zato se lahko premika le med vozlišče $v \in V(H)$, za katere velja $f(v) = v$. Torej v istem trenutku tudi za vsako vozlišče v $N_H[r]$ velja, da je sosednje senci nekega policaja. Zato policaji na H v naslednji potezi ujamejo roparja. □

Naloga 87 (*)**.** Naj bo H retrakt G. Dokaži, da velja $c(G) \leq \max\{c(H), c(G-H)+1\}$.

10.4 Spodnja meja

Izrek 10.4. *Če je G graf z ožino vsaj 5, potem je $c(G) \geq \delta(G)$.*

Dokaz. Naj bo $d = \delta(G)$ in denimo, da igro na G igra $d-1$ policajev. Dokazati želimo, da ropar zmaga.

Naj bo C množica vozlišč, ki jih za začetna vozlišča izberejo policaji. Najprej moramo dokazati, da ropar ni ujet v prvi potezi, torej da obstaja vozlišče grafa G, ki nima nobenega soseda v C. Denimo, da to ni res. Torej je C dominacijska množica.

Naj bo $u \in V(G) - C$. Označimo $X = N(u) \cap C$, $Y = N(x) - X$, $|X| = x$ in $|Y| = y$. Očitno je $x + y \geq d$. Ker je C dominacijska množica, ima vsako vozlišče iz Y nekega soseda v C. Ker ima G ožino vsaj 5, nobeno vozlišče iz Y nima soseda v X in noben par vozlišč iz Y nima skupnega soseda v C. Torej ima vsako vozlišče iz Y privatnega soseda v $C - X$. Sledi, da je $|Y| \leq |C - X| = |C| - |X|$, zato je $x + y = |C| \leq d - 1$, kar pa je protislovje. Iz tega sledi, da ropar lahko izbere začetno vozlišče tako, da ni takoj ujet.

Prestali del izreka dokažemo s pomočjo indukcije na število korakov igre t. Predpostavimo, da ropar v koraku $t \geq 0$ ni ujet in se nahaja na vozlišču r, ki ni sosednje nobenemu vozlišču iz C, ki označuje trenutno množico vozlišč, ki jih zasedajo policaji. Sedaj moramo dokazati, da lahko ropar enako zagotovi v naslednjem, tj. $t+1$-em koraku. Ker graf nima 4-ciklov, ima vsak policaj kvečjemu enega soseda v $N[r]$. Ker je $\deg(r) \geq d > |C|$, torej obstaja sosed r' vozlišča r, ki ni soseden nobenemu policaju. Roparjeva poteza je, da se premakne v vozlišče r'. Iz tega sledi, da tudi v koraku $t+1$ ne bo ujet (ker r' nima soseda v C). □

Naloga 88 (*)**.** Poišči graf z ožino 3, za katerega je $c(G) < \delta(G)$. Poišči graf z ožino 4, za katerega je $c(G) < \delta(G)$.

Naloga 89 (*)**.** Dokaži, da za graf G, ki ne vsebuje 4-ciklov, velja $c(G) \geq \frac{1}{2}\delta(G)$.

10.5 Dolžina igre

Dolžina igre policajev in roparja je število potez, ki jih policaji potrebujejo, da ujamejo roparja (0-te poteze, v kateri igralci izberejo začetne položaje, ne štejemo; premik policajev, ki mu lahko sledi premik roparja, štejemo kot eno potezo). Da je dolžina dobro definirana, moramo predpostaviti, da igro igra vsaj $c(G)$ policajev in da policaji in ropar igrajo optimalno (pri čemer policaji poskušajo roparja uloviti v čim manj potezah, ropar pa se trudi ujetju čim dlje izogibati).

Če igro igra $k \geq c(G)$ policajev, je *k-ulovitveni čas* grafa G označen z $\mathrm{capt}_k(G)$ in šteje število potez, ki jih policaji potrebujejo, da ujamejo roparja (pri vseh zgornjih predpostavkah). Če je $k = c(G)$, oznako poenostavimo v $\mathrm{capt}(G)$.

Na primer, če je $k \geq |V(G)|$, potem je $\mathrm{capt}_k(G) = 0$; če je $\gamma(G) \leq k < |V(G)|$, potem je $\mathrm{capt}_k(G) = 1$.

Naloga 90. Določi $\mathrm{capt}_k(P_9)$ za $k \in \{1, 2, 3, 4, 5\}$.

Naloga 91 (*)**.** Dokaži, da za drevo T velja $\mathrm{capt}(T) = \mathrm{rad}(T)$.

Naloga 92 (*)**.** Določi $\mathrm{capt}(C_n)$ za $n \geq 4$. (Nasvet: obravnavaj primere glede na ostanek n pri deljenju s 4.)

Literatura

[1] A. Bonato, An invitation to pursuit-evasion games and graph theory, Stud. Math. Libr., 97, American Mathematical Society, Providence, RI, 2022, xx+254 pp.

[2] A. Bonato, R.J. Nowakowski, The game of cops and robbers on graphs, Stud. Math. Libr., 61, American Mathematical Society, Providence, RI, 2011, xx+276 pp.

[3] A. Franc, Problem umetnostne galerije, Obzornik za matematiko in fiziko, letnik 61, številka 5, str. 161–172.

[4] D. Gajser, V. Iršič, S. Klavžar, T. Marc, A. Žitnik, Zapiski s predavanj in vaj na UL FMF pri predmetih Diskretna matematika 1, Diskretna matematika 2, Diskretne strukture 2 in Teorija grafov, ki so nastali ob mojem poslušanju predavanj in vaj ter kasneje ob vodenju vaj, 2015–2023.

[5] M. Konvalinka, P. Potočnik, Diskretna matematika I, vol. 1. Ljubljana: Fakulteta za matematiko in fiziko, 2019, p. 135.

[6] D.B. West, Introduction to graph theory, Prentice Hall, Inc., Upper Saddle River, NJ, 1996. xvi+512 pp.

[7] R.J. Wilson, J.J. Watkins, Uvod v teorijo grafov, vol. 63. Ljubljana: Društvo matematikov, fizikov in astronomov Slovenije, 1997, p. 397.

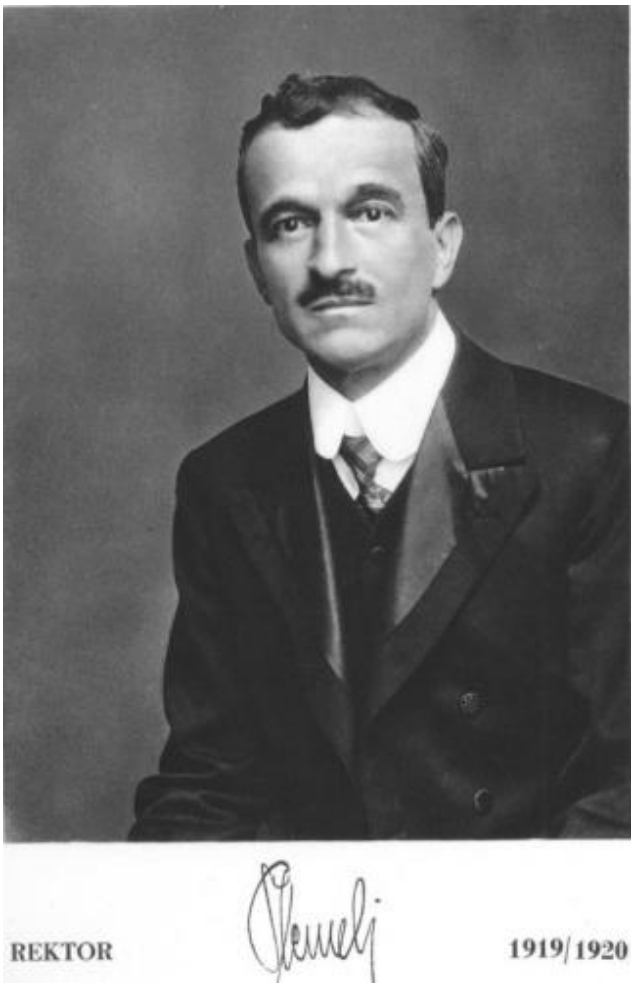
PREDAVANJA

Josip Plemelj – življenjska zgodba izjemne osebnosti

dr. Boštjan Kuzman

Pedagoška fakulteta, Univerza v Ljubljani, Slovenija

V letošnjem letu se spominjamo 150-letnice rojstva Josipa Plemlja (1873-1967), največjega slovenskega klasičnega matematika in prvega rektorja UL. Plemelj je od mladih let kazal izjemen talent za matematiko, na njegovo znanstveno pot, vrhunske mednarodne uspehe in nadaljnjo poklicno kariero pa so usodno vplivale številne osebne in zgodovinske okoliščine. Predstavil sem njegovo pestro in navdihujočo, a žal tudi nekoliko grenko življenjsko zgodbo.



Slika 1: Josip Plemelj

Kaj počnemo aktuarji?

Nejc Černe

Služba za aktuarski razvoj premoženjskih zavarovanj
Zavarovalnica Triglav, d.d.

Povzetek

Kaj se skriva za poklicem, ki se pogosto znajde na seznamu najboljših poklicev? Aktuarji v zavarovalnicah z uporabo matematike vrednotijo finančne učinke tveganj in negotovosti. Zavarovanci pogosto ne razumejo, kaj so prejeli v zameno za plačano premijo v primeru, da niso imeli škodnih dogodkov, ter kako je višina premije, ki so jo morali plačati, določena. V nadaljevanju bomo s pomočjo enostavnih primerov razložili matematične ideje, ki so osnova za delovanje zavarovalniškega sistema.

1 Verjetnost, statistika in zavarovalništvo

Škodni dogodki, za katere se zavarujemo pri zavarovalnici, se lahko zgodijo ali pa tudi ne. Pri obravnavanju takih dogodkov nam bodo pomagali osnovni pojmi verjetnosti in statistike.

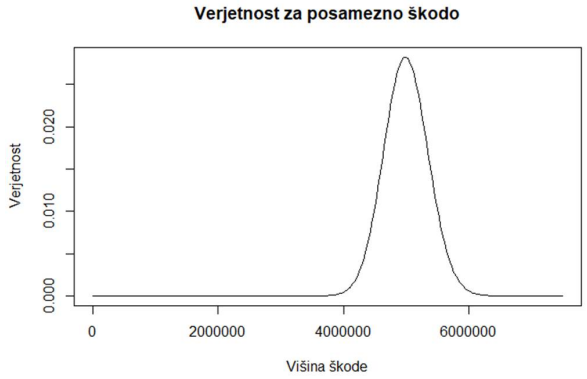
Predpostavimo, da imamo več enakovrednih izidov, ki bi se pri ponavljanju pojavili približno enako pogosto. Verjetnost je razmerje med številom ugodnih izidov in številom vseh možnih izidov. Denimo, da nas zanima verjetnost, da so nam v letu 2022 ukradli osebni avtomobil. Verjetnost lahko ocenimo z razmerjem števila ukradenih vozil (240) in števila vseh registriranih vozil v tem letu (1.200.000). Dobljena ocena je $\hat{p} = 0{,}0002$. Formalno poskusu z dvema možnima izidoma pravimo Bernoullijev poskus. Pravimo, da ima slučajna spremenljivka Bernoullijevo porazdelitev s parametrom p, če velja, da je verjetnost "uspeha" p in verjetnost "neuspeha" $1 - p$.

Posamezniku lahko vozilo v enem letu ukradejo z verjetnostjo p, ki je precej majhna. Če predpostavimo, da je vozilo vredno 25.000 EUR, potem je dejanski rezultat tega slučajnega dogodka lahko to, da smo obdržali vse svoje imetje, ali pa da smo izgubili 25.000 EUR. Zavarovanje je zaščita pred tako finančno izgubo. Zavarovalnica v zameno za plačilo stranki povrne določene izgube v primeru škode (prevzame riziko). Stranka torej plača premijo zavarovanja in zato v primeru, da nima škodnega dogodka, obdrži nekoliko manj imetja, ampak v primeru škodnega dogodka ni izpostavljena nič višji izgubi.

Zavarovalnica na škodne dogodke ne gleda z vidika posameznika, ampak z vidika vseh njenih zavarovancev naenkrat. Zanimajo jo verjetnosti za skupno število vozil, ki bodo ukradena pri njenih zavarovancih. Pri tem se običajno predpostavi, da so taki dogodki med sabo neodvisni. Verjetnost, da se hkrati zgodi več neodvisnih dogodkov, je produkt njihovih verjetnosti. Če izvedemo n neodvisnih Bernoullijevih poskusov z verjetnostjo p, potem je število uspehov porazdeljeno po Binomski porazdelitvi. Verjetnost za k "uspehov" je enaka $P(X = k) = \binom{n}{k} p^k (1-p)^{(n-k)}$.

Denimo, da ima zavarovalnica zavarovanih 1 milijon vozil. Vsako vozilo je lahko v naslednjem letu ukradeno z verjetnostjo 0,0002. Predpostavimo, da so dogodki med sabo neodvisni. Verjetnosti, da bo ukradenih manj kot 100 vozil ali več kot 300 vozil sta zelo majhni. Izidi tako postanejo bolj predvidljivi. Verjetnost, da bodo ukradena vsa vozila, zaradi predpostavk ni nič, ampak vemo, da je tak dogodek praktično nemogoč.

Pričakovana vrednost je uteženo povprečje možnih izidov spremenljivke, kjer so uteži njihove verjetnosti. Pričakovana vrednost škode v primeru kraje osebnega avtomobila vrednega 25.000 EUR z verjetnostjo 0,0002 je 5 EUR. Pričakovana vrednosti škode, če imamo 1 milijon vozil vrednih 25.000 EUR in je lahko vsako vozilo v naslednjem letu neodvisno ukradeno z verjetnostjo 0,0002, je 5 milijonov EUR oziroma 5 EUR na vozilo. Pričakovana vrednost na vozilo je torej ostala enaka, a dobili smo "lepšo" porazdelitev možnih škod.



To je formalizirano v zakonu velikih števil, ki nam pove, da je povprečna vrednost rezultatov, pridobljenih iz velikega števila neodvisnih in enako porazdeljenih poskusov, blizu njihove pričakovane vrednosti. Za 1 milijon vozil je verjetnost, da bo povprečna škoda blizu 5 EUR, višja. Če vsaka oseba prispeva 6,3 EUR, je verjetnost, da ne pokrijemo vseh škod, manjša od 0,0002 (verjetnostni kraje za posameznika). Z višanjem prispevka lahko verjetnost, da ne moremo pokriti vseh izgub, še zmanjšamo.

Če osebi vozilo ukradejo, ima veliko izgubo, zato je običajno za odstranitev takega tveganja pripravljena plačati več od pričakovane vrednosti (ang. risk aversion). Zavarovalnica za pokrivanje škod potrebuje več od pričakovane vrednosti, poleg tega pa ima dodatne stroške (obratovalni stroški, provizije, obravnava škod, …) in maržo za dobiček. Verjetnost, da bi vsota škod presegla premijo je majhna, a ni nič. Zavarovalnica se lahko za ta primer pozavaruje, sicer mora potencialne izgube kriti iz kapitala.

V praksi se lahko zgodi, da so osebe z zavarovanimi vozili manj pazljive (ang. moral hazard) ter da se bolj izpostavljene osebe prej odločijo za zavarovanje (ang. adverse selection). Nekatere osebe se poskušajo z zavarovalniškimi prevarami okoristiti, zaradi preprečevanja takih prevar pa ima zavarovalnica višje stroške.

2 Modeliranje

Denimo, da želi zavarovalnica svoj portfelj segmentirati in segmentom zaračunati različne premije, saj domneva, da se verjetnosti kraje razlikujejo glede na kraj, kjer se vozilo nahaja, ter glede na to, če ima vozilo alarm. Podatki, ki jih je uspela zavarovalnica zbrati, se nahajajo v naslednjih tabelah:

Kraj registracije	Reg. v LJ	Izven LJ
Število vozil	170.000	1.050.000
Število kraj	37	199
Delež	0,00021765	0,00018952

Alarm	Ni alarma	Alarm
Število vozil	850.000	370.000
Število kraj	164	72
Delež	0,00019294	0,00019459

Na podlagi podatkov se zavarovalnica odloči, da bo zaračunala različne premije glede na to, če je kraj registracije Ljubljana, alarmov pa ne bodo upoštevali. Premiji brez stroškov za vozilo vredno 25.000 EUR sta v Ljubljani 5,44 EUR in izven Ljubljane 4,74 EUR. Druga zavarovalnica je prejela bolj podrobne podatke:

Število vozil	Ni alarma	Alarm	Skupaj
Reg. v LJ	40.000	130.000	170.000
Izven LJ	810.000	240.000	1.050.000
Skupaj	850.000	370.000	1.220.000

Število kraj	Ni alarma	Alarm	Skupaj
Reg. v LJ	9	28	37
Izven LJ	155	44	199
Skupaj	164	72	236

Druga zavarovalnica je opazila, da je ocena verjetnosti v primeru, da ima vozilo alarm, vedno nižja od ocene verjetnosti, ko vozilo alarma nima. Glede na dobljene ocene so se odločili, da bodo upoštevali oba faktorja ločeno. Verjetnost kraje so modelirali z logističnim modelom. To pomeni, da so predpostavili določeno odvisnost verjetnosti kraje od tega, če je vozilo registrirano v Ljubljani in če ima vozilo alarm. V tej odvistnosti se nahajajo parametri, ki določajo, kako se verjetnost kraje spremeni glede na kraj registracije in glede na to, če ima vozilo alarm. Parametre so ocenili z metodo največjega verjetja. Verjetje je verjetnost realiziranih podatkov gledano kot funkcija parametrov. Pod predpostavko modela določenega po metodi največjega verjetja so realizirani podatki najbolj verjetni.

Denimo, da imamo na trgu tri zavarovalnice. Prva cenikov ni delila po segmentih, druga jih je delila po kraju registracije, tretja pa je uporabila rezultate logističnega modela. Brez stroškov so premije za vozilo vredno 25.000 EUR:

Premija	Zavarovalnica 1		Zavarovalnica 2		Zavarovalnica 3	
	Ni alarma	Alarm	Ni alarma	Alarm	Ni alarma	Alarm
Reg. v LJ	4,84 EUR	4,84 EUR	5,44 EUR	5,44 EUR	5,62 EUR	5,39 EUR
Izven LJ	4,84 EUR	4,84 EUR	4,74 EUR	4,74 EUR	4,78 EUR	4,58 EUR

Zavarovanci bodo iskali zase najcenejšo zavarovalnico. Če je segmentacija portfelja upravičena, zavarovalnice z manj razdeljenim cenikom tvegajo, da bodo pri njih ostali predvsem zavarovanci, ki podplačujejo svoj riziko. V tem primeru bo zavarovalnica imela izgubo in naslednje leto primorana dvigniti premije, s čimer bo še težje privabila manj rizične zavarovance.

V zgornjem primeru gre za poenostavljen model, ki temelji na izmišljenih podatkih. V praksi za modeliranje podatkov zavarovalnice najpogosteje uporabljajo posplošene linearne modele z več sto parametri. V zadnjem času si pomagajo tudi z modeli strojnega učenja.

Postov problem

dr. David Gajser

Fakulteta za naravoslovje in matematiko UM in II. gimnazija Maribor

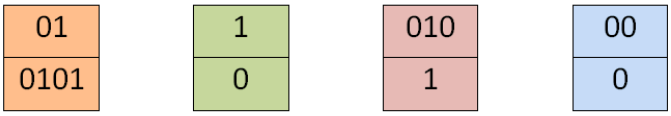
Na predavanju smo obravnavali zanimiv problem v teoretičnem računalništvu: Postov problem. Lahko ga predstavimo kot nalogo, ki izgleda kot nalašč za rešitev z računalniškim programom, a je računalnik v splošnem ne more rešiti, tudi če bi imel na voljo poljubno časa. To je izrek, torej obstaja zanj tudi dokaz. Kaj pa sploh pomeni, da nečesa "računalnik ne more rešiti"? Kaj je za matematika "računalnik"?

1 Predstavitev problema

Opišimo Postov problem z vhodom, ki nam opiše konkretno nalogo in z želenim izhodom, tj. kaj želimo pri nalogi izračunati:

- *Vhod:* Končen nabor domin, ki imajo na zgornjem delu niz, sestavljen iz ničel in enic, na spodnjem delu pa prav tako.
- *Želeni izhod:* Da ali ne. Izhod "da" želimo natanko v primeru, ko lahko domine iz vhoda postavimo v vrsto tako, da če po vrsti preberemo nize na zgornjih delih, dobimo isto, kot če po vrsti preberemo nize na spodnjih delih. Pri tem lahko vsako domino uporabimo poljubno mnogo krat.

Naslednje primere smo našli v [1].



Slika 1: Primer vhoda za Postov problem

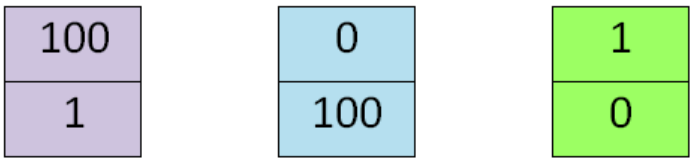
Odgovor za vhod na sliki 1 je Da, dokaz za to pa je na sliki 2.

00	1	010	1	010	01	00	1	010	1	01	01	01
0	0	1	0	1	0101	0	0	1	0	0101	0101	0101

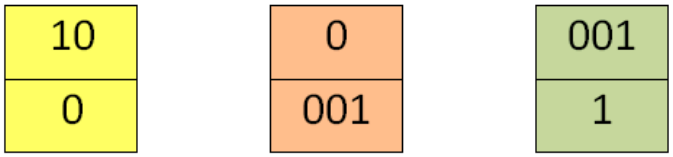
Slika 2: Rešitev primera s slike 1

Tudi odgovor za vhod na sliki 3 je Da, vendar za podobno utemeljitev kot zgoraj potrebujemo zaporedje 75 domin, pri čemer obstajata dve takšni zaporedji te dolžine [3]. Preprosto je tudi videti, da če bi pri vhodu s slike 3 pri prvi domini od spodaj nameso 1 napisali 0, bi bil odgovor Ne. Z nobeno izmed domin namreč ne bi mogli začeti želenega zaporedja.

Odgovor za vhod na sliki 4 pa še ni znan [3]. Torej je še zmeraj odprto, ali je pravilni odgovor Da ali Ne. Čeprav bi nam pri tem konkretnem vhodu morda lahko pomagal računalnik, pa nam za poljubni vhod



Slika 3: Primer vhoda za Postov problem



Slika 4: Primer vhoda za Postov problem

Postovega problema ne bi mogel zagotoviti rešitve. Velja namreč izrek, da *ne obstaja računalniški program, ki bi Postov problem rešil.* Ne le, da takega programa še nismo našli, ni ga mogoče najti. Kako bi to sploh lahko dokazali?

Najprej seveda moramo podati model za *računalniški program*, kar bo Turingov stroj. Turingov stroj je standardni model računanja v teoretičnem računalništvu in dokazano je, da z njim lahko simuliramo osebni računalnik. Kaj je Turingov stroj tukaj ne bomo rigorozno definirali, koncept bomo predstavili malenkost bolj poljudno in ob primeru Turingovega stroja s slike 5, ki smo ga naprogramirali na letošnjem taboru MaRS. Vsak Turingov stroj je natančno določen s

- končnim naborom stanj, med katerimi so tudi začetno, sprejemno in zavrnitveno stanje. V našem primeru je 7 stanj (rumeni krogci), začetno stanje je *zacetek*, sprejemno je *sprejmi*, zavrnitveno pa ni prikazano na sliki;
- končnim številom znakov, ki jih stroj lahko uporabi, med katerimi je tudi prazen znak. V našem primeru so znaki 0, 1 in prazen znak □ (na puščicah);
- predpisom, ki pove, kako naj stroj deluje v katerem stanju. V našem primeru je ta predpis predstavljen s puščicami in oznakami nad njimi.

Vsak Turingov stroj ima poleg opisanega še neskončen trak, sestavljen iz celic, ki jih lahko označimo s celimi števili. V vsaki celici je zmeraj zapisan natanko en znak. Pred začetkom računanja na zaporedne celice, začenši s celico 0, zapišemo željeni vhod, ostale celice pa zapolnimo s praznimi znaki. Vsak Turingov stroj ima tudi glavo, ki je na začetku računanja nad celico 0, nato pa se v vsakem koraku pomakne za 1 v levo ali desno, odvisno od predpisa Turingovega stroja. Turingov stroj začne računanje v začetnem stanju, nato pa sledi predpisu, ki vsakemu paru

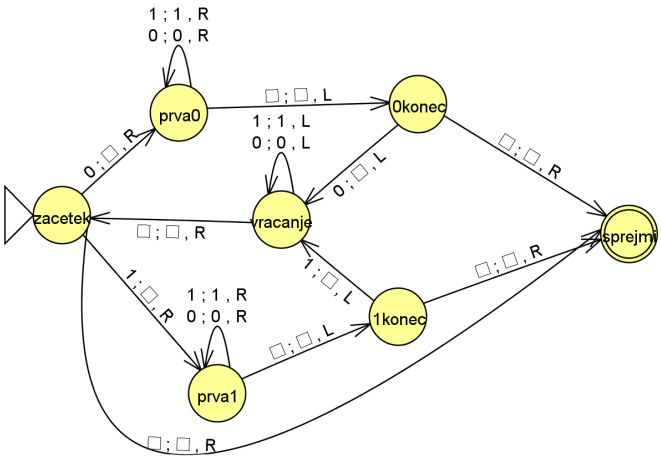
(trenutno stanje, znak pod glavo)

priredi trojico

(novo stanje, nov simbol pod glavo, smer premika - levo ali desno).

Stroj se ustavi, ko pride v sprejemno ali zavrnitveno stanje.

Na našem primeru je predpis stroja predstavljen s puščicami. Puščica iz stanja *zacetek* v stanje *prva0* nam pove, da če je stroj v začetnem stanju in pod glavo vidi 0, simbol 0 prepiše s praznim simbolom □, se pomakne desno (R) in preide v stanje *prva0*. Podobno velja za vse ostale puščice. Vidimo, da iz stanja *zacetek* gredo tri puščice, za vsak možen simbol pod glavo ena. Enako velja za stanja *prva0*, *prva1* in *vracanje*.



Slika 5: Primer Turingovega stroja

Pri vsakem od teh treh stanj sta puščici iz stanja vase združeni v eno, ki pove, da se v tem stanju simbola 0 in 1 pod glavo ohranita. Stanje *sprejmi* je končno stanje in ko se stroj premakne v to stanje, se ustavi. Posledično iz njega ne kaže nobena puščica. Omenili smo, da zavrnitveno stanje na sliki 5 ni vidno. Naš stroj lahko pride v zavrnitveno stanje le iz stanj *0konec* in *1konec*, iz katerih gresta le 2 puščici. Pri stanju *0konec* namreč ni določeno, kaj naj stroj naredi, če je v tem stanju pod glavo simbol 1. Ker to ni določeno, se v primeru, da stroj v tem stanju pod glavo vidi 1, ustavi in pravimo, da gre v zavrnitveno stanje. Podobno pri stanju *1konec* ni določeno, kaj naj stroj naredi, če je v tem stanju pod glavo simbol 0. Bralca vabimo, da ugotovi, natanko katere vhode sprejme Turingov stroj na sliki 5.

Turingov stroj je standardni model računanja v teoretičnem računalništvu, ni pa edini. Pomemben model je tudi RAM (random access machine), ki je matematični model naših osebnih računalnikov. Dobro znan je izrek, da lahko s Turingovim strojem simuliramo RAM. Še več, splošno sprejeta je tudi Church-Turingova teza, ki pravi, da je množica funkcij, ki jih lahko računamo s Turingovim strojem, enaka množici *intuitivno izračunljivih funkcij* (več o tem v [2], poglavje 3.3). Torej, če si uspemo zamisliti nek (pravilen) postopek, ki bi rešil Postov problem, bomo le-tega lahko rešili tudi s pomočjo Turingovega stroja. Iz tega sledi, da je za našo trditev, da *ne obstaja računalniški program, ki bi Postov problem rešil*, dovolj dokazati, da Postovega problema ne more rešiti noben Turingov stroj. Na letošnjem MaRSu smo si pogledali idejo dokaza te trditve. Dokaz lahko bralec najde v [2], poglavje 5.2.

Literatura

[1] Rok Gregorič, Vesna Iršič, Anja Petković in David Gajser. Postov problem in Turingov stroj. *Presek*, 41(6), 2014.

[2] Michael Sipser. *Introduction to the Theory of Computation, Second Edition.* Course Tehnology, 2006.

[3] Ling Zhao. PCP: a Nice Problem, 2003. `http://webdocs.cs.ualberta.ca/~games/PCP/` [Dostopno 24. 8. 2023].

Probabilistični algoritmi

dr. Blaž Škrlj

Outbrain d. o. o.

Probabilistični algoritmi omogočajo učinkovito štetje in primerjanje raznovrstnih struktur. Pri delu s podatkovnimi tokovi smo pogosto omejeni z delovnim spominom, dovolj so nam približne ocene npr. števila elementov v množici. V predavanju smo opisali nekaj znanih pristopov za probabilistično ocenjevanje kardinalnosti množic ter preverjanje prisotnosti elementov. Prav tako smo si pogledali par praktičnih primerov uporabe tovrstnih algoritmov pri delu z velepodatki.

Računske tehnike za deljivost binomskih koeficientov

dr. Katja Berčič in dr. Russ Woodroofe

Fakulteta za matematiko in fiziko, Univerza v Ljubljani
Fakulteta za matematiko, naravoslovje in informacijske tehnologije, Univerza na Primorskem

1 Binomi

Za celi števili $0 \leq k \leq n$ lahko definiramo *binomski koeficient* $\binom{n}{k}$ s predpisom

$$\binom{n}{k} := \frac{n!}{k!(n-k)!}.$$

Binomski koeficienti so zanimivi, saj štejejo koristne stvari. Binomski koeficient $\binom{n}{k}$ predstavlja število možnih izbir podmnožice s k elementi iz množice z n elementi. Tu predpostavljamo, da lahko predmete razločimo, ter da nas ne zanima vrstni red elementov.

Binomski koeficienti se pojavijo, kot že ime pove, kot koeficienti v razčlenjeni obliki potence binoma $(1+x)^n$. Če to razvijemo na običajen način, in za trenutek pozabimo, da je $1 \cdot x = x \cdot 1$, dobimo 2^n členov oblike $\_\ \_\ \_ \cdots \_$, kjer je vsak $\_$ bodisi 1 ali x. Na primer,

$$\begin{aligned}(1+x)^3 = {} & 1\cdot 1\cdot 1 + 1\cdot 1\cdot x + 1\cdot x\cdot 1 + x\cdot 1\cdot 1 + \\ & 1\cdot x\cdot x + x\cdot 1\cdot x + x\cdot x\cdot 1 + x\cdot x\cdot x.\end{aligned}$$

Koeficient člena x^k v izrazu $(1+x)^n$ predstavlja število načinov, da izberemo k podčrtajev, na katere bomo postavili x.

Iz definicije sledi, da velja $\binom{n}{k} = \binom{n}{n-k}$, da $\binom{n}{0} = \binom{n}{n} = 1$, ter da za $1 \leq k \leq n-1$ velja $\binom{n}{k} > 1$.

2 Vprašanje deljivosti

Naslednje vprašanje se je pojavilo pri delu drugega avtorja z Johnom Shareshianom.

Vprašanje 1. *Ali je za dano celo število n vedno mogoče najti praštevili p in r, tako da je vsak nenetrivialni binomski koeficient $\binom{n}{k}$ deljiv bodisi s p, bodisi z r?*

Z netrivialno tu mislimo »različno od 1«. Zavržemo torej $\binom{n}{0}$ in $\binom{n}{k}$ ter zahtevamo, da so preostali binomski koeficienti $\binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{n-1}$ deljivi s p ali z r. Zaradi simetrije je seveda dovolj, če obravnavamo le binomske koeficiente $\binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{\lfloor n/2 \rfloor}$.

Motivacija za to vprašanje izhaja iz teorije grup (matematične teorije simetrij). Tu je $\binom{n}{k}$ razmerje med skupnim številom načinov za preurejanje množice $1, \ldots, n$ ter številom načinov za preurejanje, pri katerih ohranimo $1, \ldots, k$ (v nekem vrstnem redu) na prvih k mestih.

Primer 2. Za $n = 15$ ni težko izračunati nenetrivialnih binomskih koeficientov: to so 15, 105, 455, 1365, 3003, 5005, 6435. Lahko opazimo, da sta praštevili $p = 3$ in $r = 5$ primerni, da na vprašanje odgovorimo z »da«. Morda ni tako očitno, vendar pa deluje tudi $r = 13$, če je p bodisi 3 bodisi 5.

Naredimo prvo opazko:

Lema 3. Če praštevili p in r vodita do odgovora »da«, potem vsaj eno deli $n = \binom{n}{1}$.

Nadaljevali bomo s predpostavko, da praštevilo p deli n.

Primer 4. Za $n = 1$ milijon $= 10^6$ preverimo, da je $r = 999.983$ tudi praštevilo. To je koristno, saj je $n!$ deljivo z r, vendar je $k!$ deljivo z r le, sče je $k \geq r$, $(n-k)!$ pa je deljivo z r le še, da je $k \leq (n-r)$. Sledi, da so vsi binomski koeficienti deljivi z r, razen $\binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{17}$ in simetričnih binomskih koeficientov na koncu seznama.

Ker je $n = 10^6 = 2^6 \cdot 5^6$, moramo zdaj preveriti le še, da števili 2 ali 5 delita teh 17 koeficientov. Delita jih obe števili, zato je odgovor na vprašanje »da« za $n = 10^6$.

Ideje iz Primera 4 se da močno posplošiti. Naslednji izrek je dokazan na enak način kot v primeru.

Lema 5 (Velika praštevila veliko pomagajo, angl. *large primes help a lot*)**.** Če je praštevilo r manjše od n, potem velja

$$r \mid \binom{n}{k} \text{ razen če } k \leq (n-r) \text{ ali } k \geq r.$$

Poleg tega potrebujemo še pogoj, ki nam bo pomagal pri obravnavi primera $k \leq (n-r)$. Kot smo opazili, bomo za to potrebovali praštevilski delitelj števila n. Naslednja lema (katere dokaz ni težak, a presega obseg tega kratkega članka) bo prišla prav.

Lema 6 (Kummer, 1852)**.** Če je a pozitivno celo število in p praštevilo, tako da velja $p^a \mid n$, potem velja

$$p \mid \binom{n}{k} \text{ razen, kadar } p^a \mid k.$$

Zaključek 7. Če sta p in r praštevili, tako da velja $p^a \mid n$ in $r < n$, hkrati pa velja $p^a + r > n$, potem p in r vodita do odgovora »da« na vprašanje.

3 Kaj je znano

Odgovora na splošno ne poznamo. Čeprav nas Sklep 7 pogosto usmerja k odgovoru »da«, včasih ne deluje.

Primer 8 (Poučna zgodba)**.** Za $n = 210 = 2 \cdot 3 \cdot 5 \cdot 7$ lahko preverimo, da je naslednje manjše praštevilo 199. Na žalost velja $199 + 7 < 210$. Vendar pa velja $206 = 103 \cdot 2$, in podoben argument kot v Primeru 4 pokaže, da so edini binomski koeficienti, ki niso deljivi z 103, tisti pri $k = 1, 2, 3, 4, 103, 104, 105$, in simetrični binomski koeficienti, ki so večji od $105 = 210/2$. Po Kummerjevi lemi so vsi ti, razen $\binom{210}{105}$, deljivi s 5 (brez računanja). S preštevanjem števila petic v števcu in imenovalcu lahko preverimo, da je tudi $\binom{210}{105}$ deljivo s 5.

Tako $p = 5$ in 103 vodita do odgovora »da« na vprašanje, a za to je potrebno nekaj dela!

Problem 1 (Ne preveč preprosto)**.** Najdi praštevili p in r, ki vodita do odgovora »da« na vprašanje za $n = 31.416$.

To, kar vemo o vprašanju, je naslednje:

Izrek 9 (Guralnick, Shareshian, in Woodroofe [2])**.** *Odgovor na vprašanje je »da« za vsa $n \leq 10^{15}$.*

Izrek 10 (Shareshian in Woodroofe [3], Teräväinen [4])**.** *Odgovor na vprašanje je »da« za skoraj vsa števila n. (Tu ima »skoraj vsa« poseben tehnični pomen.)*

4 Računske tehnike

Če se soočite z vprašanjem, na katerega ne poznate odgovora, je smiselno preveriti majhne vrednosti s pomočjo računalnika. Če vas zanimajo večje vrednosti, potem lahko bodisi program poganjate dlje časa, kupite hitrejši računalnik, ali pa izboljšate algoritem. Izboljšave algoritma imajo običajno največji učinek.

Izboljšave algoritma, ki so sčasoma privedle do Izreka 9, so primer tega.

1. Naiven, grob pristop, zapisan v programskem jeziku GAP, interpretiranem računalniškem algebrskem sistemu, nas je pripeljal do približno 10^4.

2. Sklep 7 nam omogoča hitro preveriti okoli 99.9% vrednosti. Potrebujemo seznam praštevil in največjih praštevilskih potenc. Z naivno faktorizacijo s tem trikom smo z GAP-om računali do 10^9.

3. Potrebujemo hitro metodo za pridobivanje vseh praštevil v velikem intervalu celih števil. Lahko uporabimo Eratostenovo sito, ki ste ga morda že videli. To je zelo hitro, vendar kljub nekaterim izboljšavam zahteva $O(\sqrt{n})$ pomnilnika. Z GAP-om smo računali do približno 10^{12} v nekaj dneh.

4. Ko zmanjka drugih idej, je smiselno optimizirati: prešli smo na jezik C za 20-kratno pospešitev. Izognemo se upoštevanju večjih praštevilskih faktorjev, pozorni smo na zmogljivost medpomnilnika, uporabljamo krožna faktorizacijo (angl. *wheel factorization*) in vrsto drugih manjših trikov za dodaten 50% pospešek. Na večjedrnem računalniku smo pognali 15 vzporednih kopij in tako v desetih dneh dosegli 10^{15}, kot v Izreku 9.

Triki, uporabljeni v (4), so nekoliko pomagali, vendar pa je največji napredek prišel pri (3). Več o Eratostenovem situ si lahko preberete v [1] in mnogih drugih virih.

Rada bi se zahvalila Bobu Guralnicku in Johnu Shareshianu za mnoge zanimive diskusije in večletno sodelovanje pri raziskovanju deljivosti binomskih koeficientov.

Literatura

[1] Richard Crandall and Carl Pomerance, *Prime numbers: a computational perspective*, second ed., Springer, New York, 2005.

[2] Robert M. Guralnick, John Shareshian, and Russ Woodroofe, *On invariable generation of alternating groups by elements of prime and prime power order*, Math. Comp. **92** (2023), no. 341, 1349–1361.

[3] John Shareshian and Russ Woodroofe, *Divisibility of binomial coefficients and generation of alternating groups*, Pacific J. Math. **292** (2018), no. 1, 223–238, arXiv:1505.05143.

[4] Joni Teräväinen, *Almost all alternating groups are invariably generated by two elements of prime order*, (2023), 16 pages, arXiv:2203.05427, accepted to Int. Math. Res. Not.

ČLANKI UDELEŽENCEV

Perkolacija

Nives Gošnjak, Luka Peruš, Hugo Trebše
Mentor: *David Opalič*

Povzetek

Definiramo perkolacijo na mreži $\mathbb{Z}^d$. Posebno pozornost posvetimo kritičnemu parametru p_c in pokažemo, da za $d > 1$ ni trivialen. S pomočjo dualnega grafa in unikatnosti neskončnega omrežja izračunamo $p_c = \frac{1}{2}$ za $d = 2$.

1 Uvod

Intuitivno si lahko perkolacijo predstavljamo kot probabilistični model prepustnega medija. Slednji je pogosto predstavljen z neskončnim grafom $\mathbb{Z}^d$, kjer vsako povezavo med sosednjima točkama neodvisno dodamo s fiksno verjetnostjo p. Zanimajo nas makroskopske lastnosti in geometrijska oblika množice dodanih povezav. Konkretno se v teoriji perkolacij pojavljajo vprašanja, kot so povezanost izhodišča z ostalimi točkami, obstoj neskončnih omrežij in vrednost kritične verjetnosti dodajanja povezav, pri kateri se začnejo pojavljati neskončna omrežja.

Model perkolacije je uporaben tudi zunaj matematične teorije, posebej kot model molekularnih vezi, mikroskopskih pojavov v magnetih ter širjenja bolezni v epidemiologiji. Med drugim lahko uporabimo različne ugotovitve teorije perkolacije kot mero krhkosti omrežij, izpostavljenih naključnim dejavnikom, natančneje kot merilo povezanosti med deli omrežja.

V matematiki je perkolacija relativno nov pojem, prvi članek na to temo je bil objavljen leta 1957. Področje je zanimivo, saj je enostavno razumeti model in postaviti vprašanja o njem, vendar je potrebno ogromno uvida in genialnih prebliskov, da pridemo do rešitve. Mnoge osnovne dinamike sistema se še vedno izmikajo matematični formalizaciji.

Naš model perkolacije, bolj podrobno znan kot Bernullijeva perkolacij povezav, je eden najpreprostejših primerov naključnosti na grafih, običajno mrežah $\mathbb{Z}^d$. Obstajajo številni drugi modeli z drugačno fizikalno interpretacijo, posebej velja omeniti Isingov model in Sherrington-Kirkpatrick model. Gre za zelo aktivno in popularno vejo matematike, kar demonstrira Fieldsova medalja, ki jo je leta 2022 prejel Hugo Duminil-Copin za uspešne preboje v prej omenjenih modelih. Za hiter uvod v perkolacijo, spisan na zelo visokem nivoju, priporočamo njegove zapiske [3]. Za bolj podroben in bralcu prijazen uvod priporočamo [1], iz koder so tudi vzete vse slike, ki jih uporabimo v nadaljevanju.

V članku bomo najprej uvedli nekaj verjetnostnih pojmov. Nato bomo formalno definirali perkolacijo in spoznali našega glavnega igralca – kritično vrednost verjetnosti, pri kateri se začnejo pojavljati neskončne mreže. S krajšim argumentom bomo izračunali vrednost kritične točke v enodimenzionalni različici problema ter omejili vrednost kritične točke v višjih dimezijah. Zatem brez dokaza navedemo ter diskutiramo tri dokazana dejstva, ki omogočijo vrhunec članka – izpeljavo vrednosti kritične točke v dvodimenzionalni različici problema.

2 Verjetnostno ozadje

V tem poglavju bomo definirali nekaj standardnih pojmov iz verjetnosti. Za osvežitev znanja o verjetnosti ter naključnih procesih priporočamo [1]. Naj bo $(\Omega, \mathcal{F}, \mathbb{P})$ verjetnostni prostor.

Definicija 2.1. ***(Realna) slučajna spremenljivka*** *X je funkcija $X : \Omega \to \mathbb{R}$.*

Spomnimo se, da sta dogodka A in B *neodvisna* natanko tedaj, ko velja $\mathbb{P}(A \cap B) = \mathbb{P}(A) \cdot \mathbb{P}(B)$. Neodvisnost slučajnih spremenljivk definiramo na sledeči način

Definicija 2.2. *Realni slučajni spremenljivki $X, Y : \Omega \to \mathbb{R}$ sta **neodvisni** natanko tedaj, ko velja*

$$\mathbb{P}(X = x, Y = y) = \mathbb{P}(X = x) \cdot \mathbb{P}(Y = y)$$

za vse $(x, y) \in \mathbb{R}^2$.

Neodvisnost več slučajnih spremenljivk se posploši induktivno.

Za realno slučajno spremenljivko s števno zalogo vrednosti $X : \Omega \to \mathbb{U}$ definiramo njeno *pričakovano vrednost* $\mathbb{E}[X]$ kot

$$\mathbb{E}[X] = \sum_{x \in \mathbb{U}} x \cdot \mathbb{P}(X = x).$$

Če je zaloga vrednosti X neštevna, se moramo namesto k vsotam zateči k integralom, v kar se ne bomo poglabljali. Ena izmed najpomembnejših lastnosti pričakovane vrednosti, ki jo naredi tako uporabno, je njena linearnost.

Propozicija 2.1. *Za realni slučajni spremenljivki $X, Y : \Omega \to \mathbb{R}$ velja*

$$\mathbb{E}[X + Y] = \mathbb{E}[X] + \mathbb{E}[Y].$$

Opomnimo, da zgornja trditev velja tudi za odvisni realni slučajni spremenljivki. Naslednje dejstvo je lahko dokazati. Naj bo $X : \Omega \to \mathbb{N}$. Sledi

$$\mathbb{E}[X] = \sum_{n \geq 0} n \cdot \mathbb{P}(X = n) = \sum_{n \geq 1} \mathbb{P}(X \geq n). \tag{1}$$

Spotoma omenimo še naslednjo lemo, ki je trivialna posledica enačbe (1) ter posebna oblika neenakosti Markova.

Lema 2.1. *Naj bo $X : \Omega \to \mathbb{N}$ naključna spremenljivka. Sledi:*

$$\mathbb{E}[X] = \sum_{n \geq 1} \mathbb{P}(X \geq i) \geq \mathbb{P}[X \geq 1].$$

V projektu večkrat dokažemo, da se nek dogodek zgodi z verjetnostjo 0 oziroma 1. To izrazimo z izjavo, da se dogodek *skoraj zagotovo ne zgodi* oziroma se *skoraj zagotovo zgodi*. Klasični primer, ki ilustrira potrebnost teh definicij, je primer lokostrelca in tarče. Denimo da izjemno dobro izurjen lokostrelec, ki nikoli ne zgreši tarče, strelja v tarčo. Verjetnost da lokostrelec zadane posamično točko je enaka 0. Kljub temu pa lokostrelec tarče seveda ne zgreši, temveč zadane neko točko na tarči, čeprav je verjetnost, da to točko zadane enaka 0. Sledi, da je potrebno razločiti dogodek, ki se ne more zgoditi, od dogodka, ki se zgodi z verjetnostjo nič. To storimo z izrazom skoraj zagotovo. V nadaljevanju našega članka vedno delamo na primernem podprostoru z mero ena, kjer imamo vse stvari, ki se zgodijo skoraj zagotovo, torej lahko pedantiko podobno zgornji opustimo.

3 Perkolacija

3.1 Graf

Definirajmo graf $\mathbb{L}^d$. Za njegova vozlišča vzamemo množico $\mathbb{Z}^d$ vloženo v $\mathbb{R}^d$. Razdaljo med dvema vozliščema merimo z običajno metriko na grafih, znano kot *taxi razdalja*. Za $x = (x_1, x_2, \ldots, x_n)$ in $y = (y_1, y_2, \ldots, y_n)$ je ta definirana kot

$$d(x, y) = \sum_{i=1}^{n} |x_i - y_i|.$$

Povezave na grafu so med vsemi vozlišči, ki so na razdalji dolžine 1, to so vozlišča, ki se razlikujejo v natanko eni koordinati. Vozlišča na grafu $\mathbb{L}^d$ imenujemo *točke*. Množico točk označimo z V, množico povezav pa z E.

Pot je zaporedje sosednjih povezav in točk $(v_0, e_1, v_1, e_2, \ldots)$, ki je lahko končno ali neskončno. Znotraj ene poti se nobena točka ali povezava ne ponovi. Izjemoma sta lahko prva in zadnja točka končne poti isti in tako pot imenujemo *cikel*. *Škatla* B_n je podgraf grafa $\mathbb{L}^d$ s tokami v $[-n, n]^d \cap \mathbb{Z}^d$ in vsemi povezavami znotraj njih. Velja

$$\bigcup_{n \in \mathbb{N}} B_n = \mathbb{L}^d.$$

Naj ∂B_n označuje množico točk, ki predstavljajo *mejo škatle*, to je

$$\partial B_n = \{x \in B_n : \exists\ y \notin B_n \text{ tako, da } d(x, y) = 1\}.$$

3.2 Verjetnost in geometrija

Naj bo $0 \leq p \leq 1$. Vsaka povezava v E se neodvisno od vseh ostalih odpre z verjetnostjo p, drugače ostane zaprta. Bolj formalno, naš prostor je $\Omega = \{0, 1\}^E$, σ-algebra je generirana s končnimi cilindri in verjetnostna mera je produktna mera $\mathbb{P}_p$. Za potrebe tega članka je dovolj razumeti le intuitivno definicijo perkolacije kot odpiranje povezav. Indeks p v verjetnostni meri $\mathbb{P}_p$ ali pričakovani vrednosti $\mathbb{E}_p$ označuje verjetnost, s katero se posamezna povezava odpre.

Pravimo, da sta dve točki *povezani*, če med njima obstaja pot po odprtih povezavah. Tako pot imenujemo *odprta pot*, pot po zaprtih povezavah pa *zaprta pot*. Z oznako $A \longleftrightarrow B$ označimo, da je vsaj ena točka iz množice točk A povezana z vsaj eno točko iz množice točk B v $\mathbb{L}^d$. Da poenostavimo notacijo, bomo v nadaljevanju za posamezne točke pisali $\{x\} = x$. Naj bo *omrežje* x, označeno s $C(x)$, množica točk, ki so v $\mathbb{L}^d$ povezane s točko x,

$$C(x) = \{y : x \longleftrightarrow y\}.$$

Naj bo $x \in B_n$. Če za vsak $n \in \mathbb{N}$ obstaja $y \notin B_n$, da je $x \longleftrightarrow y$, potem to označimo z $x \longleftrightarrow \infty$. Označimo s $C = C(0)$. Definirajmo $\theta(p)$, ki nam pove, kolikšna je verjetnost da je $|C| = \infty$, torej

$$\theta(p) = \mathbb{P}_p[0 \longleftrightarrow \infty].$$

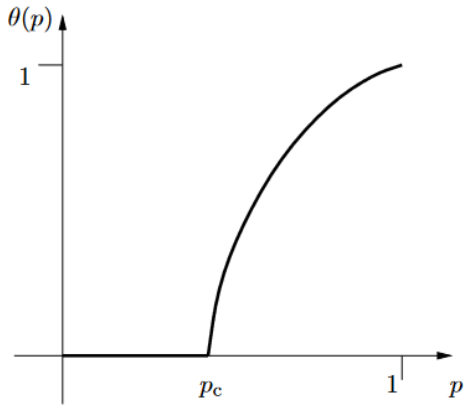
Opazimo lahko, da je $\theta(0) = 0$ in $\theta(1) = 1$. Razumeti obnašanje $\theta(p)$ je ključno za razumevanje perkolacije, a veliko njenih lastnosti se še vedno izmika matematikom. Kar vemo, je skicirano na sliki 1.

3.3 Kritična točka

Naj bo $p_c = p_c(\mathbb{L}^d)$ *kritična točka*, definirana kot

$$p_c = \sup\{p : \theta(p) = 0\}.$$

Najprej izračunajmo p_c za $d = 1$. V tem primeru imamo graf $\mathbb{L}^1$, kar je neskončna premica točk in povezav. Naj bo $\theta(p)^+$ verjetnost, da se točka 0 poveže z neskončnostjo v pozitivni smeri in $\theta(p)^-$ verjetnost, da se



Slika 1: Graf $\theta(p)$ in kritična točka p_c.

točka 0 poveže z neskončnostjo v negativni smeri. Potem, za $p < 1$, velja

$$\theta(p) \leq \theta(p)^+ + \theta(p)^- = 2 \cdot \lim_{n\to\infty} p^n = 2 \cdot 0 = 0.$$

To pomeni, da je $p = 1$ edina vrednost, za katero je $\theta(p) > 0$. Posledično velja $p_c(\mathbb{L}^1) = 1$. O p_c in $\theta(p)$ je za višje dimenzije znano malo formalnih rezultatov. Vemo pa, da se bo za večje dimenzije d vrednost p_c manjšala. To si lahko predstavljamo tako, da graf $\mathbb{L}^d$ vložimo v graf $\mathbb{L}^{d+1}$. Res opazimo, da velja $p_c(\mathbb{L}^d) \geq p_c(\mathbb{L}^{d+1})$, saj nam dodatna dimenzija lahko doda nove poti, že obstoječih pa ne more prekiniti.

V dveh dimenzijah še imamo dovolj orodij, da lahko ugotovimo točno vrednost $p_c(\mathbb{L}^2)$. Pomagamo si tako, da definiramo *dualni graf* grafa $\mathbb{L}^2$, ki ga označimo z $\mathcal{D} = \mathcal{D}(\mathbb{L}^2)$. Prvotni graf bomo včasih imenovali *original*. Dualni graf ali krajše dual je izomorfen originalu, a so njegova vozlišča glede na originalni graf zamaknjena. Množica vozlišč duala je

$$\mathbb{Z}^2 + \left(\frac{1}{2}, \frac{1}{2}\right).$$

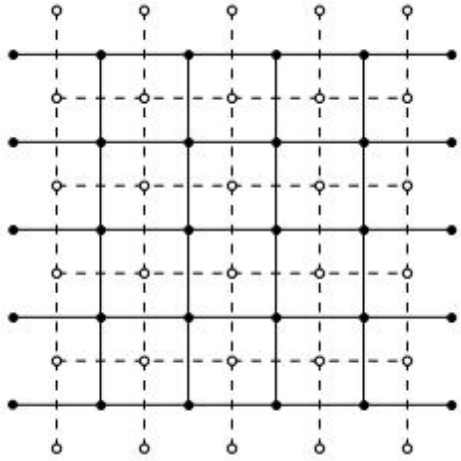
Posledično je vsaka točka v dualu ravno središče kvadrata točk v originalu, vse povezave med dualom in originalom pa se sekajo pod pravim kotom. Povezave v $\mathcal{D}$ se odpirajo in zapirajo glede na njegov original, tako da če povezava v $\mathcal{D}$ seka odprto povezavo v $\mathbb{L}^2$, se ta odpre in če povezava v $\mathcal{D}$ seka zaprto povezavo v $\mathbb{L}^2$, ostane zaprta. Tako imata original in dual enako verjetnostno mero, kar pomeni, da če opazujemo le en dogodek na enem izmed grafov, ne vemo, ali gledamo original ali njegov dual. Definiramo tudi *škatle v dualu*, ki jih označimo z B_n^d. To je najmanjši cikel v $\mathcal{D}$, ki vsebuje celotno škatlo B_n iz $\mathbb{L}^d$.

4 Netrivialnost p_c

Rezultati in opazovanja iz poglavja 3 nas vodijo do problema določitve vrednsoti p_c v odvisnosti od dimenzije d. Žal ta problem presega namen tega članka, zaradi česar se odločimo dokazati naslednjo, mnogo manj ambiciozno trditev.

Izrek 4.1. *Za $d \geq 2$ je $0 < p_c(\mathbb{L}^d) < 1$.*

Dokaz. Dokaz neenakosti $0 < p_c < 1$ v $\mathbb{L}^d$ za $d \geq 2$ razdelimo na dva dela.



Slika 2: Graf $\mathbb{L}^2$ in njegov dual.

$p_c > 0$:

Najprej definirajmo nekaj količin. Naj N_n označuje množico odprtih poti dolžine n iz 0. Obenem naj Q_n označuje množico vseh poti iz 0 (tj. ne nujno odprtih poti) dolžine n. Lahko vidimo, da je za vsak n dogodek $\{|C| = \infty\} \subset \{|N_n| \geq 1\}$. Posledično sledi, da je za vsak $n \in \mathbb{N}$

$$\theta(p) = \mathbb{P}_p[|C| = \infty] \leq \mathbb{P}_p[|N_n| \geq 1].$$

Po neenakosti (2.1) za vsak n sledi

$$\theta(p) \leq \mathbb{E}[|N_n|] = \sum_{j \in Q_n} \mathbb{E}[\mathbb{1}_{\{j \in N_n\}}] = \sum_{j \in Q_n} \mathbb{P}[j \in N_n] \leq |Q_n| \cdot p^n.$$

Na sledeči način grobo ocenimo $|Q_n|$ kot

$$|Q_n| \leq 2d(2d-1)^{n-1},$$

kjer smo prešteli prav vse možne sprehode, ne pa samo poti. Za $p < \frac{1}{2d}$ pa velja

$$\lim_{n\to\infty} 2d(2d-1)^{n-1}p^n \leq \lim_{n\to\infty} 2d(2d-1)^{n-1}\left(\frac{1}{2d}\right)^n = \lim_{n\to\infty}\left(\frac{2d-1}{2d}\right)^{n-1} = 0.$$

Dokazali smo, da ob izbiri $p < \frac{1}{2d}$ velja

$$\theta(p) \leq 0,$$

iz česar sledi $\theta(p) = 0$. Pokazali smo, da lahko izberemo dovolj majhen, a neničelen p, da omrežje točke 0 ne doseže neskončnosti. Torej je kritična vrednost p_c večja od izbrane vrednosti p, kar implicira neničelnost p_c.

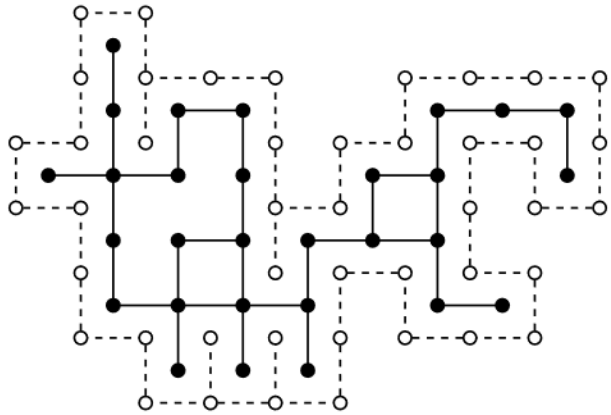
$p_c < 1$:

Definirajmo M_n kot množico zaprtih ciklov v $\mathcal{D}(\mathbb{L}^2)$, ki v svoji notranjosti vsebujejo točko 0. Dokazali bomo, da vsaj ena taka pot obstaja natanko tedaj, ko velja $|C| \neq \infty$.

Najprej dokažemo, da $|C| \neq \infty$ implicira obstoj zaprtega cikla s točko 0 v notranjosti. Vsaki točki v $\mathbb{L}^2$ dodelimo vrednost 1 v primeru, da je element omrežja C, v nasprotnem primeru točki dodelimo vrednost 0. Ker je $|C| \neq \infty$, je število točk, katerim je bila dodeljena vrednost 1, končno. Če v originalu opazujemo

cikel maksimalne dolžine točk z vrednostjo 1, je ta v originalu obkrožen s ciklom točk z vrednostjo 0. Ker je povezava med točko z vrednostjo 0 ter točko z vrednostjo 1 zaprta, to pomeni, da v dualu $\mathbb{L}^2$ obstaja zaprt cikel, ki poteka med ciklom maksimalne dolžine točk z vrednostjo 1 ter ciklom točk z vrednostjo 0, ki ga obkroža.

Sedaj dokažemo, da obstoj zaprtega cikla v $\mathcal{D}\left(\mathbb{L}^2\right)$, ki ima v notranjosti točko 0, implicira $|C| \neq \infty$. Argument je obratna verzija zgornjega. Opazujmo množico takih točk, da za poljubno točko v tej množici obstaja zaprta povezava v $\mathbb{L}^2$, ki je dualno povezana z neko potjo zaprtega cikla v $\mathcal{D}\left(\mathbb{L}^2\right)$, katerega obstoj smo predpostavili. Vsaki točki te množice dodelimo vrednost 1, če se nahaja znotraj zaprtega cikla v $\mathcal{D}\left(\mathbb{L}^2\right)$, in 0 v nasprotnem primeru. Opazimo, da točke, katerim smo dodelili vrednost 0, tvorijo sklenjen cikel v $\mathbb{L}^2$ s točko 0 v notranjosti. Enaka trditev velja za točke, ki smo jim dodelili vrednost 1. Cikel točk z vrednostjo 1 je v celoti vsebovan znotraj cikla točk z vrednostjo 0, med njimi pa poteka zaprta povezava. Iz tega sledi, da ni mogoče, da bi bilo omrežje točke 0 neskončno, saj ne more prečkati povezave med cikloma točk vrednosti 1 in 0, obenem pa je znotraj cikla točk vrednosti 1 le končno mnogo točk. Slika 3 prikaže omenjene povezane odprte in zaprte poti v grafu $\mathbb{L}^2$ ter njegovem dualu.



Slika 3: Zaprt cikel duala, ki vsebuje 0 ter končno omrežje 0.

Definirajmo K_n kot množico vseh sklenjenih poti v $\mathcal{D}(\mathbb{L}^2)$ (ne nujno zaprtih), ki vsebujejo točko 0 v svoji notranjosti. Ker je $p_c(\mathbb{L}^d)$ padajoče v d, je dovolj dokazati $p_c(\mathbb{L}^2) < 1$. V $\mathbb{L}^2$ velja

$$1 - \theta(p) = \mathbb{P}_p[|C| < \infty] = \mathbb{P}_p\left[\sum_n |M_n| \geq 1\right] \leq \mathbb{E}\left[\sum_n |M_n|\right] = \sum_n \mathbb{E}\left[|M_n|\right],$$

pri čemer neenakost velja zaradi neenakosti (2.1), zadnja enakost pa zaradi linearnosti pričakovane vrednosti. Vpeljujoč indikatorsko spremenljivko $\mathbb{1}_{\{j \in M_n\}}$ skrajno desni izraz zapišemo kot

$$\sum_n \mathbb{E}\left[|M_n|\right] = \sum_n \sum_{j \in K_n} \mathbb{E}\left[\mathbb{1}_{\{j \in M_n\}}\right] = \sum_n \sum_{j \in K_n} \mathbb{P}\left[j \in M_n\right].$$

Ker je verjetnost, da je sklenjena pot dolžine n v dualu v celoti zaprta, enaka $(1-p)^n$, lahko zapišemo naslednjo neenakost

$$\sum_n \sum_{j \in K_n} \mathbb{P}\left[j \in M_n\right] \leq \sum_n \sum_{j \in K_n} (1-p)^n \leq \sum_n n \cdot 4^n (1-p)^n.$$

Pri tem smo K_n navzgor omejili tako, da smo prešteli vse sprehode v dualu, ki sekajo pozitivno polovico

$x = 0$ osi na razdalji manj kot n od 0. Za izbiro p, ustrezno blizu, a ne enako, 1, sledi

$$\theta(p) \geq 1 - \sum_n n \cdot 4^n (1-p)^n > 0.$$

Ker je $\theta(p) > 0$, sledi $p > p_c$. Izbira $p < 1$ dokaže želeno trditev, da je $1 > p > p_c$.

□

5 Dejstva

Pri računanju vrednosti p_c za $d = 2$ bomo potrebovali tri dejstva, ki jih sicer ne bomo dokazovali, bomo pa podali ideje, zakaj ta dejstva intuitivno držijo. Bralec lahko dokaze najde v [1]. Najprej omenimo, da lahko graf $\theta(p)$ razdelimo na tri območja glede na p. To so faze *nad kritično točko*, *pod kritično točko* in *blizu kritične točke*. Medtem ko o tem, kaj točno se dogaja blizu kritične točke, vemo zelo malo, pa so faze nad in pod p_c dobro raziskane.

i) Nad kritično točko

Naj bo A dogodek in $\mathbb{P}$ poljubna mera. *Translacija* dogodka je preslikava $\mathbb{L}^d$ tako, da se vse točke premaknejo za enak vektor. Translacijo za vektor x označimo z τ_x. Če velja $\tau_x A = A$ za vsak x, pravimo, da je dogodek *invarianten pod translacijami*. Če za vse take dogodke velja, da je $\mathbb{P}[A] \in \{0, 1\}$, rečemo, da je mera $\mathbb{P}$ *ergodična*.

Ni težko pokazati, da je naša mera $\mathbb{P}_p$ ergodična za vsak p. Naj bo I število neskončnih omrežij. Hitro ugotovimo, da je dogodek $I = k$ invarianten pod translacijami, saj se pri translaciji ta omrežja le premaknejo, ne pa tudi spremenijo oblike, prav tako tudi niso vezana na začetno točko. Iz tega sledi, da je verjetnost $\Psi(p) = \mathbb{P}_p[I \geq 1] \in \{0, 1\}$. Za $p > p_c$ dobimo iz 0 neskončno omrežje s pozitivno verjetnostjo. Ker je $\mathbb{Z}^d$ neskončen, je posledično zaradi ergodičnosti $\Psi(p) = 1$. Torej velja

$$\mathbb{P}[I = k] = \begin{cases} 1 & \text{za eno vrednost } k, \\ 0 & \text{za vse ostale vrednosti } k. \end{cases}$$

A priori lahko k zavzame vrednosti v $\mathbb{N} \cup \{\infty\}$. Recimo, da je $k > 1$ končen. Izberimo takšno konfiguracijo in odprimo vse povezave na poti med dvema neskončnima omrežjema. Takšna pot je končna, torej se tudi nova konfiguracija lahko zgodi s pozitivno verjetnostjo. Tako iz k omrežij dobimo $k-1$ omrežij, ravno prej pa smo omenili, da je $\mathbb{P}[I = k] = 1$ le za eno vrednost k, za ostale pa je enaka 0. To pomeni, da ne more hkrati imeti k in $k-1$ neskončnih omrežij s pozitivno verjetnostjo. Če ta sklep še nekajkrat ponovimo, ugotovimo, da če je k končen, mora veljati $k = 1$.

Še vedno imamo možnost, da obstaja neskončno mnogo različnih neskončnih omrežij. Tukaj zgornja ideja ne deluje, saj po povezovanju še vedno ostane neskončno mnogo omrežij. Vseeno pa obstaja prelep dokaz, znan kot Burton-Keane, [2], da ne more obstajati neskončno mnogo različnih neskončnih omrežij. Za moderno verzijo Burton-Keane argumenta priporočamo [3]. Torej velja, da za $p > p_c$ obstaja natanko eno neskončno omrežje.

ii) Pod kritično točko

Za vse $p < p_c$ velja, da je $\theta(p) = 0$, vseeno pa nas zanima, kako daleč lahko pridemo od točke 0. Naj bo $\theta_n(p) = \mathbb{P}[0 \longleftrightarrow B_n]$. Opazimo, da velja $\theta_n(p) > \theta_{n+1}(p)$, saj vedno težje pridemo do naslednje večje škatle. Izkaže se, da verjetnost pada eksponentno. Natančneje velja, da za vsak n obstaja tak $c > 0$, da imamo

$$\theta_n(p) \leq e^{-cn}. \tag{2}$$

iii) FKG neenakost

Motivacija pride iz ideje, da sta dve točki bolj verjetno povezani, če že vemo, da neka povezava obstaja, saj nas sedaj zanima le še verjetnost za odprtje preostalih povezav namesto vseh. Za $x, y, z, w \in V$ velja

$$\mathbb{P}[x \longleftrightarrow y | z \longleftrightarrow w] \geq \mathbb{P}[x \longleftrightarrow y].$$

Pravimo, da je dogodek A *naraščajoč*, če za vsaka $p > q$ velja $\mathbb{P}_p[A] \geq \mathbb{P}_q[A]$. Za *padajoč* dogodek velja obratno. Če sta dogodka A in B oba naraščajoča ali oba padajoča, se izkaže, da velja

$$\mathbb{P}_p[A \cup B] \geq \mathbb{P}_p[A] \cdot \mathbb{P}_p[B]. \tag{3}$$

To je posebna verzija Fortuin–Kasteleyn–Ginibre-jeve neenakosti, ali na kratko FKG neenakosti. Ker je dogodek $0 \longleftrightarrow \infty$ naraščajoč, je ta neenakost zelo uporabna.

6 Vrednost p_c v dveh dimenzijah

Dejstva v prejšnjem poglavju je težko dokazati in so močna orodja za izračun p_c. Glavna ideja dokaza naslednjega rezultata je simetričnost med zaprtimi in odprtimi povezavami za $p = \frac{1}{2}$ ter $\mathbb{L}^2$ in njegovim dualom. V dveh dimenzijah je dovolj malo prostora, da uspemo s tem priti do rešitve.

Izrek 6.1. *Velja* $p_c(\mathbb{L}^2) = \frac{1}{2}$.

Dokaz. Naj bo $p = \frac{1}{2}$. Najprej s protislovjem dokažimo, da je $p_c \geq \frac{1}{2}$. Predpostavimo torej $p_c < \frac{1}{2}$. To pomeni, da je $p_c < p$, zato obstaja edinstveno neskončno omrežje. Če obstaja povezava med ∂B_{n-1} in neskončnim omrežjem, obstaja takšna povezava tudi za ∂B_{n-1}. Posledično je $\mathbb{P}[\partial B_n \longleftrightarrow \infty]$ naraščajoča v n in ker ima limito 1, lahko fiksiramo dovolj velik N, da velja

$$\mathbb{P}[\partial B_N \longleftrightarrow \infty] > 1 - \frac{1}{8^4}.$$

Stranice ∂B_N poimenujmo z L, D, T in B, tako da sta si L in D nasprotni, prav tako pa sta si nasprotni stranici T in B. Naj bo A_X za $X \in \{L, D, T, B\}$ dogodek, da obstaja povezava med stranico X in neskončnostjo, ki ne poteka skozi nobeno točko v B_N. Naj $\bar{A}$ označuje komplement dogodka A. Ker je $\mathbb{P}_p[A_X]$ naraščajoča, je posledično $\mathbb{P}_p\left[\bar{A}_X\right]$ padajoča v p. Med ∂B_N in neskončnim omrežjem ni povezave natanko takrat, ko ni povezave med nobeno stranico ∂B_N in neskončnim omrežjem. S pomočjo FKG neenakosti (3) velja

$$\mathbb{P}[\partial B_N \not\longleftrightarrow \infty] = \mathbb{P}_p\left[\bar{A}_L \cap \bar{A}_D \cap \bar{A}_T \cap \bar{A}_B\right] \geq \mathbb{P}_p\left[\bar{A}_L\right] \mathbb{P}_p\left[\bar{A}_D\right] \mathbb{P}_p\left[\bar{A}_T\right] \mathbb{P}_p\left[\bar{A}_B\right] = \mathbb{P}_p\left[\bar{A}_X\right]^4$$

za vsak $X \in \{L, D, T, B\}$. Torej velja

$$\mathbb{P}_p\left[\bar{A}_X\right]^4 \leq 1 - \mathbb{P}[\partial B_N \longleftrightarrow \infty] < 1 - (1 - \frac{1}{8^4}) = \frac{1}{8^4},$$

iz česar sledi $\mathbb{P}_p\left[\bar{A_X}\right] < \frac{1}{8}$ in zato

$$\mathbb{P}_p[A_X] > \frac{7}{8}.$$

Dogodek, da je posamezna stranica $X \in \{L, D, T, B\}$ meje dualne škatle ∂B_N^d povezana z neskončnostjo z zaprto potjo, ki ne poteka skozi B_N^d, označimo z D_X. Imamo dvojno simetrijo med zaprtimi in odprtimi potmi ter med originalnim grafom in njegovim dualom, zato velja $\mathbb{P}_{\frac{1}{2}}[A_X] = \mathbb{P}_{\frac{1}{2}}[D_X]$ za vsak X. Naj bo $A = A_L \cup A_D \cup D_B \cup D_T$. Računamo

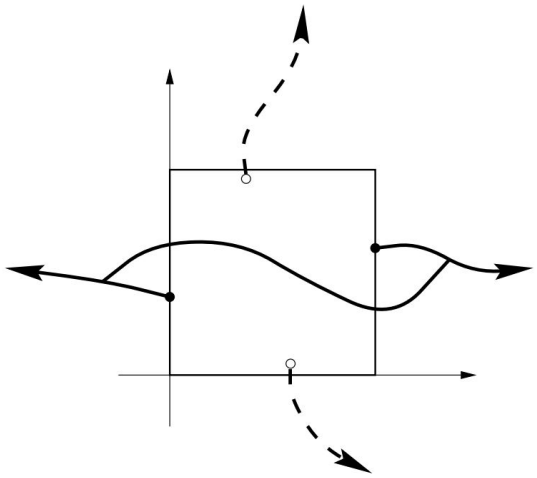
$$\begin{aligned}
\mathbb{P}[\bar{A}] &= \mathbb{P}_{\frac{1}{2}}\left[\ \overline{A_L \cap A_D \cap D_B \cap D_T}\right] \\
&= \mathbb{P}_{\frac{1}{2}}\left[\bar{A}_L \cup \bar{A}_D \cup \bar{D}_B \cup \bar{D}_T\right] \\
&\leq \mathbb{P}_{\frac{1}{2}}\left[\bar{A}_L\right] + \mathbb{P}_{\frac{1}{2}}\left[\bar{A}_D\right] + \mathbb{P}_{\frac{1}{2}}\left[\bar{A}_T\right] + \mathbb{P}_{\frac{1}{2}}\left[\bar{A}_R\right].
\end{aligned}$$

Za vsak X je $\mathbb{P}[\bar{A}_X] \leq \frac{1}{8}$, torej je $\mathbb{P}[\bar{A}] \leq \frac{1}{2}$, oziroma

$$\mathbb{P}_{\frac{1}{2}}[A] \geq \frac{1}{2}.$$

To pomeni, da je verjetnost, da je par stranic (L, D) na ∂B_N povezan z neskončnostjo hkrati kot par stranic (T, B) na ∂D_N, vsaj $\frac{1}{2}$. Ker imamo zgolj eno neskončno omrežje, je par stranic (L, D) povezan z odprto potjo v originalnem grafu, par (T, B) pa je povezan z zaprto potjo v njegovem dualu. Odprte poti v osnovnem grafu po definiciji dualnega grafa ne more prečkati njegove zaprte poti, ki povezuje T in B stranico dualne škatle in se v vsako stran nadaljuje v neskončnost. To zaprto pot lahko obravnavamo kot cikel, sklenjen skozi neskončnost, ki ravnino razdeli na dva dela. Ker pa se krajišči odprte poti začneta na nasprotnih straneh, se torej nikoli ne moreta povezati, kar pomeni, da je $\mathbb{P}_{\frac{1}{2}}[A] = 0$, to pa je protislovje. Sledi, da je naša predpostavka $p_c < \frac{1}{2}$ napačna in torej $p_c \geq \frac{1}{2}$.

Predpostavimo zdaj, da je $p_c > \frac{1}{2}$. Imamo $p < p_c$ in smo v pod kritični fazi. Definirajmo podgraf G_n, ki ima za vozlišča podmnožico našega grafa na intervalih $x_1 \in [0, n+1]$ in $x_2 \in [0, n]$, H_n pa naj bo podmnožica vozlišč duala na intervalih $x_1 \in [0, n]$ in $x_2 \in [0, n+1]$. Naj bo E dogodek, da sta leva in desna stranica G_n povezani samo preko povezav v G_n, in F dogodek, da sta zgornja in spodnja stranica na H_n povezani z zaprto potjo samo s povezavami v H_n. Opazimo, da se vedno zgodi natanko eden izmed dogodkov E in F. Ker je $p = \frac{1}{2}$ in sta grafa izomorfna z isto verjetnostno mero, velja, da sta dogodka E in F enako verjetna. Dokaz prikazuje slika 4.



Slika 4: Leva in desna stranica G_n sta povezani z odprto potjo.

Sledi $\mathbb{P}_{\frac{1}{2}}[E] = \frac{1}{2}$. Spomnimo se enačbe (2), ki nam v pod kritični fazi omeji verjetnost, da je točka 0 povezana z neko stranico v ∂B_n. Verjetnost, da se zgodi E, lahko ocenimo kot

$$\begin{aligned}\mathbb{P}[L \longleftrightarrow D] &= \mathbb{P}\left[\bigcup_{x\in L} x \longleftrightarrow D\right] \\ &\leq \sum_{x\in L} \mathbb{P}[x \longleftrightarrow D] \\ &= \sum_{x\in L} e^{-c(n+1)} \\ &= n \cdot e^{-c(n+1)}.\end{aligned}$$

Torej imamo $\frac{1}{2} \leq n \cdot e^{-c(n+1)}$ za poljuben n, kar je protislovje za velike n. S tem smo dokazali, da je $p_c \leq \frac{1}{2}$. Imamo $\frac{1}{2} \leq p_c \leq \frac{1}{2}$, iz česar sledi $p_c = \frac{1}{2}$.

□

7 Zaključek

V dveh dimenzijah nam je uspelo natančno določiti vrednost p_c. Argument ni bil enostaven in opirali smo se na številne lastnosti perkolacije, ki jih ni lahko dokazati. Prav tako je ključno vlogo igrala nizkodimenzionalnost. V višjih dimenzijah je dovolj prostora, da se lahko odprta in zaprta pot izmuzneta v neskončnost ena mimo druge, brez, da razdelita prostor na dva dela. Našo mejo $0 < p_c < 1$ lahko izboljšamo z elementarnimi tehnikami in z boljšim štetjem poti, vendar je moč neenakosti, ki jih lahko dobimo na ta način, omejena. Precej ostrejše meje dobimo s pomočjo Grimmett-Marstrandove konstrukcije, ki je višje dimenzionalna razširitev ideje o sekanju poti. Vendar tudi to ni dovolj za določitev točne vrednosti p_c za $d \geq 3$ in razumevanje kritične točke ostaja eden najbolj perečih problemov naključnih modelov na grafih.

Literatura

[1] Grimmet, GR, Sterzaker, DR, *Probability and Random Processes,* Oxford Sc. Publ, Oxford, 1992.

[2] Burton R. M., Keane, M., *Density and uniqueness in percolation*, Communications in mathematical physics, vol. 121, pp. 501–505, Springer, 1989.

[3] H. Duminil-Copin, *Introduction to Bernoulli percolation*, Lecture notes available on the webpage of the author, 2018.

Lema, ki ni Burnsideova

Manca Ernst, Rok Hudournik, Matej Knap
Mentorica: *Katarina Šipec*

Povzetek

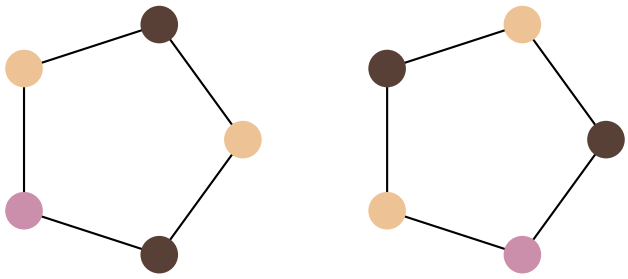
V tem članku je kombinatorični problem razlikovanja med zapestnicami rešen na algebraičen način s pomočjo delovanja grup in uporabo Burnsideove leme.

1 Uvod

Predstavljajmo si, da nam babica na zelo splošen dan podari neskončno mnogo biserov, ki se pojavljajo v n različnih barvah. Odločimo se, da bomo iz njih sestavljali zapestnice, kar pa storimo tako, da p takih biserov nanizamo na vrvico. Ker je nizanje biserov zelo naporno delo, hitro pozabimo, koliko zapestnic smo že naredili. Posledično se nam seveda porodi vprašanje, koliko različnih zapestnic bi sploh lahko sestavili.

Ker smo od mučnega dela tako utrujeni, da nam je pretežko razmišljati o splošnih zapestnicah s p biseri in n barvami, najprej premislimo za $p = 5$ in $n = 3$. Reševanja problema se lotimo kombinatorično. Ker imamo za barvo vsakega posameznega bisera na zapestnici tri možnosti, vseh biserov pa je pet, najprej pomislimo, da je rešitev kar $3^5 = 243$.

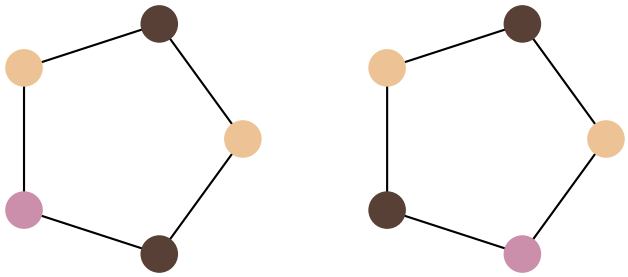
Toda hitro ugotovimo, da ima naše razmišljanje veliko pomankljivost. Oglejmo si zapestnici s slike 1. Opazimo, da lahko končno mnogokrat zavrtimo eno od zapestnic in bodo biseri na njej pristali na popolnoma enakih položajih kot na drugi zapestnici. Zapestnici, za kateri velja, da lahko eno od njiju zavrtimo in



Slika 1: Če prvo zapestnico zavrtimo za kot $\frac{2\pi}{5}$ v pozitivni smeri, biseri pristanejo na enakih položajih kot na drugi zapestnici.

dobimo enako kombinacijo biserov kot pri drugi, sta seveda enaki. Na podoben način ugotovimo, da lahko poleg rotacije izvedemo tudi zrcaljenje čez neko premico in dobimo enako zapestnico. Primer je na sliki 2.

Če ostanemo pri začetni strategiji, nam ti ugotovitvi precej otežita reševanje problema že pri $n = 3$ in $p = 5$. Zato se bomo naloge lotili na drugačen način, in sicer s pomočjo teorije grup. Spoznali bomo polgrupe in iz njih izpeljali definiciji za monoide in grupe. Posebej bomo omenili tudi diedrsko in simetrično grupo, homomorfizme ter delovanje grupe na množici. Dokazali bomo Burnsideovo lemo, s pomočjo katere bomo rešili naš problem.



Slika 2: Če prvo zapestnico prezrcalimo čez poševno premico, dobimo drugo zapestnico.

2 Grupe

V algebri poznamo mnogo različnih struktur na množicah, ki jih ločimo glede na njihove lastnosti. Ukvarjali se bomo z grupami, ki jih bomo tudi uporabili za reševanje zastavljenega problema.

Definicija 2.1. Polgrupa P *je množica skupaj z operacijo* $\cdot : P \times P \to P$*, ki je* asociativna*, torej za vse* $x, y, z \in P$ *velja*

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z.$$

Če v tej polgrupi P *obstaja neki element* e*, za katerega velja*

$$\forall x \in P : e \cdot x = x = x \cdot e,$$

to polgrupo imenujemo monoid*, element* e *pa* enota*.*

Monoide na kratko označimo kot $(M, \cdot, e)$, kjer je M množica, $\cdot$ operacija na množici M in e enota.

Trditev 2.1. *Enota je enolična.*

Dokaz. Denimo, da ima monoid M dve različni enoti e in f. Torej velja

$$f = e \cdot f = e$$

in prišli smo do protislovja, saj sta po predpostavki e in f različna. □

Primer monoida je $(\mathbb{N} \cup \{0\}, +, 0)$, saj pri seštevanju naravnih števil z naravnimi števili dobimo druga naravna števila, če pa prištevamo 0, ki je v tem primeru enota, dobimo nazaj isto naravno število. Še en primer je monoid $(\mathbb{R} - \{0\}, \cdot, 1)$.

Omeniti je vredno tudi monoid $(\{f : \mathbb{R} \to \mathbb{R}\}, \circ, x \mapsto x)$, pri katerem so elementi vse funkcije iz realnih števil v realna števila, operacija je kompozitum funkcij, ki je definiran kot $(f \circ g)(x) = f(g(x))$, in enota je simetrala lihih kvadrantov oziroma identiteta $\mathrm{id}(x) = x$.

Definicija 2.2. Inverz *elementa* x *v monoidu* $(M, \cdot, e)$ *je element* y*, za katerega velja*

$$x \cdot y = e = y \cdot x.$$

Če v monoidu M *vsak element premore inverz, je* M grupa*.*

Trditev 2.2. *Inverz je enoličen za vsak element* g *v grupi* G*.*

Dokaz. Naj bosta y in z dva različna inverza elementa x. Potem velja

$$y = y \cdot e = y \cdot (x \cdot z) = (y \cdot x) \cdot z = e \cdot z = z.$$

Prišli smo do protislovja, saj sta po predpostavki y in z različna. □

Primer grupe je $(\mathbb{Z}, +, 0)$, torej množica celih števil z operacijo seštevanja in enoto 0, ki smo jo srečali že pred definicijo, medtem ko primer omenjenega monoida $(\{f : \mathbb{R} \to \mathbb{R}\}, \circ, x \mapsto x)$ ni grupa, saj inverzi funkcij, ki niso bijektivne, ne obstajajo. Če bi se omejili le na bijektivne funkcije, bi bile te grupa za operacijo kompozitum.

Grupam lahko določimo tudi druge lastnosti. Ena od njih je *komutativnost*. Zanjo velja, da za vsaka elementa x in y velja

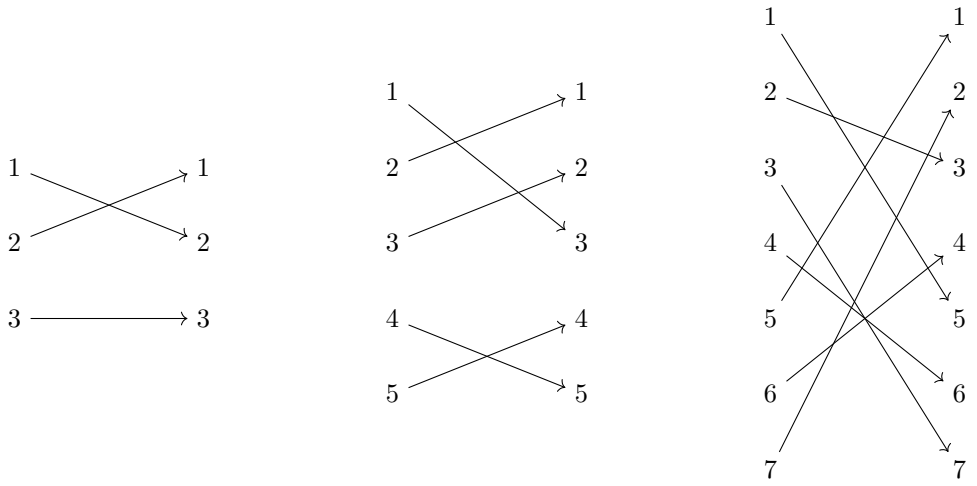
$$x \cdot y = y \cdot x.$$

2.1 Simetrične in diedrske grupe

Definicija 2.3. *Naj bo $[n] = \{1, 2, \ldots, n\}$ množica. Permutacija je bijektivna preslikava $[n] \to [n]$.* Simetrična *grupa je množica vseh permutacij, opremljena z operacijo $\circ$.*

Permutacije pišemo kot zmnožek disjunktnih ciklov, pri katerem vsak cikel zapišemo v oklepajih in v njih zaporedje slikanja elementov. Primer zapisa treh permutacij je na sliki 3. Permutacije množimo (kot komponiramo funkcije) z desne proti levi, torej velja na primer

$$(132) \cdot (12) = (23).$$



Slika 3: Na sliki so tri permutacije. Prvo pišemo kot (12), drugo kot (132)(45) in tretjo kot (15)(237)(46).

Definicija 2.4. Diedrska *grupa D_{2n} je grupa simetrij pravilnega n-kotnika. Definirana je kot množica*

$$D_{2n} = \{\mathrm{id}, r, r^2, \ldots, r^{n-1}, z, zr, zr^2, \ldots, zr^{n-1}\},$$

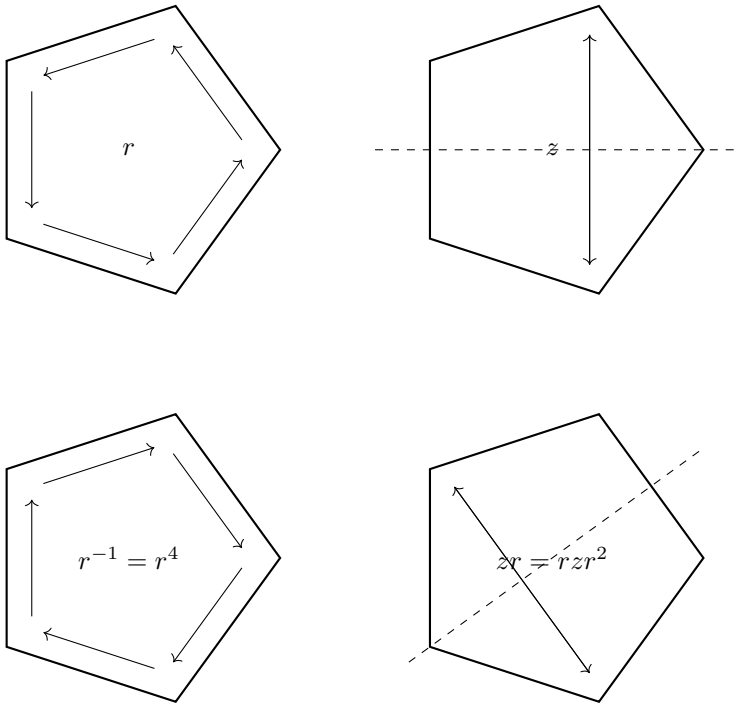
pri čemer vsak element razumemo kot preslikavo. Element r razumemo kot rotacijo n-kotnika, ki premakne vsako oglišče v sosednje oglišče v pozitivni smeri, element z pa kot zrcaljenje preko ene od simetrijskih osi n-kotnika. Operacija na množici D_{2n} je spet kompozitum.

Preslikave lahko vizualiziramo kot je prikazano na sliki 4 in jih prav tako beremo z desne proti levi.

2.2 Homomorfizmi

Preslikave med grupami, ki ohranjajo strukturo grupe, imenujemo homomorfizmi.

Definicija 2.5. *Naj bosta $(G, \cdot, e_G)$ in $(H, \cdot, e_H)$ grupi. Preslikava $\varphi : G \to H$ je* homomorfizem, *če velja*



Slika 4: Na sliki so prikazane štiri preslikave v D_{10}, ki po vrsti določajo elemente r, z, $r^{-1} = r^4$, $zr = rzr^2$.

- $\varphi(e_G) = e_H$,
- *za vsaka* g *in* h *iz* G *velja* $\varphi(gh) = \varphi(g)\varphi(h)$.

V naslednji trditvi bomo pokazali, da homomorfizem vsak inverz slika v inverz slike.

Trditev 2.3. *Naj bo* $\varphi : G \to H$. *Za vsak element* $x \in G$ *velja*

$$\varphi(x)^{-1} = \varphi(x^{-1}).$$

Dokaz. Označimo $\varphi(x^{-1}) = y$. Velja

$$\varphi(x) \cdot y = \varphi(x) \cdot \varphi(x^{-1}) = \varphi(xx^{-1}) = \varphi(e_G) = e_H.$$

Torej homomorfizem ohranja invertiranje. □

Definicija 2.6. Slika *homomorfizma* φ *je množica*

$$\mathrm{Im}(\varphi) = \{\varphi(x); x \in G\},$$

jedro *pa množica*

$$\mathrm{Ker}(\varphi) = \{x \in G; \varphi(x) = e_H\}.$$

Trditev 2.4. *Za vsak homomorfizem* φ *sta* $\mathrm{Im}(\varphi)$ *in* $\mathrm{Ker}(\varphi)$ *grupi.*

Dokaz. Naj bo $\varphi : G \to H$ homomorfizem in $\mathrm{Im}(\varphi)$ slika homomorfizma. Najprej pokažimo, da je množica $\mathrm{Im}(\varphi)$ zaprta za množenje. Naj bosta $w, z \in \mathrm{Im}(\varphi)$. Pokazati želimo, da je zw tudi v $\mathrm{Im}(\varphi)$. Vemo, da obstajata $x, y \in G$, da velja $\varphi(x) = z$ in $\varphi(y) = w$. Velja

$$zw = \varphi(x)\varphi(y) = \varphi(xy),$$

torej je zw tudi element $\mathrm{Im}(\varphi)$. Velja tudi

$$\varphi(e_G) = e_H,$$

torej je e_H v $\mathrm{Im}(\varphi)$. Vzemimo neki $y \in \mathrm{Im}(\varphi)$ in dokažimo, da je $y^{-1} \in \mathrm{Im}(\varphi)$. Vemo, da obstaja neki $x \in G$, da je $\varphi(x) = y$. Potem je

$$y^{-1} = \varphi(x)^{-1} = \varphi(x^{-1}).$$

Torej je $y^{-1} \in \mathrm{Im}(\varphi)$.

Naj bo $\mathrm{Ker}(\varphi)$ jedro homomorfizma. Najprej preverimo zaprtost za množenje. Naj bosta x in y elementa $\mathrm{Ker}(\varphi)$. Velja

$$\varphi(xy) = \varphi(x)\varphi(y) = e_H e_H = e_H,$$

torej je tudi xy element $\mathrm{Ker}(\varphi)$. Prav tako velja

$$\varphi(e_G) = e_H.$$

Torej $e_H \in \mathrm{Ker}(\varphi)$. Vzemimo neki $x \in \mathrm{Ker}(\varphi)$ in dokažimo, da je x^{-1} element $\mathrm{Ker}(\varphi)$. Vemo, da je $\varphi(x) = e_H$. Velja

$$\varphi(x^{-1}) = \varphi(x)^{-1} = e_H^{-1} = e_H.$$

Torej drži $x^{-1} \in \mathrm{Ker}(\varphi)$. □

Zgled 2.1. *Naj bo $\mathbb{Z}$ grupa celih števil za seštevanje. Vsi homomorfizmi $\mathbb{Z} \to \mathbb{Z}$ imajo predpis $n \mapsto xn$, kjer $x \in \mathbb{Z}$.*

Dokaz. Naj bo $x = \varphi(1)$. Za vsako naravno število n velja

$$\begin{aligned} \varphi(0) &= 0 = 0x, \\ \varphi(n) &= \varphi\left(\sum_{k=1}^{n} 1\right) = \left(\sum_{k=1}^{n} 1\right)\varphi(1) = nx, \\ \varphi(-n) &= -\varphi(n) = -nx. \end{aligned}$$

Torej je homomorfizem natanko določen z vrednostjo $\varphi(1)$. Za vse $n, m \in \mathbb{Z}$ velja

- $\varphi(0) = x \cdot 0 = 0$,
- $\varphi(n+m) = x(n+m) = xn + xm = \varphi(n) + \varphi(m)$,

torej je ta preslikava res homomorfizem. □

3 Delovanje grupe na množici

Začetni problem z zapestnicami bomo rešili s pomočjo Burnsideove leme, ki govori o lastnostih delovanja grupe na množici. Pri delovanju grupe na množici gre za to, da vsak element grupe razumemo kot preslikavo iz množice vase.

Definicija 3.1. *Naj bo X množica in G grupa.* Delovanje *grupe G na množici X je preslikava $G \times X \to X$, podana s predpisom $(g, x) \mapsto g \cdot x$, za katero velja:*

- $\forall x \in X\colon\ e \cdot x = x$,
- $\forall g, h \in G,\ \forall x \in X\colon\ (gh) \cdot x = g \cdot (h \cdot x)$.

Delovanje označimo kot $G \curvearrowright X$.

Zgled 3.1. *Delovanje $G \curvearrowright X$, podano s predpisom $(g, x) \mapsto x$, imenujemo* trivialno *delovanje.*

Za delovanje $G \curvearrowright X$ bomo definirali nekatere podmnožice grupe G in množice X, ki jih bomo potrebovali za dokazovanje kasnejših rezultatov.

Definicija 3.2. *Naj bo G grupa, X množica in $G \curvearrowright X$ delovanje grupe G na množici X. Definiramo sledeče pojme.*

- Orbita *elementa $x \in X$ je*
$$G \cdot x = \{g \cdot x;\ g \in G\} \subseteq X.$$
Orbito lahko ekvivalentno zapišemo kot $\{y \in X;\ \exists\, g \in G,\ y = g \cdot x\}$, kar bomo kasneje uporabili.
- Stabilizator *elementa $x \in X$ je*
$$G_x = \{g \in G;\ g \cdot x = x\} \subseteq G.$$
- Množica fiksnih točk *elementa $g \in G$ je*
$$\mathrm{fix}(g) = \{x \in X;\ g \cdot x = x\} \subseteq X.$$

Izrek 3.1 (O orbiti in stabilizatorju)**.** *Naj bo G grupa, X množica in $G \curvearrowright X$ delovanje grupe G na množici X. V tem primeru velja:*
$$|G| = |G \cdot x| \cdot |G_x|.$$

Tega izreka ne bomo dokazovali, njegov dokaz je prepuščen bralcu. Izrek bomo uporabil za dokaz Burnsideove leme.

3.1 Particije in relacije

Kasneje bomo pokazali, da nam orbite pri vsakem delovanju na množici razdelijo množico na manjše podmnožice tako, da je vsak element v natanko eni. To lahko definiramo v splošnem.

Definicija 3.3. *Naj bo X množica.* Razbitje *ali* particija *množice X je družina podmnožic $\mathcal{A} = \{A_i\}_{i \in I}$, kjer je $A_i \subseteq X$, za katero velja:*

- $\bigcup_{i \in I} \mathcal{A}_i = X$,
- $\forall i \neq j, \mathcal{A}_i \cap \mathcal{A}_j = \emptyset$.

Particijo množice porodi relacija s posebnimi lastnostmi.

Definicija 3.4. Relacija *R na množici M je podmnožica $R \subseteq M \times M$, kjer pišemo*
$$(x, y) \in R \Leftrightarrow xRy.$$

Ekvivalenčno relacijo R bomo zaradi preglednosti označevali z $\sim$.

Definicija 3.5. *Relacija $\sim\ \subseteq M \times M$, je* ekvivalenčna*, če velja:*

- *refleksivnost:* $\forall x \in M : x \sim x$,
- *simetričnost:* $\forall x, y \in M : x \sim y \Rightarrow y \sim x$,
- *tranzitivnost:* $\forall x, y, z \in M : x \sim y \wedge y \sim z \Rightarrow x \sim z$.

Pokazali bomo, da lahko na množici X, na kateri deluje grupa G, vpeljemo ekvivalenčno relacijo tako, da orbite delovanja tvorijo particijo.

Trditev 3.1. *Naj bo G grupa, X množica in $G \curvearrowright X$ delovanje grupe G na množici X. V tem primeru je družina orbit $\{G \cdot x;\ x \in X\}$ particija množice X.*

Dokaz. Naj bo $x \sim y$ relacija s predpisom $x \sim y \Leftrightarrow x \in G \cdot y$. Ker je orbita $G \cdot x = \{y \in X;\ \exists g \in G,\ y = g \cdot x\}$ in $\forall x, y, z \in X$ veljajo:

- refleksivnost: $x \sim x$, saj $e \cdot x = x$,
- simetričnost: $x \sim y \Leftrightarrow y \sim x$, saj

$$x \sim y \Leftrightarrow x = g \cdot y \Leftrightarrow g^{-1} \cdot x = y \Leftrightarrow y \sim x,$$

- tranzitivnost: $x \sim y \ \wedge\ y \sim z \Leftrightarrow x \sim z$, saj

$$(x = g_1 \cdot y,\ y = g_2 \cdot z) \Rightarrow g_1 \cdot g_2 \cdot z = x \Rightarrow x \sim z,$$

je relacija $x \sim y$ ekvivalenčna. Zato velja $y \in G \cdot x \Leftrightarrow G \cdot x = G \cdot y$, torej je družina podmnožic $\{G \cdot x;\ x \in X\}$ particija množice X. □

4 Burnsideova lema

Zdaj bomo spoznali način, s katerim lahko preštejemo število orbit. Čeprav se lema imenuje po Williamu Burnsidu, on ni bil tisti, ki jo je dokazal. Sam jo je navajal kot Frobeniusovo, toda formula je bila Cauchyju znana še pred tem. Zato se zanjo uporabljata tudi imeni Cauchy-Frobeniusova ali ne-Burnsideova lema.

Izrek 4.1 (Burnsideova lema)**.** *Naj bo G končna grupa, ki deluje na množici X. Potem je število orbit tega delovanja enako*

$$\#orbit = \frac{1}{|G|} \sum_{g \in G} |\operatorname{fix}(g)|.$$

Dokaz. Naj bosta G grupa in X množica, da velja $G \curvearrowright X$, in naj bo

$$\mathcal{A} = \{G \cdot x;\ x \in X\}$$

razbitje množice X, ki ga določajo orbite tega delovanja. Oglejmo si vsoto $\sum_{g \in G} |\operatorname{fix}(g)|$. Zapisali jo bomo kot vsoto po elementih množice X. Po definiciji množice fiksnih točk velja

$$\begin{aligned}\sum_{g \in G} |\operatorname{fix}(g)| &= \sum_{g \in G} |\{x \in X;\ g \cdot x = x\}| \\ &= |\{(g, x) \in G \times X;\ g \cdot x = x\}| \\ &= \sum_{x \in X} |\{g \in G;\ g \cdot x = x\}|.\end{aligned}$$

Ker $\{g \in G;\ g \cdot x = x\}$ predstavlja ravno predpis stabilizatorja G_x elementa $x \in X$, velja

$$\sum_{g \in G} |\operatorname{fix}(g)| = \sum_{x \in X} |G_x|.$$

Po izreku o orbiti in stabilizatorju za vsak element $x \in X$ velja

$$|G_x| = \frac{|G|}{|G \cdot x|},$$

iz česar sledi

$$\begin{aligned}\sum_{x\in X}|G_x| &= \sum_{x\in X}\frac{|G|}{|G\cdot x|}\\ &= |G|\sum_{x\in X}\frac{1}{|G\cdot x|}.\end{aligned}$$

Zdaj poglejmo, kaj predstavlja vsota $\sum_{x\in X}\frac{1}{|G\cdot x|}$. Z $|G\cdot x|$ je označena moč orbite delovanja elementa $x\in X$, ki določa razbitje $\mathcal{A}$. Ker je množica X unija vseh svojih orbit v razbitju $\mathcal{A}$, lahko vsoto po množici X razbijemo v vsote po vseh orbitah. Vsoto $\sum_{x\in X}\frac{1}{|G\cdot x|}$ lahko tako zapišemo kot

$$\begin{aligned}\sum_{x\in X}\frac{1}{|G\cdot x|} &= \sum_{A\in\mathcal{A}}\sum_{x\in A}\frac{1}{|G\cdot x|}\\ &= \sum_{A\in\mathcal{A}}1\\ &= \#\text{orbit}.\end{aligned}$$

Zaradi tranzitivnosti dobimo

$$\sum_{g\in G}|\operatorname{fix}(g)| = |G|\ \#\text{orbit},$$

kar zaključuje dokaz. □

5 Nazaj k zapestnicam

Vrnimo se na začetni problem.

5.1 Rešitev za 5 biserov v 3 barvah

Najprej obravnavajmo primer za $p=5$ in $n=3$. Opazimo, da sta zapestnici enaki natanko tedaj, ko sta v isti orbiti delovanja grupe D_{10}, ki deluje na množico zapestnic z rotacijami in zrcaljenji. Pri tem je

$$D_{10} = \{\mathrm{id}, r, r^2, r^3, r^4, z, zr, zr^2, zr^3, zr^4\}.$$

Zdaj lahko uporabimo Burnsideovo lemo, ki pravi, da je število orbit delovanja grupe na množico enako povprečnemu številu fiksnih točk. Ker je število zapestnic enako ravno številu orbit, je

$$\begin{aligned}\#\text{zapestnic} &= \#\text{orbit}\\ &= \frac{1}{|D_{10}|}\sum_{g\in D_{10}}|\operatorname{fix}(g)|\\ &= \frac{1}{10}\sum_{g\in D_{10}}|\operatorname{fix}(g)|.\end{aligned}$$

Preostane nam le, da preštejemo fiksne točke. Zanima nas, katere zapestnice bodo preslikave iz množice D_{10}, torej rotacije in zrcaljenja, ohranile.

Najprej si poglejmo identiteto id. Ker ta preslikava ohrani položaje biserov, fiksira vseh 3^5 možnih barvanj, torej je

$$|\operatorname{fix}(\mathrm{id})| = 3^5.$$

Če želimo, da rotacija ohranja barvanje, mora biti vsak biser enake barve kot biser, v katerega ga ta rotacija preslika. Edine fiksne točke so tako tista barvanja zapestnic, pri katerih so vsi biseri enake barve.[1] Iz tega sledi

$$|\operatorname{fix}(r)| = |\operatorname{fix}(r^2)| = |\operatorname{fix}(r^3)| = |\operatorname{fix}(r^4)| = 3.$$

Poglejmo še, kaj se zgodi pri zrcaljenju. Vsaka os, preko katere zrcalimo, poteka skozi natanko en biser, ostali biseri pa se bodo z zrcaljenjem paroma zamenjali. Da se bo barvanje po zrcaljenju ohranilo, je lahko biser, skozi katerega poteka os zrcaljenja, katerekoli barve, za ostale pa mora veljati, da sta bisera, ki se zamenjata, enake barve. Tako dobimo

$$|\operatorname{fix}(z)| = |\operatorname{fix}(zr)| = |\operatorname{fix}(zr^2)| = |\operatorname{fix}(zr^3)| = |\operatorname{fix}(zr^4)| = 3^3.$$

Na tak način pridemo do rešitve naloge za $p = 5$ in $n = 3$. Število zapestnic je v tem primeru enako

$$\#\text{zapestnic} = \frac{1}{10}\left(3^5 + 4 \cdot 3 + 5 \cdot 3^3\right) = 39.$$

5.2 Rešitev v splošnem

Problema se lotimo še v splošnem. Najprej obravnavamo primer, ko je p praštevilo. Zdaj imamo diedrsko grupo D_{2p}, zanima pa nas, na koliko različnih načinov lahko pobarvamo p biserov, pri čemer je p praštevilo, z n različnimi barvami. Identiteta id zdaj fiksira n^p, vsaka rotacija n in vsako zrcaljenje $n^{\frac{p+1}{2}}$ barvanj. Iz tega sledi, da je

$$\#\text{zapestnic} = \frac{1}{2p}\left(n^p + (p-1)\, n + p n^{\frac{p+1}{2}}\right).$$

Do zdaj smo upoštevali, da je število biserov p praštevilo. Razmislimo še, kaj se zgodi, ko imamo m biserov in n barv, pri čemer je m poljubno naravno število, večje od 2. Opazimo, da rotacij ne moremo obravnavati enako kot v prejšnjem primeru. Naj bo t tako naravno število, da velja $t \mid m$. Rotacija r^t fiksira vse zapestnice, ki imajo periodo t biserov. Potem moramo izbrati barvo za teh t biserov, kar naredimo na n^t načinov. Pri zrcaljenju je treba dodatno upoštevati le, da imamo zdaj lahko sodo število biserov, zato lahko gre os zrcaljenja v tem primeru bodisi skozi dva bodisi skozi nobenega od biserov. Tako z obravnavanjem deliteljev števila m rešimo nalogo še za n barv in m biserov, kjer sta n in m poljubni naravni števili.

6 Zaključek

Na videz kombinatorično nalogo nam je uspelo rešiti s pomočjo teorije grup. Spoznali smo osnovne algebrske strukture, kot so polgrupe, monoidi in grupe, posebej smo omenili simetrično in diedrsko grupo. Prav tako smo opisali homomorfizme ter delovanje grupe na množici. Tako smo prišli do Burnsideove leme, ki je bila ključna za rešitev problema z zapestnicami.

Literatura

[1] M. Brešar, *Uvod v algebro*, Matematični rokopisi (številka 26), DMFA - založništvo, Ljubljana, 2018.

[2] zapiski s predavanj Igorja Klepa pri predmetu Algebra 3, Fakulteta za matematiko in fiziko, Univerza v Ljubljani, 2020.

[1] To lahko sklepamo, ker je p praštevilo. Isti sklep deluje za praštevila, večja od 2. V splošnem to ne deluje, npr. za $p = 6$ vidimo, da lahko izmenjaje pobarvamo bisere z dvema različnima barvama in bo rotacija r^2 prvo zapestnico preslikala v drugo, ki ji je enaka, saj velja $2 \mid 6$.

Končni avtomati

Matic Bratina, Aleksander Kalacun, Vasja Žorž
Mentor: *Nejc Zajc*

Povzetek

V članku so predstavljeni koncepti formalnega jezika in končnih avtomatov. Opisano je delovanje končnih avtomatov in njihove lastnosti. Povezava med njimi in formalnimi jeziki je pojasnjena na intuitiven in dostopen način.

1 Uvod

Končni avtomati so končne množice stanj in usmerjenih povezav. So ključni računalniški modeli za prepoznavanje vzorcev in reševanje problemov s formalnimi jeziki. Obstajata dve vrsti; deterministični in nedeterministični končni avtomati. Njihovo razumevanje je temelj za številne aplikacije, kot so prevajalniki in obdelava jezika. Avtomate lahko predstavimo z nazornim vizualnim gradivom.

2 Jeziki

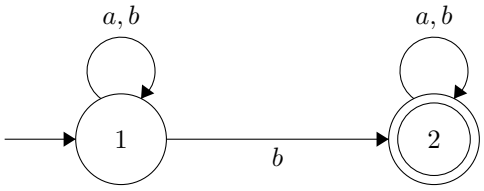
Naj bo A končna abeceda črk. Beseda $u = a_1 a_2 \cdots a_n$ je končen niz črk $a_i \in A$ za vse $i \in \{1, 2, \ldots, n\}$. Z $|u| = n$ označimo dolžino besede, ki je enaka številu črk v besedi. Besedi, ki ne vsebuje nobene črke, pravimo prazna beseda in jo označimo z ε. Množico vseh besed nad abecedo A označimo z A^*. Podmnožici $L \subseteq A^*$ rečemo jezik.

Stik besed, ki ga pišemo kot množenje, je operacija združitve dveh besed. Za besedi $u = a_1 a_2 \cdots a_n$ in $v = b_1 b_2 \cdots b_m$ je njun stik beseda

$$u \cdot v = a_1 \cdots a_n b_1 \cdots b_m \in A^*.$$

2.1 Operacije na jezikih

Oglejmo si, kako lahko z jeziki računamo. Izvajamo lahko operacije, značilne za množice, kot sta unija in presek. Standardno ju označimo z $\cup$ in $\cap$. Za lažjo berljivost bomo operacijo unije zapisovali kot $+$. Nevtralen element unije je prazna množica $\emptyset$, ki jo označimo z 0.



Slika 1: Primer diagrama končnega avtomata.

Množenje jezikov L_1 in L_2 definiramo kot operacijo, ki nam da nov jezik, v katerem so vse besede, za katere je prvi del beseda iz L_1 in drugi del beseda iz L_2. Torej je $L_1 \cdot L_2 = \{uv \mid u \in L_1, v \in L_2\}$. Nevtralen element množenja je jezik s prazno besedo $\{\varepsilon\}$, ki ga označimo z 1.

Z definicijo množenja lahko vpeljemo tudi operacijo potenciranja. Definiramo jo kot

$$L^0 = 1, \qquad L^1 = L, \qquad L^n = L \cdot L^{n-1} \quad \text{za vse } n \geq 1.$$

Definiramo še operaciji

$$L^* = 1 + L + L^2 + L^3 + \cdots \quad \text{in} \quad L^+ = L + L^2 + L^3 + \cdots .$$

Za omenjene operacije na jezikih veljajo naslednje lastnosti. Unija, presek in množenje so asociativne operacije nad jeziki. Velja tudi distributivnost množenja nad unijo. Če preverimo še komutativnost, ugotovimo, da je poleg unije tudi presek komutativen. Pri množenju vidimo, da je pri obliki besede pomembno, katera sestavlja začetek produkta besed in katera konec, tako da množenje ni komutativna operacija.

Oglejmo si še operacijo, nasprotno množenju. Kvocient je operacija, ki jo za besedo u in jezik L zapišemo kot $u^{-1}L$. Kvocient je jezik, v katerem so končnice vseh besed jezika L, ki se začnejo z u, torej

$$u^{-1}L = \{v \in A^* \mid uv \in L\}.$$

Primer operacije kvocient je

$$(aba)^{-1}\{abaa, aabbb, abab\} = \{a, b\}.$$

Množica vseh jezikov je potenčna množica $P(A^*)$. Oglejmo si množico jezikov, ki jih lahko zgradimo s končnim številom osnovnih operacij iz jezikov, ki vsebujejo le eno črko.

Definicija 2.1. *Množica $F \subseteq P(A^*)$* ***racionalnih jezikov*** *je najmanjša množica jezikov, za katero velja:*

- *F vsebuje 0 in $\{a\}$ za vsak $a \in A$,*
- *F je zaprta za končne unije, produkte in *, torej*

$$\forall L_1, L_2 \in F: \quad L_1 + L_2 \in F, \quad L_1 \cdot L_2 \in F \quad \text{in} \quad L_1^* \in F.$$

Poljuben končen jezik je racionalen, saj velja

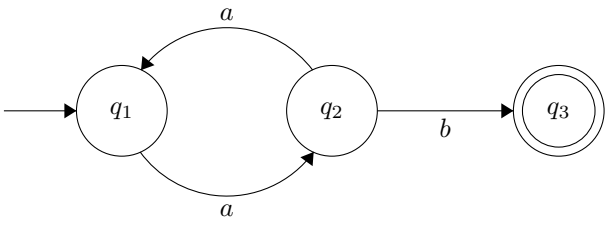
$$\{u_1, u_2, \ldots, u_n\} = \{u_1\} \cup \{u_2\} \cup \{u_3\} \cup \ldots \cup \{u_n\}.$$

Recimo, da je L_1 jezik besed sode dolžine abecede $A = \{a, b\}$. Naj bo jezik X takšen, da so v njem vse različne besede dolžine 2 iz A. V našem primeru je $X = \{aa, ab, ba, bb\}$. Velja, da je dolžina zmnožka poljubnih dveh besed iz X soda. Če dobljen produkt še naprej množimo z besedami iz X, bo dobljen produkt vedno sode dolžine. Tako lahko množico vseh možnih besed sode dolžine zapišemo kot vsoto potenc

$$L_1 = 1 + X + X^2 + X^3 + \cdots ,$$

kjer so v X^2 vse besede dolžine 4, v X^3 so besede dolžine 6 in podobno. Spomnimo se, da je to enako X^*. Označimo z L_2 še jezik besed lihe dolžine. Zapišemo ga lahko kot produkt jezika L_1 z abecedo A. Tako je dolžina vseh besed za eno večja oziroma liha. Velja

$$L_2 = L_1 \cdot A = (1 + X + X^2 + X^3 + \cdots) \cdot A.$$



Slika 2: Primer končnega avtomata z $I = \{q_1\}$ in $F = \{q_3\}$.

3 Končni avtomati

Končni avtomat je zgrajen iz stanj in usmerjenih prehodov med stanji. Formalno je avtomat $\mathcal{A}$ urejena peterica $\mathcal{A} = (A, Q, E, I, F)$. Stanja avtomata tvorijo množico $Q = \{q_1, q_2, \ldots, q_n\}$. Množica E je množica prehodov med stanji avtomata $E \subseteq Q \times A \times Q$. Avtomat lahko predstavimo z diagramom, kot je prikazano na sliki 2. Na diagramih stanja označimo s krogi, prehode pa s puščico med dvema stanjema in črko, za katero se prehod izvede. Označimo še množici začetnih in končnih stanj $I, F \subseteq Q$.

Definicija 3.1. ***Pot*** *v $\mathcal{A}$ je zaporedje stanj $q_1, q_2, \ldots, q_n$ s prehodi med njimi $(q_1, a_1, q_2), \ldots, (q_{n-1}, a_{n-1}, q_n)$ za neke črke $a_1, \ldots, a_{n-1}$.*

Beseda $a_1 \cdots a_{n-1}$ je ***oznaka poti****. Beseda je* ***sprejeta*** *s strani avtomata $\mathcal{A}$, če je oznaka poti iz začetnega stanja $q_i \in I$ v končno stanje $q_f \in F$. Takšna pot je v avtomatu $\mathcal{A}$ uspešna.*

Jezik, ki je prepoznan s strani avtomata $\mathcal{A}$, označimo z

$$\mathcal{L}(\mathcal{A}) = \{v \in A^* \mid \mathcal{A} \text{ sprejme besedo } v\}.$$

Za jezik L rečemo, da je prepoznaven, če obstaja končni avtomat $\mathcal{A}$, da velja $L = \mathcal{L}(\mathcal{A})$.

Lema 3.1 (Iteracijska lema)**.** *Naj bo $\mathcal{A}$ poljuben končni avtomat in $L = \mathcal{L}(\mathcal{A})$. Potem obstaja takšno naravno število $n \in \mathbb{N}$, da lahko vsak $u \in L$, $|u| \geq n$, zapišemo v obliki $u = xyz$, kjer so $x,\ y,\ z \in A^*$, $|xy| \leq n$ in $y \neq \varepsilon$. Beseda xy^kz je element L za vsak $k \in \mathbb{N}$.*

Dokaz. Naj bo $L = \mathcal{L}(\mathcal{A})$, kjer je $\mathcal{A} = (A, Q, E, I, F)$ končni avtomat. Naj bo $n = |Q|$ in beseda $u = a_1a_2 \cdots a_m \in L$, tako da je $m \geq n$. Ker je $u \in L$, obstaja pot od $q_- \in I$ do $q_f \in F$, ki ima oznako u.

Slika 3: Pot iz dokaza leme 3.1.

Ker je stanj na poti $m + 1 > n$, se po Dirichletovem principu gotovo vsaj eno izmed stanj avtomata $\mathcal{A}$ na tej poti ponovi. Naj bo i najmanjši indeks, da velja $q_i = q_j$ za $j > i$. Za x, y in z vpeljemo

$$\begin{aligned} x &= a_1 \cdots a_{i-1}, \\ y &= a_i \cdots a_{j-1}, \\ z &= a_j \cdots a_m. \end{aligned}$$

Velja $|xy| = j - 1 \leq n$, saj je i najmanjši indeks ponovitve, y pa ni prazna beseda, ker je $j > i$. Ponovitev stanja pomeni, da imamo na poti cikel. Ponavljanje cikla ne vpliva na to, da se pot začne v začetnem in konča v končnem stanju. Besedo y smo definirali tako, da je oznaka tega cikla. Torej za poljuben $k \in \mathbb{N}_0$ velja $xy^kz \in L$. □

Oglejmo si primer uporabe leme, ki pokaže, da jezik $L = \{a^n b^n \mid n \geq 1\}$ ni prepoznaven. To storimo s protislovjem. Denimo, da je L prepoznaven. Po lemi 3.1 obstaja tak $n_0 \in \mathbb{N}$, da lahko besedo $u = a^{n_0}b^{n_0} \in L$ zapišemo kot stik besed x, y, z, tako da je $u = xyz$. Velja $|a^{n_0}b^{n_0}| = 2n_0 \geq n_0$, ter $|xy| \leq n_0$. Torej tako x kot y vsebujeta samo črko a, torej

$$\begin{aligned} x &= a^t, \\ y &= a^s, \\ z &= a^{n_0-(t+s)}b^{n_0}, \end{aligned}$$

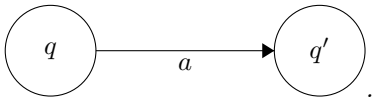
saj je $s + t \leq n_0$. Prav tako je $s \neq 0$, ker velja $y \neq \varepsilon$. Ker se pri potenciranju besede y spreminja le število a-jev, ima beseda $xy^k z$ različno število a-jev in b-jev za $k \neq 1$. Ta beseda tako ni v jeziku L, kar je v protislovju z lemo in jezik ni prepoznaven.

4 Determinizacija končnega avtomata

Oglejmo si nekaj vrst končnih avtomatov. Smiselno si je želeti, da lahko v avtomatu od poljubnega stanja z dano besedo pridemo le do enega stanja. Avtomat, ki izpolnjuje to lastnost, je deterministično.

Definicija 4.1. *Avtomat $\mathcal{A} = (A, Q, E, I, F)$ je **deterministično**, če velja*

- $|I| = 1$,
- *za vsak $q \in Q$ in za vsak $a \in A$ obstaja največ en prehod oblike*



V tem primeru zapišemo $q' = q \cdot a$.

Definicija 4.2. *Avtomata $\mathcal{A}$ in $\mathcal{A}'$ sta **ekvivalentna**, če prepoznata isti jezik, torej velja*

$$\mathcal{L}(\mathcal{A}) = \mathcal{L}(\mathcal{A}').$$

Trditev 4.1. *Vsak avtomat je ekvivalenten nekemu determinističnemu avtomatu.*

Dokaz trditve uporabi potenčno konstrukcijo, ki zgradi deterministično avtomat, ki je ekvivalenten začetnemu. Naj bo $\mathcal{A} = (A, Q, E, I, F)$ poljuben avtomat. Zgradimo deterministično avtomat

$$\mathcal{A}' = (A, P(Q), E', I, \mathcal{F}),$$

kjer je $P(Q)$ potenčna množica množice Q. Stanja avtomata $\mathcal{A}'$ so torej množice stanj avtomata $\mathcal{A}$. Za novo stanje $P \in P(Q)$ in črko $a \in A$ vpeljemo $P \cdot a$ kot množico prvotnih stanj $q \in Q$, v katera lahko pridemo iz poljubnega stanja $p \in P$ preko prehoda $(p, a, q) \in E$, torej

$$P \cdot a = \{q \in Q \mid \exists\, p \in P :\ (p, a, q) \in E\}.$$

Množica prehodov potenčne konstrukcije je izbrana tako, da omogoča vse prehode, ki so bili na voljo v začetnem avtomatu $\mathcal{A}$

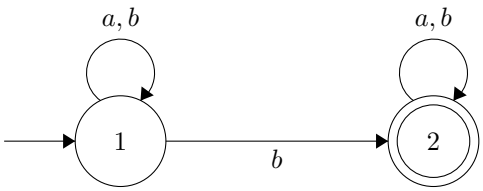
$$E' = \{(P, a, P \cdot a) \mid P \in P(Q), a \in A\}.$$

Končna stanja potenčne konstrukcije so tiste množice, ki vsebujejo katerega od končnih stanj avtomata $\mathcal{A}$,

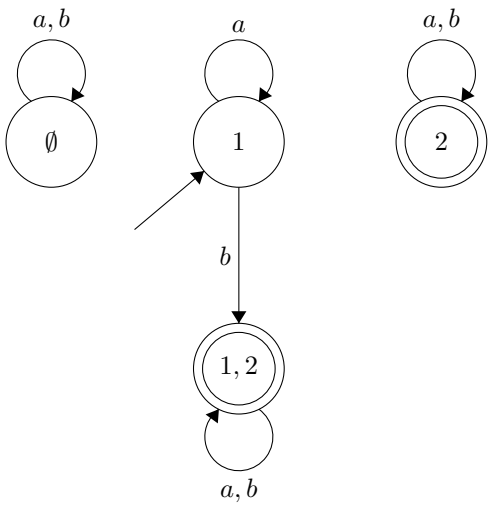
$$\mathcal{F} = \{P \subseteq Q \mid P \cap F \neq \emptyset\}.$$

Za potenčno konstrukcijo se izkaže, da prepozna isti jezik kot začetni avtomat, torej je $\mathcal{L}(\mathcal{A}) = \mathcal{L}(\mathcal{A}')$.

Na primeru si oglejmo, kako deluje potenčna konstrukcija. Slika 4 prikazuje avtomat $\mathcal{A}$. S potenčno konstrukcijo lahko zgradimo deterministično avtomat, prikazan na sliki 5, ki je ekvivalenten avtomatu $\mathcal{A}$.



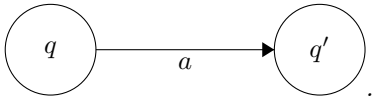
Slika 4: Avtomat $\mathcal{A}$.



Slika 5: Deterministični avtomat, ekvivalenten avtomatu $\mathcal{A}$.

Definicija 4.3. *Avtomat ima lahko naslednje lastnosti.*

- *Avtomat $\mathcal{A}$ je **poln**, če za vsak $q \in Q$ in za vsak $a \in A$ obstaja vsaj en prehod oblike*



.

- *Avtomat $\mathcal{A}$ je **dostopen**, če za vsak $q \in Q$ obstaja pot iz nekega začetnega stanja $q_i \in I$ v q.*
- *Avtomat $\mathcal{A}$ je **standarden**, če se noben prehod ne konča v začetnem stanju.*

Opazimo, da je potenčna konstrukcija poln in deterministično avtomat. Z novo konstrukcijo lahko ohranimo prepoznani jezik tudi pri prehodu na standarden avtomat.

Trditev 4.2. *Vsak deterministično avtomat je ekvivalenten nekemu standardnemu determinističnemu avtomat.*

Tudi tokrat le podamo konstrukcijo, ki jo uporabi dokaz, a ekvivalence med začetnim in novim avtomatom ne dokažemo. Naj bo $\mathcal{A} = (A, E, Q, q_-, F)$ deterministično avtomat. Če avtomat $\mathcal{A}$ ni standarden, dodamo novo stanje $p \notin Q$. Definiramo $\mathcal{A}' = (A, Q \cup \{p\}, E', p, F')$, kjer sta

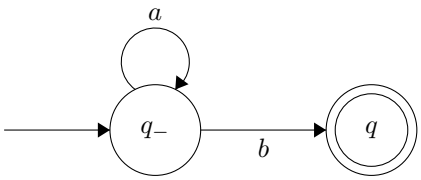
$$E' = E \cup \{(p, a, q) \mid (q_-, a, q) \in E\},$$
$$F' = \begin{cases} F; & q_- \notin F \\ F \cup \{p\}; & q_- \in F \end{cases}.$$

Avtomata $\mathcal{A}$ in $\mathcal{A}'$ sta ekvivalentna.

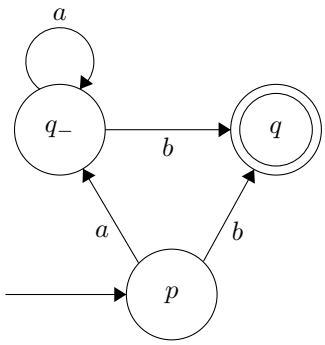
Na primeru si oglejmo še, kako deluje gradnja standardnega avtomata. Na sliki 6 vidimo deterministično avtomat $\mathcal{A}$, na sliki 7 pa standardni deterministični avtomat, ki je ekvivalenten avtomatu $\mathcal{A}$.

5 Konstrukcije avtomatov

Pokazali bomo, da so racionalni jeziki natanko prepoznavni jeziki. Najprej pokažemo, da so vsi racionalni jeziki tudi prepoznavni. V ta namen vse operacije, ki gradijo racionalne jezike, ponazorimo na avtomatih.



Slika 6: Deterministično avtomat $\mathcal{A}$.



Slika 7: Standardni deterministični avtomat ekvivalenten avtomatu $\mathcal{A}$.

5.1 Unija

Naj avtomat $\mathcal{A}_1 = (A_1, Q_1, E_1, I_1, F_1)$ prepozna jezik L_1 in naj avtomat $\mathcal{A}_2 = (A_2, Q_2, E_2, I_2, F_2)$ prepozna jezik L_2. Da dobimo avtomat $\mathcal{A}_U$, ki prepozna unijo jezikov L_1 in L_2, avtomata $\mathcal{A}_1$ in $\mathcal{A}_2$ preprosto združimo v enega. Velja torej, da avtomat

$$\mathcal{A}_U = (A_1 + A_2, Q_1 + Q_2, E_1 + E_2, I_1 + I_2, F_1 + F_2)$$

prepozna jezik $L_1 \cup L_2$.

5.2 Komplement

Naj deterministično in poln avtomat $\mathcal{A} = (A, Q, E, I, F)$ prepozna jezik L. Komplement jezika L je jezik L^C, v katerem so vse besede, ki jih ni v jeziku L. Avtomat, ki prepozna jezik L^C, ne sme sprejeti nobene besede, ki jo sprejme $\mathcal{A}$, mora pa sprejeti vse besede, ki jih avtomat $\mathcal{A}$ ne. To lahko dosežemo s tem, da zamenjamo končna stanja. To pomeni, da tista stanja, ki so v $\mathcal{A}$ končna, v $\mathcal{A}_C$ niso in obratno. Velja torej, da avtomat

$$\mathcal{A}_C = (A, Q, E, I, Q \setminus F)$$

prepozna jezik L^C.

5.3 Zvezdica

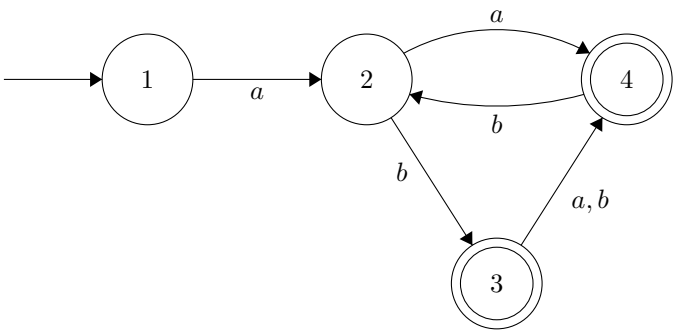
Naj deterministično in standarden avtomat $\mathcal{A} = (A, Q, E, q_-, F)$ prepozna jezik L. Če želimo zgraditi avtomat $\mathcal{A}_Z$, ki bo prepoznal jezik L^*, mora ta imeti možnost, da sprejme zaporedje besed iz jezika L. To lahko dosežemo tako, da dodamo prehode iz stanj, ki vodijo v končna stanja, nazaj do začetnega stanja. Primer te konstrukcije za končni avtomat s slike 8 vidimo na sliki 9. Natančneje, dodati moramo prehode oblike (q, a, q_-) za $q \in Q$ in $a \in A$, če in samo če obstaja tak prehod (q, a, q'), da je $q' \in F$. Tako avtomat

$$\mathcal{A}_Z = (A, Q, E', q_-, F \cup q_-),$$

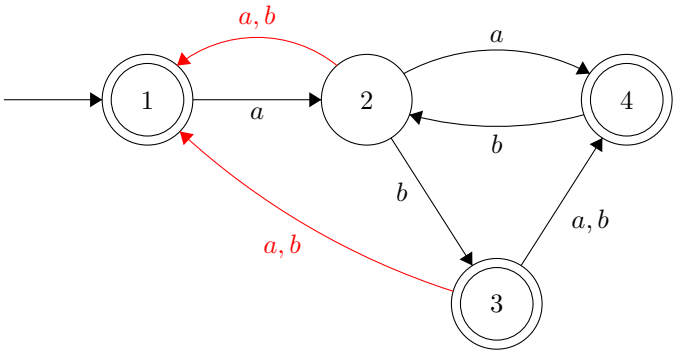
kjer velja $E' = E + \{(q, a, q_-) \mid \exists (q, a, q') \text{ za } q' \in F\}$, prepozna jezik L^*.

5.4 Produkt

Naj avtomat $\mathcal{A}_1 = (\mathcal{A}_1, Q_1, E_1, I_1, F_1)$ prepozna jezik L_1 in deterministično standarden avtomat $\mathcal{A}_2 = (\mathcal{A}_2, Q_2, E_2, q_-, F_2)$ prepozna jezik L_2. V produktu jezikov L_1 in L_2 so vse kombinacije besed, v katerih je prvi del besede iz jezika L_1 in drugi del besede iz jezika L_2. Zgraditi želimo avtomat, ki sprejme besedo,



Slika 8: Avtomat $\mathcal{A}$, ki prepozna jezik L.



Slika 9: Avtomat $\mathcal{A}_Z$, ki prepozna jezik L^*.

sestavljeno iz besede, ki jo sprejme avtomat $\mathcal{A}_1$, in besede, ki jo sprejme avtomat $\mathcal{A}_2$. Končna stanja avtomata $\mathcal{A}_1$ moramo združiti z avtomatom $\mathcal{A}_2$ tako, da nimamo nobenega dodatnega prehoda, saj bi nam ta med deli besed dodal črko. Zato iz avtomata $\mathcal{A}_2$ odstranimo začetno stanje q_- in prehode, ki so izhajali iz začetnega stanja, povežemo tako, da se začnejo že v končnih stanjih $\mathcal{A}_1$. Primer te konstrukcije za končna avtomata s slike 10 vidimo na sliki 11. Avtomat $\mathcal{A}_P$, ki prepozna zmožek jezikov $L_1 \cdot L_2$, je tako

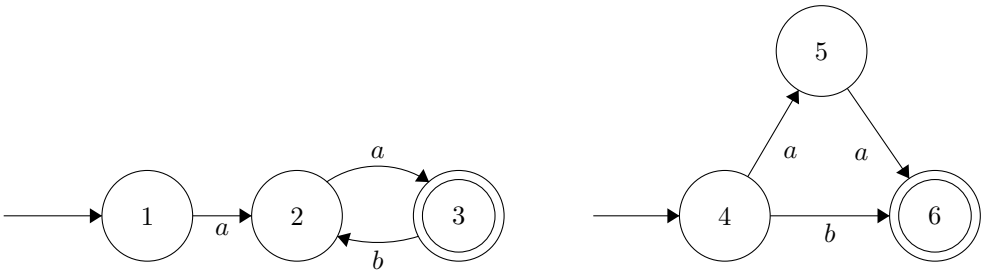
$$\mathcal{A}_P = (A_1 \cup A_2, Q', E', I', F'),$$

kjer so

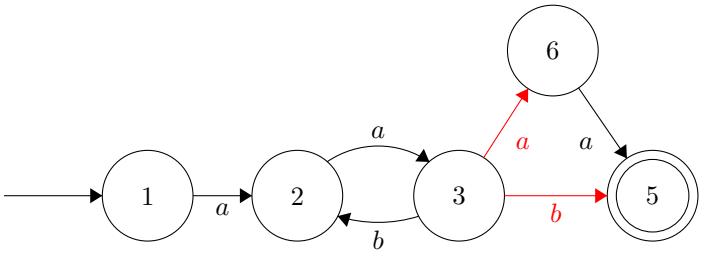
- $Q' = Q_1 + Q_2 \setminus \{q_-\}$,
- $E' = E_1 + \{(q, a, q') \in E_2 \mid q \neq q_-\}$
  $+ \{(q, a, q') \mid q \in F_1 : \exists (q_-, a, q') \in E_2\}$,
- $I' = I_1$,
- $F' = \begin{cases} F_2 & ; q_- \notin F_2 \\ F_1 + F_2 \setminus \{q_-\} & ; q_- \in F_2 \end{cases}$.

5.5 Kvocient

Naj deterministično standarden avtomat $\mathcal{A} = (A, Q, E, q_-, F)$ prepozna jezik L in naj bo $u \in A^*$ poljubna beseda. Zgraditi želimo avtomat, ki prepozna jezik $u^{-1}L$. V avtomatu $\mathcal{A}$ moramo obiti del, ki prepozna



Slika 10: Avtomata, ki prepoznata jezika L_1 in L_2.



Slika 11: Avtomat $\mathcal{A}_P$, ki prepozna jezik $L_1 \cdot L_2$.

besedo u, ko se pojavi na začetku. To naredimo tako, da začetno stanje avtomata $\mathcal{A}$ prestavimo v $q_- \cdot u$. Velja torej, da avtomat

$$\mathcal{A}_K = (A, Q, E, q_- \cdot u, F)$$

prepozna jezik $u^{-1}L$.

6 Sistem enačb jezikov

Pri delu na projektu smo pokazali tudi, da je jezik, ki ga prepozna poljuben avtomat, racionalen jezik. To smo storili tako, da smo definirali nekaj jezikov, ki so odvisni le od avtomata. Z njimi smo sestavili sistem enačb, katerega rešitev je enolična. Ta rešitev nam da jezik, ki ga avtomat prepozna. Ker je rešitev sestavljena iz končnih operacij množenja, unije in zvezdice, je ta jezik racionalen.

7 Zaključek

Ogledali smo si, kaj so formalni jeziki in definirali racionalne jezike. Spoznali smo končne avtomate in njihove različne lastnosti. Osrednji del projekta smo namenili premisleku, da so racionalni jeziki natanko jeziki, ki jih prepozna nek končni avtomat.

Literatura

[1] J.-E. Pin, *Mathematical foundations of automata theory*, version of February 18, 2022

[2] Zapiski predavanj predmeta izbrana poglavja iz diskretne matematike: končni avtomati, profesorice dr. Ganne Kudryavtseve (Univerza v Ljubljani, Fakulteta za matematiko in fiziko, študijsko leto 2022/2023)

Kompaktnost v $\mathbb{R}^n$

Katarina Grilj, Ema Hojan, Matija Skrt
Mentor: *Jan Genc*

Povzetek

V članku sta definirani topologija in kompaktnost ter predstavljene lastnosti kompaktnih prostorov. Definirana je produktna topologija in dokazana ekvivalenca med kompaktnostjo množice in zaprtostjo ter omejenostjo množice v $\mathbb{R}^n$.

1 Uvod

Moj narod je že od nekdaj gojil borbenost. Borbenost ni lastnost množic, kompaktnost pa je. Zelo zagnani, da bi se naučili uporabljati lastnosti kompaktnih množic in končno razumeli slavno šalo o fizikih, smo se podali na pot odkrivanja MaRSovskega sveta topologije.
V matematiki se pri dokazovanju nečesa specifičnega pogosto splača ogledati si posplošitev določenih akcidenc strukture, ki nas zanima. Ko se osredotočimo na bistveno lastnost objekta in iz njega odstranimo vse odvečno in manj pomembno, postanejo naš miselni tok in logične kreacije, ki iz njega sledijo, veliko jasnejše, preprostejše in lepše, kot smo si lahko predstavljali na začetku, ko smo kot noj tiščali glavo v zemljo ter poskušali tam odkriti nekaj, kar sedaj dojamemo za veliko večje, pomembnejše in bolj estetsko. Ko se, tako rekoč, povzpnemo visoko na goro in ugledamo bistrejše pojmovanje zanimanega, pa se nam odpre pogled tudi na specifične primere, ki so sprožili našo radovednost in interes.
A od kod motivacija za preučevanje kompaktnosti? Od kod sploh definicija kompaktnosti? Za zainteresiranega bralca smo med literaturo vključili povezavo do **spletnega članka**, ki poskuša odgovoriti na prav to vprašanje in ga priporočamo vsem, ki jih zanima motivacija za tem nenavadnim konceptom. Kot primer motivacije, ki se nam zdi posebej močan, navajamo naslednjo lemo, ki jo je dokazal francoski matematik Émile Borel leta 1894 in jo tudi mi dokažemo v članku:

Lema 1.1. *Če zaprt interval $[a, b]$ povsem prekrijemo s poljubno neskončno množico A odprtih intervalov, ki imajo lahko med seboj tudi neprazne preseke, lahko vedno najdemo končno podmnožico množice A, ki prav tako pokrije celoten interval $[a, b]$.*

Iz te izredno zanimive in elegantne lastnosti zaprtih intervalov pa lahko, kot bomo videli kasneje, ustvarimo splošno lastnost topološkega prostora, ki jo imenujemo kompaktnost. Vprašamo se, ali morda pod to lastnostjo specifičnega objekta v $\mathbb{R}$ leži nekaj zares lepega tudi v splošnem? V ta namen si bomo najprej pogledali nekatere splošne lastnosti topoloških prostorov in se šele nato spustili v intuitivni prostor $\mathbb{R}^n$, kjer bomo spoznali, kako se obča lepota topologije prenese v vsakdanji evklidski prostor, katerega globlje skrivnosti si tako zelo želimo odkriti.

2 Topologija

V tem poglavju bomo navedli in na kratko raziskali osnove topologije, z namenom, da bralca seznanimo s strukturami, ki jih bomo pozneje potrebovali.
Za začetek si oglejmo definicijo topologije.

Definicija 2.1. *Naj bo X neprazna množica in τ družina množic, tako da $\tau \subseteq \mathcal{P}(X)$, za katero velja:*

- *množici $\emptyset$ in X sta v τ,*
- *kadarkoli sta dve ali več množici v τ, potem je tudi njuna/njihova unija v τ,*
- *analogno velja za končen presek množic v τ.*

*Z oznako (X, τ) označujemo **topološki prostor** X **s topologijo** τ. Množice v τ imenujemo **odprte množice**, elemente množice X pa **točke** topološkega prostora. Komplementom odprtih množic pravimo **zaprte množice**.*

Oglejmo si nekaj zgledov, ki nam bodo nekoliko razsvetlili to zapleteno definicijo.

Zgled 2.1. *Topologijo $\tau = \{X, \emptyset\}$, definirano na množici X, imenujemo trivialna topologija.*

Zgled 2.2. *Topologijo $\tau = \mathcal{P}(X)$, definirano na množici X, imenujemo diskretna topologija.*

Zgled 2.3. *Topološki prostor $\{X, \tau\}$, kjer je $X = \{a, b\}$ in $\tau = \{X, \emptyset, \{a\}\}$, imenujemo **prostor Sierpińskega**.*

Pogosto želimo raziskovati le lastnosti nekega podprostora danega topološkega prostora. Naslednja definicija in izrek nam bosta pokazala, kako lahko topologijo definirano na celotnem prostoru na enostaven način priredimo na želen podprostor.

Definicija 2.2. *Naj bo (X, τ) topološki prostor in $A \subseteq X$. Če na A definiramo topologijo τ_A kot množico vseh presekov A z vsemi odprtimi množicami v X, potem (A, τ_A) imenujemo **topološki podprostor** prostora (X, τ).*

Izrek 2.1. *Topološki podprostor (A, τ_A) je topološki prostor. Topologiji τ_A pravimo **podedovana topologija**.*

Dokaz. Trditev dokažemo tako, da po vrsti preverimo, ali (A, τ_A) zadošča definiciji topološkega prostora:

- Očitno sta prazna množica in množica A v τ_A.
- Denimo, da je $\bigcup_{\lambda \in \Lambda} M_\lambda$ unija odprtih množic v A. Iz definicije podedovane topologije sledi, da za vsak M_λ obstaja tak $N_\lambda \in \tau$, da velja $N_\lambda \cap A = M_\lambda$. Velja torej $\bigcup_{\lambda \in \Lambda} M_\lambda = \bigcup_{\lambda \in \Lambda} (A \cap N_\lambda) = A \cap \bigcup_{\lambda \in \Lambda} N_\lambda$. Ker pa je $\bigcup_{\lambda \in \Lambda} N_\lambda$ odprta v X, sledi, da je $\bigcup_{\lambda \in \Lambda} M_\lambda \in \tau_A$, kar smo želeli dokazati.
- Za končne preseke je dokaz analogen.

□

Zgled 2.4. *Podprostori trivialnega prostora so trivialni, podprostori diskretnega pa diskretni.*

Pri nadaljnem dokazovanju bomo potrebovali tudi naslednji pojem:

Definicija 2.3. *Naj bo (X, τ) topološki prostor. Če za vsaki različni točki a in b v X obstajata odprti množici U in V, tako da $a \in U$, $b \in V$ in $U \cap V = \emptyset$, potem je (X, τ) **Hausdorffov prostor** oziroma T_2. Ker vsaki dve točki v X zadoščata opisanemu kriteriju pravimo, da lahko poljubni točki **ostro ločimo**.*

Zgled 2.5. *Preverimo ali so naslednji prostori Hausdorffovi:*

- *Če $|X| \geqslant 2$, trivialni prostor ni Hausdorffov, saj bi po definiciji Hausdorffovega prostora morali ostro ločiti poljubni različni točki, vsaka pa ima le eno odprto množico, v kateri je vsebovana - X. Protislovje.*
- *Diskretni prostor je Hausdorffov, ker so v njem vse točke odprte množice.*
- *Prostor Sierpińskega ni Hausdorffov prostor, saj točk a in b ne moremo ostro ločiti.*

Preden našo pozornost usmerimo na kompaktnost, si oglejmo še naslednjo definicijo, ki nam bo prišla zelo prav v prihodnje.

Definicija 2.4. *Naj bo (X, τ) poljuben topološki prostor. Pravimo, da množica M tvori* ***bazo topologije*** *τ, če za vsako odprto množico A obstaja podmnožica N množice M, da lahko A zapišemo kot unijo elementov množice N.*

3 Kompaktnost

V tem delu članka si bomo v skladu z našim končnim ciljem pogledali splošno definicijo kompaktnosti. Spoznali bomo tudi nekaj lastnosti kompaktnih prostorov, ki nam bodo pokazali vrednost preučevanja kompaktnosti v splošnem.
Oglejmo si najprej definicijo odprtega pokritja, podpokritja in nadpokritja.

Definicija 3.1. *Naj bo X množica in U_λ take odprte podmnožice množice X, da velja $X = \bigcup_{\lambda\in\Lambda} U_\lambda$. Potem je $\{U_\lambda \mid \lambda \in \Lambda\}$* ***odprto pokritje*** *množice X.*
Če velja $X = \bigcup_{\delta\in\Delta} U_\delta$ za neko množico $\Delta \subseteq \Lambda$, imenujemo $\{U_\delta \mid \delta \in \Delta\}$ ***podpokritje*** *pokritja $\{U_\lambda \mid \lambda \in \Lambda\}$ prostora X.*
Nazadnje, če velja $A \subseteq \bigcup_{\gamma\in\Gamma} V_\gamma$, za neke odprte množice $V_\gamma \in X$, pravimo množici $\{V_\gamma \mid \gamma \in \Gamma\}$ ***odprto nadpokritje*** *prostora (A, τ_A), kjer je τ_A seveda podedovana topologija.*

Sedaj lahko končno definiramo kompaktnost.

Definicija 3.2. *Naj bo (X, τ) topološki prostor. Če za vsako odprto pokritje $\{U_\lambda \mid \lambda \in \Lambda\}$ prostora X obstaja njegovo končno podpokritje $\{U_{\lambda_1}, U_{\lambda_2}, \ldots, U_{\lambda_n}\}$ prostora X, pravimo, da je (X, τ)* ***kompakten prostor****.*

Opomba 3.1. *Naj bo A podprostor topološkega prostora (X, τ) s podedovano topologijo τ_A. Prostor (A, τ_A) je kompakten natanko tedaj, ko ima vsako odprto nadpokritje $P \subseteq \tau$ prostora A končno podpokritje $Q \subseteq \tau$.*
Ta ekvivalenca velja, saj vsakemu pokritju $\bigcup_{\lambda\in\Lambda} U_\lambda; U_\lambda \in \tau_A$ prostora (A, τ_A) lahko priredimo nadpokritje $\bigcup_{\lambda\in\Lambda} V_\lambda; V_\lambda \in \tau \wedge U_\lambda = A \cap V_\lambda$ in obratno. Torej, če $A \subseteq X$, lahko kompaktnost A dokazujemo kar z nadpokritji v originalnem prostoru (X, τ).

Opomba 3.2. *Kompaktnost lahko preverjamo le na bazi topologije. Če ima namreč vsako pokritje X z baznimi množicami končno podpokritje, ga ima očitno tudi vsako drugo pokritje, ki je sestavljeno iz množic, ki so unije ali preseki baznih množic. To zelo očitno in intuitivno dejstvo se pogosto izkaže za veliko bolj prikladen način dokazovanja kompaktnosti, saj nam omogoča večjo mero nadzora nad obravnavanimi pokritji.*

Poglejmo si nekaj zgledov kompaktnih in nekompaktnih prostorov.

Zgled 3.1. *Končen prostor je vedno kompakten, saj so vsa odprta pokritja končnega prostora končna.*

Zgled 3.2. *Neskončen prostor z diskretno topologijo ni kompakten, saj za prostor $(X, \mathcal{P}(X))$ pokritje $\{a \mid a \in X\}$ očitno nima končnega podpokritja.*

Dokažimo sedaj dva izreka, ki nam bosta dala dobro intuicijo glede povezave med kompaktnostjo in koncepti definiranimi v prejšnjem poglavju ter tvorila osnovo za dokazovanje lastnosti podprostorov $\mathbb{R}^n$.

Izrek 3.1. *Kompakten podprostor Hausdorffovega prostora je zaprt.*

Dokaz. Naj bo X Hausdorffov prostor in K njegov kompakten podprostor. Če bi bil K zaprt, bi moral biti K^c odprt. Dovolj je torej dokazati, da lahko K^c zapišemo kot unijo odprtih množic.
Oglejmo si vse takšne točke T_λ, $\lambda \in \Lambda$, da velja $K = \bigcup_{\lambda\in\Lambda} T_\lambda$ in poljubno točko $P \in K^c$. Ker je X Hausdorffov prostor vemo, da za vsak $\lambda \in \Lambda$ obstajata taki disjunktni odprti množici U_λ in V_λ, da velja $P \in U_\lambda$ in $T_\lambda \in V_\lambda$, kjer je $\bigcup_{\lambda\in\Lambda} V_\lambda$ očitno odprto pokritje K. Ker pa je K kompakten, obstaja $n \in \mathbb{N}$ in $V_1, \ldots, V_n \in \{V_\lambda \mid \lambda \in \Lambda\}$, da je $\bigcup_{i=1}^{n} V_i$ končno podpokritje K.
Naj bo $U = \bigcap_{i=1}^{n} U_{\lambda_i}$. Ker je U končen presek odprtih množic, velja $U \in \tau$. Hkrati pa velja tudi $U \cap K = \emptyset$, s čimer smo dokazali, da lahko P ostro ločimo od vsake točke v K. Za vsako točko $P \in K^c$ torej obstaja odprta množica, ki to točko vsebuje in ima s K prazen presek. Unija vseh takih odprtih množic pa je ravno K^c, kar dokaže, da je K res zaprt. □

Izrek 3.2. *Zaprt podprostor kompaktnega prostora je kompakten.*

Dokaz. Naj bo K kompakten prostor in $Z \subseteq K$ zaprt podprostor s podedovano topologijo. Ker je Z zaprt, velja $Z^c \in \tau$. Naj bodo U_λ, kjer $\lambda \in \Lambda$, take odprte podmnožice K, da je $\bigcup_{\lambda\in\Lambda} U_\lambda$ odprto nadpokritje Z. Vemo torej, da je $Z^c \cup \left(\bigcup_{\lambda\in\Lambda} U_\lambda\right)$ odprto pokritje K. Ker pa je K kompakten prostor, mora obstajati končno podpokritje našega pokritja, torej tak $n \in \mathbb{N}$ in $U_{\lambda_1}, \ldots, U_{\lambda_n} \in \{U_\lambda \mid \lambda \in \Lambda\}$, da je $Z^c \cup \left(\bigcup_{i=1}^{n} U_{\lambda_i}\right)$ odprto pokritje K. Vemo pa, da je potem $\bigcup_{i=1}^{n} U_{\lambda_i}$ končno odprto podpokritje Z, saj imata Z^c in Z prazen presek. S tem smo dokazali, da je Z kompakten prostor. □

4 Produktna topologija

Ali obstaja preprosta razširitev topologij dveh topoloških prostorov, ki definira topologijo na njunem kartezičnem produktu? Izkaže se, da namen doseže kar najintuitivnejša razširitev - produkt topologij samih.

Definicija 4.1. *Naj bosta (X, τ_X) in (Y, τ_Y) topološka prostora. Potem topologijo τ_P z bazo*

$$\{U \times V; U \in \tau_X \wedge V \in \tau_Y\}$$

imenujemo ***produktna topologija*** *topološkega prostora $(X \times Y, \tau_P)$.*

Zlahka preverimo, da smo s tem zares definirali topologijo, saj:

- $\emptyset = \emptyset \times \emptyset$ in $X \times Y = X \times Y$, torej res velja $X \times Y, \emptyset \in \tau$,
- Vsako odprto množico lahko zapišemo kot unijo baznih množic, torej je poljubna unija odprtih množic prav tako odprta,

- $\bigcap_{i\in\{1,2,\ldots,n\}} (X_i \times Y_i) = \left(\bigcap_{i\in\{1,2,\ldots,n\}} X_i\right) \times \left(\bigcap_{i\in\{1,2,\ldots,n\}} Y_i\right)$, torej je poljuben končen presek odprtih množic prav tako odprt.

τ_P torej zares zadošča vsem lastnostim topologije.
Ali imajo produkti topoloških prostorov kakšne lepe lastnosti? V skladu z osrednjim vprašanjem članka, nas seveda posebej zanima, kdaj je produkt prostorov kompakten. Imamo že dovolj znanja, da lahko dokažemo naslednji izrek, ki nam bo pokazal, da se kompaktnost vedno prenese s posameznih faktorjev na njihov produkt.

Izrek 4.1. *Končen produkt kompaktnih prostorov je kompakten.*

Dokaz. Ker izrek dokazujemo zgolj za končno število kompaktnih prostorov, je trditev dovolj dokazati za dva prostora, indukcija pa poskrbi za preostanek dokaza. Naj bosta torej (X, τ_X) in (Y, τ_Y) kompaktna topološka prostora. Potem želimo dokazati, da je prostor $(X \times Y, \tau_P)$ s produktno topologijo τ_P kompakten. Dovolj je torej dokazati, da ima vsako odprto pokritje $X \times Y$ končno podpokritje. Naj bo $K = \bigcup_{\lambda\in\Lambda} (U_\lambda \times V_\lambda)$ odprto pokritje $X \times Y$, kjer je $U_\lambda \in \tau_X$ in $V_\lambda \in \tau_Y$ za vse $\lambda \in \Lambda$. Kompaktnost torej preverjamo na bazi. Konstruirali bomo končno podpokritje pokritja K.
Oglejmo si najprej prostor $\{a\} \times Y$, za nek poljuben $a \in X$. Iz definicije produktne topologije sledi, da obstaja odprto pokritje $\bigcup_{\delta\in\Delta} V_\delta$ prostora Y, kjer velja $(U_\delta \times V_\delta) \cap (\{a\} \times Y) \neq \emptyset$. Ker pa je Y kompakten, obstaja neko končno podpokritje $V_{a_1} \cup V_{a_2} \cup \ldots \cup V_{a_{n_a}}$ pokritja $\bigcup_{\delta\in\Delta} V_\delta$ prostora Y. Sledi, da je $(U_{a_1} \times V_{a_1}) \cup \ldots \cup (U_{a_{n_a}} \times V_{a_{n_a}})$ končno pokritje prostora $\{a\} \times Y$. Tako dobimo odprto pokritje $C = \bigcup_{a\in X} \left(U_{a_1} \cap U_{a_2} \cap \ldots \cap U_{a_{n_a}}\right)$ prostora X. Ker pa je X kompakten, obstaja končno podpokritje D pokritja C. Torej velja $D = \bigcup_{a\in A} \left(U_{a_1} \cap U_{a_2} \cap \ldots \cap U_{a_{n_a}}\right)$, za neko končno podmnožico $A \in X$. Od tod pa sledi, da je

$$\bigcup_{a\in A} \left((U_{a_1} \times V_{a_1}) \cup (U_{a_2} \times V_{a_2}) \cup \ldots \cup \left(U_{a_{n_a}} \times V_{a_{n_a}}\right)\right)$$

končno podpokritje prostora $X \times Y$, kar smo želeli dokazati. □

5 Kompaktnost prostorov v $\mathbb{R}^n$

V zadnjem delu članka si bomo ogledali, kako se splošne definicije topologije, pokritja in kompaktnosti prenesejo v podprostore $\mathbb{R}^n$.
Osvežimo za začetek nekatere osnovne definicije, ki jih bralec najverjetneje že pozna iz osnovne analize.

Definicija 5.1. *$\mathbb{R}^n$ je množica vseh urejenih n-teric, katerih komponente so realna števila.*

Za lažjo predstavo:

$$\mathbb{R}^n = \mathbb{R} \times \mathbb{R} \times \cdots \times \mathbb{R}. \quad \text{(produkt } n\text{-členov } \mathbb{R})$$

Definicija 5.2. ***Kvader*** *v $\mathbb{R}^n$ je množica oblike $[a_1, b_1] \times \cdots \times [a_n, b_n]$, kjer $-\infty < a_i < b_i < \infty$.*

Definicija 5.3. *Definiramo* ***odprto kroglo*** *v $\mathbb{R}^n$ s središčem v $a = (a_1, a_2, a_3, a_4, ..., a_n)$ in radijem r kot*

$$K(a, r) = \left\{ (x_1, x_2, \ldots, x_n) \in \mathbb{R}^n; \sqrt{\sum_{i=1}^{n} (a_i - x_i)^2} = |a - x| < r \right\}.$$

Definicija 5.4. *Množico $\mathbb{R}^n$ opremimo z **evklidsko topologijo** τ_e tako, da vzamemo za bazo topologije τ_e množico vseh odprtih krogel.*

V nadaljevanju opremimo vse prostore z evklidsko topologijo, izhodišče koordinatnega sistema pa označimo z I.

Poglejmo si zgled nekompaktnega prostora s podedovano evklidsko topologijo.

Zgled 5.1. *Interval $(0,1)$ ni kompakten. Pokritje $\bigcup_{n\in\mathbb{N},n\geq 2}\left(\frac{1}{n},1\right)$ namreč nima končnega podpokritja. To lahko dokažemo s protislovjem. Predpostavimo, da obstaja tak $n\in\mathbb{N}$ in $a_1,a_2\dots a_n\in\mathbb{N}$, da je $\bigcup_{i=1}^{n}\left(\frac{1}{a_i},1\right)$ odprto pokritje intervala $(0,1)$. Brez škode za splošnost naj bo $a_1\geq a_2\geq\dots\geq a_n$. Potem vemo, da $\frac{1}{a_1}\in(0,1)$, vendar $\frac{1}{a_1}\notin\bigcup_{i=1}^{n}\left(\frac{1}{a_i},1\right)$, protislovje.*

Definicija 5.5. *Naj bo $M\subseteq\mathbb{R}$ množica. Število $s\in\mathbb{R}$ je **supremum množice** M, če velja:*

- *$s\geq m$ za vsak $m\in M$*
- *$\forall\varepsilon>0$, obstaja tak $x\in M$, da $x\in(s-\varepsilon,s]$*

Prvi pogoj nam pove, da je s zgornja meja množice M, drugi pogoj pa nam pove, da je to najnižja zgornja meja.

Aksiom 5.1. ***Dedekindov aksiom.*** *Vsaka neprazna navzgor omejena množica ima supremum.*

Definicija 5.6. *Množica $M\subseteq\mathbb{R}^n$ je **omejena**, če obstaja neka odprta/zaprta krogla $K(I,r)$ za nek $0<r<\infty$, da je $M\subseteq K(I,r)$.*

Sedaj se z osveženim spominom lahko vrnemo k dokazovanju. Ker smo končno definirali evklidsko topologijo, lahko dokažemo dokaj očitno trditev, da je $\mathbb{R}^n$ Hausdorffov.

Izrek 5.1. *$\mathbb{R}^n$ je Hausdorffov.*

Dokaz. Naj bosta A in B točki v $\mathbb{R}^n$ in naj bo M razpolovišče daljice AB. Poglejmo si odprti krogli s središčema v A in B ter s polmeroma AM in BM. Ker sta krogli disjunktni, smo s tem ostro ločili poljubni točki A in B. □

Naslednji izrek bo močno omejil naše raziskovanje kompaktnih prostorov v $\mathbb{R}^n$.

Izrek 5.2. *Vsak kompakten podprostor $\mathbb{R}^n$ je omejen.*

Dokaz. Trditev bomo dokazali s protislovjem. Denimo, da obstaja kompakten $K\subseteq\mathbb{R}^n$, ki je neomejen. Oglejmo si pokritje $\bigcup_{n\in\mathbb{N}}K(I,n)$ prostora K. Po definiciji kompaktnosti obstaja končno podpokritje

$$K(I,n_1)\cup K(I,n_2)\cup\ldots\cup K(I,n_k)$$

množice K, za neke $n_1<n_2<\ldots<n_k\in\mathbb{N}$. Od tod sledi $K\subseteq K(I,n_k)$. Ker pa smo predpostavili, da je K neomejen, smo prišli do protislovja, kar zaključi dokaz. □

Naravno vprašanje, ki se samo postavlja, je, ali sploh obstajajo kakšni preprosti, vsakdanji prostori v $\mathbb{R}^n$, ki so kompaktni? Naslednji izreki nam bodo pokazali, da do sedaj dokazani splošni izreki niso samo elegantni in lepi sami po sebi, temveč nam nudijo vpogled tudi v pomembne lastnosti prostorov, s katerimi se najpogosteje srečujemo v analizi.

Izrek 5.3. *Naj bosta $a < b$ poljubni realni števili. Potem je interval $[a, b]$ kompakten.*

Dokaz. Trditev bomo dokazali s protislovjem. Naj bo $\bigcup_{\lambda\in\Lambda} U_\lambda$ neko odprto nadpokritje $[a, b]$ brez končnega podpokritja. Definirajmo množico M vseh realnih $x \in [a, b]$, za katere ima interval $[a, x]$ končno podpokritje pokritja $\bigcup_{\lambda\in\Lambda} U_\lambda$. Množica M je očitno neprazna, saj obstaja taka odprta množica U_{λ_0}, ki vsebuje a in zato vsebuje tudi $a + \varepsilon$ za nek dovolj majhen $\varepsilon > 0$. Ker pa smo predpostavili, da $b \notin M$, je množica M navzgor omejena. Od tod pa sledi, da ima po Dedekindovem aksiomu supremum $x_0 \in (a, b)$. Naj bo U_0 odprta množica našega nadpokritja, ki vsebuje x_0. Vemo pa, da obstaja neka točka $c \in U_0$ manjša od x_0, za katero obstaja končno podpokritje intervala $[a, c]$ našega začetnega nadpokritja. Obstaja pa tudi nek majhen $\varepsilon > 0$, da velja $x + \varepsilon \in U_0$. Od tod sledi, da obstaja končno podpokritje intevala $[a, x + \varepsilon]$, namreč unija U_0 in pokritja intervala $[a, c]$, kar je v protislovju z dejstvom, da je x_0 supremum množice M. Sledi, da ima vsako pokritje $[a, b]$ končno podpokritje, kar smo želeli dokazati. □

Z našim znanjem o produktni topologiji lahko sedaj enostavno dokažemo kompaktnost vseh kvadrov.

Izrek 5.4. *Kvadri so kompaktni v $\mathbb{R}^n$*

Dokaz. Trditev je direktna posledica definicije kvadra in izreka **4.1** ter izreka **5.3**. □

Končno smo pripravljeni, da popolnoma kategoriziramo vse kompaktne prostore v $\mathbb{R}^n$.

Izrek 5.5. *(Heine, Borel, Lebesgue) Podprostor $\mathbb{R}^n$ je kompakten v $\mathbb{R}^n$ natanko tedaj, ko je zaprt in omejen.*

Dokaz. Izrek bomo dokazali v vsako smer posebej. Naj bo K podprostor $\mathbb{R}^n$.

$(\implies)$:
Naj bo prostor K kompakten v $\mathbb{R}^n$. Iz izreka **5.2** sledi, da je prostor K omejen. Ker pa je $\mathbb{R}^n$ Hausdorffov sledi po izreku **3.1**, da je K zaprt.

$(\impliedby)$:
Naj bo prostor K zaprt in omejen v $\mathbb{R}^n$. Ker je prostor K omejen, je po definiciji vsebovan v odprti krogli $K(I, R)$, z dovolj velikim $R \in \mathbb{R}^+$. Ta pa je seveda vsebovana v zaprtem kvadru $[-R, R]^n$. Od tod sledi, da je tudi K vsebovan v tem zaprtem kvadru, ki je po izreku **5.4** kompakten v $\mathbb{R}^n$. Sedaj pa nam izrek **3.2** pove, da je prostor K kompakten v $\mathbb{R}^n$, kar smo želeli dokazati. □

6 Zaključek

V projektu smo se spoznali s pojmi topologije, kot so topološki prostor, odprte in zaprte množice, Hausdorffov prostor in odprto pokritje. Seznanili smo se s konceptom kompaktnosti in naše pridobljeno znanje uporabili za preučevanje lastnosti kompaktnih množic. Na podlagi tega smo klasificirali vse kompaktne podprostore v $\mathbb{R}^n$ in tako dokazali, da so vsi kompakti v $\mathbb{R}^n$ natanko zaprti in omejeni podprostori $\mathbb{R}^n$.

Literatura

[1] P. Pavešić, *Splošna topologija*, Izbrana poglavja iz matematike in računalništva **43**, 2. natis, DMFA – založništvo, Ljubljana, 2017.

[2] M. Raman-Sundström, *A pedagogical history of compactness*, 10. 6. 2014, pridobljeno 4. 8. 2023 z `https://arxiv.org/pdf/1006.4131.pdf`

Simetrične funkcije

Ajda Brnot, Martin Gubina, Kiana Petrič
Mentorica: *Petra Podlogar*

Povzetek

V članku definiramo dve družini simetričnih funkcij, to so monomske simetrične funkcije in Schurove funkcije. Izkaže se, da so prve baza vektorskih prostorov Λ^n in Λ. Drugim pa se posvetimo zaradi povezave z Youngovimi polstandardnimi tabelami, sproti ugotovimo, da so tudi te simetrične.

1 Uvod

Narava permutacij in njihova globoka povezava z različnimi matematičnimi koncepti so že dolgo navdihovale raziskovalce v številnih vejah matematike. V tem članku bomo raziskali osnovne ideje in povezave med permutacijami, simetričnimi polinomi in simetričnimi funkcijami. Spoznali bomo dve družini simetričnih funkcij, monomske simetrične funkcije in Schurove funkcije.

Permutacije predstavljajo razporeditve elementov v določenem vrstnem redu. Te lahko razumemo kot bijektivne preslikave množice same vase. Simetrični polinomi so algebraični izrazi, ki ostanejo nespremenjeni, če zamenjamo vrstni red njihovih spremenljivk. Poglobljeno raziskovanje simetričnih polinomov privede do koncepta simetričnih funkcij, ki so pravzaprav razširitev simetričnih polinomov na neskončne vrste.

Monomske simetrične funkcije so poseben razred simetričnih funkcij, ki igrajo pomembno vlogo pri razvoju teorije simetričnih polinomov. Youngove polstandardne tabele so kombinatorična orodja, ki so povezana s simetričnimi funkcijami in permutacijami ter so bistvene pri raziskovanju simetrične grupe. Schurove funkcije pa so posebne simetrične funkcije, ki so povezane z reprezentacijami simetrične grupe in imajo številne aplikacije v različnih matematičnih kontekstih.

V nadaljevanju članka bomo podrobno preučili vsakega od teh konceptov in raziskali njihove medsebojne povezave.

2 Permutacije

Najprej si oglejmo osnovno matematično strukturo, ki igra ključno vlogo pri razporejanju elementov ter razumevanju simetrije in kombinatorike.

Definicija 2.1. ***Permutacija*** $\pi : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ *je bijektivna preslikava množice* n *elementov same vase. Množico vseh permutacij množice* n *elementov označimo s* S_n*. Posebna vrsta permutacije je* ***transpozicija****, pri kateri se zamenjata le dva elementa.*

Permutacijo množice števil $\{1, 2, \ldots, n\}$ lahko zapišemo na tri načine, in sicer dvovrstično kot

$$\begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \pi(1) & \pi(2) & \pi(3) & \ldots & \pi(n) \end{pmatrix},$$

enovrstično kot

$$\begin{pmatrix} \pi(1) & \pi(2) & \pi(3) & \ldots & \pi(n) \end{pmatrix}$$

ali ciklično. Ciklični zapis permutacije je način predstavitve permutacije s pomočjo ciklov in omogoča bolj pregledno in kompaktno predstavitev permutacij z uporabo ciklov, kjer se elementi, ki so med seboj povezani, združijo v cikle.

Primer 2.1. *Zapišimo eno izmed permutacij* $\{1, 2, \ldots, n\}$ *z dvovrstičnim, enovrstičnim in cikličnim zapisom.*

$$\begin{aligned}\begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 2 & 1 & 3\end{pmatrix} &= \begin{pmatrix}4 & 2 & 1 & 3\end{pmatrix}\\ &= (1,\ 4,\ 3)\,(2)\\ &= (1,\ 4,\ 3)\end{aligned}$$

Lahko jo zapišemo tudi kot produkt transpozicij.

$$\begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 2 & 1 & 3\end{pmatrix} = (1,\ 4)\,(4,\ 3)$$

Trditev 2.1. *Vsako permutacijo je mogoče zapisati kot produkt transpozicij.*

Dokaz. Poljubno permutacijo $(a_1,\ a_2,\ a_3,\ \ldots,\ a_n)$ lahko zapišemo kot produkt transpozicij na sledeč način

$$(a_1,\ a_2,\ a_3,\ \ldots,\ a_n) = (a_1,\ a_2)\,(a_2,\ a_3)\cdots(a_{n-1},\ a_n)\,.$$

Transpozicije, ki jih dobimo na zgornji način, niso nujno oblike $(i,\ i+1)$ za $i \geq 1$. Pri nekaterih dokazih bi nam bolj prav prišlo, če bi znali permutacijo zapisati kot produkt transpozicij te posebne oblike. To lahko naredimo na sledeč način:

$$(k,\ l) = (k,\ k+1)\,(k+1,\ k+2)\cdots(l-1,\ l)\,(l-2,\ l-1)\cdots(k,\ k+1)\,,$$

pri čemer smo predpostavili, da je $k < l$.

Ko združimo oba načina, lahko vidimo, da lahko vsako permutacijo zapišemo kot produkt transpozicij oblike $(i,\ i+1)$ za neke $i \in \mathbb{N}$. □

3 Simetrični polinomi in Vietove formule

Definicija 3.1. ***Simetrični polinom*** *v spremenljivkah* $x_1, x_2, \ldots, x_n$ *je tak polinom, da za vsako permutacijo* $\pi \in S_n$ *velja*

$$f(x_1, x_2, x_3, \ldots x_n) = f(x_{\pi(1)}, x_{\pi(2)}, x_{\pi(3)}, \ldots x_{\pi(n)}).$$

Primer 3.1. *Dana sta polinoma*

$$f(x_1, x_2, x_3) = x_1 + x_2 + x_3$$

in

$$g(x_1, x_2, x_3) = x_1^2 + 2x_2 + 3x_3^3 + 2 + x_1x_2$$

ter permutacija $\pi = (1, 2, 3)$. *Za polinom* f *je*

$$\begin{aligned}f(x_{\pi(1)}, x_{\pi(2)}, x_{\pi(3)}) &= f(x_2, x_3, x_1)\\ &= x_2 + x_3 + x_1\\ &= f(x_1, x_2, x_3).\end{aligned}$$

Ker to velja tudi za vse ostale permutacije, je polinom f *simetričen. Za polinom* g *pa velja*

$$\begin{aligned}g(x_{\pi(1)}, x_{\pi(2)}, x_{\pi(3)}) &= g(x_2, x_3, x_1)\\ &= x_2^2 + 2x_3 + 3x_1^3 + 2 + x_2x_3\\ &\neq g(x_1, x_2, x_3),\end{aligned}$$

kar pomeni, da polinom g *ni simetričen.*

Simetrične polinome lahko opazimo pri Vietovih formulah za iskanje ničel v polinomih. Za poljuben polinom druge stopnje $f(x) = ax^2 + bx + c = a(x - x_1)(x - x_2)$, kjer sta x_1, x_2 ničli kvadratne funkcije, sta to formuli

$$x_1 + x_2 = -\frac{b}{a}$$

in

$$x_1 x_2 = \frac{c}{a},$$

kjer na levi strani očitno zagledamo simetričen polinom.

Za poljuben polinom $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x^1 + a_0$, ki ga lahko izrazimo kot $f(x) = a_n(x - x_1)(x - x_2)\cdots(x - x_n)$, imamo Vietove formule

$$\begin{aligned} x_1 + x_2 + \cdots + x_n &= -\frac{a_{n-1}}{a_n} \\ x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n &= \frac{a_{n-2}}{a_n} \\ &\cdots \\ x_1x_2x_3\cdots x_n &= (-1)^n \frac{a_0}{a_n}. \end{aligned}$$

Opazimo, da je leva stran enačb simetrična.

4 Simetrične funkcije

Da lahko definiramo simetrične funkcije, najprej poglejmo, kaj so formalne potenčne vrste.

Definicija 4.1. ***Formalna potenčna vrsta v neskončnem številu spremenljivk s koeficienti v*** $\mathbb{Q}$ *je preslikava* $f : A \to \mathbb{Q}$*, kjer je*

$$A = \{(a_1, a_2, a_3, \ldots) \mid \textit{končno mnogo členov } a_i \textit{ neničelnih}\}.$$

Označimo $f \in \mathbb{Q}[[x_1, x_2, \ldots]] = \mathbb{Q}[[x]]$.

V zgornji definiciji smo poenostavili zapis, upoštevali smo $x = (x_1, x_2, \ldots)$.

Primer 4.1. *Primer formalne potenčne vrste je*

$$\begin{aligned} f : (1,0,0,0,\ldots) &\mapsto 2 \\ (0,1,1,0,\ldots) &\mapsto 5 \\ (1,0,2,0,\ldots) &\mapsto 3 \\ &\cdots, \end{aligned}$$

kar lahko zapišemo tudi kot

$$2x_1 + 5x_2x_3 + 3x_1x_3^2 + \cdots .$$

Definicija 4.2. ***Simetrična funkcija s koeficienti v*** $\mathbb{Q}$ *je taka* $f \in \mathbb{Q}[[x]]$*, za katero za vsako permutacijo* π *množice* $\{1, 2, \ldots\}$ *velja*

$$f(x_1, x_2, x_3, \ldots) = f(x_{\pi(1)}, x_{\pi(2)}, x_{\pi(3)}, \ldots).$$

Simetrična funkcija je torej posebna vrsta formalne potenčne vrste, pri kateri lahko spremenljivke poljubno preurejamo. Poznamo tudi homogene simetrične funkcije.

Definicija 4.3. ***Homogena simetrična funkcija stopnje*** n *je simetrična funkcija, za katero velja, da so lahko neničelni le koeficienti členov z vsoto potenc enako* n*.*

Primer 4.2. *Oglejmo si nekaj primerov homogenih simetričnih funkcij:*

- $f(x) = x_1 + x_2 + x_3 + \cdots$ $(n = 1)$,
- $g(x) = x_1x_2 + x_1x_3 + \cdots + x_2x_3 + x_2x_4 + \cdots$ $(n = 2)$,
- $h(x) = x_1^2 + x_2^2 + x_3^2 + \cdots$ $(n = 2)$.

5 Vektorski prostor

V nadaljevanju bomo definirali bazo simetričnih funkcij, zato moramo poznati definicijo grupe, vektorskega prostora in baze.

Definicija 5.1. ***Grupa*** *je par $(V, +)$, sestavljen iz množice V in operacije*

$$+ : G \times G \to G,$$

ki zadošča pogojem:

1. *operacija $+$ je asociativna:*

$$(a + b) + c = a + (b + c) \quad \text{za vsak } a, b, c \in V,$$

2. *obstaja nevtralni element:*

$$0 + x = x + 0 = x \quad \text{za vsak } x \in V,$$

3. *vsak element $a \in V$ je obrnljiv:*

$$\text{za vsak } a \text{ obstaja } -a, \text{ tako da je } a + (-a) = -a + a = 0.$$

Grupa $(V, +)$ je komutativna, če za vsaka elementa $u, v \in V$ velja

$$u + v = v + u.$$

Poznavanje definicije grupe je potrebno za uvedbo vektorskega prostora.

Definicija 5.2. ***Vektorski prostor*** *V* ***nad*** *$\mathbb{Q}$ je množica V z notranjo operacijo*

$$+ : V \times V \to V$$

in zunanjo operacijo

$$\cdot : \mathbb{Q} \times V \to V,$$

za kateri za poljubne $\alpha, \beta \in \mathbb{Q}$ in $u, v \in V$ velja:

1. *$(V, +)$ je komutativna grupa,*
2. *asociativnost:*

$$(\alpha\beta)u = \alpha(\beta u),$$

3. *distributivnost:*

$$(\alpha + \beta)u = \alpha u + \beta u,$$
$$\alpha(u + v) = \alpha u + \alpha v,$$

4. *$1 \cdot v = v$, kjer je $1 \in \mathbb{Q}$ nevtralni element za množenje.*

Vsak vektorski prostor ima bazo. V nadaljevanju bomo iskali bazo simetričnih funkcij.

Definicija 5.3. *Množica $B \subseteq V$ je* ***baza vektorskega prostora*** *V, če zanjo velja, da:*

1. *je ogrodje:*

   $$\text{vsak } v \in V \text{ lahko zapišemo kot linearno kombinacijo elementov množice } B,$$

2. *so elementi množice B linearno neodvisni:*
   za vsako končno podmnožico $B' \subseteq B$ je

   $$\sum_{v_i \in B'} a_i v_i = 0 \iff \text{vsi koeficienti } a_i \text{ so enaki } 0.$$

6 Množici Λ^n in Λ

V kontekstu simetričnih funkcij se bomo v tem poglavju osredotočili na množici Λ^n in Λ, v katerih so združene simetrične funkcije z nekimi lastnostmi.

Definicija 6.1. ***Množico vseh homogenih simetričnih funkcij stopnje*** *n za $n \geq 0$ označimo z Λ^n.*

V množici Λ želimo končne vsote homogenih simetričnih funkcij. Z množicami Λ^i za $i \geq 0$ definiramo

$$\Lambda := \Lambda^0 \oplus \Lambda^1 \oplus \Lambda^2 \oplus \cdots,$$

elementi Λ pa so enaki

$$f = f_0 + f_1 + f_2 + \cdots,$$

kjer je $f_i \in \Lambda^i$, neničelnih f_i pa je končno mnogo.

Za Λ^n in Λ definiramo seštevanje kot seštevanje po členih ter množenje s skalarjem na očiten način.

Razmislimo, da sta Λ^n in Λ vektorska prostora. Ni težko videti, da večino računskih pogojev izpolnjujeta; asociativnost seštevanja in množenja s skalarjem ter distributivnost sta očitni. Očitno je tudi, da je $1 \in \mathbb{Q}$ nevtralni element za množenje, saj formalna potenčna vrsta po množenju z 1 ostane nespremenjena. Prav tako hitro opazimo, da ima vsak element v Λ in Λ^n nasprotno vrednost, saj so koeficienti simetričnih funkcij iz Λ in Λ^n elementi $\mathbb{Q}$ in imajo zato vsak svojo nasprotno vrednost. Edini pogoj, ki ni najbolj očiten, je pogoj za nevtralni element. Če si še enkrat pogledamo definicijo homogene simetrične funkcije, vidimo, da dopušča, da je koeficient člena, katerega vsota potenc je n, lahko enak 0, torej so lahko koeficienti vseh členov neke funkcije $f_n \in \Lambda^n$ enaki 0. Tako lahko dobimo $f_n = 0 \in \Lambda^n$ za vsak n. Poljubna Λ^n torej vsebuje element 0. Razmisliti moramo še, da je 0 tudi element Λ. Ker je vsak element iz Λ je sestavljen iz elementov iz poljubnega končnega števila množic Λ^n, vsaka množica Λ^n pa vsebuje element 0, je tudi $0 \in \Lambda$.

Premislili smo, da sta Λ in Λ^n vektorska prostora, saj zadostujeta vsem pogojem zanj. Ker sta vektorska prostora, je smiselno zanju iskati baze – dve predstavimo v nadaljevanju.

7 Particije in šibke kompozicije

Preden se poglobimo v raziskovanje družin simetričnih funkcij, je ključno razumeti koncept particij – razdelitev števila na pozitivne celoštevilske komponente.

Definicija 7.1. ***Particija števila*** *n je padajoče zaporedje naravnih števil, katerih vsota je enaka n. Da je λ particija števila n, označimo z $\lambda \vdash n$, da je λ particija, pa z $\lambda \in Par$, kjer je Par množica vseh particij.*

Particije lahko med seboj primerjamo z relacijo dominance.

Definicija 7.2. *Naj bosta $\lambda, \mu \in Par$. Rečemo, da je λ manjša ali enaka kot μ v **relaciji dominance**, če za vsak $n \in \mathbb{N}$ velja*

$$\sum_{i=1}^{n} \lambda_i \leq \sum_{i=1}^{n} \mu_i.$$

To označimo z $\lambda \leq \mu$.

Upoštevali smo, da je λ_i i-ti element v particiji λ. Za $\lambda \vdash n$ definiramo oznaki $l(\lambda)$, ki je enak številu elementov v particiji, in $|\lambda| = \lambda_1 + \lambda_2 + \lambda_3 + \cdots + \lambda_{l(\lambda)} = n$.

Primer 7.1. *Za $n = 4$ so tako 4, 31, 22, 211 in 1111 vse možne particije, $l(31) = 2$ in $|31| = 4$. Vidimo, da je $1111 \leq 31$.*

Šibka kompozicija $\alpha \vDash n$ je podobno kot particija sestavljena iz števil, katerih vsota je enaka n, vendar pa so tokrat števila izbrana iz $\mathbb{N} \cup \{0\}$ in niso nujno urejena v padajočem vrstnem redu.

Primer 7.2. *Za $n = 4$ je ena od šibkih kompozicij enaka $(0, 0, 1, 0, 0, 0, 3, 0, \ldots)$.*

8 Monomske simetrične funkcije

Ena izmed osnovnih družin simetričnih funkcij so monomske simetrične funkcije.

Definicija 8.1. *Naj bo $n \geq 0$. Za $\lambda \vdash n$ definiramo **monomske simetrične funkcije** kot*

$$m_\lambda(x) = \sum_{\substack{\omega:\{1,2,\ldots,l(\lambda)\}\to\{1,2,3,\ldots\} \\ \omega \text{ injektivna preslikava}}} x_{\omega(1)}^{\lambda_1} x_{\omega(2)}^{\lambda_2} \cdots x_{\omega(l(\lambda))}^{\lambda_{l(\lambda)}}.$$

Primer 8.1. *Poglejmo prvih nekaj primerov monomskih simetričnih funkcij:*

- $m_1(x) = x_1 + x_2 + x_3 + \cdots$,
- $m_2(x) = x_1^2 + x_2^2 + x_3^2 + \cdots$,
- $m_{11}(x) = x_1x_2 + x_1x_3 + \cdots$,
- $m_{21}(x) = x_1^2x_2 + x_1x_2^2 + \cdots$.

V prejšnjem razdelku smo razmislili, da sta Λ^n in Λ vektorska prostora. Pokažimo zdaj, da lahko v družini monomskih simetričnih funkcij zanju najdemo bazi.

Trditev 8.1. *Za monomske simetrične funkcije velja:*

1. *$\{m_\lambda \mid \lambda \vdash n\}$ je baza za Λ^n,*
2. *$\{m_\lambda \mid \lambda \in Par\}$ je baza za Λ.*

Dokaz. Najprej dokažimo, da je $\{m_\lambda \mid \lambda \vdash n\}$ baza za Λ^n, saj si bomo s tem pomagali tudi pri dokazu, da je $\{m_\lambda \mid \lambda \in Par\}$ baza za Λ.

1. Najprej dokažimo, da je $\{m_\lambda \mid \lambda \vdash n\}$ ogrodje. Očitno je, da poljuben $f \in \Lambda^n$ lahko zapišemo kot

$$f = \sum_{\alpha \vDash n} c_\alpha x^\alpha,$$

kjer je $x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \cdots$ za $\alpha = (\alpha_1, \alpha_2, \ldots)$, saj lahko s šibkimi kompozicijami predstavimo poljuben člen, ki se pojavi v f. Člen $4x_1x_2^3x_5$ bi se tako pojavil v zgornji vsoti pri šibki kompoziciji $\alpha = (1, 3, 0, 0, 1, 0, \ldots)$ s $c_\alpha = 4$.

Skupaj lahko združimo šibke kompozicije, ki so po prerazporeditvi enake, zato je

$$f = \sum_{\lambda \vdash n} \sum_{\substack{\omega(\alpha)=\lambda \\ \alpha \vDash n}} c_\alpha x^\alpha.$$

Pri tem $\omega(\alpha)$ prerazporedi števila v α tako, da neničelna števila postavi na začetek in jih uredi po velikosti, na ta način nastane particija λ. Ker je f simetrična funkcija, je $c_\alpha = c_{\omega(\alpha)}$. Dobimo

$$\begin{aligned} f &= \sum_{\lambda \vdash n} \sum_{\substack{\omega(\alpha)=\lambda \\ \alpha \vDash n}} c_{\omega(\alpha)} x^\alpha \\ &= \sum_{\lambda \vdash n} c_\lambda \sum_{\substack{\omega(\alpha)=\lambda \\ \alpha \vDash n}} x^\alpha \\ &= \sum_{\lambda \vdash n} c_\lambda m_\lambda, \end{aligned}$$

kjer smo pri zadnjem enačaju uporabili definicijo monomske simetrične funkcije. S tem smo dokazali, da množica monomskih simetričnih funkcij tvori ogrodje za vektorski prostor Λ^n.

Pokazati moramo še linearno neodvisnost, dokazujemo torej

$$\sum_{\lambda \vdash n} c_\lambda m_\lambda = 0 \iff c_\lambda = 0$$

za vsak $\lambda \vdash n$. Naj bosta λ in μ različni particiji števila n. Zaradi različnih elementov v particiji in posledično različnih potenc se člen, ki se pojavi v m_λ, ne more pojaviti v m_μ. Iz tega sledi, da bo vsota enaka 0 natanko tedaj, ko bodo vsi koeficienti enaki 0.

2. Dokažimo še, da je $\{m_\lambda \mid \lambda \in Par\}$ baza za Λ. Ker je $f \in \Lambda$, lahko f zapišemo kot

$$f = f_0 + f_1 + f_2 + \cdots,$$

kjer so $f_i \in \Lambda^i$ za vsak $i \geq 0$. Da je ogrodje, je očitno, saj lahko vsako funkcijo $f_n \in \Lambda^n$ zapišemo z elementi množice $\{m_\lambda \mid \lambda \in Par\}$. Za particije različnih števil spet ne moremo dobiti enakih členov in res je $\sum_{\lambda \in Par} a_\lambda m_\lambda = 0$ natanko takrat, ko so vsi koeficienti a_λ enaki 0.

□

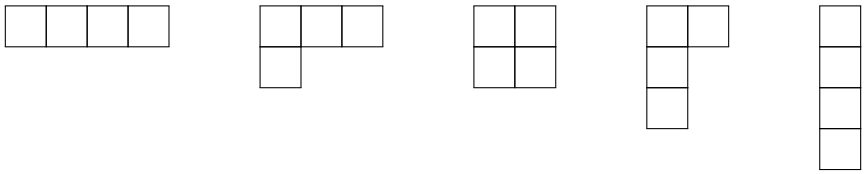
9 Youngove polstandardne tabele

Youngovi diagrami in polstandardne tabele so ime dobile po britanskemu matematiku Alfredu Youngu. V nadaljevanju bomo s pomočjo pojmov, ki jih bomo spoznali v tem poglavju, definirali naslednjo družino simetričnih funkcij.

Definicija 9.1. ***Youngov diagram*** *je nabor celic, zbranih v levo poravnanih vrsticah, ki se proti dnu diagrama krajšajo. Število vrstic in celic v posamezni vrstici je določeno s particijo λ nenegativnega števila n. Število vrstic je določeno z $l(\lambda)$, število celic v i-ti vrstici pa z λ_i.*

Primer 9.1. *Za $\lambda \vdash 4$ so vse možne oblike Youngovih diagramov prikazane na sliki 1.*

Definicija 9.2. ***Youngova polstandardna tabela*** *je Youngov diagram z vstavljenimi pozitivnimi naravnimi števili, ki po vrstici šibko, po stolpcu pa strogo naraščajo. Vsaka izmed števil se lahko v tabeli pojavi več kot enkrat. Tabeli, v kateri se števila ne ponavljajo, rečemo* ***Youngova standardna tabela****.*



Slika 1: Youngovi diagrami oblik 4, 31, 22, 211 in 1111.

Youngovi polstandardni tabeli T lahko določimo obliko in tip. Oblika $sh(T)$ je enaka $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_{l(\lambda)})$, kjer je λ particija in λ_i število celic v vrstici i. Tip $type(T)$ je enak $\alpha = (\alpha_1, \alpha_2, \ldots)$, kjer je α_i število pojavitev i v T.

Primer 9.2. *Oglejmo si nekaj primerov Youngovih polstandardnih tabel. Na sliki 2 je prikazana ena izmed Youngovih polstandardnih tabel oblike* 431 *in tipa* $(4, 3, 1)$*, na sliki 3 pa ena izmed Youngovih standardnih tabel oblike* 431 *in tipa* $(1, 1, 1, 1, 1, 1, 1, 1)$*.*

1	1	1	1
2	2	2	
3			

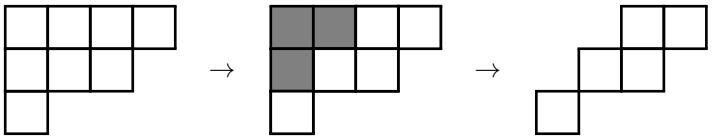
Slika 2: Youngova polstandardna tabela oblike 431 in tipa $(4, 3, 1)$.

1	2	3	4
5	6	7	
8			

Slika 3: Youngova standardna tabela oblike 431 in tipa $(1, 1, 1, 1, 1, 1, 1, 1)$.

Obliko Youngovega diagrama lahko določata tudi dve particiji (npr. λ in μ), kjer nam druga (μ) pove, katere izmed celic v diagramu izbrišemo. Obliko Youngovega diagrama, ki jo določimo s particijama λ in μ, zapišemo kot λ/μ.

Primer 9.3. *Na sliki 4 je prikazan Youngov diagram oblike* λ/μ *za* $\lambda = 431$ *in* $\mu = 21$*.*



Slika 4: Youngov diagram oblike 431/21.

10 Schurove funkcije

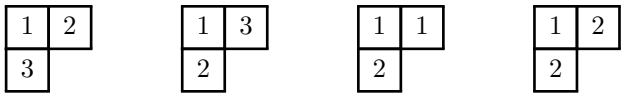
Oglejmo si še drugo družino simetričnih funkcij, ki so ime dobile po ruskemu matematiku Issaiu Schuru. Schurove funkcije definiramo s pomočjo Youngovih polstandardnih tabel.

Definicija 10.1. *Za $\lambda \in Par$ definiramo* ***Schurove funkcije*** *kot*

$$s_\lambda(x) = \sum_{sh(T)=\lambda} x^T,$$

kjer je T Youngova polstandardna tabela in $x^T = x_1^{\alpha_1(T)} x_2^{\alpha_2(T)} x_3^{\alpha_3(T)} \cdots$.

Primer 10.1. *Za lažjo predstavo narišimo Youngove polstandardne tabele oblike* 21 *in tipov* $(1,1,1)$, $(2,1)$ *in* $(1,2)$. *Youngova polstandardna tabela oblike* 21 *in tipa* (3) *ne obstaja, prav tako ne obstaja Youngova polstandardna tabela oblike* 21 *in tipa* $(1,1,1)$.



Slika 5: Youngove polstandardne tabele oblike 21 in tipov $(1,1,1)$, $(2,1)$ in $(1,2)$.

Schurova funkcija za $\lambda = 21$ je tako enaka

$$\begin{aligned} s_{21}(x) &= x_1x_2x_3 + x_1x_3x_4 + \cdots \\ &\quad + x_1x_2x_3 + x_1x_3x_4 + \cdots \\ &\quad + x_1^2x_2 + x_1^2x_3 + \cdots \\ &\quad + x_1x_2^2 + x_1x_3^2 + \cdots \\ &= 2x_1x_2x_3 + 2x_1x_3x_4 + \cdots \\ &\quad + x_1^2x_2 + x_1^2x_3 + \cdots \\ &\quad + x_1x_2^2 + x_1x_3^2 + \cdots . \end{aligned}$$

Nekateri produkti z enakimi stopnjami in indeksi se pojavijo večkrat, zato jih lahko združimo, kot vidimo pri zadnji enakosti. Koeficiente, ki jih na ta način dobimo, imenujemo **Kostkova števila** in jih označimo s $K_{\lambda\alpha}$, kjer je $\lambda \in Par$ in $\alpha \vDash |\lambda|$. Na zgornjem primeru smo tako videli, da je $K_{21,111} = 2$.

Ko Schurove funkcije zapišemo s Kostkovimi števili, dobimo

$$s_\lambda(x) = \sum_{\substack{\alpha=(\alpha_1,\alpha_2,\dots) \\ \alpha \vDash |\lambda|}} K_{\lambda\alpha} x_1^{\alpha_1} x_2^{\alpha_2} \cdots .$$

Oglejmo si dve lepi lastnosti Kostkovih števil.

Trditev 10.1. *Za $\lambda, \mu \in Par$ imajo Kostkova števila naslednji lastnosti:*

1. $K_{\lambda\lambda} = 1$,
2. $K_{\lambda\mu} = 0$, *razen če je $\mu \leq \lambda$, kjer je $\leq$ relacija dominance.*

Dokaz. Naj bosta $\lambda, \mu \in Par$ poljubni particiji.

1. Ker sta oblika in tip enaka, lahko števila razporedimo na en sam način, da bo Youngova polstandardna tabela veljavna. Enka se bo pojavljala po celotni prvi vrstici, dvojka po drugi in podobno tudi ostale.

2. Enka ne more biti hkrati v prvi in drugi vrstici zaradi pogoja strogega naraščanja po vrsticah Youngove polstandardne tabele. Število enic μ_1 je torej manjše ali enako številu celic v prvi vrstici, torej λ_1. Po podobnem razmisleku se enke in dvojke lahko pojavijo le v prvi in drugi vrstici, torej je $\mu_1+\mu_2 \leq \lambda_1+\lambda_2$. Za poljuben $k \in \mathbb{N}$ je torej
$$\sum_{1\leq i\leq k} \mu_i \leq \sum_{1\leq i\leq k} \lambda_i,$$
sledi $\mu \leq \lambda$. V nasprotnem primeru Youngova polstandardna tabela ne obstaja in je Kostkovo število enako 0.

□

Ker lahko Youngovo polstandardno tabelo določimo tudi z dvema particijama, je smiselno gledati tudi Schurove funkcije za λ/μ, kjer sta $\lambda, \mu \in Par$. Zapišemo lahko
$$s_{\lambda/\mu} = \sum_{sh(T)=\lambda/\mu} x^T.$$

Trditev 10.2. *Za $\lambda, \mu \in Par$ je $s_{\lambda/\mu}$ simetrična funkcija.*

Dokaz. Vemo že, da lahko poljubno permutacijo π zapišemo kot produkt transpozicij oblike $(i,\ i+1)$, kjer je $i \in \mathbb{N}$, torej lahko trditev dokažemo le za transpozicije te oblike.

Naj bosta $\lambda, \mu \in Par$. Dokazujemo, da je $s_{\lambda/\mu}$ simetrična funkcija, torej mora po definiciji veljati
$$s_{\lambda/\mu}(x_1, x_2, x_3, \dots) = s_{\lambda/\mu}(x_{\pi(1)}, x_{\pi(2)}, x_{\pi(3)}, \dots).$$
Da bo to res, morajo biti koeficienti pri x^α enaki koeficientom pri $x^{\tau(\alpha)}$, kjer je τ poljubna transpozicija oblike $(i,\ i+1)$ za $i \in \mathbb{N}$.

Iščemo bijekcijo, ki bo Youngovo polstandardno tabelo T oblike λ/μ in tipa $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_{i-1}, \alpha_i, \alpha_{i+1}, \dots)$ preslikala v Youngovo polstandardno tabelo T' oblike λ/μ in tipa $\alpha' = (\alpha_1, \alpha_2, \dots, \alpha_{i-1}, \alpha_{i+1}, \alpha_i, \alpha_{i+2}, \dots)$. Bijekcija v tabeli T pusti števila, različna od i in $i+1$, na istih mestih. Prav tako ne spreminja tistih i, ki imajo pod seboj $i+1$ ter tistih $i+1$, ki imajo nad seboj i. Ostala števila i in $i+1$ zamenja, kot je predstavljeno na slikah 6 in 7.

							i	i	i
i	i	i	$i+1$	$i+1$	$i+1$	$i+1$	$i+1$	$i+1$	$i+1$
$i+1$									

Slika 6: Youngova polstandardna tabela T.

Hitro se lahko prepričamo, da smo z bijekcijo ohranili veljavno Youngovo polstandardno tabelo, saj števila po vrsticah še vedno šibko naraščajo, strogo naraščanje po stolpcih pa sledi iz dejstva, da so nad členi, ki se zamenjajo, strogo manjše vrednosti od i, pod njimi pa strogo večje vrednosti od $i+1$. To pomeni, da teh stolpcev z menjavo nismo mogli "pokvariti". Prav tako lahko vidimo, da je število pojavitev i v T' enako številu pojavitev $i+1$ v T, število pojavitev $i+1$ v T' pa enako številu pojavitev i v T. Ostala števila se v obeh tabelah pojavljajo enakokrat. □

							i	i	i
i	i	i	i	i	$i+1$	$i+1$	$i+1$	$i+1$	$i+1$
$i+1$									

Slika 7: Youngova polstandardna tabela T', ki jo dobimo, ko z bijekcijo preslikamo Youngovo polstandardno tabelo T.

11 Zaključek

V članku smo predstavili pojem simetrične funkcije in nato z znanjem o permutacijah, particijah in Youngovih polstandardnih tabelah razumeli monomske simetrične funkcije in Schurove funkcije.

Literatura

[1] Zapiski predavanj predmeta Kombinatorika prof. dr. Matjaža Konvalinke (Univerza v Ljubljani, Fakulteta za matematiko in fiziko, študijsko leto 2018/2019).

[2] E. S. Egge, *An introduction to symmetric functions and their combinatorics*, American Mathematical Soc., 2019.

[3] *Permutacija*, v: Wikipedia: The Free Encyclopedia, [ogled 3. 8. 2023], dostopno na `https://sl.wikipedia.org/wiki/Permutacija`.

Končne podgrupe SO_3

Neca Camlek, Lenart Frankovič, Tina Tiara Opalič
Mentor: *Matija Likar*

Povzetek

V članku klasificiramo končne podgrupe SO_3 in ponazorimo ujemanje med njimi in grupami rotacijskih simetrij platonskih teles. Definiramo grupe in dokažemo Lagrangeev izrek. Nato še definiramo delovanje grupe in dokažemo izrek o orbitah in stabilizatorjih.

1 Grupe

Definicija 1.1. Grupa $(G, \cdot)$ *je par množice* G *in binarne operacije* $\cdot$, *ki vsakemu elementu* $a, b \in G$ *pripiše natanko en element v* G, *ki ga označimo z* $a \cdot b$.

Za grupe veljajo sledeči aksiomi:

- *operacija grupe je asociativna, torej za vsake tri elemente* $a, b, c \in G$ *velja* $(a \cdot b) \cdot c = a \cdot (b \cdot c)$,
- *grupa ima enoto, torej tak* $e \in G$, *da za vsak* $a \in G$ *velja* $a \cdot e = e \cdot a = a$,
- *vsak element grupe ima svoj inverz, torej za vsak* $a \in G$ *obstaja tak* $a^{-1} \in G$, *tako da* $a \cdot a^{-1} = a^{-1} \cdot a = e$.

Če za vsaka $a, b \in G$ velja $a \cdot b = b \cdot a$, rečemo, da je grupa Abelova.

Definicija 1.2. *Moč grupe* G *je število elementov v njeni množici. Označimo jo z* $|G|$.

Na primeru si poglejmo, ali je množica celih števil $\mathbb{Z}$ grupa za seštevanje. Asociativnost očitno drži, prav tako ima $\mathbb{Z}$ enoto (to je število 0). Obratni element za poljubno celo pa je njegovo nasprotno število $-a$. Množica celih števil $\mathbb{Z}$ je torej grupa za seštevanje.

Dokažimo še dve temeljni lastnosti grup.

Trditev 1.1. *V grupi obstaja natanko ena enota.*

Dokaz: Predpostavimo, da obstajata vsaj dve različni enoti, e_1 in e_2. Po definiciji sledi $e_1 = e_1 \cdot e_2 = e_2$. Očitno velja enakost $e_1 = e_2$, torej je enota v dani grupi natanko ena. □

Trditev 1.2. *Vsak element grupe ima natanko en inverz.*

Dokaz. Predpostavimo, da imamo dva različna inverza, ${a_1}^{-1}$ in ${a_2}^{-1}$. Sledi

$$ {a_1}^{-1} = {a_1}^{-1} a {a_2}^{-1} = {a_2}^{-1}, $$

torej morata inverza biti ista, kar je protislovje. Torej za vsak element obstaja natanko en inverz. □

Definicija 1.3. *Naj bo* H *podmnožica elementov grupe* $(G, \cdot)$. *Potem je* $(H, \cdot)$ *podgrupa* $(G, \cdot)$, *če:*

- *podmnožica* H *vsebuje enoto grupe* G,

- *je za vsaka* $a, b \in H$ *tudi* $a \cdot b \in H$,
- *za vsak* $a \in H$ *je* $a^{-1} \in H$.

Za primer vzemimo grupo $(\mathbb{R} \setminus \{0\}, \times)$, kjer operacija $\times$ označuje množenje, in podmnožico njenih elementov $\mathbb{Q} \setminus \{0\}$. Pokazati želimo, da je $(\mathbb{Q} \setminus \{0\}, \times)$ podgrupa $(\mathbb{R} \setminus \{0\}, \times)$. Enota grupe (število 1) je res vsebovana v neničelnih racionalnih številih. Prav tako je produkt dveh poljubnih neničelnih racionalnih števil neničelno racionalno število. Nazadnje, inverz neničelnega naravnega števila p/q je njegova obratna vrednost q/p. Dokazali smo, da je $(\mathbb{Q} \setminus \{0\}, \times)$ podgrupa $(\mathbb{R} \setminus \{0\}, \times)$.

Definicija 1.4. *Naj bo* H *podgrupa grupe* G *in* a *poljuben element* G. *Množico* $aH = \{ax | x \in H\}$ *imenujemo* levi odsek *grupe* G *po podgrupi* H.

Lema 1.1. *Leva odseka* aH *in* bH *sta bodisi enaka bodisi nimata skupnega elementa.*

Dokaz. Denimo, da imata aH in bH skupen element $ah_1 = bh_2$. Sledi, da je $a(h_1 {h_2}^{-1}) = b$. Vidimo, da je $h_3 = h_1 {h_2}^{-1}$ element podgrupe H, torej je $b \in aH$. Naj bo b_x element $|bH|$, kjer je x element množice H. To lahko zapišemo kot $b_x = (ah_3)x = a(h_3 x)$, kar je element podgrupe H. Torej je bH podmnožica aH. Simetrično lahko dokažemo tudi $aH \subseteq bH$. Iz tega sledi $aH = bH$, torej sta odseka enaka. □

Definicija 1.5. *Družina množic* $\mathcal{A} = \{A_1, A_2, \dots\}$ *je* razbitje *ali* particija *množice* B, *če so množice v družini neprazne, paroma disjunktne in če* $A_1 \cup A_2 \cup \dots = B$.

Vidimo, da tvorijo levi odseki G po H particijo grupe G, saj so paroma disjuntni in ker je vsak $a \in G$ vsebovan v levi particiji aH. Množico vseh levih odsekov grupe G po podgrupi H imenujemo kvocientna množica in jo označimo z G/H. Moč kvocientne grupe imenujemo *indeks* podgrupe H v G in ga zapišemo kot $[G : H]$.

Lema 1.2. *Vsi levi odseki grupe* G *po podgrupi* H *imajo isto moč.*

Dokaz. Tudi podgrupa H je levi odsek, saj lahko vzamemo $a = e$. Sedaj moramo dokazati, da za poljuben $a \in G$ velja $|aH| = |H|$. Spomnimo se, da aH dobimo tako, da vsak element iz H na levi pomnožimo z a. Vsi elementi so različni, ker $ah_1 = ah_2$ implicira $h_1 = h_2$. □

Ker levi odseki tvorijo razbitje grupe, je pri končnih grupah vsota moči levih odsekov enaka moči grupe.

$$|H| + |a_2 H| + |a_3 H| + \dots + |a_r H| = |G|$$
$$r \cdot |H| = |G|$$

Iz slednje enačbe je razviden naslednji izrek.

Izrek 1.1 (Lagrangeev izrek)**.** *Moč končne grupe* G *je deljiva z močjo njene poljubne podgrupe* H, *torej velja* $|G| = |H|[G : H]$.

Sicer splošno uporaben izrek nam bo prišel prav šele kasneje ob dokazovanju izreka o orbitah in stabilizatorjih.

2 Ciklična in diedrska grupa

V nadaljevanju bomo spoznali dva pogosta tipa grup, to sta ciklična in diedrska grupa, ki ju bomo definirali preko množice elementov, ki ju generirajo.

Definicija 2.1. *Naj bo X neprazna podmnožica elementov grupe G. Množico vseh elementov v G, ki jih lahko zapišemo kot $y_1y_2y_3\dots y_k$, kjer za vsak člen velja $y_i \in X$ ali $y_i^{-1} \in X$, označimo z $\langle X\rangle$. Poljubna neprazna množica X* generira *podgrupo G. Elementom množice X pravimo* generatorji.

Kot primer, grupo pozitivnih racionalnih števil za množenje generira njena podmnožica naravnih števil. Podobno lahko grupo celih števil za seštevanje generira podmnožica $\{1\}$.

Definicija 2.2. *Grupi, ki jo generira en sam element, pravimo* ciklična grupa. *Označimo jo z*

$$C_n = \{1, a, a^2, \dots, a^{n-1}\}.$$

Definicija 2.3. Simetrija *je preslikava, ki preslika nek matematični objekt v samega vase.*

Definicija 2.4. *Grupi simetrij pravilnega n-kotnika pravimo* diedrska grupa. *Označimo jo z*

$$D_{2n} = \langle\{r, z\}\rangle = \{1, r, r^2, \dots, r^{n-1}, z, rz, r^2z, \dots, r^{n-1}z\},$$

kjer r ustreza rotaciji za kot $\frac{2\pi}{n}$ v pozitivni smeri in z ustreza zrcaljenju preko izbrane simetrale n-kotnika. Enota 1 je v tem primeru simetrija, ki lik pusti pri miru.

Za diedrsko grupo veljajo še naslednje relacije:

$$r^n = 1,\ z^2 = 1,\ r^{-1}z = zr.$$

Definicija 2.5. *Naj bo $a \in G$. Najmanjšemu naravnemu številu s, da je $a^s = 1$, pravimo* red *elementa a. Pravimo, da ima a v tem primeru* končen red. *V nasprotnem primeru, če je $a^s \neq 1$ za vsak $s \in \mathbb{N}$, pa rečemo, da ima a* neskončen red.

Da ponazorimo, v grupi $C_4 = \langle\{a\}\rangle$ je red elementa a enak 4, red elementa a^2 pa je enak 2. Podobno je v grupi $D_{12} = \langle\{r, z\}\rangle$ red elementov r^3z ter r^5z enak 2, red elementa r pa je enak 6.

3 Delovanje grup

V sklepnem delu prejšnega poglavja smo spoznali diedrsko grupo v kontekstu simetrij pravilnega n-kotnika. Tako smo implicitno spoznali delovanje grupe na množici točk n-kotnika. V slednjem delu članka bomo spoznali še grupe, ki delujejo na platonska telesa. Za začetek pa, seveda, utemeljimo delovanje grup.

Definicija 3.1. Delovanje *grupe G na množici X je preslikava*

$$G \times X \to X, (g, x) \qquad\qquad \mapsto g \cdot x,$$

za katero velja:

- $1 \cdot x = x$,
- $a \cdot (b \cdot x) = (ab) \cdot x$.

Za prej opisano delovanje grupe D_{2n} na pravilnem n-kotniku lahko bralec preveri, da zgornji lastnosti res veljata. V nadaljevanju nam bodo prišli prav tudi naslednja definicija in lemi.

Definicija 3.2. *Naj bo G grupa, ki deluje na poljubno množico X. Potem pravimo množici $O_x = G \cdot x = \{g \cdot x|\ g \in G\}$* orbita elementa x, *množici $G_x = \{a \in G|\ a \cdot x = x\}$ pa* stabilizator elementa x.

Lema 3.1. *Stabilizator G_x je podgrupa G za poljuben $x \in X$.*

Dokaz. Preveriti moramo, da stabilizator vsebuje enoto, je zaprt za grupno operacijo ter vsebuje inverze vseh svojih elementov. Vemo, da velja

$$1 \cdot x = x,$$

torej je $1 \in G_x$. Pokažimo, da je G_x zaprta za operacijo. Naj bosta $a, b \in G_x$, sledi

$$(ab) \cdot x = a \cdot (b \cdot x) = a \cdot x = x,$$

torej je $ab \in G_x$. Prav tako G_x vsebuje inverze svojih elementov, saj za vsak $a \in G_x$ velja

$$a^{-1} \cdot x = a^{-1} \cdot (a \cdot x) = (a^{-1}a) \cdot x = 1 \cdot x = x,$$

torej je tudi $a^{-1} \in G_x$. S tem smo dokazali, da je G_x podgrupa G.

Lema 3.2. *Naj grupa G deluje na množici X. Potem tvorijo orbite elementov razbitje množice*

$$X = O_1 \cup O_2 \cup \cdots \cup O_k.$$

Za dokaz te leme si bomo pomagali z ekvivalenčnimi relacijami.

□

Definicija 3.3. *Relacija $\sim$ na množici A je ekvivalenčna, če za poljubne $a, b, c \in A$ velja:*

- *refleksivnost: $a \sim a$,*
- *simetričnost: če $a \sim b$ potem $b \sim a$,*
- *tranzitivnost: če $a \sim b$ in $b \sim c$, potem je $a \sim c$.*

Izrek 3.1. *Dana ekvivalenčna relacija v množici porodi particijo, kjer sta dva elementa v isti množici razbitja natanko tedaj, ko med njima velja ekvivalenčna relacija.*

Dokaz izreka 3.2. Želimo, da sta dva elementa množice X v isti množici razbitja, če je eden izmed elementov v orbiti drugega. Definiramo torej relacijo $s \sim s' \iff \exists g \in G : s' = g \cdot s$. Potrebno je dokazati, da je relacija ekvivalenčna. Refleksivnost velja, ker je $s = id \cdot s$ za vsak $s \in S$. Prav tako velja, da $s' = g \cdot s$ implicira $g^{-1} \cdot s' = s$, torej je relacija simetrična. Dokažimo še tranzitivnost. Za elemente $a, b, c \in X$ predpostavimo $a \sim b$ in $b \sim c$, to pomeni, da velja $b = g_1 \cdot a$ in $c = g_2 \cdot b$. Prvo enačbo vstavimo v drugo in dobimo $c = g_2 \cdot (g_1 \cdot a)$, iz česar sledi $c = (g_2 \cdot g_1) \cdot a$, torej je tudi $a \sim c$, zato je relacija tranzitivna in posledično ekvivalenčna. Po izreku 3.1 torej orbite elementov množice X tvorijo razbitje množice X. □

Izrek 3.2 (Izrek o orbiti in stabilizatorju)**.** *Naj bo X končna množica, na kateri deluje končna grupa G. Naj bosta G_x in O_x stabilizator ter orbita nekega elementa $x \in X$. Potem velja*

$$|G| = |G_x| \cdot |O_x|.$$

Bralec bo pri zgornji enačbi opazil podobnost z Lagrangeevim izrekom 1.1. Res, ker vemo, da je G_x podgrupa G, je dovolj dokazati, da je indeks podgrupe G_x v grupi G enak $|O_x|$. Preden se lotimo dokaza izreka, si poglejmo še definicijo in lemo, s katerima si bomo pomagali.

Definicija 3.4. *Naj bo f preslikava iz množice A v množico B. Preslikava f je* injektivna*, če $f(a_1) = f(a_2)$ implicira $a_1 = a_2$, za vsaka $a_1, a_2 \in A$. Preslikava f je* surjektivna*, če za vsak $b \in B$ obstaja tak $a \in A$, da je $f(a) = b$. Preslikavi, ki je hkrati injektivna in surjektivna, pravimo* bijekcija*.*

Če obstaja bijekcija iz ene končne množice v drugo, potem imata množici enako moč.

Lema 3.3. *Naj grupa G deluje na množici X. Potem za poljuben element $x \in X$ obstaja bijekcija*

$$\begin{aligned} \varepsilon : G_x &\to O_x, \\ aG_x &\longmapsto a \cdot x. \end{aligned}$$

Zgoraj smo z aG_x označili levi odsek grupe G po podgrupi G_x.

Dokaz. Najprej je treba pokazati, da je preslikava ϵ dobro definirana. Želimo pokazati, da je vrednost funkcije neodvisna od izbire predstavnika levega odseka, z drugimi besedami $aG_x = bG_x \Rightarrow a \cdot s = b \cdot s$.

Vzemimo torej, isti levi odsek, ki ga zapišemo z dvema predstavnikoma $a, b \in G$. Obe strani enačbe $aG_x = bG_x$ pomnožimo na levi z a^{-1} in dobimo $G_x = a^{-1}bG_x$. Ker je G_x podgrupa in je torej zaprta za operacijo grupe, mora veljati $a^{-1}b \in G_x$, kar pomeni, da je element $a^{-1}b$ v stabilizatorju elementa x, oziroma $(a^{-1}b) \cdot s = s$. Končamo s tem, da pomnožimo obe strani enačbe na levi z a in dobimo $b \cdot s = a \cdot s$, kot smo želeli.

Iz tega sledi, da je preslikava ε dobro definirana. Pokazati moramo še bijektivnost. Najprej dokažemo injektivnost, tako da ponovimo dokaz dobre definiranosti v obratno smer. Surjektivnost pa sledi iz dejstva, da za vsak element orbite $g \cdot x$ obstaja levi odsek gG_x, da velja $\varepsilon(gG_x) = g \cdot x$. Iz tega sledi, da je ε bijektivna preslikava. □

Dokaz izreka 3.2. Izberemo neki $x \in X$. Naj bo G_x stabilizator elementa x. Po lemi 3.1 je G_x podgrupa G. Po Lagrangeevem izreku 1.1 sledi

$$|G| = |G_x| \cdot [G : G_x].$$

Namesto indeksa podgrupe G_x v G lahko po definiciji pišemo moč kvocientne grupe

$$|G| = |G_x| \cdot [G/G_x].$$

Po lemi 3.3 obstaja bijekcija med G/G_x in O_x, torej imata ti dve množici isto moč $|G| = |G_x| \cdot |O_x|$, s čimer smo dokazali izrek o orbiti in stabilizatorju. □

4 Končne podgrupe SO_3

Izkaže se, da sta Lagrangeev izrek 1.1 ter izrek 3.2 o orbiti in stabilizatorju splošno uporabna na področju klasifikacije grup. V sklepnem delu svojega članka si bomo pogledali klasifikacijo podgrup SO_3 in njihovo ujemanje z grupami simetrij znanih likov in teles.

Definicija 4.1. *Grupa SO_3 je* grupa vseh rotacij *okoli izhodišča v tridimenzionalnem Evklidskem prostoru* ($\mathbb{R}^3$). *Operacija te grupe je kompozitum.*

Za namene klasifikacije nam bo prav prišel naslednji izrek, ki ga navedemo brez dokaza, saj bi ta presegal obseg našega članka.

Izrek 4.1. *Vsak element SO_3 razen enote je rotacija okoli neke premice skozi izhodišče.*

Vidimo, da poljuben od enote različen element ohranja vse točke vzdolž takšne premice. Za namene preprostosti bomo opazovali zgolj tisti dve točki na premici, ki ležita na enotski sferi.

Definicija 4.2. *Naj bo G končna podgrupa grupe SO_3.* Pol *grupe G je točka na enotski sferi, ki jo neki od enote različen element $g \in G$ ohranja. Množico vseh polov podgrupe G označimo s $\mathcal{P}$.*

Pri klasifikaciji si bomo natančneje ogledali delovanje poljubne končne podgrupe G na množico njenih polov $\mathcal{P} \subset \mathbb{R}^3$. Pred tem si poglejmo še eno ključno lastnost.

Lema 4.1. *Množica $\mathcal{P}$ je unija nekaterih orbit, ki nastanejo ob delovanju grupe G na $\mathbb{R}^3$.*

Dokaz. Želimo dokazati, da je za poljuben $p \in \mathcal{P}$ njegova orbita O_p podmnožica $\mathcal{P}$. Iz definicije sledi, da obstaja od enote različen element $g \in G$, da velja $g \cdot p = p$. Pokažimo, da za poljuben element $h \in G$ velja, da je $h \cdot p$ element množice $\mathcal{P}$.

Naj bo $q = h \cdot p$. Da bo $q \in \mathcal{P}$, mora obstajati od enote različen element G, ki ohranja q. Opazimo, da element hgh^{-1} zadošča našemu pogoju

$$\begin{aligned} hgh^{-1} \cdot q &= hgh^{-1} \cdot (h \cdot p) \\ &= hg(h^{-1}h) \cdot p \\ &= hg \cdot p \\ &= h \cdot (g \cdot p) \\ &= h \cdot p \\ &= q. \end{aligned}$$

Sledi, da je q prav tako element $\mathcal{P}$. □

Izrek 4.2 (Klasifikacija končnih podgrup SO_3)**.** *Vsaka končna podgrupa SO_3 ima eno izmed naslednjih oblik:*

- C_n*: grupa rotacij za večkratnik kota* $\frac{2\pi}{n}$ *okoli neke premice,*
- D_{2n}*: grupa rotacijskih simetrij pravilnega n-kotnika,*
- T*: tetraedrska grupa (*12 *rotacijskih simetrij tetraedra),*
- O*: oktaedrska grupa (*24 *rotacijskih simetrij oktaedra ali kocke),*
- I*: ikozaedrska grupa (*60 *rotacijskih simetrij ikozaedra ali dodekaedra).*

Dokaz. Naj bo G končna podgrupa SO_3 in $p \in \mathcal{P}$. Označimo $|G_p| = r_p$, $|O_p| = n_p$ in $|G| = N$. Pomagali si bomo še z naslednjima dejstvoma:

- Velja, da je $r_p > 1$ za poljuben $p \in \mathcal{P}$. Grupa stabilizatorjev mora namreč vsebovati identiteto in po definiciji pola vsaj še en drug element G. Omenimo še, da za nek pol $p \in \mathcal{P}$ obstaja $r_p - 1$ netrivialnih elementov grupe G, ki pol p ohranjajo.
- Vsak element G, ki ni enota, ima 2 pola. Po izreku 4.1 ohranja vsak netrivialen element grupe G natanko vse točke določene premice skozi izhodišče. Pola, ki ustrezata temu elementu, sta torej presečišči premice z enotsko sfero.

Želimo prešteti vse pare (p, q), kjer sta $p \in \mathcal{P}$, $q \in G \setminus \{1\}$ in $q \cdot p = p$. Preštejemo jih na dva načina, in sicer po polih ter po elementih grupe. Iz prej navedenih lastnosti velja

$$2(N-1) = \sum_{p \in \mathcal{P}} (r_p - 1).$$

Po lemi 4.1 lahko $\mathcal{P}$ zapišemo kot

$$\mathcal{P} = O_1 \cup O_2 \cup O_3 \cup \cdots \cup O_k.$$

Ker imajo poli znotraj iste orbite isti n_p in ker po izreku 3.2 velja $r_p n_p = N$, imajo poli znotraj iste orbite

isto moč stabilizatorja r_p. Tako lahko vsoto po polih izrazimo kot vsoto po vseh k orbitah:

$$\sum_{i=1}^{k}(r_i-1)n_i = 2N-2$$
$$\sum_{i=1}^{k}\left(1-\frac{n_i}{N}\right) = 2-\frac{2}{N}$$
$$\sum_{i=1}^{k}\left(1-\frac{1}{r_i}\right) = 2-\frac{2}{N}.$$

Vidimo, da je vsak seštevanec na levi strani večji ali enak $\frac{1}{2}$, desna stran enačbe pa je strogo manjša od 2. Iz tega sledi, da imamo največ 3 orbite.

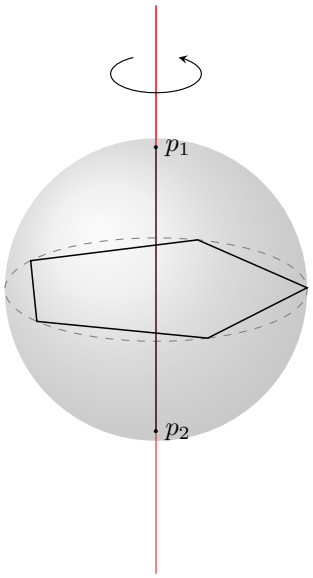
Obravnavati moramo torej 3 primere:

- Obstaja samo 1 orbita. Velja torej
$$1-\frac{1}{r_1} = 2-\frac{2}{N}.$$
Ker je leva stran enačbe vedno manjša od 1, desna pa večja ali enaka 1, enakosti nikoli ni zadoščeno. Zaključimo, da končna podgrupa SO_3, katere poli tvorijo eno samo orbito, ne more obstajati.

- Obstajata 2 orbiti. Velja torej
$$\left(1-\frac{1}{r_1}\right)+\left(1-\frac{1}{r_2}\right) = 2-\frac{2}{N}$$
$$\frac{1}{r_1}+\frac{1}{r_2} = \frac{2}{N}.$$
Po Lagrangeevem izreku velja $r_1, r_2 \leq N$, iz česar sledi, da je $\frac{1}{r_1}+\frac{1}{r_2} \geq \frac{2}{N}$. Enakosti je zadoščeno natanko tedaj, ko je $r_1 = r_2 = N$. Po izreku 3.2 o orbitah in stabilizatorjih velja še $n_1 = n_2 = 1$.

Trdimo, da takšni velikosti orbit in stabilizatorjev ustrezata ciklični grupi C_N. Res, pri grupi rotacij za kot $\frac{2\pi}{N}$ okoli izbrane premice imamo dva pola, ki ju stabilizira vsak element grupe, zato vsak od njiju posebej tvori svojo orbito z enim elementom.

Primer ciklične podgrupe C_5 lahko vidimo na sliki 1. Gre za grupo rotacij za kot $\frac{2\pi}{5}$ okoli navpične osi. Vse rotacije ohranjajo v enotsko sfero vrisan pravilni petkotnik, pravokoten na os.



Slika 1: Ciklična podgrupa C_5 in njena pola p_1 ter p_2.

- Obstajajo 3 orbite. Velja torej

$$\left(1-\frac{1}{r_1}\right)+\left(1-\frac{1}{r_2}\right)+\left(1-\frac{1}{r_3}\right)=2-\frac{2}{N}$$
$$\frac{1}{r_1}+\frac{1}{r_2}+\frac{1}{r_3}=1+\frac{2}{N},$$

iz česar sledi

$$\frac{1}{r_1}+\frac{1}{r_2}+\frac{1}{r_3}>1. \tag{1}$$

Brez škode za splošnost naj velja $r_1 \leq r_2 \leq r_3$. Želimo dokazati, da je $r_1 = 2$. Predpostavimo, da je $r_1 \geq 3$. Izraz $\frac{1}{r_1}+\frac{1}{r_2}+\frac{1}{r_3}$ ocenimo navzgor

$$\frac{1}{r_1}+\frac{1}{r_2}+\frac{1}{r_3}\leq\frac{1}{r_1}+\frac{1}{r_1}+\frac{1}{r_1}=\frac{3}{r_1}\leq 1,$$

kar je v protislovju z neenakostjo (1). Ob dejstvu, da je $r_i > 1$, sledi $r_1 = 2$.
Denimo, da je $r_1 = r_2 = 2$, potem sledi

$$\frac{1}{r_1}+\frac{1}{r_2}+\frac{1}{r_3}=1+\frac{2}{N}$$
$$\frac{1}{2}+\frac{1}{2}+\frac{1}{r_3}=1+\frac{N}{2}$$
$$\frac{1}{r_3}=\frac{2}{N},$$

iz česar sledi, da za poljuben $r_3 = k$ velja $N = 2k$.

Trdimo, da tak nabor orbit ustreza diedrski grupi $D_{2k} = \langle\{r, z\}\rangle$. Spomnimo se, da je to grupa simetrij pravilnega k-kotnika. Tako kot na sliki 1 liku očrtamo sfero. Konfiguracijo prestavimo v izhodišče in jo

povečamo, da je sfera enotska. Skozi središče lika potegnemo premico, ki je pravokotna na ploskev lika, nato pa presečišči premice s sfero označimo s p_1 in p_2. Enako kot pri ciklični grupi element r ustreza rotaciji okoli te premice za kot $\frac{2\pi}{k}$. Vidimo, da rotacije $1, r, \ldots, r^{k-1}$ tvorijo stabilizator naših dveh polov. Opazimo tudi, da zrcaljenje z v treh dimenzijah ustreza rotaciji za kot π, ki med seboj menja pola p_1 in p_2. Sledi, da ta dva pola tvorita našo tretjo orbito.

Podobno lahko preverimo, da so oglišča lika poli, ki tvorijo našo prvo orbito s k elementi, kjer vsak pol stabilizirata elementa grupe 1 in z. Drugo orbito tvorijo projekcije središč stranic na enotsko sfero. Ugotovili smo, da naš nabor velikosti orbit ter stabilizatorjev ustreza diedrski grupi.

Preostane nam torej le še primer, ko je $r_2 \geq 3$. Denimo, da je $r_2 \geq 4$. Sledi, da je izraz $\frac{1}{r_1} + \frac{1}{r_2} + \frac{1}{r_3}$ lahko kvečjemu enak 1 in tako ponovno pridemo do protislovja z neenakostjo (1). Torej je $r_2 = 3$. Poglejmo še, katere vrednosti lahko zasede r_3. Vemo, da velja $\frac{1}{2} + \frac{1}{3} + \frac{1}{r_3} > 1$, iz česar sledi $\frac{1}{r_3} > \frac{1}{6}$. Tako je $r_3 < 6$, oziroma $r_3 \in \{3, 4, 5\}$. Vse preostale možne velikosti orbit in stabilizatorjev lahko zdaj zberemo v tabeli 1.

	r_1, r_2, r_3	n_1, n_2, n_3	N
T	2, 3, 3	6, 4, 4	12
O	2, 3, 4	12, 8, 6	24
I	2, 3, 5	30, 20, 12	60

Tabela 1: Možne velikosti preostalih orbit in stabilizatorjev končne podgrupe.

Trdimo, da prva izmed preostalih možnosti ustreza grupi rotacijskih simetrij tetraedra, druga ustreza grupi rotacijskih simetrij oktaedra ali kocke, telesi imata namreč isto grupo simetrij. Treja možnost pa ustreza grupi rotacijskih simetrij ikozaedra oziroma dodekaedra. Zaradi obsežnosti dokaza in dolžine tega članka ne bomo dokazovali, zakaj te velikosti orbit in stabilizatorjev enolično določijo navedene tri grupe simetrij platonskih teles. Bralec lahko dokaz poišče v zapiskih avtorja Hong Thien An Bui [4]. Vendarle pa si bomo kot zanimivost pogledati primer grupe rotacijskih simetrij kocke.

□

4.1 Grupa rotacijskih simetrij kocke

Začnimo s preštevanjem vseh simetrije kocke, ki porodijo grupo:

- Grupa mora vsebovati identito, ki preslika vse točke kocke same vase.
- Imamo po 3 rotacije okoli premice skozi središči nasprotnih si ploskev na kocki. Primer take rotacije imamo na sliki 2. Te premice so 3, torej je teh rotacij skupaj 9.
- Sledita še po 2 rotaciji okoli posamezne telesne diagonale v kocki, torej okoli premice skozi nasprotni si oglišči. Primer lahko vidimo na sliki 3. Kocka ima 3 telesne diagonale, torej je teh elementov skupaj 6.
- Na koncu imamo še 1 rotacijo okoli premice skozi središči nasprotnih si robov na kocki, kot lahko vidimo na sliki 4. Teh premic je skupaj 6.

Skupaj ima grupa rotacijskih simetrij kocke torej 24 elementov.

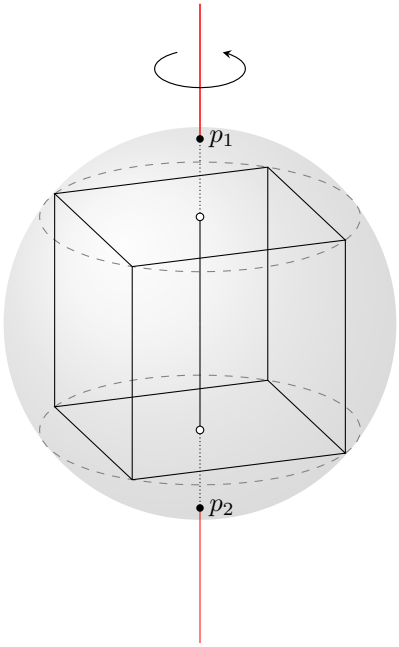
Poglejmo si še pole posameznih od enote različnih rotacij. Vzemimo enotsko sfero, v katero vrišemo kocko. Poli grupe rotacijskih simetrij kocke bodo tvorili tri orbite, in sicer glede na ploskve, oglišča in robove:

1. Prvo orbito tvorijo radialne projekcije središč robov na enotsko sfero, kot je vidno na primeru na sliki 4. Opazimo, da je moč stabilizatorja $r_1 = 2$, saj posamezen rob stabilizirata identiteta in rotacija za kot π okoli premice skozi nasprotna si robova. Vidimo še, da je moč orbite $n_1 = 12$, ker lahko posamezen rob preslikamo v poljubnega izmed 12 robov kocke z ustrezno rotacijo.

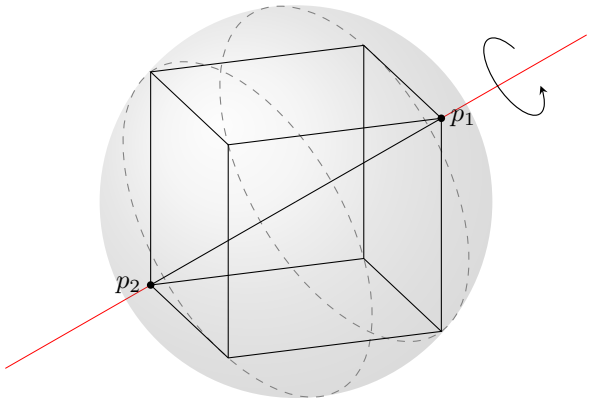
2. Drugo orbito tvorijo oglišča kocke. Za moč stabilizatorja velja $r_2 = 3$, saj posamezno oglišče stabilizirajo identiteta in dve rotaciji okoli ustrezne telesne diagonale kocke, kot vidimo na sliki 3. Prav tako je $n_2 = 8$, ker se lahko posamezno oglišče zarotira v poljubno oglišče kocke.

3. Tretjo orbito tvorijo radialne projekcije središč ploskev kocke na enotsko sfero. Moč stabilizatorja je tokrat $r_3 = 4$, saj posamezno ploskev stabilizirajo identiteta in tri rotacije okoli premice skozi središči nasprotnih si ploskev. Podobno je moč orbite $n_3 = 6$, ker se lahko neka ploskev kocke zarotira na mesto poljubne izmed 6 ploskev kocke.

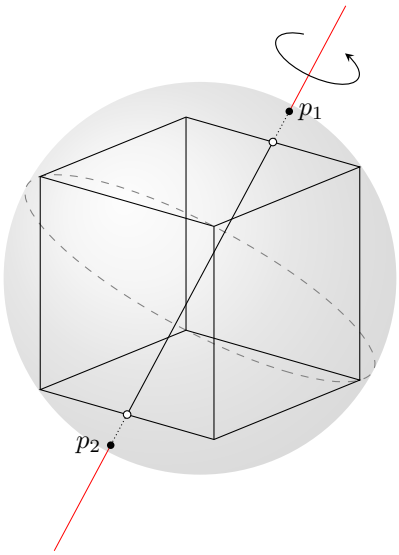
Ker ima vsak od enote različen element natanko 2 pola, lahko zaključimo, da smo res obravnavali vse pole grupe rotacijskih simetrij. Opazimo, da vrednosti velikosti orbit ter stabilizatorjev res sovpadajo z vrednostmi oktaedrske grupe v tabeli 1.



Slika 2: Rotacija kocke okoli premice skozi središči nasprotnih si ploskev.



Slika 3: Rotacija kocke okoli premice skozi telesno diagonalo.



Slika 4: Rotacija kocke okoli premice skozi središči nasprotnih si robov.

Literatura

[1] Matej Brešar, *Uvod v algebro*, poglavje 1 DMFA–založništvo, Ljubljana, 2018.

[2] Michael Artin, *Algebra*, poglavji 2 in 5, Pearson, 2010.

[3] Ivan Vidav, *Algebra*, DMFA–založništvo, poglavji 1 in 2, Ljubljana, 2017.

[4] Hong Thien An Bui, *Classifying the finite subgroups of SO3*, dostopno na: `https://math.uchicago.edu/~may/REU2020/REUPapers/Bui,An.pdf`, 2023, poglavje 9, dostopano: 21. avgust 2023.

De Bruijnovi grafi

Lovro Kastelic, Ana Krošl, Ronja Pražnikar
Mentor: *Juš Kocutar*

Povzetek

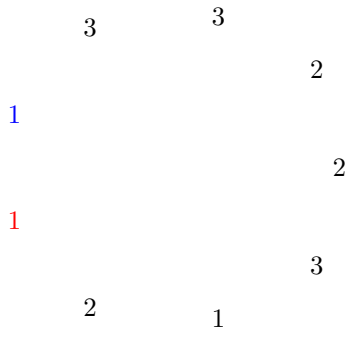
Elemente množice velikosti r želimo razporediti v krožno zaporedje, tako da se vsako zaporedje dolžine n kot podzaporedje zaporednih členov pojavi natanko enkrat. S pomočjo De Bruijnovega grafa in z obstojem Eulerjevega obhoda na njem dokažemo, da je to mogoče za vse pare (r, n).

1 Uvod

Zanima nas, ali lahko prvih r naravnih števil razporedimo v krog na poseben način. Za neko naravno število n želimo v krog razporediti r^n členov tako, da se bo vsako zaporedje dolžine n ponovilo natanko enkrat. Odgovor na vprašanje, ali takšna razporeditev obstaja, je za vsaki števili r in n pritrdilen, v projektu želimo potrditi to tezo. Za rešitev problema bomo spoznali teorijo grafov, definirali De Bruijnov graf in problem iskanja ustreznega krožnega zaporedja prevedli na iskanje Eulerjevega obhoda na De Bruijnovem grafu.

2 Predstavitev problema

Imamo množico naravnih števil $A = \{1, 2, 3, \ldots, r\}$ velikosti r in naravno število n. Poiščemo vsa zaporedja dolžine n, ki vsebujejo elemente množice A. Vemo, da je vseh takih zaporedij r^n, saj imamo za vsakega izmed n členov zaporedja r možnosti za izbiro. Cilj je, da elemente množice A krožno razporedimo na takšen način, da dobimo kot podzaporedja zaporednih členov vsa zaporedja dolžine n. To pomeni, da lahko izberemo n zaporednih elementov na krogu in se premikamo za eno mesto v izbrani smeri, na primer v obratni smeri urinega kazalca. Če so elementi pravilno razporejeni, bi morali dobiti vsa zaporedja elementov množice A dolžine n.



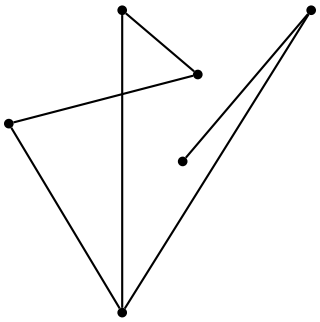
Slika 1: Ustrezno krožno zaporedje za števili $r = 3$ in $n = 2$.

Primer ustreznega krožnega zaporedja za števili $r = 3$ in $n = 2$ opazimo na sliki 1. Začnemo na modri 1 in nadaljujemo pot v obratni smeri urinega kazalca. Prvo podzaporedje dolžine 2 je 11, po vrsti nato sledijo 12, 21, 13, 32, 22, 23, 33 in 31. Enostavno preverimo, da so to vsa zaporedja, saj je vseh $3^2 = 9$.

Zanima nas, ali ustrezna krožna razporeditev obstaja za vse pare naravnih števil (r, n), kjer je r velikost množice možnih členov in n dolžina zaporedja. Problem bomo rešili s teorijo grafov, natančneje z De Bruijnovim grafom in z obstojem usmerjenega Eulerjevega obhoda na njem.

3 Osnovne definicije

Graf je matematični prikaz omrežja. Sestavljata ga množica točk oziroma vozlišč V in množica povezav E med njimi.



Slika 2: Primer grafa.

Na sliki 2 je enostaven zgled grafa. Vozlišča so prikazana s točkami, povezave pa z daljicami med njimi.

Definicija 3.1. *Naj bo V končna množica.* ***Graf*** *G je par $G = (V, E)$, kjer je E družina podmnožic velikosti 2 množice V. Elementom množice V pravimo* ***vozlišča*** *in elementom množice E pravimo* ***povezave****.*

Pogosto pišemo $V = V(G)$ in $E = E(G)$, ko želimo poudariti, da se množici vozlišč in povezav nanašata na specifični graf G. Grafom, definiranim na zgornji način, pravimo tudi *enostavni grafi*, saj ne dopuščajo možnosti večkratnih povezav, zank ali usmerjenih povezav. Vemo zgolj, kdaj je par različnih vozlišč povezan. Pogosto lahko definiramo grafe tudi z neskončno množico vozlišč V in tako dobimo neskočne grafe. Naš projekt obsega končne grafe, zato se z neskončnimi množicami V ne ukvarjamo podrobneje.

Če velja $u, v \in V$ in $\{u, v\} \in E$, potem to zapišemo krajše kot $uv \in E$.

Definicija 3.2. *Množico vseh vozlišč, ki so povezana s poljubnim vozliščem grafa G, imenujemo* ***soseščina*** *vozlišča v, označimo jo z*

$$N(v) = \{u \in V \mid vu \in E\}.$$

Moč množice $N(v)$ imenujemo ***stopnja*** *vozlišča v in jo označimo z $d(v)$, torej $d(v) = |N(v)|$.*

Dokažimo dva enostavna izreka, da pokažemo zveze med novo definiranimi pojmi.

Izrek 3.1 (Lema o rokovanju)**.** *Naj bo G graf. Potem velja*

$$\sum_{v \in V(G)} d(v) = 2|E(G)|.$$

Dokaz. Definirajmo množico M, ki vsebuje urejene pare vozlišč v in povezav e, ki imajo vozlišče v za enega od krajišč, torej

$$M = \{(v, e) \mid v \in V(G) \text{ in } e = vu \text{ za neki } \ u \in V(G)\}.$$

Moč množice M bomo izračunali na dva načina. Najprej se osredotočimo na vozlišča. Zanima nas število povezav okoli vsakega vozlišča, kar je po definiciji enako stopnji vozlišča. Zato seštejemo stopnje vseh vozlišč v grafu. Velja

$$|M| = \sum_{v \in V(G)} d(v).$$

Po drugi strani se lahko osredotočimo na povezave. Za poljubno povezavo e nas zanima število vseh vozlišč v, ki so povezana z njo. Iz definicije povezave vemo, da je povezava povezana z natanko dvema vozliščema. Za povezavo e imamo torej natanko dva para, vsak vsebuje eno od dveh vozlišč, med katerima povezava poteka. Velikost množice M je zato enaka dvakratniku velikosti množice E, torej velja

$$2|E| = |M| = \sum_{v \in V} d(v),$$

kar smo želeli dokazati. □

Izrek 3.2. *Naj bo G graf, potem ima G sodo mnogo vozlišč lihe stopnje.*

Dokaz. Za dokaz uporabimo izrek 3.1. Vemo, da velja

$$\sum_{v \in V(G)} d(v) = 2|E(G)|.$$

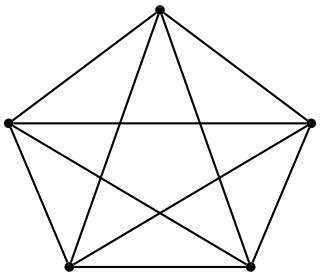
Vsoto stopenj vseh vozlišč lahko razdelimo na vsoto vseh sodih stopenj in vsoto vseh lihih stopenj

$$\sum_{\substack{u \in V(G) \\ d(u)\ sodo}} d(u) + \sum_{\substack{v \in V(G) \\ d(v)\ liho}} d(v) = 2|E(G)|.$$

Desna stran enakosti je soda in vsota vseh sodih stopenj je vedno soda. Zato velja, da je vsota vseh lihih stopenj soda, kar je res natanko tedaj, ko bo vozlišč z liho stopnjo sodo mnogo. □

Poimenujmo grafe, ki imajo vse možne povezave.

Definicija 3.3. ***Polni graf*** *na n vozliščih, ki ga označimo s K_n, je graf, v katerem je vsako vozlišče povezano z vsemi ostalimi vozlišči v grafu.*



Slika 3: Poln graf K_5 na petih vozliščih.

Radi bi imeli definirane pojme za različne vrste zaporedij sosednjih vozlišč v grafu. Razlikovati želimo, na primer med zaporedji, pri katerih dopuščamo ponavljanje vozlišč ali povezav. Radi bi ločili tudi med zaporedji, pri katerih je začetno vozlišče enako končnemu, od zaporedij, pri katerih ni.

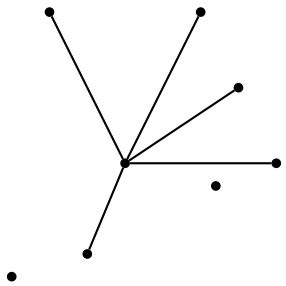
Definicija 3.4. *Naj bo $G = (V, E)$ graf. Zaporedje vozlišč $v_0, v_1, \ldots, v_n$ je* ***sprehod****, če velja $v_i v_{i+1} \in E$ za vse $0 \leq i \leq n-1$.* ***Obhod*** *je sprehod, za katerega velja $v_0 = v_n$.* ***Pot*** *je sprehod, v katerem se vsako vozlišče pojavi največ enkrat.* ***Cikel*** *je sprehod, za katerega velja $v_0 = v_n$ in v katerem se vsako vozlišče razen v_0 pojavi največ enkrat.*

Povezani grafi so tisti, pri katerih lahko iz vsakega vozlišča s potjo pridemo do poljubnega drugega vozlišča.

Definicija 3.5. *Graf G je* ***povezan****, če za vsaki vozlišči $v, w \in V(G)$ obstaja pot $v_0, v_1, v_2, \ldots, v_n$, da velja $v_0 = v$ in $v_n = w$.*

Tudi če graf ni povezan, lahko govorimo o njegovih povezanih delih.

Definicija 3.6. ***Povezana komponenta*** *grafa $G = (V, E)$ je podmnožica W množice V, tako da je graf H, ki ima za vozlišča množico W in za množico povezav vse povezave med vozlišči množice W, ki so v grafu G, maksimalno povezan. To pomeni, da je graf H povezan, hkrati pa v grafu G ni nobenih povezav med vozlišči množice W in vozlišči izven množice W.*



Slika 4: Nepovezan graf s tremi povezanimi komponentami.

Primer nepovezanega grafa s tremi povezanimi komponentami je na sliki 4.

Definirajmo pomembno vrsto sprehoda, ki gre skozi vsako povezavo grafa natanko enkrat in se vrne na začetno vozlišče sprehoda.

Definicija 3.7. ***Eulerjev obhod*** *je obhod, tako da za vsak $v \in V$ velja, da je $v = v_i$ za vsaj en $i \in \{0, 1, \ldots, n-1\}$, vsaka povezava $e \in E$ je enaka $e = v_i v_{i+1}$ za natanko en $i \in \{0, 1, \ldots, n-1\}$ in velja $v_0 = v_n$.*

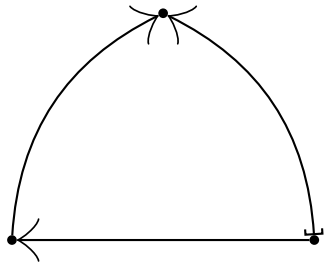
3.1 Usmerjeni grafi

Pri nekaterih omrežjih nas ne zanimajo le povezave ampak tudi njihova smer. Matematično to modeliramo s pojmom usmerjenega grafa. Definicija je podobna kot za enostavne grafe, le da množico E spremenimo v podmnožico kartezičnega produkta $V \times V$ in tako upoštevamo smer povezave.

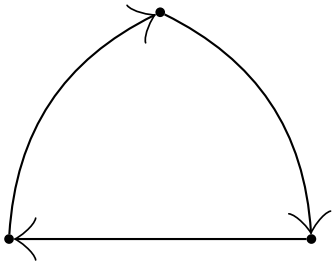
Definicija 3.8. *Naj bo V končna množica. Par $G = (V, E)$, kjer je E podmnožica kartezičnega produkta $V \times V$, imenujemo* ***usmerjen graf****.*

Če velja $u, v \in V$ in $(u, v) \in E$, potem to zapišemo kot $uv \in E$. Za pojme sprehodov, poti in ciklov v usmerjenih grafih vzamemo enake definicije kot v primeru enostavnih grafov, le da za povezave uporabljamo pojem usmerjene povezave. V skicah usmerjenih grafov bomo daljico med točkama, ki je prej nakazovala povezavo, nadomestili s puščico, ki nakazuje usmerjeno povezavo. Usmerjena povezava uv bo torej prikazana s puščico, ki kaže od vozlišča u do vozlišča v.

Definicija 3.9. *Naj bo G usmerjen graf. Potem je G* ***močno povezan****, ko za vsaki vozlišči $v, w \in V$ obstaja pot $v_0, v_1, \ldots, v_n$ z $v_0 = v$ in $w = v_n$.*



Slika 5: Usmerjeni graf, ki ni močno povezan.



Slika 6: Usmerjeni graf, ki je močno povezan.

Podobno kot v primeru enostavnih grafov želimo tudi v primeru usmerjenih definirati pojma soseščine in stopnje vozlišča. Opazimo, da je v tem primeru pomembna smer povezave, kar moramo upoštevati v definicijah.

Definicija 3.10. ***Izhodna soseščina*** *vozlišča v je množica vseh vozlišč u, ki so z vozliščem v povezana s povezavo, usmerjeno od vozlišča v proti vozlišču u, torej $N^+(v) = \{u \in V(G) \mid vu \in E(G)\}$.*

Vhodna soseščina *vozlišča v je množica vseh vozlišč w, ki so z vozliščem v povezana s povezavo, usmerjeno od vozlišča w do proti vozlišču v, torej $N^-(v) = \{w \in V(G) \mid wv \in E(G)\}$.*

Številu $d^+(v) := |N^+(v)|$ pravimo ***izhodna stopnja*** *vozlišča v, številu $d^-(v) := |N^-(v)|$ pa* ***vhodna stopnja****.*

Kot v primeru enostavnih grafov imamo tudi v primeru usmerjenih grafov izrek, ki opisuje vsote stopenj in število povezav. Dokaz je analogen dokazu leme o rokovanju in ga lahko bralec poizkusi narediti sam.

Izrek 3.3. *Naj bo $G = (V, E)$ usmerjen graf. Potem velja*

$$\sum_{v \in V(G)} d^+(v) = \sum_{v \in V(G)} d^-(v) = |E(G)|.$$

4 Obstoj Eulerjevega obhoda

Recimo, da nas zanima, ali ima poljuben graf Eulerjev obhod. Z uporabo definicije bi morali preveriti zelo veliko obhodov. Želeli bi poiskati zadostne in potrebne pogoje, ki bi jih preverili bolj enostavno kot z uporabo definicije, in bi natanko določili, kdaj ima poljuben graf Eulerjev obhod. Izkaže se, da obstajata dve lastnosti, ki natanko določata grafe z Eulerjevimi obhodi. To sta povezanost in lastnost, da so stopnje vseh vozlišč v grafu soda števila. V tem poglavju bomo dokazali to ekvivalenco.

4.1 Eulerjev obhod v enostavnih grafih

Izrek o obstoju Eulerjevega obhoda lahko dokažemo na dva načina - z uporabo indukcije ali s protislovjem. Mi ga bomo dokazali s protislovjem, saj lahko slednji dokaz z nekaj spremembami prilagodimo v dokaz obstoja Eulerjevega obhoda na usmerjenih grafih.

Najprej bomo dokazali lemo, ki jo bomo uporabili v nadaljnjem dokazu.

Lema 4.1. *Če za graf $G = (V, E)$ velja $|V| \geq 3$ in ima vsako vozlišče v grafu stopnjo vsaj 2, potem ima graf G cikel.*

Dokaz. Izberemo vozlišče $v_0 \in V$, v katerem začnemo pot. Po predpostavki ima v_0 stopnjo vsaj 2, zato sta v soseščini $N(v)$ vsaj dve vozlišči. Naj bo najdaljša pot $W = \{v_0, v_1, \ldots, v_k\}$. Takšna pot obstaja, ker je V končna množica. Vozlišče v_k ima stopnjo vsaj 2, zato mora imeti vsaj še enega soseda u poleg v_{k-1}. Če vozlišče u ni na poti W, je pot $W' = \{v_0, v_1, ..., v_k, u\}$ daljša od poti W, kar pomeni, da smo v protislovju.

Druga možnost je, da vozlišče u je na poti W. Zato je vozlišče u enako vozlišču v_i za neki i. Graf G ima torej cikel $W'' = \{v_i, v_{i+1}, v_{i+2}, \ldots, v_k, v_i\}$. □

Zdaj bomo dokazali glavni izrek iz teorije grafov, ki ga potrebujemo. To je karakterizacija enostavnih grafov z Eulerjevim obhodom.

Izrek 4.1. *Graf G ima Eulerjev obhod, če in samo če je G povezan in je stopnja $d(v)$ sodo število za vsak $v \in V$.*

Dokaz. ($\Longrightarrow$) Predpostavimo, da ima graf $G = (V, E)$ Eulerjev obhod. Najprej dokažimo, da je graf povezan in je stopnja vsakega vozlišča soda. Ker ima graf G Eulerjev obhod, je povezan, saj je Eulerjev obhod po definiciji sprehod, ki vključuje vsa vozlišča.

Naj bo $u \in V$ vozlišče na grafu G. Če je u poljubno vozlišče, ga med Eulerjevim obhodom dosežemo vsaj enkrat in posledično iz njega izstopimo vsaj enkrat. Ker je obhod Eulerjev, vemo, da so v sprehodu vse povezave v grafu. Vemo tudi, da v vsako vozlišče vstopimo tolikokrat, kolikokrat iz njega izstopimo, in skozi nobeno povezavo ne gremo več kot enkrat, torej je število vseh povezav, ki imajo za eno krajišče dano vozlišče, sodo.

($\Longleftarrow$) Predpostavimo, da je graf $G = (V, E)$ povezan in velja, da je za vsako vozlišče $v \in V$ njegova stopnja soda. Najmanjši graf, ki zadošča tem pogojem je graf na enem vozlišču, za katerega izrek očitno velja.

Recimo, da velja $|V| > 1$. Ker je G povezan in imamo vsaj dve vozlišči, mora imeti vsako vozlišče stopnjo vsaj 1. Ker mora biti vsaka stopnja soda, velja $d(v) \geq 2$ za vsako vozlišče $v \in V$. Noben izmed dveh grafov na dveh vozliščih (dve nepovezani točki in točki, povezani s povezavo) tudi ne more imeti vseh stopenj sodih in biti povezan hkrati, zato lahko brez škode za splošnost predpostavimo, da velja $|V| \geq 3$. Velja torej, da je G povezan, vsako vozlišče ima sodo stopnjo in $|V| \geq 3$, zato G izpolnjuje oba pogoja leme 4.1, torej ima cikel. Bolj splošno, vemo, da ima graf G zagotovo obhod brez ponavljanja povezav. Sedaj predpostavimo za protislovje, da izrek ne velja.

Naj bo graf $H = (W, F)$ minimalni protiprimer, torej protiprimer z najmanjšim možnim številom povezav. Velja torej, da je graf H povezan in ima vsako vozlišče sodo stopnjo, vendar H nima Eulerjevega obhoda. Vemo, da je $|W| > 1$, zato zaradi leme 4.1 vemo, da ima graf H obhod brez ponavljanja povezav.

Izberimo obhod brez ponavljanja povezav z največ uporabljenimi povezavami in naj bo W' množica vseh vozlišč v obhodu ter F' množica vseh povezav v obhodu. Po predpostavki vemo, da graf H nima Eulerjevega obhoda, zato velja $F' \neq F$.

Trdimo tudi, da obstajata vozlišči $u \in W'$ in $v \in W$, da velja $uv \in F - F'$ oziroma, da obstaja vozlišče v najdaljšem obhodu, ki je krajišče povezave, ki je ni v obhodu.

Za dokaz ločimo dva primera. V prvem predpostavimo, da velja $W = W'$, torej, da so v najdaljšem obhodu vsa vozlišča grafa H. V tem primeru trditev drži, saj vemo, da je množica $F - F'$ neprazna, zato obstaja neka povezava $f \in F - F'$, ki ima obe krajišči v množici W' po predpostavki. Zato sta obe krajišči iskani vozlišči in f iskana povezava.

V drugem primeru predpostavimo, da je množica $W - W'$ neprazna. Kot že vemo, najdaljši obhod obstaja, zato obstajata vozlišči $z \in W'$ in $x \in W - W'$. Graf H je povezan, zato obstaja pot $z = z_0, \ldots, z_n = x$ med z in x. Velja $z \in W'$ in $x \notin W'$, zato obstaja najmanjše število i, tako da velja $0 \leq i < n$, za katerega je $z_i \in W$ in $z_{i+1} \notin W'$. Po definiciji opazimo, da velja $z_i z_{i+1} \notin F'$, saj vozlišče z_{i+1} ni v najdaljšem obhodu, zato sta iskani vozlišči z_i in z_{i+1}.

Naj bo torej $e = uv$ povezava, ki ni v najdaljšem sprehodu in $u \in W'$. Definirajmo podgraf $X = (W, F - F')$. Naj bo Y povezana komponenta grafa X, ki vključuje povezavo e. Po definiciji je Y povezan graf. Trdimo še, da ima vsako vozlišče v grafu Y sodo stopnjo. Vemo, da so vse stopnje vozlišč grafa G sode. Po odstranitvi povezav obhoda vsakemu vozlišču na obhodu odstranimo sodo število povezav, pri ostalih se stopnje ne spremenijo. Vidimo, da so zato tudi v podgrafu X in posledično v povezani komponenti Y vse stopnje sode.

Vemo, da ima vsako vozlišče v grafu Y sodo stopnjo in da je graf Y povezan. Hkrati velja tudi, da ima graf Y strogo manj povezav kot graf H. Ker velja, da je graf H protiprimer za izrek z najmanjšim številom povezav, in ker graf Y zadošča pogojem izreka (sode stopnje in povezanost) ter ima manj povezav, ima graf Y Eulerjev obhod. Dodatno vemo, da ima Eulerjev obhod v grafu Y vsaj eno povezavo, ker imamo povezavo e.

Trdimo, da lahko v grafu H najdemo obhod, ki vključuje več povezav kot množica F'. Začnemo s prejšnjim najdaljšim obhodom. Ko pridemo do vozlišča u, naredimo Eulerjev obhod na podgrafu Y, po definiciji tako dodamo vsaj eno povezavo, to je povezava e, ne obiščemo nobene povezave najdaljšega obhoda in se vrnemo na vozlišče u. Končamo tako, da od vozlišča u nadaljujemo najdaljši obhod do konca.

Torej smo prišli v protislovje, saj prvotni obhod ni najdaljši obhod brez ponavljanja povezav, ker smo našli daljšega. Obhod z dodanim Eulerjevim obhod v povezani komponenti Y je namreč daljši. □

4.2 Eulerjev obhod v usmerjenih grafih

Pokazali bomo, kdaj ima usmerjen graf Eulerjev obhod. S protislovjem lahko izrek dokažemo, tako da prilagodimo dokaz neusmerjenega primera. Ponovno bomo dokazali preprosto lemo, ki jo kot orodje uporabimo v glavnem dokazu.

Lema 4.2. *Če za usmerjen graf $G = (V, E)$ velja $|V| \geq 1$ in $d^+(v) = d^-(v)$ za vsako vozlišče $v \in V$, potem ima graf G cikel.*

Dokaz. Izberemo začetno vozlišče $v_0 \in V$. Naredimo najdaljšo pot $W = \{v_0, v_1, \ldots, v_k\}$, ki obstaja, ker je množica V končna množica. Vozlišče v_k ima poleg vhodne povezave $v_{k-1}v_k$ vsaj eno izhodno povezavo, saj velja $d^+(v_k) = d^-(v_k)$. Naj bo vozlišče $u \in V$ takšno, da velja $v_k u \in E$. Če vozlišče u ni na poti W, je $W' = \{v_0, \ldots, v_k, u\}$ daljša pot in dobimo protislovje. Druga možnost je, da vozlišče u je na poti, torej je vozlišče u enako vozlišču v_i za neko število i. Usmerjen graf G ima torej cikel $W'' = \{v_k, v_i, v_{i+1}, \ldots, v_k\}$. □

Izrek 4.2. *Graf G ima usmerjen Eulerjev sprehod, če in samo če je graf G povezan in velja $d^+(v) = d^-(v)$ za vsako vozlišče $v \in V$.*

Obe smeri izreka lahko dokažemo s posnemanjem dokaza izreka 4.1. Na mestih, kjer je to potrebno, zamenjamo lastnost, da so vse stopnje sode, z lastnostjo, da je vhodna stopnja enaka izhodni za vsako vozlišče, in uporabljamo lemo 4.2 namesto leme 4.1.

5 De Bruijnov graf

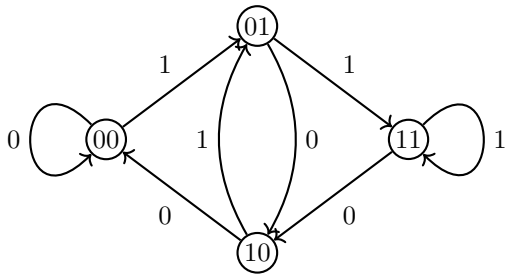
Preden rešimo zadani problem, si oglejmo posebno vrsto usmerjenega grafa.

Definicija 5.1. *Množico naravnih števil do r označimo z $[r] = \{1, 2, ..., r\}$. Množico vseh zaporedij dolžine $n-1$ s členi v množici $[r]$ označimo z V_r^n, torej*

$$V_r^n = \{(r_1, r_2, ..., r_{n-1}) \mid r_i \in [r] \ \text{ za vsak } 1 \leq i \leq n-1\}.$$

Sedaj lahko definiramo De Bruijnov graf. To storimo tako, da opredelimo množico vozlišč in množico povezav med njimi.

Definicija 5.2. ***De Bruijnov graf*** *je usmerjen graf, ki ima za množico vozlišč množico V_r^n. Poljubni vozlišči $u = (u_1, u_2, ..., u_{n-1})$ in $v = (v_1, v_2, ..., v_{n-1})$ sta povezani natanko tedaj, ko velja $u_i = v_{i-1}$ za vse $i \in \{2, 3, \ldots, n\}$. Označimo ga z $G_r^n = (V_r^n, E)$.*



Slika 7: De Bruijnov graf G_2^3.

Za ilustracijo De Bruijnovega grafa določimo $r = 2$ in $n = 3$.
V vsakem vozlišču grafa G_2^3 je neko zaporedje števil 0 in 1 dolžine 2. Med njimi so povezave, ki vodijo od enega vozlišča do drugega. Neformalno si lahko predstavljamo, da gre povezava od izhodnega zaporedja k vhodnemu takrat, ko lahko celotno začetno zaporedje premaknemo za eno mesto v levo, na zadnje mesto pa lahko dodamo katerokoli številko in tako dobimo vhodno zaporedje.

Nad vsako povezavo se nahaja število 0 ali 1. Izberemo tisto, ki je v grafu dodana na konec izhodnega zaporedja, da dobimo vhodno. Na primer, če zaporedje 01 premaknemo za eno mesto v levo, dobimo $1*$, kjer je $*$ lahko katerokoli število. Povezava, nad katero je zapisano število 0, gre do zaporedja 10, in povezava, nad katero je zapisano število 1, gre do zaporedja 11.

Na grafu na sliki 7 lahko opazimo nekaj lastnosti. Ugotovimo, da so vsa vozlišča povezana in da sta vhodna in izhodna stopnja enaki za vsako vozlišče. Izgleda, da De Bruijnov graf G_2^3 izpolnjuje pogoja za obstoj usmerjenega Eulerjevega obhoda, iz izreka 4.2. Prepričajmo se, da to velja tudi v splošnem.

Izrek 5.1. *Za vsaki naravni števili r in $n \in \mathbb{N}$ De Bruijnov graf G_r^n vsebuje usmerjen Eulerjev obhod.*

Dokaz. Izrek bomo dokazali z uporabo izreka o Eulerjevem obhodu v usmerjenih grafih. Dokazati moramo, da je De Bruijnov graf vedno močno povezan in da sta vhodna in izhodna stopnja enaki za vsako vozlišče. Najprej bomo dokazali močno povezanost De Bruijnovega grafa. Izberimo poljubni vozlišči u in v iz množice V_r^n, torej $u = (u_1, u_2, ..., u_{n-1})$ in $v = (v_1, v_2, ..., v_{n-1})$. Za obstoj močne povezanosti moramo med njima poiskati pot. Poglejmo naslednjo pot

$$\begin{aligned} u = w_1 &= (u_1, u_2, ..., u_{n-1}) \\ w_2 &= (u_2, u_3, ..., u_{n-1}, v_1) \\ w_3 &= (u_3, u_4, ..., u_{n-1}, v_1, v_2) \\ &\vdots \\ w_{n-1} &= (u_{n-1}, v_1, v_2, ..., v_{n-2}) \\ w_n &= (v_1, v_2, ...v_{n-1}) = v, \end{aligned}$$

torej $w_i = (u_i, u_{i+1}, ..., u_{n-1}, v_1, v_2, ..., v_{i-1})$. Opazimo, da sta po definiciji De Bruijnovega grafa w_i in w_{i+1} povezana za vsak $i \in \{1, 2, \ldots, n-1\}$ in, da smo našli iskano pot. Iz konstrukcije namreč lahko zasledimo, da smo iz vozlišča u prišli v vozlišče v. To smo naredili tako, da smo zaporedju u dodajali člene zaporedja v. De Bruijnov graf je torej vedno močno povezan.

Zdaj moramo dokazati še, da sta vhodna in izhodna stopnja enaki za vsako vozlišče De Bruijnovega grafa. Naj bo u poljubno vozlišče, v pa vozlišče, tako da velja $uv \in E$. Iz vozlišča $u = (u_1, u_2, ..., u_{n-1})$ obstaja izhodna povezava v $v = (u_2, ..., u_{n-1}, *)$, saj po definicji De Bruijnovega grafa vozlišče u enolično določa v z izjemo zadnjega mesta. Znak $*$ predstavlja poljubno število iz množice $[r]$, zato je $d^+(v) = r$.

V obratni smeri, naj bo u poljubno vozlišče, v pa vozlišče, tako da velja $vu \in E$. Vemo, da vhodna povezava do $u = (u_1, u_2, ..., u_{n-1})$ obstaja za poljuben $v = (*, u_1, u_2, ..., u_{n-2})$. Znak $*$ ponovno predstavlja katerokoli število iz množice $[r]$, zato je $d^-(v) = r$, torej je $d^+(v) = r = d^-(v)$.

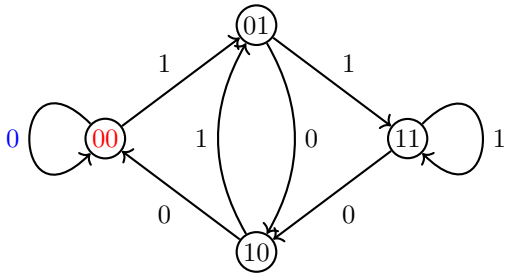
Dokazali smo, da ima vsako vozlišče v G_r^n enako vhodno in izhodno stopnjo ter da je G_r^n močno povezan. Z uporabo izreka 4.2 o Eulerjevem obhodu v usmerjenih grafih sklepamo, da ima G_r^n vedno Eulerjev obhod. □

6 Rešitev problema

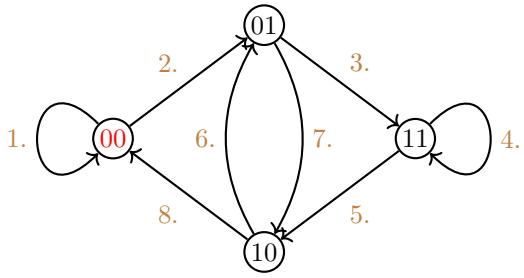
Zdaj, ko imamo vsa orodja, lahko rešimo naš prvotni problem. Za to uporabimo De Bruijnov graf in Eulerjev obhod na njem. Obravnavamo graf G_r^n.

Najprej določimo število vozlišč in povezav De Bruijnovega grafa. Število vseh vozlišč je enako $|V_r^n| = r^{n-1}$, vsako vozlišče ima r izhodnih povezav, zato je vseh povezav $r \cdot r^{n-1} = r^n$.

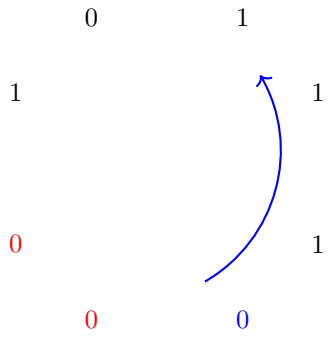
Na primeru grafa G_2^3 pokažimo, kako z Eulerjevim obhodom na njem skonstruiramo ustrezno krožno zaporedje.



Slika 8: De Bruijnov graf G_2^3.



Slika 9: Eulerjev obhod na G_2^3.



Slika 10: Krožno zaporedje, ki pripada Eulerjevemu obhodu na sliki 9.

Na sliki 9 opazimo skico Eulerjevega obhoda na G_2^3. Sprehod začnemo na vozlišču 00, označenim z rdečo barvo. Prva povezava v obhodu je zanka, nad katero je rjava 1. Nato sledimo rjavim številkam od ena do osem, ki so po vrsti napisane nad povezavami na sliki 9.

Na sliki 10 opazimo krožno zaporedje, ki pripada Eulerjevemu obhodu na sliki 9. Najprej napišemo v obratni smeri urinega kazalca zaporedje, ki pripada začetnemu vozlišču, v našem primeru je to zaporedje 00. Nato začnemo s konstrukcijo krožnega zaporedja. **Nadaljujemo ga tako, da v obratni smeri urinega kazalca zaporedoma dodajamo števila nad povezavami, prepotovanimi v Eulerjevemu sprehodu.** Prvo število, ki ga dodamo na sliki 10, je torej modra 0, tako kot začetna povezava v Eulerjevem sprehodu na sliki 8. Nadaljujemo ga z 1 nad povezavo od 00 do 01 in tako dalje. Postopek prekinemo dva koraka pred koncem, ko bi morali dodati dve 0, ki smo jih dodali v prvem koraku zaradi začetnega vozlišča. Skupno je tako res $2^3 = 8$ členov krožnega zaporedja, en člen za vsako povezavo.

Poglejmo, ali je nastalo krožno zaporedje ustrezno. Preveriti moramo, da se v krogu vsako zaporedje dolžine 3 pojavi natanko enkrat. Začnemo v poljubnem členu in v obratni smeri urinega kazalca preverimo podzaporedja dolžine 3. Od začetnega 000 dobimo podzaporedja 000, 001, 011, 111, 110, 101, 010 in 100, ki so res vsa možna.

Enak postopek kot za graf G_2^3 velja tudi za splošni graf G_r^n. Začne se tako, da izberemo poljubno vozlišče, kjer začnemo Eulerjev sprehod in v obratni smeri urinega kazalca zapišemo zaporedje dolžine $n-1$, ki ga začetno vozlišče predstavlja. Nato opravimo Eulerjev sprehod in zaporedoma v obratni smeri urinega kazalca dodajamo števila nad prepotovanimi povezavami v Eulerjevem sprehodu. Postopek zaključimo $n-1$ povezav pred koncem Eulerjevega sprehoda, ko bi morali dodati še eno kopijo začetnega zaporedja, ki smo ga dodali v začetnem koraku.

Utemeljiti moramo, da bo tako sestavljeno krožno zaporedje vedno ustrezno. Po konstrukciji bo krožno zaporedje vedno imelo

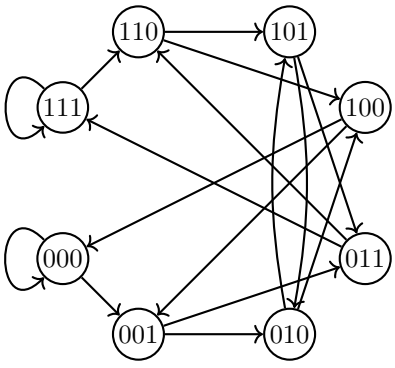
$$(n-1) + (r^n - (n-1)) = r^n$$

členov. To velja, ker najprej dodamo $n-1$ členov prvega vozlišča in potem en člen za vsako izmed r^n povezav ter se ustavimo $n-1$ povezav pred koncem Eulerjevega sprehoda, ko krožno zaporedje zlepimo skupaj. Po konstrukciji je vseh členov krožnega zaporedja r^n, zato je vseh zaporedji dolžine n, ki se pojavijo v obratni smeri urinega kazalca, tudi r^n, saj je vsak člen začetek enega. Vemo torej, da je edini možni problem, da bi se katero od zaporedji dolžine n pojavilo večkrat (in se posledično katero sploh ne bi), saj je dobljeno krožno zaporedje primerne dolžine.

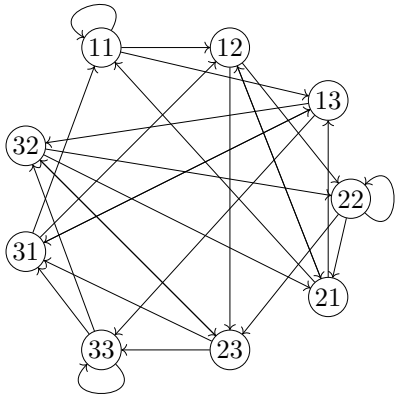
Preostane nam še, da pokažemo, da se vsako zaporedje pojavi. Najprej se osredotočimo na konkretni primer zgoraj. Zaporedje 000 bomo v krožno zaporedje zapisali natanko tedaj, ko bomo v Eulerjevem sprehodu od vozlišča 00 šli po povezavi z oznako 0. Podobno bomo zaporedje 101 v krožno zaporedje zapisali takrat, ko bomo od vozlišča 10 šli po povezavi z oznako 1.

Opažen vzorec ni naključen, zaradi naše konstrukcije to velja v splošnem. Pomembno je, da zaradi konstrukcije, prvo zaporedje dolžine n zapišemo tako, da od vozlišča, ki predstavlja začetnih $n-1$ členov začetnega zaporedja, gremo po povezavi, označeni z zadnjim členom zaporedja dolžine n. Na takšen način začnemo verigo in pozvročimo, da se vsako zaporedje dolžine n pojavi na enak način. Poljubno zapredje dolžine n, recimo $a_1, a_2, \ldots, a_n$ se v krožnem zaporedju pojavi, ko gremo od vozlišča $(a_1, \ldots, a_{n-1})$, do naslednjega vozlišča po povezavi z oznako a_n. Ključna lastnost obhoda je, da je Eulerjev, torej gremo skozi vsako možno povezavo natanko enkrat in zato res vsako zaporedje dolžine n dobimo na en način.

Na slikah 11 in 12 lahko vidimo primera bolj zapletenih De Bruijnovih grafov G_2^4 in G_3^3.



Slika 11: De Bruijnov graf G_2^4.



Slika 12: De Bruijnov graf G_3^3.

7 Zaključek

Odgovorili smo na začetno vprašanje in dokazali, da lahko prvih r naravnih števil vedno razporedimo v krožno zaporedje, tako da se vsako izmed r^n zaporedij dolžine n pojavi natanko enkrat. Najprej smo spoznali osnovne pojme teorije grafov in dokazali lemo o rokovanju. Nato smo utemljili, pod katerimi pogoji ima enostaven graf Eulerjev obhod in dokaz prilagodili za usmerjene grafe. Definirali smo De Bruijnov graf in dokazali, da ima vedno Eulerjev obhod. Na koncu smo utemeljili, kako iz Eulerjevega obhoda na njem pridemo do iskanega krožnega zaporedja.

Literatura

[1] D. B. West, *Introduction to Graph Theory*, 2nd ed., Prentice Hall, Upper Saddle River, N.J, 2001.

Čudesa čudežne teorije grup

Eva Bračun, Gašper Grm, Katja Šimenc
Mentor: *Izak Jenko*

Povzetek

Ukvarjali smo se s simetrijami ravninskih vzorcev, ki so povezani s teorijo grup. Spoznali smo, kaj je grupa in kako lahko slikamo iz ene grupe v drugo. Definirali smo tapetne grupe. Nazadnje smo spoznali način označevanja ravninskih vzorcev, ki nam je pomagal pri njihovi klasifikaciji.

1 Uvod in terminologija

Simetrije splošnih (geometrijskih) objektov in v posebnem ravninskih vzorcev študiramo preko precej abstraktnih objektov imenovanih *grupe*. V tem poglavju si bomo ogledali definicijo grup in nekaj osnovnih pojmov povezanih z njimi.

Definicija 1.1. Grupa *je množica G opremljena z binarno operacijo*

$$* : G \times G \to G,$$

za katero veljajo naslednje lastnosti:

i.) Asociativnost: *za vse a, b, $c \in G$ velja $(a * b) * c = a * (b * c)$.*

ii.) Enota: *obstaja tak $e \in G$, da za vse $a \in G$ velja $e * a = a * e = e$.*

iii.) Inverzi: *za vsak $a \in G$ obstaja tak $b \in G$, da velja $a * b = e$ in $b * a = e$.*

Primer 1.1. *Oglejmo si nekaj primerov grup.*

i.) Primer grupe so cela števila ter operacija seštevanja. Označimo jo z $(\mathbb{Z}, +)$. Za seštevanje velja asociativnost, enota te grupe je 0, inverz poljubnega elementa x pa je $-x$.

ii.) Še en primer grupe je množica racionalih števil ter operacija seštevanja. Označimo jo s $(\mathbb{Q}, +)$. Enota te grupe je 0, inverz poljubnega elementa x pa je $-x$. Podobna primera grup sta $(\mathbb{R}, +)$ in $(\mathbb{C}, +)$.

iii.) Še en primer grupe je množica kompleksnih števil brez števila 0 ter operacija množenja. Označimo jo s $(\mathbb{C} \setminus \{0\}, \cdot)$. Enota te grupe je 1, inverz poljubnega elementa x pa je x^{-1}.

v.) Primer grupe so tudi cela števila po modulu 3 ter operacija seštevanje z oznako $(\mathbb{Z}/3, +)$. Enota te grupe je 0, ki predstavlja ostanek 0 pri deljenju s 3. Inverz elementa x pa je $-x$.

Primer 1.2. *Za boljšo predstavo si oglejmo še dva protiprimera.*

i.) Množica naravnih števil ter operacija seštevanja z oznako $(\mathbb{N}, +)$ pa ni primer grupe, saj po definiciji v množici naravnih števil ni števila 0 ter zato enota ne obstaja. Inverzov pa tudi ni, saj med naravnimi števili ni negativnih števil. Tako ne moremo sešteti dveh naravnih števil in kot rezultat dobiti enote.

ii.) Za množico celih števil ter operacijo odštevanja z oznako $(\mathbb{Z}, -)$ pa ne *velja asociativnost, saj v splošnem izraza $(a - b) - c$ in $a - (b - c) = a - b + c$ nista enaka.*

1.1 Diedrska grupa

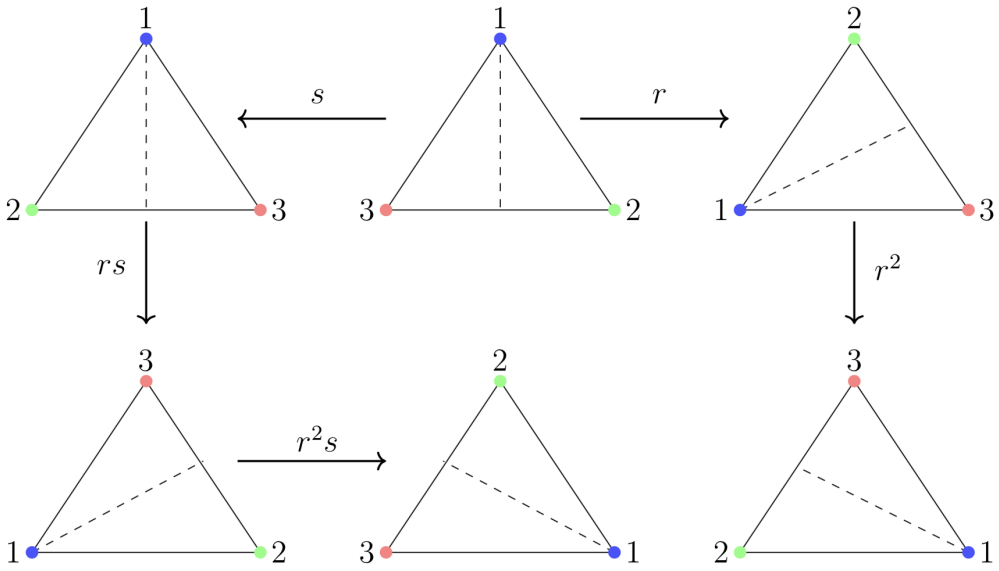
1.1.1 Izometrije enakostraničnega trikotnika

Na enakostraničnem trikotniku lahko izvajamo naslednje transformacije, ki ohranjajo njegovo obliko:

i.) **Rotacijo** označimo z r, ki v enakostraničnem trikotniku predstavlja rotacijo za kot $\frac{2\pi}{3} = 120°$ v pozitivni smeri. Enota e pa predstavlja rotacijo za kot $0°$.

ii.) **Zrcaljenje** označimo s s in v enakostraničnem trikotniku predstavlja zrcaljenje čez eno od težiščinic trikotnika. Dvojno zracljenje ustreza enoti, zato velja zveza $s^2 = e$.

Premislimo lahko, da velja relacija $sr = r^{-1}s$, in da relacija $sr = rs$ ne velja. Množico vseh 6 simetrij enakostraničnega tirkotnika skupaj s kompozicijo imenujemo *diedrska grupa* s šestimi elementi in ima oznako $D_6 = \{e, r, r^2, s, sr, sr^2\}$. Vseh 6 simetrij enakostraničnega trikotnika vidimo na sliki 1.



Slika 1: Vseh 6 simetrij enakostraničnega trikotnika.

Definicija 1.2. Splošna diedrska grupa *je definirana kot*

$$D_{2n} = \{e, r, r^2, \dots r^{n-1}, s, sr, \dots, sr^{n-1}\},$$

njeni elementi pa predstavljajo izometrije pravilnega n-kotnika.

1.2 Generatorji grup in redi

Grupe je pogosto lažje razumeti, če poznamo samo nekaj njenih ključnih elementov, ki jim pravimo *generatorji*. Igrajo vlogo osnovnih koščkov grupe, s katerimi lahko dobimo vse ostale. To natančneje opisuje naslednja definicija.

Definicija 1.3. *Naj bo $(G, *)$ grupa. Rečemo, da podmnožica $X \subseteq G$* generira *G, če lahko vsak element iz G zapišemo kot končni produkt elementov iz X in njihovih inverzov. To označimo z $\langle X \rangle = G$.*

Primer 1.3. *Množica celih števil $(\mathbb{Z}, +)$ je lahko generirana z množicami $\{-1, 1\}$, $\{1\}$ ali $\{-1\}$. Diedrska grupa s šestimi elementi je generirana z množico $\{r, s\}$.*

Definicija 1.4. *Naj bo G grupa in $g \in G$.* Red *elementa g je najmanjše naravno število $n \in \mathbb{N}$, za katero velja, da je $g^n = e$, če takšen n obstaja. Če tak n ne obstaja, je red elementa g neskončen. Red označimo z* $\mathrm{ord}(g) = n$.

Primer 1.4. *Primer elementa reda 3 v grupi D_6 je rotacija enakostraničnega trikotnika r, saj velja $r^3 = e$ (ko trikotnik trikrat obrnemo za $120°$, se vrnemo v začetno stanje) in $r^2 \neq e$.*

Primer 1.5. *Primer elementa z neskončnim redom, tj.* $\mathrm{ord}(1) = \infty$, *je število 1 v grupi $(\mathbb{Z}, +)$, saj vrednost $1 + 1 + \cdots + 1 = n \cdot 1$, za neki $n \in \mathbb{N}$, v množici $\mathbb{Z}$ ne bo nikoli dosegla enote 0.*

2 Konstrukcije novih grup

2.1 Podgrupe

Pri množicah je uporabno in smiselno govoriti o podmnožicah, zato bi tudi pri grupah radi imeli analogen formalizem. V ta namen definiramo pojem *podgrupe*.

Definicija 2.1. *Naj bo G grupa. Podmnožica $H \subseteq G$ je* podgrupa *grupe G, kadar je tudi H grupa za isto operacijo kot grupa G. To označimo s $H \leq G$.*

Podgrupa vsake grupe je podgrupa $\{e\}$, t. i. *trivialna podgrupa*, ki vsebuje le enoto.

Primer 2.1. *Podgrupa celih števil $(\mathbb{Z}, +)$ je množica sodih celih števil*

$$2\mathbb{Z} = \{2k \in \mathbb{Z} | k \in \mathbb{Z}\} \subseteq \mathbb{Z}$$

skupaj z operacijo seštevanja. Vsota dveh sodih števil je še vedno sodo število, v množici $2\mathbb{Z}$ imamo element 0, ki je enota in za poljuben $2x \in 2\mathbb{Z}$ obstaja inverz $-2x \in 2\mathbb{Z}$. Zato je $(2\mathbb{Z}, +)$ podgrupa grupe $\mathbb{Z}$.

Primer 2.2. *Primeri podgrup diedrske grupe $D_6 = \{e, r, r^2, s, sr, sr^2\}$ so $\{e\}$, $\{e, r, r^2\}$ in $\{e, s\}$.*

2.2 Direktni produkt

Definicija 2.2. *Naj bosta $(G, *)$ in $(H, \circ)$ grupi. Na množici urejenih parov $G \times H$ definirajmo produkt elementov (g, h) in (g', h') kot $(g * g', h \circ h')$. Za to operacijo je $G \times H$ grupa, ki jo imenujemo* direktni produkt *grup G in H. Enota te grupe je (e_G, e_H).*

2.3 Presek podgrup

Naj bo G grupa z dvema podgrupama K in H. Imenujmo presek teh dveh podgrup E. Za E velja, da je podgrupa G. Naslednja trditev pokaže, da je E zaprta za operacijo $*$ grupe G.

Trditev 2.1. *Produkt elementov a in b iz preseka E je element preseka E.*

Dokaz. Če sta a in b oba elementa H, velja, da je tudi njun zmnožek v H. Enako lahko rečemo za K. Ker to velja za obe množici, pomeni, da je $a * b$ element preseka H ter K, torej je $a * b \in E$. □

2.4 Homomorfizem grup

Tako kot množice med seboj primerjamo s preslikavami, bi radi primerjali tudi grupe. Vendar zgolj s preslikavami tega ne moremo storiti na ustrezen način, saj v splošnem te ne ohranjajo ključne strukture grup – njene operacije. Preslikavam, ki spoštujejo strukturo grup, rečemo *homomorfizmi* in jih definiramo v tem razdelku.

Definicija 2.3. Homomorfizem grup *je preslikava $\phi : G \to H$, za katero velja $\phi(a * b) = \phi(a) * \phi(b)$ za vse a in b, ki pripadajo G.*

Primer 2.3. *Primer homomorfizma je eksponenciranje iz grupe $(\mathbb{R}, +)$ v grupo $((0, \infty), \cdot)$. Naj bo $\phi : \mathbb{R} \to (0, \infty)$ preslikava podana s predpisom $x \mapsto e^x$. Ker velja $e^{x+y} = e^x \cdot e^y$, velja zveza $\phi(x + y) = \phi(x) \cdot \phi(y)$, torej je ϕ homomorfizem.*

Lema 2.1. *Za vsak $g \in G$ obstaja natanko en inverz $h \in G$, za katerega velja $g * h = h * g = e$.*

Dokaz. Naj bosta h in k elementa G, za katera veljata naslednji zvezi

$$g * h = h * g = e,$$

$$g * k = k * g = e.$$

Drugo enačbo lahko vstavimo v enakost $h = h * e$ in dobimo

$$h = h * e = h * g * k = e * k = k.$$

Tako velja enakost $h = k$. □

Trditev 2.2. *Naj bo $\phi : G \to H$ homomorfizem. Potem je $\phi(e_G) = e_H$ in za vse $g \in G$ velja*

$$\phi(g^{-1}) = \phi(g)^{-1}.$$

Dokaz. Enoto grupe G pomnožimo samo s seboj

$$e_G = e_G * e_G.$$

Ker je ϕ homomorfizem, lahko zapišemo

$$\phi(e_G) = \phi(e_G * e_G) = \phi(e_G) * \phi(e_G).$$

Obe strani enačbe pomnožimo z inverzom elementa $\phi(e_G)$

$$e_H = \phi(e_G) * e_H = \phi(e_G).$$

Tako res velja $e_H = \phi(e_G)$. Pokažimo še, da za vsak $g \in G$ velja

$$\phi(g)^{-1} = \phi(g^{-1}).$$

Ker je ϕ homomorfizem, velja

$$\phi(e_G) = \phi(g * g^{-1}) = \phi(g) * \phi(g^{-1}).$$

Celotno enačbo pomnožimo s $\phi(g)^{-1}$ z leve in s tem dokažemo enakost

$$\phi(g)^{-1} = \phi(g^{-1}).$$

□

2.5 Jedro

V tem razdelku definiramo pojem *jedra* danega homomorfizma grup.

Definicija 2.4. *Naj bo preslikava $\phi : G \to H$ homomorfizem.* Jedro *homomorfizma ϕ sestavljajo vsi elementi iz G, ki jih slika ϕ v enoto H. Jedro ima oznako* $\ker \phi$ *in zanj velja*

$$\ker \phi = \{g \in G \mid \phi(g) = e_H\}.$$

Trditev 2.3. *Naj bo $\phi : G \to H$ homomorfizem grup. Potem je* $\ker \phi$ *podgrupa grupe G.*

Dokaz. Da je element g v jedru ϕ, lahko velja le, če je njegova slika v množici H enaka enoti H, torej

$$g \in \ker \phi \Leftrightarrow \phi(g) = e_H.$$

Naj bosta a in b elementa jedra homomorfizma ϕ, potem velja $\phi(a) = e_H$ in $\phi(b) = e_H$. Ker je ϕ homomorfizem, lahko ločimo zmnožek slik a in b

$$\phi(a * b) = \phi(a) * \phi(b) = e_H * e_H = e_H.$$

Zato zares velja

$$\phi(a * b) = e_H,$$

torej je $a * b \in \ker \phi$.

Ker vedno velja $\phi(e_G) = e_H$, kot smo pokazali v trditvi 2.2, je $e_G \in \ker \phi$.

Naj bo element g iz jedra $\ker \phi$ in pokažimo, da njegov inverz g^{-1} tudi leži v jedru $\ker \phi$. Ker je $g \in \ker \phi$, velja $\phi(g) = e_G$. Tedaj izračunamo

$$e_H = \phi(e_G) = \phi(g * g^{-1}) = \phi(g) * \phi(g^{-1}) = e_H * \phi(g^{-1}) = \phi(g^{-1}).$$

Torej je $\phi(g^{-1}) = e_H$ in zato je $g^{-1} \in \ker \phi$. □

Trditev 2.4. *Naj bo $\pi : G \to H$ homomorfizem in $a \in \ker \pi$ ter $g \in G$. Potem je*

$$gag^{-1} \in \ker \pi.$$

Dokaz. Ker je preslikava π homomorfizem, lahko izračunamo

$$\pi(gag^{-1}) = \pi(g) \cdot \pi(a) \cdot \pi(g)^{-1} = \pi(g) \cdot e_H \cdot \pi(g)^{-1} = \pi(g) \cdot \pi(g)^{-1} = e_H.$$

Tako zares velja enakost $\pi(gag^{-1}) = e_H$, torej je $gag^{-1} \in \ker \pi$. □

Definicija 2.5. Izomorfizem *ψ: $G \to H$ je bijektivni homomorfizem med dvema grupama G in H. Kadar obstaja izomorfizem med grupama G in H, pravimo, da sta grupi G in H* izomorfni*, kar označimo z $G \cong H$.*

Primer 2.4. *Primer izomorfizma je preslikava iz grupe ostankov po modulu* 3 *v grupo rotacij enakostraničnega trikotnika. Ostanek* 0 *slikamo v rotacijo za kot* $0°$*, ostanek* 1 *v rotacijo za kot* $120°$*, ostanek* 2 *pa v rotacijo za kot* $240°$*.*

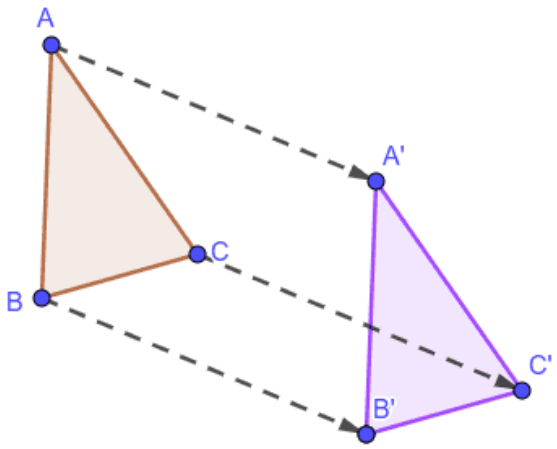
3 Evklidska grupa

Izometrija evklidske ravnine $\mathbb{R}^2$ je bijektivna preslikava $f : \mathbb{R}^2 \to \mathbb{R}^2$, ki preslika ravnino samo vase in pri tem ohranja razdalje med poljubnima dvema točkama.

Definicija 3.1. Evklidska grupa $E(2)$ *je grupa vseh izometrij evklidske ravnine* $\mathbb{R}^2$*.*

$$E(2) = \{f : \mathbb{R}^2 \to \mathbb{R}^2 \mid f \text{ je izometrija}\}$$

Evklidska grupa obsega vse translacije, rotacije in zrcaljenja.



Slika 2: Primer translacije.

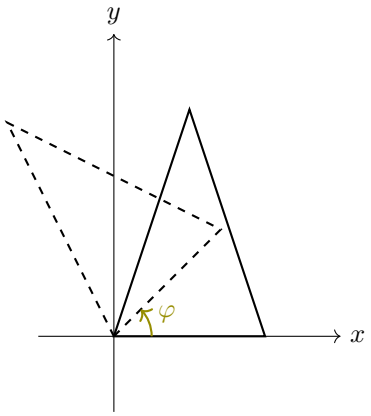
3.1 Translacija

Translacija opisuje premik vseh točk iz ravnine vzdolž nekega vektorja. To pomeni, da vsak lik ohrani svojo obliko in velikost, le premakne se v določeno smer za določeno razdaljo. Translacija za vektor $\vec{w} \in \mathbb{R}^2$ ima predpis

$$f(\vec{v}) = \vec{v} + \vec{w}.$$

3.2 Rotacija

Rotacije predstavimo s pomočjo matrik. Matrike so razpredelnice števil. Večinoma jih uporabljamo za zapis podatkov, ki so odvisni od dveh kategorij, in za preučevanje koeficientov sistemov linearnih enačb in linearnih transformacij. Element matrike A, ki leži v i-ti vrstici in j-tem stolpcu (kjer vrstice in stolpce navadno štejemo od 1 naprej), se imenuje element i, j.



Slika 3: Primer rotacije.

Naj bo Q_φ matrika 2×2, ki predstavlja rotacijo za kot φ okoli izhodišča. Poiščimo vrednosti njenih elementov. Začnimo s standardnima enotskima baznima vektorjema $\vec{i}$ in $\vec{j}$ s koordinatama

$$\vec{i} = (1, 0) \quad \text{in} \quad \vec{j} = (0, 1).$$

Če zavrtimo $\vec{i}$ za kot φ v pozitivni smeri okoli izhodišča, dobimo vektor

$$(\cos\varphi, \sin\varphi).$$

Če zavrtimo $\vec{j}$ za kot φ, dobimo vektor

$$(\cos(\varphi + 90°), \sin(\varphi + 90°)) = (-\sin\varphi, \cos\varphi).$$

Nato v prvi stolpec zapišemo koordinate zavrtenega vektorja $\vec{i}$, v drugega pa koordinate zavrtenega vektorja $\vec{j}$. Dobimo matriko, ki predstavlja rotacijo za kot φ v pozitivni smeri okoli izhodišča

$$Q_\varphi = \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}.$$

Za takšne matrike velja

$$Q_\psi \cdot Q_\varphi = Q_{\psi+\varphi}.$$

Ta zveza je razvidna iz računa

$$\begin{aligned} Q_\varphi \cdot Q_\psi &= \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix} \cdot \begin{pmatrix} \cos\psi & -\sin\psi \\ \sin\psi & \cos\psi \end{pmatrix} \\ &= \begin{pmatrix} \cos\varphi\cos\psi - \sin\varphi\sin\psi & -\cos\varphi\sin\psi - \sin\varphi\cos\psi \\ \sin\varphi\cos\psi + \cos\varphi\sin\psi & -\sin\varphi\sin\psi + \cos\varphi\cos\psi \end{pmatrix} \\ &= \begin{pmatrix} \cos(\varphi+\psi) & -\sin(\varphi+\psi) \\ \sin(\varphi+\psi) & \cos(\varphi+\psi) \end{pmatrix} \\ &= Q_{\varphi+\psi}. \end{aligned}$$

3.3 Zrcaljenje

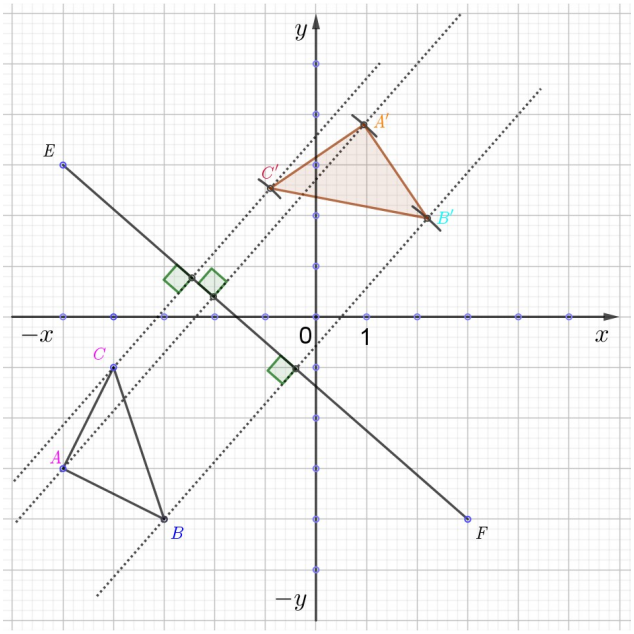
Zrcaljenje v ravnini je transformacija, ki slika vsako točko na ravnini v točko, ki je enako oddaljena od določene osi zrcaljenja, leži na pravokotnici skozi izbrano točko in os zrcaljenja, vendar na nasprotni strani osi. Os zrcaljenja je premica, ki deli ravnino na dva dela.

Zrcaljenje predstavimo s pomočjo matrik. Najprej predstavimo zrcaljenje čez x-os. Pri tem se vektor $\vec{i}$ preslika sam vase, vektor $\vec{j}$ pa v $-\vec{j}$. S pomočjo teh podatkov izpeljemo matriko zrcaljenja čez x-os

$$S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Sedaj pa se lotimo še zrcaljenja preko poljubne osi, ki poteka skozi koordinatno izhodišče. Denimo, da os zrcaljenja in pozitiven poltrak x-osi oklepata kot φ. Zrcalili bomo na način, da os zrcaljenja najprej zavrtimo za kot $-\varphi$, nato točko oziroma vektor zrcalimo prek x-osi in nazadnje spet vse skupaj, torej os zrcaljenja in točko oziroma vektor, zavrtimo za kot φ. Predpis za matriko, ki predstavlja to zrcaljenje, lahko izpeljemo na naslednji način

$$\begin{aligned} Q_\varphi \cdot S \cdot Q_\varphi^{-1} &= \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} \cos\varphi & \sin\varphi \\ -\sin\varphi & \cos\varphi \end{pmatrix} \\ &= \begin{pmatrix} \cos 2\varphi & \sin 2\varphi \\ \sin 2\varphi & -\cos 2\varphi \end{pmatrix}. \end{aligned}$$



Slika 4: Primer zrcaljenja.

Matriko, ki predstavlja zrcaljenje čez premico, ki poteka skozi izhodišče in s pozitivnim poltrakom x-osi oklepa kot $\varphi/2$, označimo s S_φ, torej je

$$S_\varphi = \begin{pmatrix} \cos\varphi & \sin\varphi \\ \sin\varphi & -\cos\varphi \end{pmatrix}.$$

Opazimo, da obstaja grupa, ki vsebuje vse rotacije okoli izhodišča kot tudi zrcaljenja čez premice, ki vsebujejo izhodišče. Imenuje se *ortogonalna grupa* in jo označimo z

$$O(2) = \left\{ \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix} \middle| \varphi \in [0, 2\pi) \right\} \cup \left\{ \begin{pmatrix} \cos\phi & \sin\phi \\ \sin\phi & -\cos\phi \end{pmatrix} \middle| \phi \in [0, 2\pi) \right\}.$$

Sedaj pa moramo pokazati, da je to res grupa.

Trditev 3.1. *Množica $O(2)$ je grupa za kompozicijo oziroma operacijo množenja matrik.*

Dokaz. Pokazati moramo, da je kompozicija poljubnih dveh elementov množice $O(2)$ tudi v $O(2)$.

Od prej že vemo, da je

$$Q_\psi \cdot Q_\varphi = Q_{\psi+\varphi}.$$

Nato izračunamo

$$\begin{aligned} S_\varphi \cdot S_\psi &= \begin{pmatrix} \cos\varphi & \sin\varphi \\ \sin\varphi & -\cos\varphi \end{pmatrix} \cdot \begin{pmatrix} \cos\psi & \sin\psi \\ \sin\psi & -\cos\psi \end{pmatrix} \\ &= \begin{pmatrix} \cos\varphi\cos\psi + \sin\varphi\sin\psi & \cos\varphi\sin\psi - \sin\varphi\cos\psi \\ \sin\varphi\cos\psi - \cos\varphi\sin\psi & \sin\varphi\sin\psi + \cos\varphi\cos\psi \end{pmatrix} \\ &= \begin{pmatrix} \cos(\varphi-\psi) & -\sin(\varphi-\psi) \\ \sin(\varphi-\psi) & \cos(\varphi-\psi) \end{pmatrix} = Q_{\varphi-\psi}. \end{aligned}$$

Ugotovimo, da je kompozicija poljubnih dveh zrcaljenj rotacija. S podobnim računom dokažemo

$$Q_\varphi \cdot S_\psi = S_{\varphi-\psi}.$$

Nazadnje izračunamo še

$$S_\varphi \cdot Q_\psi = S_{\varphi+\psi}.$$

Opazimo, da ta grupa ni komutativna.

Enota je matrika, ki vse točke preslika same vase. To pomeni, da se $\vec{i}$ preslika nazaj v $\vec{i}$ in $\vec{j}$ se preslika v $\vec{j}$. Kar pomeni, da je matrika enote

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

ki jo imenujemo *identiteta* in jo označimo z I.

Nazadnje pokažimo še, da $O(2)$ vsebuje inverze vseh svojih elementov. Inverz rotacije za kot φ je rotacija za kot $-\varphi$, zato je

$$Q_\varphi^{-1} = Q_{-\varphi}.$$

Ker vemo, da velja $S_\varphi \cdot S_\psi = Q_{\varphi-\psi}$, sledi

$$S_\varphi \cdot S_\varphi = I.$$

Kar pomeni, da je S_φ sam sebi inverz, zato je

$$S_\varphi^{-1} = S_\varphi.$$

□

Izkaže se, da je vsaka izometrija kompozicija translacij, rotacij in zrcaljenj, zato je podana s predpisom

$$\vec{v} \mapsto Q\vec{v} + \vec{w}.$$

Pokažimo, da je kompozicija dveh izometrij te oblike spet te oblike in poglejmo, kako izgleda njen predpis. Naj bosta $f \in E(2)$ in $g \in E(2)$ izometriji, podani s predpisoma

$$f : \vec{v} \mapsto Q\vec{v} + \vec{w} \qquad \text{in} \qquad g : \vec{v} \mapsto R\vec{v} + \vec{u}$$

za neke $\vec{w}, \vec{u} \in \mathbb{R}^2$ in $Q, R \in O(2)$. Izračunamo

$$(f \circ g)(\vec{v}) = f(g(\vec{v})) = f(R\vec{v} + \vec{u}) = Q(R\vec{v} + \vec{u}) + \vec{w} = QR\vec{v} + Q\vec{u} + \vec{w}.$$

Kompozicija $f \circ g$ je torej podana s predpisom

$$f \circ g : \vec{v} \mapsto QR\vec{v} + Q\vec{u} + \vec{w}, \tag{1}$$

kjer je jasno razvidno

$$QR \in O(2) \quad \text{in} \quad Q\vec{u} + \vec{w} \in \mathbb{R}^2.$$

Enota za kompozicijo funkcij je *identiteta*, ki je podana s predpisom

$$\mathrm{id}(\vec{v}) = \vec{v}$$

in zanjo velja

$$f \circ \mathrm{id} = f \quad \text{in} \quad \mathrm{id} \circ f = f$$

za vse izometrije $f \in E(2)$.

Izpeljimo še predpis za inverz izometrije f s pomočjo predpisa (1) za kompozicijo dveh izometrij. Če predpostavimo, da je $f \circ g = \mathrm{id}$, lahko trdimo

$$\vec{v} = (f \circ g)(\vec{v}) = QR\vec{v} + Q\vec{u} + \vec{w}.$$

Ampak, če želimo, da to drži, mora veljati

$$QR = I \quad \text{in} \quad Q\vec{u} + \vec{w} = 0.$$

Iz tega izpeljemo

$$R = Q^{-1} \quad \text{in} \quad \vec{u} = -Q^{-1}\vec{w}.$$

Tako vidimo, da je inverz izometrije f podan s predpisom

$$f^{-1} : \vec{v} \mapsto Q^{-1}\vec{v} - Q^{-1}\vec{w}.$$

Vidimo, da je vsaka izometrija določena z vektorjem $\vec{w} \in \mathbb{R}^2$ in ortogonalno matriko $Q \in O(2)$. Tako lahko izometrijo $f : \vec{v} \mapsto Q\vec{v} + \vec{w}$ alternativno predstavimo tudi kot urejeni par $(\vec{w}, Q)$. Skladno s predpisom (1) za kompozicijo dveh izometrij lahko definiramo produkt dveh takšnih parov $(\vec{w}, Q)$ in $(\vec{u}, R)$ kot

$$(\vec{w}, Q) \cdot (\vec{u}, R) = (Q\vec{u} + \vec{w}, QR). \tag{2}$$

Množica, na kateri je definiran ta produkt, je kartezični produkt $\mathbb{R}^2 \times O(2)$. Vendar pa ta produkt urejenih parov ni enak produktu, ki bi ga dobili pri direktnem produktu grup $\mathbb{R}^2$ in $O(2)$, saj operacija na prvi komponenti ni zgolj seštevanje vektorjev. Zaradi te posebnosti ga imenujemo *semidirektni produkt* grup $\mathbb{R}^2$ in $O(2)$ in ga označimo z

$$\mathbb{R}^2 \rtimes O(2).$$

Odslej bomo evklidsko grupo izometrij $E(2)$ identificirali s tovrstnimi urejenimi pari in množenjem, definiranim s predpisom (2). Za to identifikacijo stoji izomorfizem

$$E(2) \cong \mathbb{R}^2 \rtimes O(2).$$

4 Grupa simetrij ravninskih vzorcev

V tem poglavju bomo definirali pojem *grupe simetrij ravninskega vzorca* ali *tapetne grupe*, ki jo sestavljajo vse izometrije evklidske ravnine, ki ohranjajo dani ravninski vzorec. Pokazali bomo tudi trditev, ki je na poti do klasifikacije vseh tapetnih grup.

Definicija 4.1. Translacijska podgrupa *evklidske grupe* $E(2)$ *je podgrupa vseh translacij. V grupi* $\mathbb{R}^2 \rtimes O(2)$ *translacijska podgrupa ustreza množici parov*

$$T = \{(\vec{v}, I) \mid \vec{v} \in \mathbb{R}^2\}.$$

Definicija 4.2. Točkasta grupa *dane podgrupe* $G \leq \mathbb{R}^2 \rtimes O(2)$ *je*

$$J = \{Q \in O(2) \mid (\vec{v}, Q) \in G \text{ za neki } \vec{v} \in \mathbb{R}^2\}.$$

Definicija 4.3. Grupa simetrij ravninskga vzorca *ali* tapetna grupa *je podgrupa* $G \leq \mathbb{R}^2 \rtimes O(2)$*, za katero velja, da je njena točkasta grupa* J *končna in da je podgrupa translacij* $G \cap T$ *generirana z dvema linearno neodvisnima translacijama. To pomeni, da je*

$$G \cap T = \langle (\vec{u}, I), (\vec{w}, I) \rangle$$

za neka linearno neodvisna vektorja $\vec{u}$ *in* $\vec{w} \in \mathbb{R}^2$*.*

Trditev 4.1. *Končne podgrupe* $O(2)$ *so bodisi ciklične (vsebujejo samo rotacije) bodisi diedrske grupe (vsebujejo rotacije in zrcaljenja).*

Mreža grupe simetrij ravninskega vzorca G je množica

$$\Lambda = \{\vec{u} \in \mathbb{R}^2 \mid (\vec{u}, I) \in G \cap T\} = \{k\vec{u} + l\vec{w} \in \mathbb{R}^2 \mid k, l \in \mathbb{Z}\},$$

kjer sta $\vec{u}$ in $\vec{w}$ vektorja, vzdolž katerih translaciji generirata grupo $G \cap T$. Skupaj z naslednjo trditvijo se mreža grupe simetrij ravninskega vzorca uporabi v dokazu izreka 4.1, ki pa ga ne bomo dokazali.

Trditev 4.2. *Točkasta grupa J deluje na mreži Λ.*

Dokaz. Dokazujemo, da je $Q\vec{u}$ element Λ za poljubna $Q \in O(2)$ in $\vec{u} \in \Lambda$. Uporabili bomo trditev 2.4, zato definirajmo preslikavo

$$\pi : E(2) \to O(2), \quad \pi((\vec{v}, Q)) = Q.$$

Preverimo, da je π homomorfizem. Izberimo poljubna elementa $(\vec{v}, Q)$, $(\vec{w}, R) \in E(2)$ in izračunamo

$$\pi((\vec{v}, Q) \cdot (\vec{w}, R)) = \pi((Q\vec{w} + \vec{v}, QR)) = QR = \pi((\vec{v}, Q)) \cdot \pi((\vec{w}, R)).$$

Torej je π homomorfizem in

$$\begin{aligned} \ker \pi &= \left\{ (\vec{v}, Q) \in E(2) \middle| \pi((\vec{v}, Q)) = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\} \\ &= \left\{ (\vec{v}, I) \in E(2) \mid \vec{v} \in \mathbb{R}^2 \right\} = T \end{aligned}$$

je njegovo jedro, kar je ravno podgrupa vseh translacij. Naj bo $\tau = (\vec{u}, I) \in G$. Ker je $Q \in J$, obstaja neki $\vec{v} \in \mathbb{R}^2$, da je par $g = (\vec{v}, Q) \in G$. Izračunamo

$$g\tau g^{-1} = (\vec{v}, Q)(\vec{u}, I)(-Q^{-1}\vec{v}, Q^{-1}) = (Q\vec{u}, I),$$

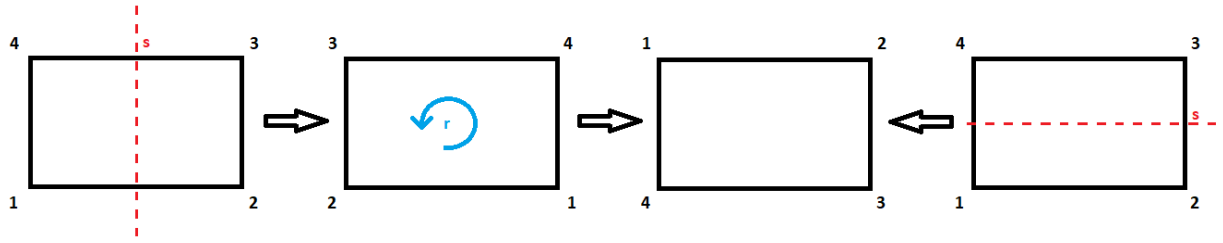
ki je produkt treh elementov iz G, zato leži v G in hkrati v T po trditvi 2.4. Torej je res $Q\vec{u} \in \Lambda$. □

Izrek 4.1. *Red rotacije v grupi simetrijskih ravninskih vzorcev je lahko le:* 2 *(rotacija za* 180°*),* 3 *(rotacija za* 120°*),* 4 *(rotacija za* 90°*) ali* 6 *(rotacija za* 60°*).*

Posledica 4.1. *Točkasta grupa J je generirana z eno od rotacij za kot* 180°*,* 120°*,* 90° *ali* 60° *in morda z zrcaljenjem. Točkasta grupa J je zato izomorfna eni od grup:*

$$\mathbb{Z}/2, \quad \mathbb{Z}/3, \quad \mathbb{Z}/4, \quad \mathbb{Z}/6, \quad D_4, \quad D_6, \quad D_8, \quad D_{12}.$$

Primer 4.1. *Diedrska grupa D_4 je grupa simetrij pravokotnika, ki ni kvadrat. Grupo sestavljajo enota, rotacija in dve zrcaljenji $D_4 = \{e, r, s, sr\}$, med njimi pa veljajo relacije $sr = rs$, $r^2 = e$ in $s^2 = e$. To vidimo na sliki 5.*



Slika 5: Prikaz diedrske grupe D_4 ravninske simetrije.

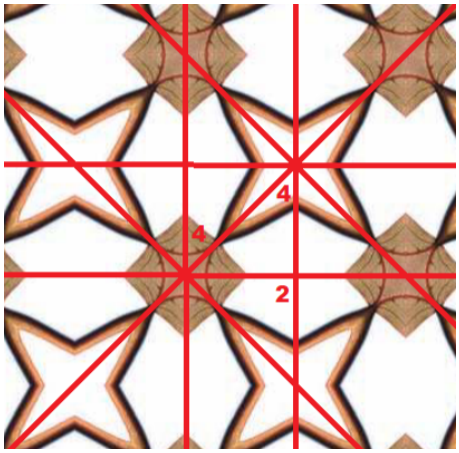
5 Klasifikacija ravninskih vzorcev

Vzorce bi radi klasificirali, zato jih v razrede razporedimo s pomočjo signatur. Vsak vzorec ima eno možno signaturo, ki nam pove, na koliko načinov lahko vzorec zrcalimo ali rotiramo.

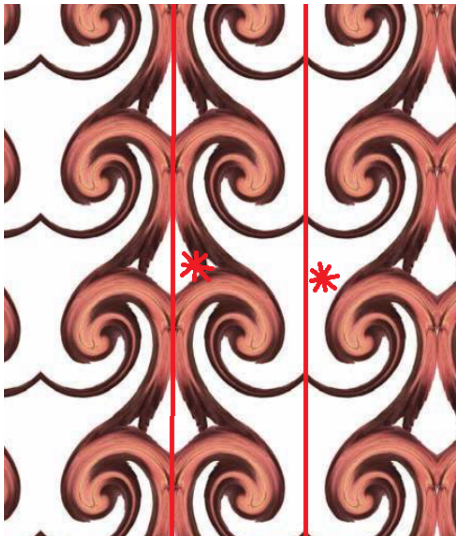
5.1 Signature

Raziskali bomo štiri različne tipe signatur. Te pripadajo zrcalnim osem, rotacijam, zrcalnim pomikom, ki jim pravimo tudi čudeži, in tranlacijam v parih, ki jim rečemo čudesa.

Če se vzorec prezrcali čez dano premico v zrcalno sliko samega sebe, tej premici pravimo *zrcalna os*. Vsak vzorec ima lahko eno, več ali nobene zrcalne osi. Kadar se v vzorcu pojavi zrcalna os, bomo v signaturo zapisali $*$, nato pa bomo v padajočem vrstnem redu zapisali število zrcalnih osi, ki se stikajo v prvem stičišču, število zrcalnih osi, ki se stikajo v drugem stičišču in tako dalje. Številke tako predstavljajo število zrcalnih osi, ki se stikajo v eni točki in jih pišemo z rdečo. Primera zrcalnih osi vidimo na slikah 6 in 7.



Slika 6: Vzorec s signaturo $*442$.



Slika 7: Vzorec s signaturo $**$.

Rotacijske točke so točke, v katerih je središče vrtenja. Vzorec se lahko okrog točke rotira za 180°, 120°, 90° ali 60°, kot nam pove izrek 4.1 o redu rotacij. Kadar se v vzorcu pojavi rotacijska točka, bomo v signaturi z modro barvo v padajočem vrstnem redu zapisali red rotacije okrog prve točke, nato red rotacije okrog druge točke in tako dalje. Primer rotacijskih točk vidimo na sliki 8.

Čudeži so zrcalni pomiki. Oznaka za čudež je $\times$, ogledamo pa si jih lahko na sliki 9.

Čudesa so translacije v parih, označimo jih s simbolom $\circ$. Primer čudes vidimo na sliki 10.

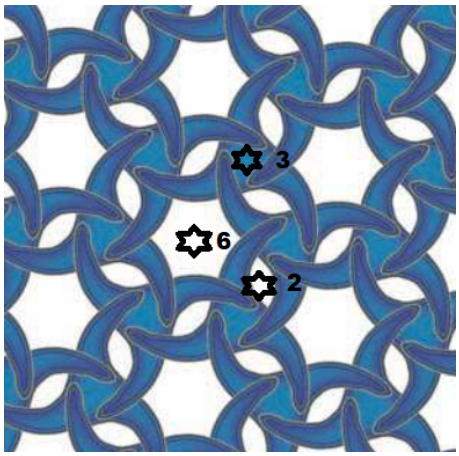
Opomba 5.1. *Razlog, da so ti štirje tipi edini možni tipi simetrij ravninskega vzorca, izhaja iz klasifikacije sklenjenih ploskev in teorije orbiterosti v katere se ne bomo spuščali. Več o tem lahko izvemo v knjigi* [1].

Vsakemu od simbolov v signaturi lahko pripišemo ceno, kot jih podaja tabela 1. *Cena signature* je seštevek cen vseh njenih simbolov. Za cene signatur ravninskih vzorcev velja naslednji presenetljiv rezultat.

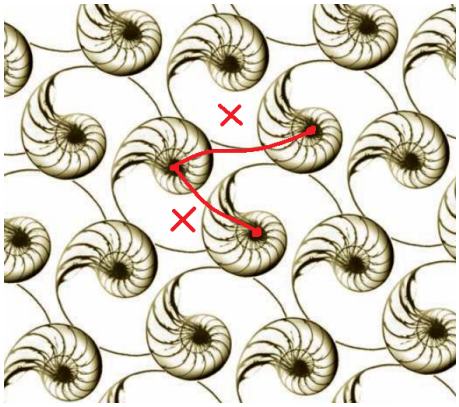
Izrek 5.1 (Magični izrek)**.** *Signatura poljubnega ravninskega vzorca ima skupno ceno* 2.

Magični izrek nam pomaga vse ravninske vzorce opisati s 17 različnimi signaturami.

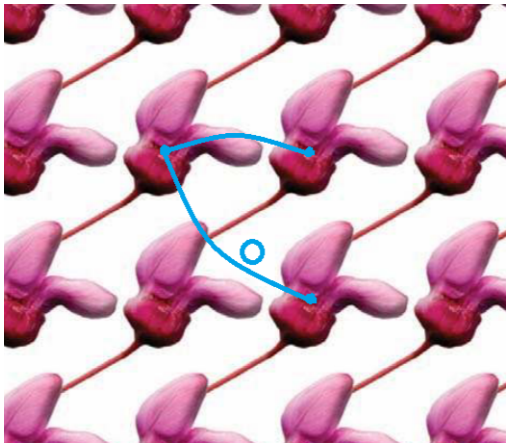
Trditev 5.1. *Vseh signatur ravninskih vzorcev je* 17.



Slika 8: Vzorec s signaturo 632.



Slika 9: Vzorec s signaturo ××.

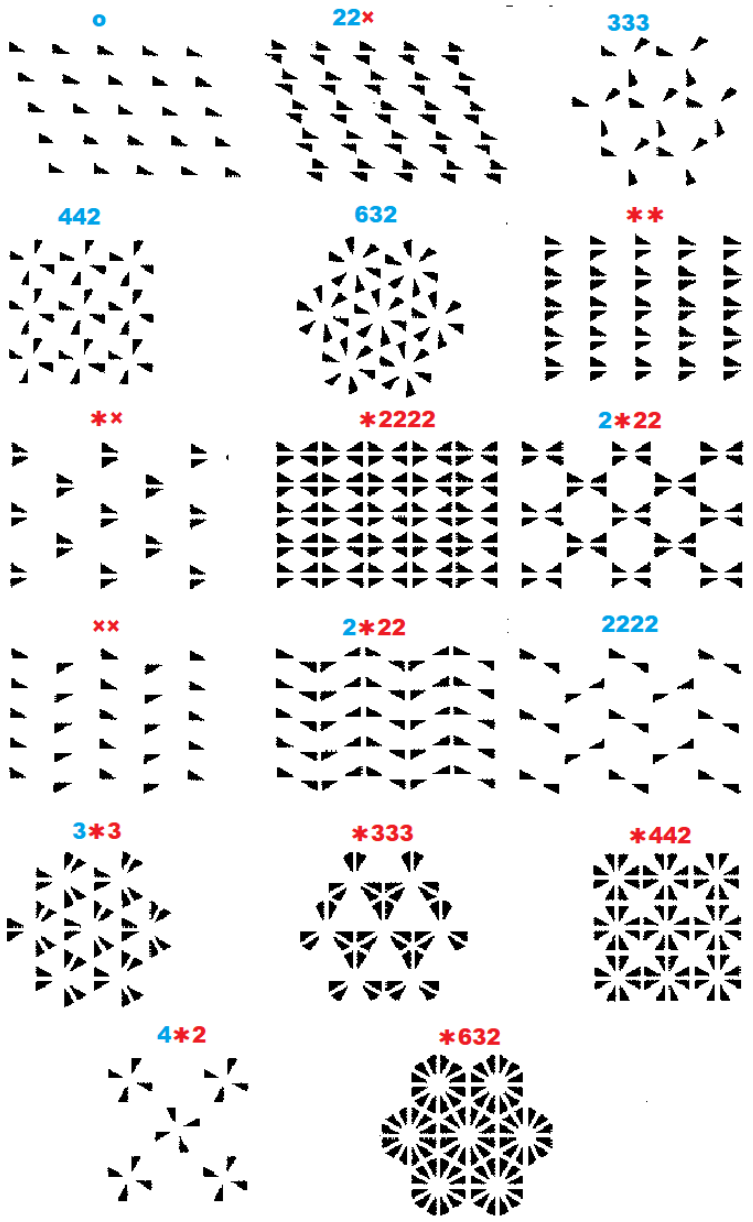


Slika 10: Vzorec s signaturo ∘.

Simbol	Cena ($)	Simbol	Cena ($)
∘	2	$*$ ali ×	1
2	$\frac{1}{2}$	2	$\frac{1}{4}$
3	$\frac{2}{3}$	3	$\frac{1}{3}$
4	$\frac{3}{4}$	4	$\frac{3}{8}$
5	$\frac{4}{5}$	5	$\frac{2}{5}$
6	$\frac{5}{6}$	6	$\frac{5}{12}$
⋮	⋮	⋮	⋮
N	$\frac{N-1}{N}$	N	$\frac{N-1}{2N}$

Tabela 1: Tabela cen simbolov.

Dokaz. Ceno signature dobimo tako, da seštejemo vrednosti njenih simbolov. Če ima vzorec v eni rotacijski točki red rotacije 6, v drugi red 3 in v tretji red 2 lahko iz zgornje tabele vidimo, da se njegova cena izračuna

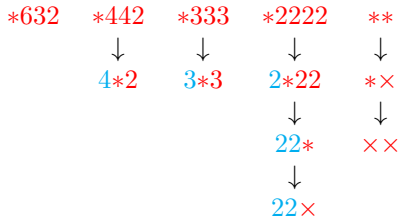


Slika 11: Vseh 17 tipov simetrij v ravnini.

s $\frac{3}{4}+\frac{3}{4}+\frac{1}{2}$, torej je njegova cena 2. Vseh 17 signatur je navedenih spodaj.

632	$\frac{5}{6}+\frac{3}{4}+\frac{1}{2}=2$	$*333$	$1+\frac{1}{3}+\frac{1}{3}+\frac{1}{3}=2$	$3*3$	$\frac{2}{3}+1+\frac{1}{3}=2$
442	$\frac{3}{4}+\frac{3}{4}+\frac{1}{2}=2$	$*442$	$1+\frac{3}{8}+\frac{3}{8}+\frac{1}{4}=2$	$4*2$	$\frac{3}{4}+1+\frac{1}{4}=2$
333	$\frac{2}{3}+\frac{2}{3}+\frac{2}{3}=2$	$*632$	$1+\frac{5}{12}+\frac{1}{3}+\frac{1}{4}=2$	$2*22$	$\frac{1}{2}+1+\frac{1}{4}+\frac{1}{4}=2$
2222	$\frac{1}{2}+\frac{1}{2}+\frac{1}{2}+\frac{1}{2}=2$	$*2222$	$1+\frac{1}{4}+\frac{1}{4}+\frac{1}{4}+\frac{1}{4}=2$	$22\times$	$\frac{1}{2}+\frac{1}{2}+1=2$
$\circ$	2	$**$	$1+1=2$	$22*$	$\frac{1}{2}+\frac{1}{2}+1=2$
				$\times\times$	$1+1=2$
				$*\times$	$1+1=2$

Teh 17 tipov ravninskih vzorcev delimo v tri skupine, prvih pet je modrega tipa (rotacije), drugih pet je rdečega tipa (zrcaljenja), zadnjih sedem pa je hibridov. Dobimo jih tako, da v signaturi bodisi $*nn$ zamenjamo z $n*$ bodisi zamenjamo $*$ z $\times$, kadar v signaturi ni nobene rdeče številke. To je smiselno, saj se pri teh dveh menjavah cena signature ohrani.



Te menjave so v zgornjem diagramu ponazorjene s puščicami. □

Vseh 17 možnih tipov ravninskih vzorcev je na sliki 11.

6 Zaključek

Definirali smo grupe in nekaj osnovnih pojmov teorije grup kot so podgrupe in homomorfizmi grup. Ogledali smo si evklidsko grupo vseh izometrij evklidske ravnine in natančneje razdelali strukturo njeje podgrupe – ortogonalne grupe. Nazadje smo vpeljaji pojem grupe simetrij ravninskega vzorca in idejno opisali, kako lahko s pomočjo signatur klasificiramo vse možne tipe ravninskih vzorcev.

Literatura

[1] J. H. Conway, H. Burgiel, C. Goodman-Strauss, *The Symmetries of Things*, CRC Press, Taylor & Francis Group, Boca Raton, 2008, poglavja 2, 3, 10 in 14.

[2] M. A. Armstrong, *Groups and Symmetry*, Undergraduate texts in mathematics, Springer-Verlag, New York, 1988, poglavji 25 in 26.

Hitra faktorizacija velikih števil

Lenart Dolinar, Kaja Rajter, Jakob Žorž
Mentor: *Nino Cajnkar*

Povzetek

Problem hitre faktorizacije velikih števil je eden od najpomembnejših problemov v sodobni kriptografiji, saj je temelj za reševanje problema diskretnega logaritma in sorodne oblike kodiranja. V nalogi smo obravnavali enega od hitrejših znanih algoritmov za faktorizacijo in sicer metodo eliptičnih krivulj (ECM) ter analizirali njegovo časovno zahtevnost.

1 Grupe

Definicija 1.1. ***Grupa*** *$(G,\circ)$ je par neprazne množice G in binarne operacije $\circ : G\times G\to G$, za katero veljajo sledeči aksiomi grup.*

- *Za vse $x, y, z \in G$ velja* asociativnost*: $x \circ (y \circ z) = (x \circ y) \circ z$.*
- *Obstaja tak element $e \in G$, da za vsak element $x \in G$ velja $x \circ e = e \circ x = x$. Element e imenujemo* enota *grupe.*
- *Za vsak element $x \in G$ obstaja tak x^{-1}, da je $x \circ x^{-1} = x^{-1} \circ x = 1$. Element $x^{-1} \in G$ imenujemo* inverz *elementa x.*

Definicija 1.2. *Če je operacija $\circ$ v grupi $(G, \circ)$ dodatno* komutativna*, torej za vse pare $x, y \in G$ velja $x\circ y = y\circ x$, je G* Abelova grupa*.*

Definicija 1.3. *Grupa je* ciklična*, če je generirana z enim samim elementom.* Red elementa $x \in G$ *je najmanjše naravno število n, da je $x^n = e$. Torej je ciklična grupa G oblike $G = \{e, x, x^2, \ldots, x^{n-1}\}$.*

Primer 1.1. *Naj bo množica G množica vseh celoštevilskih ostankov pri deljenju s praštevilom p in operacija $*$ množenje po modulu p. Potem rečemo, da je $(G, *)$* multiplikativna grupa *in jo označimo $\mathbb{Z}_p^\star$.*

Multiplikativna grupa je primer Abelove ciklične grupe, saj predstavlja množenje po modulu p in je generirana z enim samim elementom, t.j. p. Grupa $\mathbb{Z}_p^\star$ je torej oblike $\mathbb{Z}_p^\star = \{e, p, p^2, \ldots, p^{n-1}\}$.

1.1 Kolobarji

Definicija 1.4. *Naj bo množica K opremljena z binarnima operacijama seštevanja $(x, y) \to x + y$ in množenja $(x, y) \to xy$. Tako strukturo imenujemo* ***kolobar****, če velja*

- *$(K, +)$ je Abelova grupa,*
- *Za vse $x, y, z \in G$ velja asociativnost $x(yz) = (xy)z$ in obstaja tak element $e \in K$, da za vsak $x \in K$ velja $xe = ex = x$. Imenujemo ga enota kolobarja K,*
- *Velja* distributivnost*: za vse $x, y, z \in K$ velja $(x + y)z = xz + yz$ in $z(x + y) = zx + zy$.*

Kolobar, v katerem je operacija množenja komutativna, imenujemo ***komutativen kolobar****.*

1.2 Polja

Definicija 1.5. Polje *je komutativen kolobar, v katerem je vsak neničelen element obrnljiv.*

Polje je torej kolobar, z dodatnima pogojema, da je množenje komutativno in ima vsak element inverz.

Definicija 1.6. *Naj bo K polje. Polje L je* podpolje *polja K, če je L polje in velja $L \subseteq K$. K imenujemo* razširitev *polja L.*

Naj bo $a \in K$ in K razširitev polja L. Pravimo, da je a *algebraičen* nad L, če obstaja nekonstanten polinom $f(x) \in L[x]$, da je $f(a) = 0$. Razširitev K polja L je *algebraična*, če je vsak element $a \in K$ algebraičen nad L.
Polje K je *algebraično zaprto*, če je vsak nekonstanten polinom stopnje $n \geq 1$ nad K razcepen na linearne faktorje.

Izrek 1.1. *Naj bo I podgrupa za seštevanje kolobarja K z operacijo seštevanja $+$. Potem postane množica vseh odsekov $K/I = \{a + I \mid a \in K\}$ aditivna grupa z operacijo $(a + I) + (b + I) = (a + b) + I$.*

Če še dodatno velja $a + I = a' + I$ in $b + I = b' + I$, potem $ab + I = a'b' + I$, kar je ekvivalentno, da za vsaka $a, b \in K$ velja, da

$$ab \in I \implies a \in I \vee b \in I.$$

Definicija 1.7. *Če je K/I kolobar, potem I imenujemo* ideal. *Če je I ideal in K/I polje, potem I imenujemo* praideal.

2 Gladkost

Definicija 2.1. *Naj bosta B in n naravni števili, pri čemer ima n praštevilski razcep $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$. Število n je* B-gladko *natanko tedaj, ko za vsak $i \in \{1, \dots, k\}$ velja: $p_i < B$.*

S $\Psi(x, y)$ označimo število praštevil, ki so manjša od x in so y-gladka. Verjetnost, da je poljubno izbrano naravno število y-gladko, je

$$P_{gladko}(x, y) = \frac{\Psi(x, y)}{x}.$$

Izrek 2.1. *Naj bo $\pi(x) : \mathbb{R}^+ \to \mathbb{N}$ funkcija, ki pozitivnemu realnemu številu x priredi število vseh praštevil, manjših ali enakih x.* Izrek o praštevilih *nam pove, da se funkcija π asimptotsko obnaša enako kot $x \to \frac{x}{\log x}$, oziroma*

$$\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1.$$

Izrek 2.2. *Naj bo $\varepsilon > 0$ in $3 \leq u \leq (1 - \varepsilon)\frac{\log x}{\log \log x}$ ter x kot v prejšnjem izreku. Potem velja*

$$\Psi(x, x^{\frac{1}{u}}) = x \cdot u^{-u+o(u)},$$

pri čemer je $o(u)$ funkcija x in u, ki enakomerno konvergira proti 0, ko gre x proti neskončno.

Posledica 2.1. *Naj bo $y \leq x_1, x_2 \leq x$ in $u = \frac{\log x}{\log y}$, pri čemer u zadošča pogojem prejšnjega izreka. Potem velja, da je*

$$P_G(x_1, y) \cdot P_G(x_2, y) = P_G(x_1 \cdot x_2, y)^{1+o(u)}.$$

Dokaz: Naj bo $u_1 = \frac{\log x_1}{\log y}$ in $u_2 = \frac{\log x_2}{\log y}$. Brez škode za splošnost lahko predpostavimo, da je $u_2 \geq u_1$. Ker sta u_1 in u_2 večja ali enaka 1, vemo, da sta $\log u_1$ in $\log u_2$ večja od 0. Sledi, da je $\log(u_1 + u_2)$ večje od 0. Naj bo $L(u_1, u_2) = u_1 \cdot \log u_1 + u_2 \cdot \log u_2$ in $R(u_1, u_2) = (u_1 + u_2)\log(u_1 + u_2)$.

Ker je $\log(u_1 + u_2)$ večje od $\log u_1$ in od $\log u_2$, velja $L(u_1, u_2) \leq R(u_1, u_2)$. Če je $u_1 \geq \frac{u_2}{\log u_2}$, velja tudi $\log u_1 \geq \log u_2 - \log\log u_2$.
Ker je $u_1 = \frac{u_2}{\log u_2}$, dobimo:

$$\begin{aligned} \log u_2 + \log 2 &\geq \log(u_1 + u_2), \\ \log(2u_2) &\geq \log(u_1 + u_2), \\ L(u_1, u_2) &\geq (u_1, u_2) \cdot (\log(u_1 + u_2) - \log 2 - \log\log u_2. \end{aligned}$$

Ko gre u_2 proti neskončno, velja $L(u_1, u_2) \geq (1 - \varepsilon)R(u_1, u_2)$.

Če je $u_1 \leq \frac{u_2}{\log u_2}$, velja tudi $L(u_1, u_2) \geq u_2 \log u_2$ in dobimo

$$u_2 \cdot \log u_2 \cdot (1 + \frac{1}{\log u_2}) \cdot (1 + \log(1 + \frac{1}{\log u_2})) \geq (u_1 + u_2)\log(u_1 + u_2).$$

Ponovno, ko gre u_2 proti neskončno velja

$$R(u_1, u_2) \leq (1 + \varepsilon)u_2 \log u_2 \leq (1 + \varepsilon)L(u_1, u_2).$$

Sledi

$$P_G(x_1, y) \cdot P_G(x_2, y) = P_G(x_1 \cdot x_2, y)^{1+o(u)},$$

kar je točno to, kar smo želeli dokazati. □

3 L-notacija

Z algoritmom želimo faktorizirati velika števila v razumnem času.

Definicija 3.1. ***Časovna zahtevnost*** *je podatek o tem, koliko bitnih operacij bo program naredil pri danih vhodnih podatkih, preden bo vrnil rešitev.*

Časovno zahtevnost označimo z O notacijo, ki označuje red rasti problema.

Notacija	Zahtevnost
$O(1)$	konstantna
$O(\log n)$	logaritemska
$O(n)$	linearna
$O(n \log n)$	vmesna
$O(n^2)$	kvadratna
$O(n^c); c > 1$	polinomska
$O(c^n)$	eksponenta

Definicija 3.2. *Algoritmi, ki imajo večjo časovno zahtevnost od polinomske in manjšo od eksponentne glede na bitni zapis vnosa, so* subeksponentni.

Časovno zahtevnost algoritma lahko predstavimo z L-notacijo

$$L_x(\alpha, c) = exp\{c(\log x)^\alpha (\log\log x)^{1-\alpha}\}.$$

Izrek 3.1. *Naj bodo a, b, c in d pozitivna realna števila ter naj velja $a > c$. Potem velja*

$$P_G(L_x(a,b), L_x(c,d) = L_x\left(a-c, (a-c)\,\frac{b}{d}\right)^{-1+o(u)}.$$

L-notacije želimo tudi seštevati in množiti, kar lahko storimo s pomočjo formul iz naslednjega izreka.

Izrek 3.2. *Naj bosta (a,b) in (c,d) para pozitivnih realnih števil. Potem velja*

$$L_{\{L_x(a,b)\}} = L_x\left(ac, db^c a^{(1-c)}\right)^{(1+o(u))}$$

in

$$L_x(a,b)\cdot L_x(c,d) = \begin{cases} L_x(a,b)^{1+o(u)}; a > c \\ L_x(a, b+d); a = c \end{cases}.$$

Dodatno lahko predpostavimo, da je (a,b) leksikografsko večje od (c,d), torej velja, ko je $a > c$ ali $a = c$ in $b > d$. Potem velja

$$L_x(a,b) + L_x(c,d) = L_x(a,b)^{1+o(u)}.$$

4 Pollardova $p-1$ metoda

Pollardova $p-1$ metoda je algoritem za faktorizacijo velikih števil. Deluje na principu, da poišče take praštevilske faktorje, da velja, da je $p-1$ B_0-gladko. Koraki v algoritmu so sledeči.

1. Izberemo poljubno število $x_0 \in [2, N-2]$, tako da je $gcd(x_0, N) = 1$.
2. Izračunamo $M = \prod_{q\in\mathbb{P}, q\le B_0} q^{\lfloor log_q N\rfloor}$.
3. Izberemo poljubno število tuje N.
4. Izračunamo $g = gcd(x_0^M - 1, N)$.
5. Če je $1 < g < N$, vrnemo g.
6. Če je $g = 1$, potem izberemo večjo mejo gladkosti B_0 in se vrnemo nazaj na 2. korak.
7. Drugače izberemo drugačen x_0 in ponovimo korake od začetka.

Primer 4.1. *Poskusili bomo faktorizirati število $N = 299$.*

1. *Za B_0 izberemo število 5.*
2. *Izračunamo $M = 2^2 \times 3^1 \times 5^1 = 60$.*
3. *Izberemo $x_0 = 2$.*
4. *$g = gcd(2^{60} - 1, 299) = 13$.*
5. *Ker je $1 < 13 < 299$, vrnemo 13.*
6. *Velja $299/13 = 23$, ker je praštevilo, torej dobimo popolno faktorizacijo; $299 = 13 \times 23$.*

5 Algoritem za hitro potenciranje

Želimo izračunati a^b za $a \in \mathbb{Z}, b \in \mathbb{N}$. Naivno se da b-krat pomnožiti a. Množenje porabi $O(1)$ korakov, torej cel algoritem porabi $O(b)$ časa. Izkaže se, da obstaja veliko hitrejši algoritem, ki deluje za poljubne grupe. Oglejmo si primer izračuna a^{32}. To lahko naredimo na naslednji način:

$$\begin{aligned} a^2 &= a \cdot a \\ a^4 &= a^2 \cdot a^2 \\ a^8 &= a^4 \cdot a^4 \\ a^{16} &= a^8 \cdot a^8 \\ a^{32} &= a^{16} \cdot a^{16} \end{aligned}$$

Uporabili smo torej le 5 množenj, namesto 31, kot bi jih, če bi računali naiven način. Izkaže se, da je to mogoče za vse potence.

Izrek 5.1. *Naj bo $(G, \cdot)$ grupa za množenje in $a \in G$. Potem lahko a^n izračunamo v $O(\log n)$ časa.*

Dokaz: Naj bo $n = \sum_{i=0}^{k} b_i 2^i$ binarna razčlenitev števila n, torej je za $\forall i : b_i \in \{0, 1\}$ in k mora biti dovolj velik. Velja tudi $k \leq \log_2 n$, ker je 2^k največji člen v razčlenitvi števila n. Potem je $a^n = \prod_{i=0}^{k} a^{b_i 2^i}$. Torej je a^n produkt največ $k+1$ potenc a^{2^i}. Potence a^{2^i} lahko izračunamo tako, da začnemo z $a^1 = a$ in potem $a^{2^i} = (a^{2^{i-1}})^2$. Torej lahko vse potence a^{2^i} izračunamo v $O(\log n)$ časa in posledično tudi a^n. □

6 Razširjen evklidov algoritem

Bezoutova identiteta pravi, da za vsaki števili $a, b \in \mathbb{Z}$ obstajata taki števili $x, y \in \mathbb{Z}$, da velja $ax + by = d$, kjer je $d = \gcd(a, b)$. V tem razdelku bomo spoznali algoritem, ki nam bo omogočil, da bomo našli x in y. Zaradi preglednosti bomo iskanje najmanjšega skupnega delitelja s pomočjo razširjenega Evklidovega algoritma označili s $gcdx(x, y)$.

Algoritem 6.1. $gcdx(a, b) \to (d, x, y)$

- *Če je $b = 0$, potem vrnemo $(a, 1, 0)$.*
- *Izračunamo $(d, x', y') = gcdx(b, a \bmod b)$.*
- *Vrnemo $(d, y', x' - \lfloor a/b \rfloor y')$.*

Dokaz: Če je $b = 0$, je $\gcd(a, b) = a$ in $ax + by = a$ za $x = 1$ in $y = 0$.
Predpostavimo, da $gcdx(b, a \bmod b)$ vrne pravilen rezultat. Potem velja

$$bx' + (a \bmod b)y' = d.$$

Velja tudi zveza $a \pmod b = a - \lfloor a/b \rfloor b$, zato jo lahko vstavimo v zgornjo enačbo in dobimo

$$\begin{aligned} bx' + (a - \lfloor a/b \rfloor b)y' &= d, \\ bx' + ay' - \lfloor a/b \rfloor by' &= d, \\ ay' + b(x' - \lfloor a/b \rfloor y') &= d, \end{aligned}$$

Torej vrne tudi naš algoritem pravilni rezultat. □

Velja $gcdx(a, b) = gcdx(b, a)$, zaradi česar lahko brez škode za splošnost rečemo, da je $a \geq b$. Časovna

zahtevnost je $O(\log a)$, ker se v vsakem koraku a zmanjša za vsaj polovico.
Za velika števila, ki so večja od 2^{64}, so operacije z njimi $O(\log n)$, zato je časovna zahtevnost algoritma $O(\log^2 a)$.

7 Algoritem Metode eliptičnih krivulj (ECM)

7.1 Eliptične krivulje

Definicija 7.1. Projektivna ravnina $\mathbb{P}^2$ *nad poljem* $\mathbb{F}$ *je kvocientni prostor* $\mathbb{F}^3 - \{0\}/\sim$, *kjer je ekvivalenčna relacija podana s predpisom* $(a,b,c) \sim (\alpha a, \alpha b, \alpha c)$ *za vsak* $\alpha \in \mathbb{F} - \{0\}$. *Točke v* $\mathbb{P}^2$ *so torej podane s homogenimi koordinatami* $[a,b,c] = [\alpha a, \alpha b, \alpha c]$ *za vse* $\alpha \neq 0$.

Definicija 7.2. *Polinom* P *je* homogen*, če velja*

$$P(\lambda x, \lambda y, \lambda z) = \lambda^d (x, y, z)$$

za vse $\lambda \in \mathbb{F}$.

Definicija 7.3. Algebraična krivulja*, podana s homogenim polinomom* P*, je množica točk* $C_p = \{A \in \mathbb{P}^2, P(A) = 0\}$. *Algebraična krivulja je* gladka*, če nima nobenih samopresečišč ali singularnosti.*

Definicija 7.4. Gladko kubično krivuljo *nad algebraično zaprtim poljem lahko zapišemo v kratki Weierstrassovi obliki:* $y^2 z = x^3 + axz^2 + bz^3$.

7.2 Algoritem

Algoritem metode eliptičnih krivulj ima dve fazi in sicer glavno fazo ter 1. fazo.

Algoritem 7.1. *Glavna Faza:*
Vhod: *eliptična krivulja* $E_{W,A,B}$ *nad* $\mathbb{Q}$*, točka* P_0 *neskončnega reda in meja gladkosti* B_1.

- *Izberemo poljubno eliptično krivuljo in neko poljubno netrivialno točko na njej. Imamo mejo gladkosti* B_1. *Število elementov v grupi točk na eliptični krivulji mora biti manjše od* B_1.
- *Izračunamo* $M = \prod_{q \in \mathbb{P} \wedge q \leq B_1} q^{\lfloor \log_q(N) \rfloor}$.
- *Seštejemo točke na eliptični krivulji* $P_0^M \pmod N$.
- *Izračunaj* $gcdx(z, N)$.
- *Če je* $gcdx(z, N) \neq 1$*, potem je* $gcdx(z, N)$ *faktor števila* N.

Faza 1:

- $B_1 = L_B\left(\frac{1}{2}, \frac{\sqrt{2}}{2}\right)$ *je dobra meja za gladkost.*
- *Ponavljaj, dokler ne najdeš prafaktorja:*
- $S = \{B_1$*-gladki elementi iz* $(p - \sqrt{p}, p + \sqrt{p})\}; u = |S|$.
  - *Izvedi glavno fazo na* N*, za mejo gladkosti* B_1 *in za eliptično krivuljo* E.

Dokaz: Pravilnost algoritma:

Obstaja praštevilo p, ki deli število N. Ker je red $E(\mathbb{F}_p)$ B_1-gladek, so vsi prafaktorji od $E(\mathbb{F}_p)$ B_1 gladki. Ker je B_1 majhen glede na N, so $\lfloor \log_2 N \rfloor$ za vsak q iz M višji ali enaki potencam praštevil iz razcepa $\mathbb{F}_p$. Posledično $|\mathbb{F}_p|$ deli M. Opazimo, da veljata enakosti $Z \equiv 0 \pmod{p}$ in $g \equiv 0 \pmod{p}$, kar pomeni, da je p hkrati faktor od Z in g, torej je res g praštevilski faktor od N. □

8 Časovna zahtevnost

Pokazali bomo, da je časovna kompleksnost celega algoritma enaka

$$T(ECM) = \log^3(N) L_B\left(\frac{1}{2}, \sqrt{2}\right).$$

Najprej pogledamo glavno fazo. Tukaj imamo tri korake, ki nezanemarljivo prispevajo h končni časovni zahtevnosti algoritma:

- $M = \prod_{q \in \mathbb{P} \wedge q \leq B_1} q^{\lfloor \log_q(N) \rfloor}$,
- $P_0^M \pmod{N}$,
- $xgcd(z, N)$.

Vzamemo definicijo M in logaritmiramo obe strani:

$$\begin{aligned}
\log M &= \sum_{q \in \mathbb{P} \wedge q \leq B_1} \lfloor \log_q N \rfloor \log q \\
&\leq \log(N) \sum_{q \in \mathbb{P} \wedge q \leq B_1} \log q \\
&\leq \log(N) \sum_{q \in \mathbb{P} \wedge q \leq B_1} \log B_1 \\
&= \log(N) \frac{B_1}{\log B_1} \log B_1 \\
&= B_1 \log(N).
\end{aligned}$$

Torej je časovna zahtevnost druge operacije $O(B_1 \log N)$. Časovna zahtevnost tretje operacije je $O(\log^2 N)$, ker je to časovna zahtevnost potenciranja za velike številke. Zaradi implementacije se časovni zahtevnosti zmnožita, torej je časovna zahtevnost glavne faze $O(B_1 \log^3 N)$.

Naj bo $P_B(B_1)$ verjetnost, da bo algoritem našel praštevilo p v fazi 1, če je p B_1-gladko.

Izrek 8.1. *Obstaja pozitivna izračunljiva konsatnta c, da velja:*
Naj bodo $n, v, w \in \mathbb{Z}_{a>1}$. Števila n, v, w so taki, da ima n vsaj dva različna praštevilska delitelja, ki sta večja od 3. Za manjši praštevilski delitelj od n, ki je večji od 3, velja $p \leq v$. Označimo

$$u = |\{s \in \mathbb{Z} : |s - (p+1)| \leq \sqrt{p} \text{ in vsak praštevilski delitelj od } s \text{ je } \leq w\}|.$$

Z N označimo število trojic $(a, x, y) \in (\mathbb{Z}_n)^3$ za katere je ECM uspešen. Potem velja

$$\frac{N}{n^3} > \frac{c(u-2)}{(\log p)(2\sqrt{p}+1))}.$$

Potem je $P_B(B_1) \geq \frac{c(u-2)}{(\log p)(2\sqrt{p}+1))}$, kar se upošteva pri O notaciji. Časovna zahtevnost celega algoritma je torej

$$T(ECM) = B_1 \log^3(N) P_G^{-1}(B, B_1).$$

Nadalje izberemo mejo gladkosti B_1 tako, da bo časovna zahtevnost minimalna. To se zgodi natanko tedaj, ko velja $B_1 = L_B(\alpha, c)$. Sedaj izračunamo verjetnost, da je poljubno izbrano število manjše od B, B_1-gladko

$$\begin{aligned} P_G(B, B_1) &= (L_B(1,1), L_B(\alpha, c)) = \\ &= L_B(1-\alpha, \frac{1-\alpha}{c})^{1+o(1)} \end{aligned}$$

Najboljša vrednost α je $\frac{1}{2}$, torej je časovna zahtevnost

$$T(ECM) = \log^3(N) L_B\left(\frac{1}{2}, \sqrt{2}\right).$$

Faktor $\log^3(N)$ je zanemarljiv, zato je

$$T(ECM) = L_B\left(\frac{1}{2}, \sqrt{2}\right).$$

IZKUŠNJE UDELEŽENCEV

Izkušnje udeležencev

Manca Ernst, Jakob Žorž, Hugo Trebše

Manca

Ko sem se nekega sobotnega jutra z družino odpravila na dolgo vožnjo do rovt, kjer je letos potekal MaRS, sem že dobro vedela, kaj me čaka – teden, poln reševanja problemov in neprespanih noči, v sobi pa Mars čokoladica ter majica (letos preverjeno v barvi parketa).

Čeprav se na taboru res bolj malo spi, razlog za to ni nujno razmišljanje o problemih, ki nam jih s projekti predstavijo mentorji. Morda se nas je tokrat veliko ukvarjalo s teorijo grup, smo pa zato bili deležni tudi terapije grup, ki je brez težav trajala pozno v noč. Večina MaRSovcev se namreč med igro Avalona rada prelevi v viteze okrogle mize, še raje pa v njihove sovražnike ter povsem navadne in nemočne kmete, tako za trenutek pozabi, da je z ljudmi okrog sebe stkala nova prijateljstva, in upravičeno vpije nanje.

Ni nam primanjkovalo niti organiziranega družabnega programa, ki ga je letos zagotovo obogatil Estimathon, kljub temu da je bila naša ekipa gladko poražena. Eni v prostem času radi računajo Fibonaccijevo zaporedje in štejejo objave na Instagramu, eni pa pač ne.

Naši mentorji so imeli ob sestavi programa v mislih tudi našo fizično kondicijo. Vsako jutro smo se morali udeležiti začetnega tečaja joge ali česa hujšega, vsi zamudniki so redno krepili mišice zgornjega dela telesa, nekateri pogumneži so se celo lotili košarke, čeprav so kmalu ugotovili, da bi bilo lažje le izračunati, koliko časa žoga potrebuje, da priplava iz jezera, potem ko se nesrečno znajde v njem.

Po tednu, polnem matematičnih ugank, barvanja pobarvank in pitja cedevite, je bil žal čas za odhod domov. Ta nam je skoraj bil onemogočen, saj ni malo manjkalo, da bi zaradi vremenskih razmer Slovenija čez noč postala nepovezan graf. Kljub temu pa vsi zagotovo komaj čakamo, da se vrnemo. Na MaRSu smo spoznali veliko novega, od matematičnih tem do pogojev lastništva kape, večinoma stvari, ki se jih pri pouku matematike sicer ne bi naučili, pa vendar zanimivih tudi tistim, ki se z njimi kasneje morda ne bodo več srečali.

Jakob

Moje doživetje na taboru MaRS je bilo izjemno pozitivno. Posebej sem užival v družabnih dogodkih, ki so bili vsi izjemno zanimivi. Velik plus tabora je priložnost, da spoznaš vrstnike, ki so med najboljšimi matematiki svoje generacije, pa tudi nekdanje udeležence olimpijad, s katerimi si lahko izmenjaš par besed.

Naš projekt, ki se je ukvarjal z eliptičnimi krivuljami, je bil precej zahteven in napreden. Skozi delo na projektu sem pridobil veliko novega znanja. Presenetilo me je, kako koristna je teorija grup pri reševanju računalniških problemov s področja teorije števil. Čeprav nismo uspeli implementirati končnega produkta, smo se poglobili v teorijo, kar se je izkazalo za zahteven, a ključen korak.

Najljubši del tabora zame je bil trenutek, ko smo pozno v noč ali zgodaj zjutraj igrali razne igre. Spomnim se, kako smo skoraj dokončali Hanabi ali ugotavljali, kdo med nami je mafija. Nepozabno je bilo tudi prenajedanje kruha ob treh zjutraj in poslušanje novic. Tabor je presegel moja pričakovanja, saj sem se že na začetku spraševal, ali bo zame, saj me programiranje bolj zanima kot matematika. A spoznal sem, da ni potrebno biti matematični genij, da bi bil del tabora. Vsakdo, ki je pripravljen izzvati samega sebe, je primeren za na tabor. Ključno je, da matematiko raziskuješ z veseljem.

Tabor MaRS zame pomeni veliko več kot le pridobljeno matematično znanje. Naučil sem se pomembnih življenjskih lekcij, ki niso omejene na računalniško ali matematično področje. Prepričan sem, da bo ta izkušnja ostala trajno zapisana v mojem spominu.

Hugo

MaRS je vsekakor eden izmed najbolj zanimivih, poučnih ter obče informativnih dogodkov za matematično interesiranega srednješolca oz. srednješolko.

Sam pripisujem to dejstvo modernemu pristopu do poučevanja, ki ga gojijo že od začetka tabora. Poleg klasičnega pristopa do poučevanja matematike, ki zagovarja predavanje znanja predavatelja poslušalcem, mentorji vztrajajo pri tem, da se udeleženci sami spoprimemo z dvema najpomembnejšima deloma raziskovalne matematike: spoznavanju novih, zapletenih konceptov, ki se mnogim na prvi pogled zdijo skorajda strašljivi, ter pisanju člankov, ki hkrati deluje kot filter, ki preverja pisateljevo razumevanje, ter kot način širjenja spoznanj.

Poleg pridobivanja oprijemljivega znanja, ki ga dijaki prejmejo med predavanji ter delavnicami, je MaRS priložnost za spoznavanje matematično nadarjenih sovrstnikov ter komuniciranje z mentorji. Slednje predstavlja odlično priložnost, preko katere udeleženci iz prve roke pridobijo informacije o študiju matematike, za poučnost katerih lahko odkrito jamčim sam. Med mnoga neoprijemljiva znanja, ki jih udeleženci pridobijo, šteje tudi neke vrste matematična zrelost, kar bi lahko opisali kot skupek znanj, hevristik, ter splošnih prijemov o tem, kako pristopiti do matematičnega problema, katero mentorji predajo udeležencem skozi celotno trajanje tabora, še posebej pa med skupinskim delom na projektih.

Izvzemši gost matematični žargon pa je MaRS tudi priložnost za druženje ter družabne aktivnosti, bodisi v obliki številnih iger taroka, dolgih noči Una bodisi pa kot mnoge, postopoma vse manj smiselne uganke.

Skupek vseh teh dejavnikov naredi MaRS odlično priložnost tako za dijake, katerih matematična zanimanja se šele začenjajo, kot za zagrizene matematike.

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.

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.

Zavarovalnica Triglav

Zavarovalnica Triglav je vodilna slovenska klasična zavarovalnica in matična družba Skupine Triglav. Je največja zavarovalno-finančna skupina v Sloveniji in regiji Adria, ki posluje v šestih državah in na sedmih trgih ter širše mednarodno preko partnerskega povezovanja z družbami za zavarovalno posredovanje, zastopanje in pozavarovanje. Ključna stebra njenega poslovanja sta zavarovalništvo in upravljanje premoženja. Z znanjem, izkušnjami in finančno močjo že več kot 120 let upravičuje zaupanje strank in drugih deležnikov.

Teces

TECES, grozd zelenih tehnologij, Maribor
TECES je z več kot dvajsetletnimi izkušnjami eden od najizkušenejših slovenskih nosilcev in koordinatorjev strateških razvojnih partnerstev in razvojnih projektov. Z Ministrstvom za obrambo RS je 2020 ustanovil Slovensko partnerstvo za energijo in okolje na obrambnem področju (SiEnE), od leta 2017 pa je soustanovitelj Strateškega razvojno-inovacijskega partnerstva Pametne stavbe in dom z lesno verigo (SRIP Pametne stavbe). Pod svojim okriljem združuje več kot 60 članov: vodilnih slovenskih podjetij, raziskovalno-razvojnih ter drugih organizacij. Glavno poslanstvo TECES je izboljšanje konkurenčnosti članov z ustvarjanjem sinergij in spodbujanjem sodelovanja med člani, partnerji in državo. TECES nudi podporo članom na področjih: skupni razvoj in verige vrednosti (pobude za in koordinacija razvojno projektov in strateških razvojnih partnerstev), mednarodno sodelovanje (aktivna vloge v mednarodnih iniciativah in programih), sodelovanje z državo (aktivna vloga pri pripravi strategij), sofinanciranje razvojnih aktivnosti članov in partnerjev (iskanje primernih EU in SLO razpisov), usposabljanja in razvoj kadrov ter mreženje članov (ustvarjanje priložnosti za sinergije med člani in partnerji).

AFLabs

Smo mednarodno razvojno raziskovalno podjetje, ki se ukvarja z unikatnimi projekti, ki zahtevajo visoko raven tehničnega znanja, natančnosti, ekipnega dela, izkušenj in zanesljivosti.

Mil Sistemika

MIL Sistemika je visoko tehnološko podjetje, registrirano za razvoj programske opreme. Je specializirano podjetje za razvoj aplikacij na področju navigacije, sledenja vozil, sistemov poveljevanja in kontrole, geografskih informacijskih sistemov (GIS) ter radijskih in satelitskih komunikacij. Programsko opremo podjetja Mil Sistemika uporabljajo različne državne inštitucije, organizacije za zaščito in reševanje, policija in vojska. Programska oprema je prilagojena za delovanje v mobilnih omrežjih in preko radijskih naprav. Posebnost Mil Sistemike so zahtevne integracije namenske strojne opreme v enovito celoto, kar omogoča razširitev spektra uporabe integrirane rešitve. Na podlagi fleksibilnosti razvoja, je Mil sistemika na svetovnem trgu pridobila različne partnerje, ki delujejo po celem svetu. Mil Sistemika trži svoje proizvode skoraj izključno preko svojih partnerjev. Na ta način lahko zagotovi učinkovito prodajo in podporo strankam na oddaljenih trgih, bližnjega vzhoda in jugo-vzhodne Azije.

Outbrain

UL FMF

Univerza v Ljubljani
Fakulteta za matematiko in fiziko

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

Univerza v Mariboru

Fakulteta za naravoslovje
in matematiko

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.

3K IT

3K IT d.o.o.

V podjetju 3K IT d.o.o. se od ustanovitve leta 2003 ukvarjamo z razvojem lastnih programskih rešitev za obvladovanje poslovnih procesov in poslovne dokumentacije. Svojo glavno programsko rešitev smo poimenovali 3K Document Cycle. Z aplikacijo 3K Document Cycle boste digitalizirali vaše poslovne procese in uredili poslovno dokumentacijo. Rezultati so večja učinkovitost, prihranek časa, boljše sodelovanje in zadovoljni sodelavci. Svoje delo opravljamo s strastjo11 in se nenehno trudimo biti ustvarjalni in boljši. Smo pošteni, odprti in etični. Na vaši poti vam bomo pomagali z našim znanjem in izkušnjami. In verjemite, z IT podjetjem se lahko tudi dobro razumete.