MaRS 2024

Matematično raziskovalno srečanje 2024

Pohorje, 14.–20. julij

DMFA Slovenije

Matematično raziskovalno srečanje 2024

Zbornik

Avtorji: *dr. Nino Bašić, Nino Cajnkar, mag. Andreja Čič, dr. Jernej Činč, Jan Genc, Katarina Grilj, Žan Hafner Petrovski, Izak Jenko, Juš Kocutar, Matija Likar, Tim Milanez, dr. Matija Pretnar, Kaja Rajter, Nejc Zajc*

Uredila: *Matija Likar, Nejc Zajc*

Recenzenti: *Nino Cajnkar, Jan Genc, Katarina Grilj, Izak Jenko, Juš Kocutar, Matija Likar, Tim Milanez, Kaja Rajter, Nejc Zajc*

Oblikoval: *Žan Hafner Petrovski*

Predstavnica: *dr. Mojca Vilfan*

Kraj in leto izida: Ljubljana, 2024

Izdalo: Društvo matematikov, fizikov in astronomov Slovenije

Prva elektronska izdaja objavljena na povezavi:
http://mars.dmfa.si/clanki/zbornik-2024.pdf

Cobiss ID: 218011139

Kataložni zapis o publikaciji (CIP) pripravili v Narodni in univerzitetni knjižnici v Ljubljani
COBISS.SI-ID 218011139
ISBN 978-961-96854-0-2 (PDF)

Kazalo

UVOD

Uvodnik

Nejc Zajc

O taboru

Matematično raziskovalno srečanje ali MaRS je poletni matematični tabor za srednješolke in srednješolce. Z zbornikom bomo bralcem poskusili približati dogajanje letošnje izvedbe.

To poletje smo izpeljali že devetnajsti MaRS zapored. Potekal je v tednu med nedeljo, 14. julijem, in soboto, 20. julijem. Udeležilo se ga je 22 dijakinj in dijakov iz vse Slovenije, ki so pod mentorstvom devetih študentov širili svoja matematična obzorja.

Strokovni del tabora je sestavljen iz treh delov – osrednje delavnice, večernih predavanj in projektov. Pri osrednji delavnici tabora, ki jo je spretno vodil dr. Nino Bašić, so udeleženci spoznali osnove spektralne teorije grafov in Hücklove teorije. Delavnica je potekala v treh delih med torkom in četrtkom. Druga skupina matematičnih vsebin tabora so večerna predavanja gostujočih profesorjev slovenskih univerz in naših podpornikov. Letos so nas obiskali trije. Dr. Jernej Činč je predaval o diskretnih dinamičnih sistemih, dr. Matija Pretnar o kvantnem računalništvu in Andreja Čič o modeliranju življenjskih zavarovanj.

Kot vedno so bili projekti glavna matematična vsebina tabora. Skupine treh ali dveh udeležencev so pod mentorstvom člana študentske ekipe organizatorjev raziskale v naprej izbrano matematično temo. Delo na projektih je potekalo cel teden in je zajelo večino strokovnih ur programa. Dijaki so se s temo svojega projekta najprej spoznali preko uvodnih primerov, jo raziskali in prišli do zaključkov. Delo na projektih obsega tudi pripravo članka, ki podrobno opiše spoznano in je vključen v zbornik, ter kratke predstavitve za starše in ostale udeležence ob zaključku tabora.

Poleg vseh omenjenih matematičnih dejavnosti smo za udeležence pripravili tudi pester družabni program. Skozenj so se udeleženci preizkusili v spretnosti ocenjevanja, domišljije in medsebojnega poznavanja. Vsak dan po koncu strokovnega programa so se udeleženci in mentorji do poznih ur družili ob raznolikih družabnih igrah. Tudi letos ni manjkal tradicionalni del programa, ki zajema pohod, Veliko MaRSovsko pustolovščino in MaRSovski piknik. Velika MaRSovska pustolovščina je orientacijski pohod po naravi s kratkimi in zabavnimi nalogami za udeležence na kontrolnih točkah.

Urnik tabora je bil tako polno zaseden. S pomočjo naših podpornikov nam ga je uspelo tudi v celoti izvesti. Kot zmeraj je bil tabor izveden pod okriljem DMFA Slovenije, naši podporniki pa so letos bili Zavarovalnica Sava, Jane Street, Fakulteta za matematiko in fiziko Univerze v Ljubljani, Fakulteta za naravoslovje in matematiko Univerze v Mariboru, AFLabs, 3K IT in Dewesoft. Z njihovo pomočjo smo tabor uspešno izvedli, udeleženci pa so z nami preživeli zanimiv, poučen in nepozaben teden.

Beseda odgovorne osebe

Drage udeleženke, udeleženci in posadka, spoštovani predavatelji, podporniki in ostali bralci zbornika. Letošnji polet na MaRS je uspešno zaključen. Navkljub pomlajeni posadki, smo mentorji pripravili in izpeljali še eno izvedbo tabora, na katero smo lahko ponosni. Zahvalil bi se rad vsakemu posebej, ker prav vsak predstavlja pomemben in nepogrešljiv del organizacije našega tabora. Vseeno pa tako obsežnega in kvalitetnega tabora ne bi mogli izvesti sami. Tudi v tem letu ste predavatelji in podporniki pokazali neverjetno pripravljenost za sodelovanje. Zahvaljujem se vam za vse.

Glavni del tabora ste seveda udeleženci. Tabor je pripravljen z vami v mislih in vsako leto ga neverjetnega naredi vaša radovednost, navdušenost in želja po spoznavanju novega. Tudi letos ni bilo nič drugače. Upam, da ste v tednu na Pohorju, ki smo ga preživeli skupaj, uživali, navezali nova prijateljstva in spoznali veliko novega. Vsem udeležencem, ki ste letos zaključili s srednješolskim šolanjem, želim, da ohranite MaRSovsko energijo tudi pri prihodnjih podvigih. Za vse ostale pa upam, da tudi naslednje poletje skupaj poletimo na MaRS.

Lep MaaaaRSovski pozdrav, Nejc!

Word of the president of the committee

Dear participants, crew members, respected lecturers, supporters, and other readers. This year's flight to MaRS has been completed successfully. Despite the rejuvenated crew, the mentors prepared and carried out another implementation of the camp that we can be proud of. I would like to thank each and every one of them because each represents an important and indispensable part of the organization of our camp. However, we could not have carried out such an extensive and high-quality camp alone. As in previous years, the lecturers and supporters have shown an incredible willingness to participate. Thank you for everything.

The main part of the camp are of course the participants. The camp is prepared with you in mind and every year it is your curiosity, enthusiasm, and desire to learn new things that make it amazing. This year was no different. I hope you enjoyed the week we spent together on Pohorje, made new friends, and learned a lot of new things. To all the participants who graduated from high school this year, I wish you to keep your Martian energy in your future endeavors. For the rest of the participants, I hope that we will fly to MaRS again next summer.

Greetings from MaaaaRS, Nejc!

Dnevnik

Jan Genc 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, 14. julij 2024

Sem mislil, da naj bi to bil nek cvet inteligence, je bliskovito kot današnji heroj Mikel Oyarzabal eden izmed udeležencev razblinih ves napuh marsovske posadke, ki smo ga pridno akumulirali čez leto, medtem ko smo mu demonstrirali svojo jubilejno nemoč ob inštalaciji LaTeX-a.

Kot Čehoslovaki v natikačih smo tudi letošnji Marsovci zarinili navkreber – na Pohorje. Nadobudni mladi matematiki so se zasidrali v CŠOD Planinka, kjer so v skladu z lokalnim okoljem izrazili svoje preference glede ležišča na pogradu (zgornje hoče).

V uvodnem programu smo člani posadke svojo generacijsko travmo MaRSovskega pozdrava uspešno prenesli na novopečene pozdravkarje. Lansko hako so v epidemiološkem slogu nasledili mehiški valovi, izpod peresa Jana in vanilijeve kokakole.

Preidimo k srčiki. Basmatinsko pravljico v obliki kepice riža je pospremila basen, ki nam je dala povod za estimiranje števila dekliških las v krožniku žarke goveje juhe. Miselni proces smo zmagovito oplemenili na pooobednem Jane Streetovem Estimathonu.

Ponedeljek, 15. julij 2024

V rosnih enoštevčnih urah nas je prebaletilo plahutanje Pohorskih veščic. Čeprav jim nismo opdustili dolga prikrajšanih ur v Dolnjih Ležečah, smo bili vendarle postreženi s vsakdanjim kruhom, običajnim maseljcem in tradicionalnim medom.

Navsezgodaj smo na šolskem igrišču razgibali svoje ude in ume. *Narobe sem se usedel* je domnevno izjavil eden izmed udeležencev igre dan in noč, ki se je naglo razplamtela v turnir med dvema ognjema, kjer smo pokazali svoje ostrostrelske sposobnosti tudi na igrišču večje razsežnosti.

Dopoldanski svit smo popestrili z uvodom v svoje projekte. Pod taktirko odgovornoodraslih mentorjev smo spoznavali bralcem dobro znane koncepte, kot so drevo, gozd, list in centralni limitni izrek ter periodična raba stikala za luč. Svetovljanske Marsovce smo iniciirali v mLaTeŠki viteški red z madagaskarja.

Tako kot Koreja je tudi pri našem dnevu ta boljši del južna. Tokrat nam je metabolizem vzburil lakonski kos Kalimera in ljubiteljem palindromov na kožo pisan kuskus ter vegetacija. Njam njam. Siceršnjo manjko telečje pečenke smo Cajnkarjevsko nadomestili z basnijo o Kvadratomirju in Bogomolki (*Narveč sveta otrokam sliši Salle*) ter detektivsko povestjo o Smrketi z USB-ja.

Za sklepni dogodek dneva smo bili pogoščeni gurmansko obaro z sinjim hlebčkom, ki ajdovski se žganec imenuje.

Bralcu želimo prijeten avalonski večer.

Torek, 16. julij 2024

S počasnim uvajanjev v MaRSovski (ne)spalni cikel smo začeli nov dan. Na praktičnem primeru smo rešili problem petih uživačev ščetkanja zob in enega umivalnika. Današnji zajtrk najbolje opiše spodnja enačba.

kruh s pašteto

Sledeč verižnemu pravilu nam je nizozemski animator serviral še en répete dveh ognjev. Maratonsko sesijo projektov smo zalili še s tradicionalnim zasedanjem ljubiteljev pitonov. Novi užavači so spoznavali, kako se jih prime za vrat, stari mački pa so se z Ninozemcem po žentlmensko posvetili svojim kraljicam 🙏🙏.

Tradicionalno torkovo govejo juhco smo pospremili z razpadajočimi kruhovimi cmoki, ob katerih smo se še bolj zbližali. Za vrhunec košnje pa je poskrbela gospa kuharica z vrečo sladolednih lučk, za kar je tudi prejela stoječo ovacijo.

V popoldanskih urah se nam je pridružil MaRSovksi veteran in letošnji delavničar Nino Bašić. S šnelkursom linearne algebre smo se v natrpani predavalnici potopili v spektralno teorijo grafov. Obdani z benzinskimi

hlapi požigalca Nina, ki se je po svojih besedah tega dne *zašvical ful* smo zkozi odisejado razpoloženjskih medmetov epifanično spoznali, da živimo v Z_8 in ne na Pohorju.

Seveda pa dobra seansa linearne algebra ne more preseči centralnega limitnega dogodka dneva – še zadnjega pogona gastrointestinalnega trakta. Pasjo vročino smo zabetonirali z vročimi psi in aranžmajem kebabarske zelenjave in omakic (brez pekoče).

Gostujoči predavatelj Jernej Činč je postavil dinamične sisteme iz teorije v prakso in otvoril cikel letošnjih večernih predavanj. Omenimo, da je pretežno štajerski MaRSovski posadki še posebej sedla razprava o mehaniki fluidov.

Bralca še za na konec kulturno obogatimo s citatom znanega algebraičnega topologa V. Coceta:

Prije jutra umoran, MaRSovec čeka novi dan.
Dok svi ljudi spavaju, medvedi se karaju.

Sreda, 17. julij 2024

Po pričakovanem parabolično-padajočem spanju na MaRS-u smo se s kupom budilk prebudili v novo jutro. V jedilnici so nas pričakale sladoledne kepice bele nutelle in čokolino generaciji primerno živilo. Po več porcijah nepričakovane poslastice smo se brž odpravili na pohod do Pohorske vzpenjače. Med potjo so nas dežurni za*ebanti navdušili z novim arsenalom zagonetk, ki jih bomo razkrili v jutrišnjem dnevniškem vnosu.

V domu nas je pričakalo tisto boljše od napredka in svobode, kar smo ob logistični podpori dežurnih dežurnih z brzim repetiranje neugnano pospravili v svoja astrotenalne trakte. Tako smo dobili dovolj energije, da se znova potopimo v svet linearne algebre z gospodom Bašićem, ki smo ga pomotoma iztirili z alkoholnim pršilom obrisano tablo. Vendar tudi napojeni s hlapi aromatičnih obročev, seveda ne smemo našteti $\sqrt{2}$ dvakrat, namesto da napišemo $(\sqrt{2})^2$, majkemi.

Kljub konkretnemu potopu, smo morali začeti pisati članke o izreku CLiT, pa tudi o tem, kako se lahko naravna porazdelitev na določenih območjih dvigne zelo visoko.

Na koncu smo še marsovsko pozdravili nocojšnjega predavatelja iz FMF UL – Matija Pretnarja, ki nam je dijakom predstavil svet kvantnega računalništva. Predavanje bi bilo zagotovo tudi zanimivo našim fizikalnim kolegom z njihovega tabora FaRS-a. Bolj življensko, spoznali smo tudi vodotesen način osvajanja deklet – ponudiš ji svoje filtre in začneš razlagati o super pozicijah.

Danes pa ni pesmice :(
(bo jutri, oblubmo)

Četrtek, 18. julij 2024

Po predolgo prebedeni noči predolgega Salema, risanja cikla v morilcu in igre Codenames, je končno napočilo novo jutro s še večjim negativnim odvodom spalne krivulje. Dokončno nas je prebudila telovadba – tokrat kar s smrtonosno igro iz serije Squid game s kančkom neuravnoteženega med dvema ognjema. Seveda ne smemo pozabiti na običajen zajtrk, vendar ta je bil toliko običajen, da je bolje iti naprej.

Gospod Bašić nas je tokrat še zadnjič razvedril s Kiklovo teorijo, da bomo dobro pripravljeni na prihod našega starega MaRSovskega znanca. Po tridnevnem naporu je prejel tudi svojo najpomembnejšo MaRSovsko nagrado – čokoladico in majico. S strahom pred morilci smo se odpravili na delo projektov, kjer smo dokonca obdelali centralni limitni izrek, dokončno dočakali neskončne vrste in dokončali preštevanje neskončnih množic.

Izak je poskrbel za demonstriranje pogostih napak na predstavitvah projektov, za kosilo pa nam je kuharica med drugim pripravila izvrstne sladice. Kasneje smo mešano rešili družinske spore s projekti, vmes smo dobivali za prvo vedno več budgeta.

Za večerjo se sicer več ne spomnim, kaj je bilo, vendar verjamem, da je doseglo neko pričakovano vrednost in centralno limito, verjetno tudi morda kak nižji percentil, a ne spet preveč, saj se ne spomnim. Na koncu

nas je s spalnimi maskami pospremila v svet zavarovalnic gospa Čič iz Zavarovalne skupine Sava, ki nam je podelila nagrade tudi za naše ime, za naše korake, nas pa je naučila tudi kako se zavarovati. Večer je končala še bolj ekstremna različica morilca, pa tudi vse standardne igre preteklih dni, za jutri pa nestrpno pričakujemo MaRSovsko pustolovščino in MaRSovski piknik, kljub višku kalorij, ki smo ga verjetno zaužili zaradi vrhunskih tortic, ki nam jih je pripravila gospa kuharica, se razume.

Petek, 18. julij 2024

Konec veselice
Izjava udeleženca jutranje telovadbe, nekaj trenutkov po tem, ko je bil izključen iz igre

Dali ji bomo, dali ji bomo, naši novici kar ji gre.
MaRSovski kvartet

Dan D svojega tabora smo začeli, kot smo že vajeni, z igro Med dvema ognjema. Športni navdušenci so pod rafalom odbojkarske žoge že četrtič ugotovili, da s Primožem pač ni dobro češenj zobati, kar smo gladko pozabili ob večerji šmorna in češnjevega kompota. Tedensko delo na projektih smo sklenili z uporabo žarkovnika in izdelave predstavitev. Svoje poznavanje retorike smo nato tudi preizkusili na generalki pred komisijo Zajca in Košute.

V popoldanskih urah smo po dvoletnem premoru ponovno zagnali MaRSovsko pustolovščino. Neustrašni dijaki so se podali na avanturo v neznana razpostranstva Pohorja in ob poti reševali zagonetke, ki jim jih je zastavila posadka. Pustolovščino so letos zmagali Teroristi grafov in si s tem prislužili večno čast in slavo ter pravico do lomljenja ta velike čokolade.

Na Pohorski plato so se začeli valiti nevihtni oblaki, z njimi pa tudi stari MaRSovski obrazi, ki so nam razjasnili vremena s kakšno anekdoto z olimpijad ali pa basnijo o vinjetah. Dežurne pikničanje je medtem opazno prizadela odsotnost požigalca Nina B., ko so se spopadali s prižiganjem žara (ali pa avtomobilskega motorja). Navkljub aprilskim vremenskim razmeram, že drugo leto zapored, nam je uspelo potešiti matematično lakoto s hodom vegetacije in mesnih specialitet po leskovačko.

V pikniškem času se je veličastno zaključila celotedenska igra marsovskega morilca. Z masakrom v jedilnici je Marseli (zahvala gre staršem, da so jo poimenovali po našem taboru) uspelo razbiti škofjeloško alianso in medicinsko oskrbeti ter hip zatem še medicinsko odskrbeti dežurnega roštiljarja. Krvoločne dogodke je z izvedbo istrske ljudske *Dajte, dajte* pospremil začasni MaRSovsi kvartet. Kljub očitkom o prednosti domačega terena se je Hočanka zapisala v zgodovino kot prva marsovska morilka. Čestitke!

Preostali dogodki najboljšega taborskega večera bodo širši javnosti ponovno ostali skrivnost. Kot pravi star slovenski pregovor – *če te ni, manjkaš :P* .

Sobota, 18. julij 2024

Tedensko uvajanje v vojaško disciplino je zadoščalo, da je željo po jutranjem dremežu preglasilo tveganje porcije sklec. Zmačkani od cedevite in spesani od čevapčičev smo napeli svoje mišice, zavihali rokave na svojih majicah MaRS 2024 in se podali v boj z zadnjim izzovom tabora – ~~predstavitvijo projektov~~ vstajanjem iz postelje.

Po uspešnih nekaj krogih igre – ne zaspati z glavo v čokolinu – sta igričarki K in K razglasili veliko zmagovalko morilca – mlado lice, nje, ki kriva moritve je velike. Medtem so v MaRSovsko bazo počasi začeli pritekati najbližji udeležencev, ki so se nam pridružili ob ciklu predstavitev. Letošnjo komično glasbeno spremljavo uvodne špice smo velikodušno pozdravili z oglušujočo tišino in se raje posvetili srčiki sklepnega dogodka – predstavitvam projektov. Dijaki so brez dlake na jeziku, brez cmoka v grlu in (povzemajoč besede N.B.) ne da bi se začvicali ful, predstavili svoje delo in sklenili tedensko matematično popotovanje.

S solzami v očeh, potovalkami v dlaneh, dežjem v laseh in cedevito v želodcu smo si še zadnjič segli v roke in odjahali vsak na svoj konec kokoške.

OSREDNJA DELAVNICA

Hücklova teorija

dr. Nino Bašić

Cilj osrednje delavnice je bil predstavitev Hücklove teorije. Najprej smo se seznanili z osnovami linearne algebre, vključno z matrikami, linearnimi preslikavami, determinantami in lastnimi vrednostmi matrik. Nato smo prikazali, kako je mogoče molekule v kemiji predstaviti z grafi. Vpeljali smo sosednostno matriko grafa in definirali spekter grafa kot množico lastnih vrednosti teh matrik. Z izračunom spektra lahko pridobimo pomembne informacije o molekuli, na primer energijo grafa, kar je koristno v razlagi strukture molekul v kemiji. Izračunali smo lastne vrednosti za nekatere enostavne družine grafov, kot so cikli in polni grafi. Eksperimentalne izračune smo izvedli v Pythonu, natančneje v okolju NumPy.

PREDAVANJA

Od fizikalnih procesov do matematike in nazaj

dr. Jernej Činč

Fakulteta za Naravoslovje in Matematiko, Univerza v Mariboru & ICTP Trst

1 Uvod in motivacija

Številne probleme, ki izhajajo iz fizike in tehnike, je mogoče rigorozno študirati s pomočjo teorije dinamičnih sistemov. Na primer, gibanje viskozne tekočine je modelirano s parcialnimi diferencialnimi enačbami (to so enačbe, ki povejo odvisnost med funkcijami in njihovimi odvodi po eni izmed spremenljivk), ki so bile podane v začetku 19. stoletja in so postale znane kot Navier-Stokesove enačbe.

C.-L. Navier G. G. Stokes

$$\frac{\partial u}{\partial x}+\frac{\partial v}{\partial y}+\frac{\partial w}{\partial z}=0$$

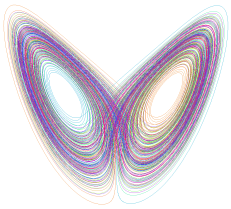
$$\rho\left[\frac{\partial u}{\partial t}+\frac{\partial u}{\partial x}u+\frac{\partial u}{\partial y}v+\frac{\partial u}{\partial z}w\right]=-\frac{\partial p}{\partial x}+\mu\left(\frac{\partial^2 u}{\partial x^2}+\frac{\partial^2 u}{\partial y^2}+\frac{\partial^2 u}{\partial z^2}\right)+\rho g_x$$

$$\rho\left[\frac{\partial v}{\partial t}+\frac{\partial v}{\partial x}u+\frac{\partial v}{\partial y}v+\frac{\partial v}{\partial z}w\right]=-\frac{\partial p}{\partial y}+\mu\left(\frac{\partial^2 v}{\partial x^2}+\frac{\partial^2 v}{\partial y^2}+\frac{\partial^2 v}{\partial z^2}\right)+\rho g_y$$

$$\rho\left[\frac{\partial w}{\partial t}+\frac{\partial w}{\partial x}u+\frac{\partial w}{\partial y}v+\frac{\partial w}{\partial z}w\right]=-\frac{\partial p}{\partial z}+\mu\left(\frac{\partial^2 w}{\partial x^2}+\frac{\partial^2 w}{\partial y^2}+\frac{\partial^2 w}{\partial z^2}\right)+\rho g_z$$

Slika 1: Navier-Stokesove diferencialne enačbe

Razumevanje njihovih rešitev je še vedno izven našega dosega in ostaja eden najzahtevnejših problemov v sodobni matematiki ter je med drugim uvrščen na seznam sedmih „Nagrad Tisočletja“ Matematičnega Inštituta Clay v Torontu, Kanadi (CMI) z raspisano nagrado miljon dolarjev. Parametrizirane družine čudnih atraktorjev so bile osrednjega pomena za dinamične sisteme od zgodnjih sedemdesetih let prejšnjega stoletja, nekaj let po tem, ko je ameriški matematik in meteorolog Edward N. Lorenz [14] preučeval model za toplotno konvekcijo s pomočjo okrnjenih Navier-Stokesovih enačb in predlagal njihov poenostavljen model z uporabo sistema treh diferencialnih enačb za podrobno matematično študijo. Rešitve teh enačb so postale znane kot Lorenzovi atraktorji. Pojem „učinek metulja“



Deterministic Nonperiodic Flow[1]

EDWARD N. LORENZ

Massachusetts Institute of Technology

(Manuscript received 18 November 1962, in revised form 7 January 1963)

ABSTRACT

Finite systems of deterministic ordinary nonlinear differential equations may be designed to represent forced dissipative hydrodynamic flow. Solutions of these equations can be identified with trajectories in phase space. For those systems with bounded solutions, it is found that nonperiodic solutions are ordinarily unstable with respect to small modifications, so that slightly differing initial states can evolve into considerably different states. Systems with bounded solutions are shown to possess bounded numerical solutions.

A simple system representing cellular convection is solved numerically. All of the solutions are found to be unstable, and almost all of them are nonperiodic.

The feasibility of very-long-range weather prediction is examined in the light of these results.

Slika 2: E. N. Lorenz in aproksimacija Lorenzovega atraktorja. Na skrajni desni je slikan izvleček članka od Lorenza, kjer je poudarjen odmevna prva opazka "učinka metulja".

je široko popularizíral idejo o občutljivi odvisnosti od začetnih pogojev, ki jih prikazujejo enačbe. Namreč, če začnemo z le nekoliko različnima začetnima pogojema, bomo končali z zelo različno obliko (t.j. topološko strukturo) teh atraktorjev.

Zgodba o matematični obravnavi parameteriziranih družin čudnih atraktorjev se začne z Lorenzovimi atraktorji, ki jih je v zgodnjih šestdesetih letih prejšnjega stoletja predlagal Lorenz [14] kot poenostavljen model „kaotičnega" atmosferskega gibanja.

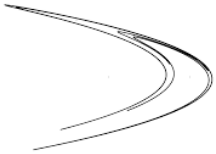
Od takrat je v matematični skupnosti prisotno izjemno zanimanje glede dinamičnih in topoloških lastnosti Lorenzovih atraktorjev. V iskanju nižjedimenzionalne različice preproste družine difeomorfizmov, ki dopušča „kaotično" vedenje, je francoski astronom in matematik Michele Hénon [9] uporabil računalniške simulacije, in našel ravninsko difenciabilno *Hénonovo funkcijo*

$$H_{a,b}(x,y) = (1 + y - ax^2, po),$$

ki kaže podobne „kaotične" pojave za $a = 1,4$ in $b = 0,3$, kot so jih opazili pri Lorenzovih atraktorjih. Benedicks in Carleson [2] sta dokazala, da za mnogo parametrov a in b preslikava $H_{a,b}$ premore *atraktorje* $\Lambda_{a,b}$ t.j.

$$\Lambda_{a,b} = \bigcap_{n\in\mathbb{N}} \overline{H^n_{a,b}(U)}.$$

Rečemo, da je $\Lambda_{a,b}$ družina *čudnih* atraktorjev, če za majhno spremembo parametrov (a, b) dobimo topološko različne (nehomeomorfne) atraktorje; po motivaciji zgoraj lahko temu pojavu rečemo tudi „topološka različica učinka metulja".



Slika 3: M. Hénon in aproksimacija atraktorja $\Lambda_{a,b}$ za parametre $a = 1.4$ in $b = 0.3$.

Matematiki so pozneje ugotovili, da so Hénonovi atraktorji daleč od enostavnih dinamičnih sistemov in da premorejo številne zanimive topološke in mersko-teoretične lastnosti. Zlasti topološka klasifikacija Hénonovih atraktorjev še vedno predstavlja enega osrednjih odprtih problemov v topoloških dinamičnih sistemih.

Da bomo bolje razumeli matematične pristope k študiji teh kompleksnih sistemov, moramo najprej razumeti naslednje pojme.

1.1 Metrični prostori

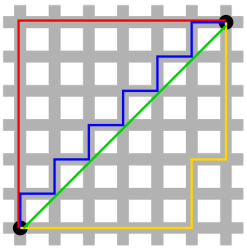
Metrične prostore uvedemo, ko želimo govoriti o razdalji med točkami v neki množici. Čeprav so matematiki uporabljali in vedeli za pojem razdalje že prej, ga je prvi formaliziral francoski matematik René Maurice Fréchet v začetku dvajsetega stoletja.

Definicija 1.1 (Fréchet 1906)**.** *Metrični prostor M je množica točk s pripadajočo funkcijo (*metriko ali razdaljo*) $d : M \times M \to \mathbb{R}$ tako, da za vse $x, y, z \in M$ veljajo naslednji pogoji:*

1. $d(x, y) \geq 0$ *(nenegativnost)*
2. $d(x, y) = 0$*, če in samo če* $x = y$ *(nerazdeljivost)*
3. $d(x, y) = d(y, x)$ *(simetričnost)*
4. $d(x, z) \leq d(x, y) + d(y, z)$ *(trikotniška neenakost).*

Primer 1.2 (Evklidska metrika)**.** $x = (x_1, x_2),\ y = (y_1, y_2) \in \mathbb{R}^2$, $d_E(x, y) := \sqrt{(x_1 - y_2)^2 + (x_2 - y_2)^2}$.

Primer 1.3 (Manhattan metrika)**.** $x = (x_1, x_2),\ y = (y_1, y_2) \in \mathbb{R}^2$, $d_M(x, y) := |x_1 - y_1| + |x_2 - y - 2|$.



Slika 4: Zelena pot ponazarja Evklidsko razdaljo med dvema črnima točkama, vse ostale poti pa Manhattan razdaljo.

Naloga 1.4. *Preveri, da sta d_E in d_M iz primerov zgoraj zares metriki na $\mathbb{R}^2$.*

1.2 Kratek uvod v teorijo diskretnih dinamičnih sistemov

Metrični prostor X je *zaprt*, če ima vsako zaporedje točk iz X limito prav tako v X.

Naloga 1.5. *Argumentiraj, da sta točka $x \in \mathbb{R}$ in zaprt interval $[0, 1] \subset \mathbb{R}$ zaprta prostora kot podprostora v $\mathbb{R}$. Argumentiraj tudi, da interval $[0, 1)$ ni zaprt prostor v $\mathbb{R}$.*

Metrični prostor X z metriko d je *omejen*, če obstaja realno število $r > 0$, tako da za vsaka $x, y \in X$ velja $d(x, y) < r$. To pomeni, da so vse točke v prostoru oddaljene med seboj za neko končno razdaljo.

Naloga 1.6. *Argumentiraj, da sta točka $x \in \mathbb{R}$ in zaprt interval $[0, 1] \subset \mathbb{R}$ omejena prostora kot podporstora v $\mathbb{R}$. Argumentiraj tudi, da interval $[0, \infty)$ ni omejen prostor v $\mathbb{R}$.*

Glavni objekti preučevanja v topoloških dinamičnih sistemih so funkcije $f \colon X \to X$ kjer je X *kompakten*[1] metrični prostor in f je zvezna surjekcija. Prvi pristop je študija *iteracij* od f, ki so definirane induktivno: $f^0 = \mathrm{id}_X$ in $f^{n+1} = f^n \circ f$. Torej,

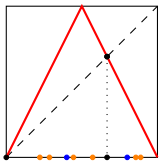
$$f^n = \underbrace{f \circ f \circ \ldots \circ f}_{n \text{ krat}}.$$

Osnovna tehnika študiranja $\{f^n\}_{n \in \mathbb{N}}$ je analiza *periodičnih točk*[2]. Označimo z $\mathrm{Per}(f, n)$ množico periodičnih točk periode n in $\mathrm{Per}(f) = \cup_{n \in \mathbb{N}} \mathrm{Per}(f, n)$. Označimo $I := [0, 1]$.

Primer 1.7. *Študirajmo funkcijo $T : I \to I$ definirano s predpisom $T(x) = \min_{x \in I}\{2x, 2 - 2x\}$. Dokažite, da je $\overline{\mathrm{Per}(T)} = I$.*

[1] Metrični prostor $X \subset \mathbb{R}^n$ je *kompakten*, če je zaprt in omejen.

[2] Točka $x \in X$ z *orbito* $\mathrm{orb}(x, f) := \{x, f(x), f^2(x), \ldots\}$ je *periodična s periodo n*, če je $f^n(x) = x$, $n \geq 1$ in je n najmanjše tako število.

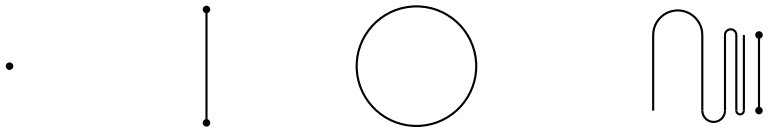


Slika 5: Funkcija T iz Primera 5. S črno piko so označene točke s periodo 1 (fiksne točke), z modro točke s periodo 2 in z oranžno točke s periodo 3. Množico funkcij za katere je $\overline{\mathrm{Per}(f)} = I$ označimo s $C_{DP}(I)$ in jih imenujemo *kaotične*. Take funkcije so bile popularizirane v odmevnem članku [13].

1.3 Kratek uvod v teorijo kontinuumov

Definicija 1.8. Kontinuum *je kompakten povezan metrični prostor.*

Kot je v teoriji dinamičnih sistemov osnovna tehnika študij periodičnih točk je v teoriji kontinuumov osnovna tehnika konstrukcija novih kontinuumov vgnezdenih presekov. Intuitivno, tehnika kot vhodni podatek vzame vgnezden neskončen nabor kontinuumov z neprazno notranjostjo in njihov presek je nato novi kontinuum kot izhodni podatek. Formalno je za to vedel že nemško-ruski matematik Georg Cantor konec devetnajstega stoletja.



Slika 6: Preprosti primeri kontinuumov (od leve proti desni): točka, zaprti interval, krožnica in $\sin(\frac{1}{x})$-kontinuum. Kot lep uvod v teorijo kontinuumov se zainteresiranemu bralcu priporoča knjiga od Nadlerja [16].

Izrek 1.9 (Cantor, 1880)**.** *Naj bo* $\{A_k\}_{k=1}^{\infty} \subset \mathbb{R}^n$ *množica kontinuumov, tako da velja* $A_1 \supset A_2 \supset A_3 \supset A_4 \supset \ldots$. *Potem je* $\Lambda = \bigcap_{k=1}^{\infty} A_k$ *neprazen kontinuum.*

Čeprav je tehnika intuitivno zelo enostavna, pa je njena uporaba toliko težja, saj je težko določiti, kaj bo dejansko izhodni kontinuum. Organiziran način razmišljanja predstavljajo inverzne limite.

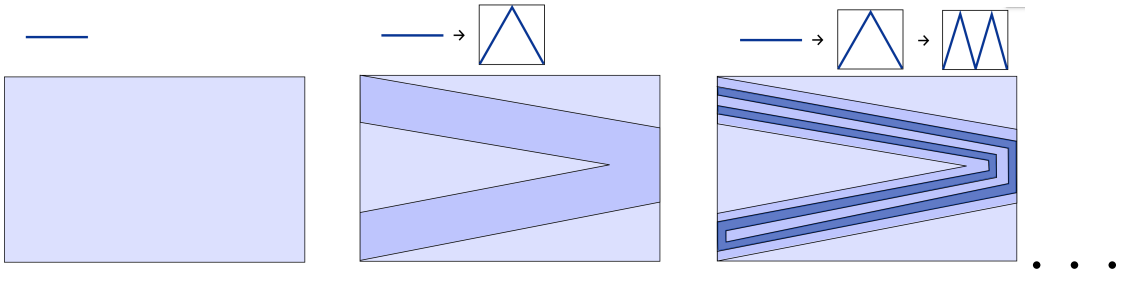
Naj bodo X_i kontinuumi in $f_i : X_{i+1} \to X_i$ zvezne surjekcije za vsak $i \geq 0$. *Inverzna limita* je definirana kot

$$\varprojlim(X_i, f_i) := \{(x_0, x_1, x_2, \ldots) \in X_0 \times X_1 \times \ldots ; f_i(x_{i+1}) = x_i\}.$$

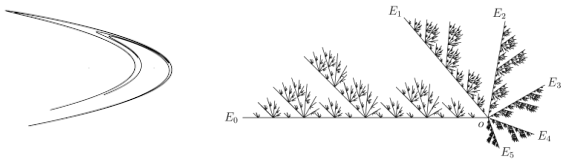
Čeprav definicija izgleda dokaj zahtevna, pa obstaja intuitivna razlaga, kako razmišljati o inverznih limitah kontinuumov, ki se dajo vložiti v ravnino $\mathbb{R}^2$. Podlaga za to je zgoraj naveden Cantorjev presečni izrek. Le-ta zagotavlja, da je vgnezdeni presek kontinuumov zopet kontinuum. Povezavo z inverznimi limitami pa predstavlja Anderson-Choquetov vložitveni izrek [1], ki ga bomo zaradi bolj jasne predstavite razložili le intuitivno.

Anderson-Choquetov vložitveni izrek reče, da imamo ravninsko predstavitev vgnezdenih presekov neke inverzne limite, če lahko za vsak $i \in \mathbb{N}$ narišemo graf funkcije $f_i : X_{i+1} \to X_i$ v ravnini poljubno blizu kontinuumu X_i, tako da je za vsako točko $x \in X_i$ točka $f_i(x)$ narisana v ravnini poljubno blizu točki x.

Primer 1.10. *Recimo, da je za vsak* i, $X_i = I$ *in funkcija* $f_i = T$ *kot v Primeru 5. Potem se lahko inverzna limita predstavi kot vgnezden presek podmnožic v ravnini na Sliki 7; prvi korak je, da se odebeli interval* $[0, 1]$, *v njega se nariše odebljen graf funkcije* T *in v njega odebeljen graf funkcije* T^2, *itd. Z uporabo Anderson-Choquetovega vložitvenega izreka se da dokazati, da je vgnezdeni presek teh diskov homeomorfen*[3] $\varprojlim(I, T)$.



Slika 7: Vizualna interpretacija Anderson-Choquetovega izreka za Primer 5.



Slika 8: Na levi aproksimacija $\Lambda_{a,b}$ za $a = 1.4$ in $b = 0.3$ in na desni dendrit (lokalno povezan kontinuum brez sklenjenih krivulj) z gosto množico razvejišč.

1.4 Hénonovi atraktorji in inverzne limite

Eden izmed najbolj pomembih nedavnih rezultatov na področju topoloških dinamičnih sistemov je naslednji izrek, ki reče, da se Hénonove atraktorje da predstaviti kot inverzno limito z eno vezno preslikavo, kar predstavlja prvi korak proti dokazovanju topološke klasifikacije teh atraktorjev.

Izrek 1.11 (Boroński, Štimac 2023)**.** *Za vsak parameter* $(a, b) \in \mathcal{BC}$ *obstaja* dendrit[4] z gosto množico razvejišč $D_{a,b}$ *in zvezna surjektivna preslikava* $f_{a,b} : D_{a,b} \to D_{a,b}$ *tako da je* $\Lambda_{a,b} \approx \varprojlim(D_{a,b}, f_{a,b})$.

Slika 9: J. Boroński in S. Štimac

1.5 Psevdo-lok

V teoriji kontinuumov raziskovalci dostikrat iščejo primere kontinuumov z zanimivimi in posebnimi lastnostmi. Kontinuum K je *razcepen*, če obstajata prava podkontinuuma $A \neq B \subset K$ tako da velja $A \cup B = K$. Kontinuum K je *nerazcepen*, če ni razcepen.

Naloga 1.12. *Argumentiraj, da je interval* $[0, 1]$ *razcepen kontinuum. Kaj pa točka; je točka razcepen ali nerazcepen kontinuum?*

[3] Funkcija $f : X \to Y$ je homeomorfizem, če je zvezna bijekcija in je tudi njen inverz zvezen.
[4] *Dendrit* je lokalno povezan kontinuum brez podkontinuumov, ki so homeomorfni krožnici.

Naloga 1.13. *Argumentirajte, da je vsak pravi podkontinuum od I homeomorfen I.*

Primer 1.14. *Kontinuum $\varprojlim(I, T)$ se v literaturi imenuje Knasterjev ali BJK (Brouwer-Janiszewski-Knasterjev) kontinuum. Prva konstrukcija je bila dana s strani Brouwerja* [7]*, ki ga je opisal kot prvi primer nerazcepnega kontinuuma.*

Kontinuum K je *dedno nerazcepen*, če je vsak njegov podkontinuum nerazcepen. Matematiki so se po opisu BJK kontinuuma začeli spraševati, če obstaja še bolj kompliciran kontinuum, ki ima vsak svoj podkontinuum nerazcepen: takim kontinuumom pravimo *dedno nerazcepni* kontinuumi. Da bi nek kontinuum bil dedno nerazcepen, ne sme, recimo, vsebovati nobenega *loka* (homeomorfne slike enotskega intervala).

Tukaj se začne zgodba psevdo-loka. Opišimo pot do njegovega odkritja in do formulacije imena.

Rečemo, da je Y pravi podkontinuum od X, če ni točka in ni celoten X. Rečemo, da je kontinuum nedegeneriran, če vsebuje več kot eno točko.

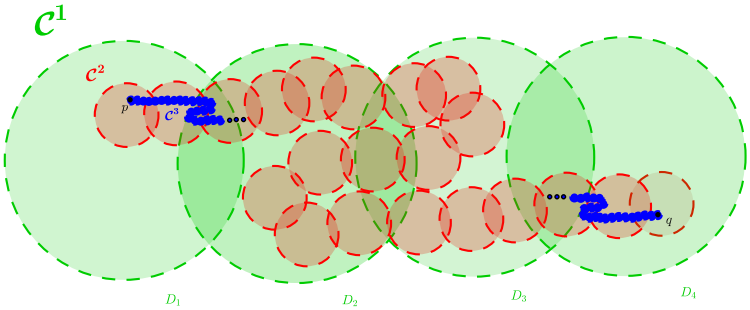
Knaster 1922 [12]*:* prvi primer nedegeneriranega dedno nerazcepnega kontinuuma.

Moise 1949 [15]*:* nov primer kontinuuma, ki je homeomorfen vsem svojim pravim podkontinuumom ("psevdo-lok").

Bing, 1948 [3]: nov primer homogenega kontinuuma.
Kontinuum K *homogen*: $\forall x, y \in K$ $\exists$ homeomorfizem $h : K \to K$ tako da $h(x) = y$.
Bing, 1951 [4]:
vsi trije primeri so homeomorfni med sabo (**zvitost!**).

Kljub temu, da ima psevdo-lok zanimive lastnosti, pa bi lahko kdo rekel, da nima smisla preučevati ta kontinuum, saj se zaradi svojih zelo specifičnih lastnosti psevdo-lok najverjetneje naravno ne pojavlja pogosto. Da ta intuicija ni pravilna je pokazal že ameriški matematik R. H. Bing leta 1951 [4], ko je dokazal, da so topološko tipični podkontinuumi v $\mathbb{R}^n$ za vsak $n \geq 2$ prav psevdo-loki.

1.6 Psevdo-lok in nedavne klasifikacije



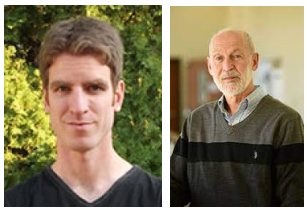
Slika 10: Psevdo-lok lahko konstruiramo kot zaprtje vgnezdenega zaporedja vse bolj zvitih verig kot na tej sliki.

Kmalu po konstrukciji psevdo-loka in dokazih njegovih posebnih lastnosti so se matematiki začeli spraševati, če obstajao še drugi kontinuumi s temi lastnostmi. Dolgo časa sta bila dva izmed največjih odprtih problemov v teoriji kontinuumov naslednja: karakterizacija ravninskih homogenih kontinuumov in karakterizacija ravninskih

kontinuumov, ki so homeomorfni vsem svojim nedegeniranim podkontinuumom. Nedavno sta kanadski matematik Logan C. Hoehn in nizozemski matematik Lex Oversteegen odgovorila na obe odprti vprašanji in tako potrdila, da je psevdo-lok zelo poseben ravninski kontinuum.

Izrek 1.15 (Hoehn, Oversteegen 2016 [10])**.** *Točka, krožnica, psevdo-lok in* krožnica psevdolokov[5] *so do homeomorfizma edini homogeni planarni kontinuumi.*

Izrek 1.16 (Hoehn, Oversteegen 2020 [11])**.** *Psevdo-lok je edini planarni kontinuum, ki je homeomorfen vsem svojim nedegerneriranim podkontinuumom.*

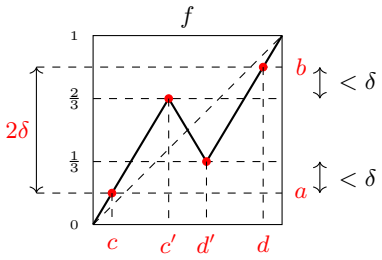


Slika 11: L. C. Hoehn in L. Oversteegen

1.7 Zvitost in psevdo-lok

V tem poglavju bomo podali še definicijo psevdo-loka preko inverznih limit na intervalu; ta temelji na posebnem pogoju (zvitosti) glede funkcijskih vrednosti funkcij na intervalu.

Definicija 1.17. *Naj bo $f : I \to I$, $a < b \in I$ in $\delta > 0$. Pravimo, da je funkcija f* δ-zvita med a in b*, če za vsaki dve točki $c, d \in I$, za kateri je $c < d$ in tako da je $f(c) = a$ in $f(d) = b$, obstajata točki $c < c' \leq d' < d$, tako da velja $|b - f(c')| \leq \delta$ in $|a - f(d')| \leq \delta$. Rečemo, da je f* δ-zvita*, če je δ-zvita med poljubnima paroma točk.*



Slika 12: 1/3-zvita funkcija na intervalu

Naloga 1.18. *Dokaži, da je funkcija f iz Slike 12 1/3-zvita, ni pa 1/4-zvita.*

Naloga 1.19. *Konstruiraj 1/4-zvito funkcijo $f : I \to I$, tako da je $f(0) = 0$ in $f(1) = 1$.*

Izrek 1.20 (Bing 1951 [4])**.** *Nedegeneriran kontinuum $\varprojlim(I, f)$ je psevdo-lok $\iff$ $f \colon I \to I$ je taka da $\forall \delta > 0$ $\exists n \geq 0$, tako da je f^n δ-zvita.*

[5] Za definicijo poglejte [5].

1.8 Od matematike nazaj k naravnim procesom?

Nedavno sva se z kolegom raziskovalcem vprašala kako pogosto se pojavlja psevdo-lok kot inverzna limita funkcij na intervalu in dokazala naslednji rezultat.

Izrek 1.21 (Č., Oprocha, 2022 [8])**.** *Za* tipične *funkcije* $f \in C_{DP}(I)$ *je* $\varprojlim(I, f)$ *psevdo-lok.*

Ugotovila sva tudi, da ima psevdo-lok velik potencial, da se pojavi kot atraktor naravnih procesov in pa tudi kot limitni proces določenih računalniških simulacij. Za več informacij naj zainteresiran bralec pogleda v članek [8].

Izrek 1.22 (Č., Oprocha, 2022 [8])**.** *Parametrizirane družine homeomorfizmov z atraktorji homeomorfnimi* psevdolokom *se lahko pojavijo kot* čudni atraktorji fizikalnih modelov *in kot atraktorji določenih računalniskih simulacij.*

Zgornja izreka (ki sta z več podrobnostmi navedena v [8]) sva dokazala z rigoroznimi mateňatičnimi metodami, kar pa še vedno manjka, je dejanska povezava s fiziko; to odpira možnost raziskav v prihodnosti.

Literatura

[1] R. D. Anderson, G. Choquet, G, *A plane continuum no two of whose nondegen- erate subcontinua are homeomorphic: an application of inverse limits.* Proc. Am. Math. Soc. **10**, 347–353 (1959).

[2] M. Benedicks, L. Carleson, *The dynamics of the Hénon Map*, Ann. of Math. **133**, No. 1, (1991), 73–169.

[3] R. H. Bing, *A homogeneous indecomposable plane continuum.* Duke Math. J. **15** (1948), 729–742.

[4] R. H. Bing, *Concerning hereditarily indecomposable continua,* Pacific J. Math. **1** (1951), 43–51.

[5] R. H. Bing, F. B. Jones, *Another homogeneous plane continuum* Trans. Amer. Math. Soc., **90** (1959), 171–192.

[6] J. P. Boroński, S. Štimac, *Densely branching trees and as models for Hénon-like and Lozi-like attractors*, Advances in Mathematics **429** (2023) 109191.

[7] L. E. J. Brouwer, *Zur Analysis Situs*, Mathematische Annalen, **68**: 422–434.

[8] J. Činč, P. Oprocha, *Parameterized family of pseudo-arc attractors: physical measures and prime end rotations*, Proceedings of the London Mathematical Society **125**(2) (2022), 318–357.

[9] M. Hénon, *A two-dimensional mapping with a strange attractor*, Communications in Mathematical Physics **50** (1976), 69–77.

[10] L. C. Hoehn, L. G. Oversteegen, *A complete classification of homogeneous plane continua.* Acta Math. **216** (2016), 177–216.

[11] L. C. Hoehn, L. G. Oversteegen, *A complete classification of hereditarily equivalent plane continua.* Adv. Math. **368** (2020), 8 pp.

[12] B. Knaster, *Un continu dont tout sous-continu est indecomposable,* Fund. Math. **3** (1922), 247–286.

[13] T. Y. Li, J. A. Yorke, *Period three implies chaos.* Amer. Math. Monthly **82** (1975), no. 10, 985–992.

[14] E. Lorenz, *Deterministic non-periodic flow*, J. Atmosph. Sci. **20** (1963), 130–141.

[15] E. E. Moise, *A note on the pseudo-arc.* Trans. Amer. Math. Soc. **67** (1949), 57–58.

[16] S. B. Nadler, Jr.,Continuum theory. An introduction. Monographs and Textbooks in Pure and Applied Mathematics, 158. Marcel Dekker, Inc., New York, 1992. xiv+328 pp.

Kvantni računalniki

dr. Matija Pretnar

Fakulteta za matematiko in fiziko, Univerza v Ljubljani

V medijih pogosto beremo, da so kvantni računalniki hitri, ker jim kvantna superpozicija omogoča, da so v več stanjih hkrati, s čimer lahko izračunajo vse možne rezultate v enem samem koraku. Kot smo videli, stvari niso tako preproste, saj se kvantni svet obnaša tudi tako, da na koncu lahko preberemo le enega od vseh rezultatov, pa še ta je naključno izbran. Da bi vseeno pripravili računalnik do tega, da izračuna rezultat, ki si ga želimo, moramo biti malo bolj zviti in uporabiti interferenco, s katero se neželeni rezultati med seboj izničijo. Na predavanju smo spoznali nenavadne vidike kvantnega sveta ter si ogledali Groverjev algoritem za iskanje igle v kopici sena (natančneje, zaporedja bitov, za katerega dana funkcija vrne 1).

Modeliranje življenjskih zavarovanj

mag. Andreja Čič

Zavarovalnica Sava

1 Uvod

Na kratko bomo predstavili življenjska zavarovanja in kako ustrezno predvideti prihodnje dogajanje, ki se lahko razteza čez več desetletij. Kateri so ključni dejavniki, ki vplivajo na prihodnje dogajanje in kako jih ustrezno zajeti v modelu? Osredotočili se bomo na biometrične predpostavke, ki temeljijo na spolu, starosti, lahko pa je upoštevan tudi življenjski slog, zdravstveno stanje in poklic. Poskušali bomo zgraditi poenostavljen model za napovedovanje prihodnjega dogajanja z uporabo verjetnosti.

2 Življenjska zavarovanja

Življenjska zavarovanja so namenjena zaščiti pred finančnimi posledicami dogodkov kot so smrt, nastanek bolezni, trajna ali začasna delovna nesposobnost in invalidnost. Nekatera življenjska zavarovanja kot je mešano zavarovanje in rentno zavarovanje so tudi oblika varčevanja z možnostjo pripisa dobička. Ob osnovnem zavarovanju so možna tudi dodatna zavarovanja kot na primer za nezgodno smrt, nezgodno invalidnost in drugo mnenje. Natančna opredelitev življenjskega zavarovanja je v splošnih in dodatnih pogojih zavarovanja. Delitev življenjskih zavarovanj na zavarovalne vrste je določena v Zakonu o zavarovalništvu.

2.1 Primer riziko življenjskega zavarovanja za kritje smrti

Zanima nas kaj so prihodki zavarovalnice, kaj so odhodki zavarovalnice in kaj vpliva na višino prihodkov in odhodkov. Prihodki so v grobem premije, odhodki pa izplačila škod in stroški.

Na prihodke in odhodke vpliva verjetnost smrtnosti, vendar je to le eden izmed dejavnikov. Pri tem je verjetnost smrtnosti odvisna od starosti, spola, poklica, zdravstvenega stanja in vpliva tako na prihodke torej premije in odhodke torej izplačila škod. V informativnem primeru je premija odvisna tudi od števila korakov, ki jih posameznik opravi na dan in se meri z aplikacijo. Dodatno na plačilo premije vplivajo prekinitve pogodb in plačilna disciplina. Stroški zavarovalnice so vezani na sklepanje polic, plačilo premije, izplačilo škod ter vodenje polic.

Na koncu pokažemo še projekcijo življenjskih zavarovanj, ker upoštevamo le smrtnost in vpliv število korakov na premijo. Ostale dejavnike zanemarimo, ker je pridobivanje predpostavk kompleksno, ni dostopno, hkrati pa se prepletajo različni dejavniki, ki so lahko odvisni. Zavarovalnice uporabljajo programska orodja za projekcije, kjer se modelira portfelj zavarovalnice in uporabijo primerne predpostavke, ki temeljijo na strokovni presoji.

Literatura

[1] Riziko življenjsko zavarovanje, Zavarovalnica Sava, 2023, `https://savang.savaregroup.si/media/store/sl-SI/slike/Mapa-Riziko-2023.pdf` [Dostopno 15. 8. 2024].

INFORMATIVNI PRIMER:

Blaž želi pri dopolnjenem 40. letu starosti skleniti Riziko življenjsko zavarovanje. Zaradi najema dolgoročnega kredita potrebuje zavarovanje z zavarovalno vsoto 100.000 EUR za obdobje 20 let. Na voljo ima **dve možnosti – konstantno ali padajočo zavarovalno vsoto**, ki sta prikazani v spodnji tabeli in grafu.

STAROST	40 let	
DOBA ZAVAROVANJA	20 let	
ZAVAROVALNA VSOTA	100.000 EUR	
VRSTA ZAVAROVALNE VSOTE	**Konstantna zavarovalna vsota**	**Padajoča zavarovalna vsota**
	Zavarovalna vsota, dogovojena ob sklenitvi, ostane enaka ves čas trajanja zavarovanja.	Zavarovalna vsota, dogovorjena ob sklenitvi, se v času trajanja zavarovanja po letih znižuje, tako da je v zadnjem zavarovalnem letu enaka 3.000 EUR.

Osnovna premija	20,92	8,81
Bonus kategorija C** (povprečno min. 4.500 korakov	18,10	7,78
Bonus kategorija B** (povprečno min 6.000 korakov)	17,15	7,44
Bonus kategorija A** (povprečno min. 9.000 korakov)	16,21	7,10

* Mesečne premije so v EUR in ne upoštevajo 8,5 % DPZP. Premije so informativne narave in za zavarovalnico niso zavezujoče. Premije upoštevajo, da zavarovanec ne opravlja tveganega poklica oz. se ne ukvarja s tvegano prostočasno dejavnostjo.

** Dosežena bonus kategorijea je osnova za obračunski popust na premijo na osnovi izmenjave podatkov o doseženem številu korakov v obdobju beleženja v skladu s Splošnimi pogoji Programa spodbud za zdrav življenjski slog SavaFit.

Slika 1: Informativni primer riziko življenjskega zavarovanja [1].

ČLANKI UDELEŽENCEV

Številske vrste

Katja Anzeljc, Aljaž Bratkovič Odar, Val Čokl
Mentorica*: Kaja Rajter*

Povzetek

V projektu so obravnavana številska zaporedja in vrste. Predstavljena sta pojma konvergence in divergence, računanje s številskimi vrstami ter ključni izreki, ki povedo, kdaj preureditev vrstnega reda členov vpliva na vsoto vrste.

1 Uvod

Pri klasičnem seštevanju števil lahko uporabimo komutativnost, torej možnost prerazporejanja členov, saj velja $a + b = b + a$. Zanima nas, ali komutativnost velja tudi za neskončne vsote. Pred nami je naloga, s katero bomo poskusili ugotoviti, kaj se dogaja.

Naloga 1.1. *Z upoštevanjem rezultata*

$$\sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} = \ln 2$$

poišči vsoto spodnje vrste, ki jo dobimo z zamenjavo vrstnega reda členov dane vrste na naslednji način

$$1 - \frac{1}{2} - \frac{1}{4} + \frac{1}{3} - \frac{1}{6} - \frac{1}{8} + \ldots + \frac{1}{2n-1} - \frac{1}{4n-2} - \frac{1}{4n} + \ldots$$

Vsoto prvih treh členov in naslednjih treh členov lahko zapišemo v obliki

$$1 - \frac{1}{2} - \frac{1}{4} = \frac{1}{2} - \frac{1}{4} = \frac{1}{2}\left(1 - \frac{1}{2}\right),$$

$$\frac{1}{3} - \frac{1}{6} - \frac{1}{8} = \frac{1}{6} - \frac{1}{8} = \frac{1}{2}\left(\frac{1}{3} - \frac{1}{4}\right).$$

Vsoto n-te trojice členov pa lahko izrazimo v obliki

$$\frac{1}{2n-1} - \frac{1}{4n-2} - \frac{1}{4n} = \frac{1}{4n-2} - \frac{1}{4n} = \frac{1}{2}\left(\frac{1}{2n-1} - \frac{1}{2n}\right).$$

Z upoštevanjem, da je vrednost vsote

$$\sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \ldots = \ln 2,$$

dobimo

$$1 - \frac{1}{2} - \frac{1}{4} + \frac{1}{3} - \frac{1}{6} - \frac{1}{8} + \ldots = \frac{1}{2}\left(1 - \frac{1}{2}\right) + \frac{1}{2}\left(\frac{1}{3} - \frac{1}{4}\right) + \ldots = \frac{1}{2}\ln 2.$$

Opazimo, da lahko z združevanjem različnih členov vrste pridemo do dveh različnih rezultatov. V članku bomo spoznali, zakaj se to zgodi.

2 Številska zaporedja

Preden se poglobimo v zanimivosti številskih vrst, spoznajmo nekaj osnovnih pojmov in lastnosti številskih zaporedij, ki so osnova za številske vrste.

Definicija 2.1. ***Zaporedje*** *je preslikava iz naravnih števil v realna števila. Označimo ga z* $(a_n)_n$.

Nekatera pomembna zaporedja so aritmetična zaporedja in geometrijska zaporedja. Posebej znano je tudi Fibonaccijevo zaporedje, ki ga definiramo kot

$$F_1 = 1,\ F_2 = 1,\ F_3 = F_1 + F_2 = 2,\ \ldots,\ F_{n+2} = F_n + F_{n+1},\ \ldots$$

Oglejmo si nekaj lastnosti, ki jih lahko ima zaporedje.

Definicija 2.2. *Zaporedje je* ***navzgor omejeno****, če obstaja takšen* $M \in \mathbb{R}$*, da velja* $a_n \leq M$ *za vsak* $n \in \mathbb{N}$*. Število* M *imenujemo* ***zgornja meja****. Najmanjšo zgornjo mejo navzgor omejenega zaporedja imenujemo* ***supremum****.*
Podobno definiramo pojme ***navzdol omejeno zaporedje****,* ***spodnja meja*** *in* ***infimum****.*
Zaporedje je ***omejeno****, če ima zgornjo in spodnjo mejo.*

Zaporedje $(a_n)_n$ vsebuje neskončno mnogo členov, zato nas pogosto zanima, kaj se dogaja s členi zaporedja za velike n.

Definicija 2.3. *Zaporedje* $(a_n)_n$ ***konvergira proti*** $a \in \mathbb{R}$*, če za vsak* $\varepsilon > 0$ *obstaja* $N \in \mathbb{N}$*, da za vsak* $n \geq N$*, velja* $|a_n - a| < \varepsilon$*. Število* a *se imenuje* ***limita zaporedja****. Zaporedje, ki ne konvergira proti nobenemu realnemu številu* a*,* ***divergira****.*
Limito zaporedja $(a_n)_n$ *označimo z* $\lim_{n\to\infty} a_n$.

Zaporedje s splošnim členom $a_n = \frac{1}{n}$ ima limito 0. Prav tako ima limito 0 geometrijsko zaporedje s splošnim členom $b_n = \frac{1}{2^n}$.

Definicija 2.4. *Zaporedje* ***konvergira proti neskončno****, če za vsak* $M \in \mathbb{R}$ *obstaja nek* $N \in \mathbb{N}$*, da za vsak* $n \geq N$ *velja* $a_n \geq M$.

Zaporedje naravnih števil konvergira proti neskončno.
Med lastnostmi, ki veljajo za konvergentna zaporedja, lahko dokažemo naslednjo trditev.

Trditev 2.1. *Vsako konvergentno zaporedje je omejeno.*

Dokaz. Naj bo $\varepsilon = 1$ in a limita zaporedja $(a_n)_n$. Po definiciji konvergence obstaja tak $N \in \mathbb{N}$, da za vse $n \geq N$ velja, da a_n leži na intervalu $(a-1, a+1)$. Potem je zgornja meja zaporedja enaka $\max\{a_1, \ldots, a_{N-1}, a+1\}$, spodnja meja pa je $\min\{a_1, \ldots a_{N-1}, a-1\}$. □

Omenimo še, kdaj je zaporedje naraščajoče in kdaj padajoče.

Definicija 2.5. *Zaporedje je* ***naraščajoče****, če velja* $a_{n+1} \geq a_n$ *za vsak* $n \in \mathbb{N}$*. Zaporedje je* ***strogo naraščajoče****, če velja* $a_{n+1} > a_n$ *za vsak* $n \in \mathbb{N}$.
Podobno definiramo ***padajoče*** *in* ***strogo padajoče*** *zaporedje.*

Zaporedje naravnih števil je strogo naraščajoče zaporedje. Konstantno zaporedje je naraščajoče in padajoče, ni pa niti strogo naraščajoče niti strogo padajoče.
Za naraščajoča in padajoča zaporedja velikokrat veljajo podobne lastnosti, zato uvedemo naslednje poimenovanje.

Definicija 2.6. *Zaporedje je* ***monotono****, če je naraščajoče ali padajoče. Zaporedje je* ***strogo monotono****, če je strogo naraščajoče ali strogo padajoče.*

Tako kot se v življenju srečujemo z resnicami, se v matematiki srečujemo z izreki. Pri dokazovaju konvergence nam velikokrat pomaga naslednji izrek.

Izrek 2.1. *Monotono zaporedje je konvergentno natanko tedaj, ko je omejeno.*

Dokaz. Če je monotono zaporedje konvergentno, je po trditvi 2.1 omejeno. Denimo, da je monotono zaporedje $(a_n)_n$ omejeno. Dovolj je obravnavati primer, ko je $(a_n)_n$ naraščajoče zaporedje. Ker je zaporedje $(a_n)_n$ omejeno, ima supremum, ki ga označimo s S. Izberemo poljuben $\varepsilon > 0$. Ker velja $S - \varepsilon < S$, število $S - \varepsilon$ ni natančna zgornja meja. Torej obstaja nek člen a_l, da velja $a_l > S - \varepsilon$. Ker je $(a_n)_n$ naraščajoče zaporedje, velja $a_{n+1} \geq a_n$ za vsak $n \in \mathbb{N}$. Ker je S zgornja meja, so vsi členi manjši od S, med drugim tudi členi od a_l naprej, ki zato ležijo na intervalu $(S - \varepsilon, S)$. Po definiciji 2.3 zaporedje konvergira proti S, saj za vsak $\varepsilon > 0$ obstaja tak N, da za vse n večje ali enake N člen a_n leži na intervalu $(S - \varepsilon, S + \varepsilon)$. □

Seveda pa moramo teorijo preizkusiti tudi v praksi, zato si oglejmo primer.

Naloga 2.1. *Ugotovi, ali je zaporedje s splošnim členom*

$$a_n = \frac{1}{n+1} + \frac{1}{n+2} + \ldots + \frac{1}{2n}$$

monotono. Ali je omejeno?

Na začetku si oglejmo prvih nekaj členov zaporedja

$$\begin{aligned} a_1 &= \frac{1}{2}, \\ a_2 &= \frac{1}{3} + \frac{1}{4} = \frac{7}{12}, \\ a_3 &= \frac{1}{4} + \frac{1}{5} + \frac{1}{6} = \frac{37}{60}. \end{aligned}$$

Poskusimo dokazati, da je zaporedje naraščajoče. To bo veljalo natanko tedaj, ko velja $a_{n+1} \geq a_n$ za vsak $n \in \mathbb{N}$. Vstavimo predpis za a_n in dobimo

$$\frac{1}{n+2} + \frac{1}{n+3} + \ldots + \frac{1}{2n} + \frac{1}{2n+1} + \frac{1}{2n+2} \geq \frac{1}{n+1} + \frac{1}{n+2} + \ldots + \frac{1}{2n},$$

kar je ekvivalentno

$$\frac{1}{2n+1} + \frac{1}{2n+2} \geq \frac{1}{n+1}.$$

Neenakost pomnožimo z izrazom $(n+1)(2n+2)(2n+1)$ in dobimo

$$(n+1)(2n+2) + (n+1)(2n+1) \geq (2n+1)(2n+2).$$

Zgornji izraz se poenostavi v

$$2 \geq 1,$$

zato je zaporedje naraščajoče.

Dokažimo še, da je zaporedje omejeno. Velja

$$a_n = \frac{1}{n+1} + \frac{1}{n+2} + \ldots + \frac{1}{2n} < \frac{1}{n+1} \cdot n < 1,$$

zato je zaporedje navzgor omejeno. Zaporedje je omejeno tudi navzdol, saj so po definiciji vsi členi pozitivni. Spodnja meja zaporedja je 0. Po izreku 2.1 vemo, da zaporedje konvergira.

S konvergentnimi zaporedji lahko tudi računamo. Naj bosta $(a_n)_n$, $(b_n)_n$ konvergentni zaporedji in naj bo $\lim_{n\to\infty} a_n = A$ ter $\lim_{n\to\infty} b_n = B$. Potem konvergirajo tudi zaporedja $(a_n \pm b_n)_n$ in $(a_n \cdot b_n)_n$. Limita zaporedja $(a_n \pm b_n)_n$ je $A \pm B$, limita zaporedja $(a_n \cdot b_n)_n$ pa je enaka $A \cdot B$. Če je $b_n \neq 0$ za vsak $n \in \mathbb{N}$ in $B \neq 0$, konvergira tudi $(a_n/b_n)_n$, limita tega zaporedja pa je enaka A/B.

3 Številske vrste

Definicija 3.1. *Naj bo $(a_n)_n$ zaporedje. Neskončna vrsta $a_1 + a_2 + \ldots + a_n + \ldots$ se imenuje* ***številska vrsta*** *zaporedja $(a_n)_n$, ki jo označimo z*

$$\sum_{n=1}^{\infty} a_n.$$

Člen a_n imenujemo ***n-ti splošni člen vrste****.*

Ker ne znamo določiti vsote neskončno mnogo števil, si lahko pri tem pomagamo z zaporedjem delnih vsot.

Definicija 3.2. *Dana je številska vrsta $\sum_{n=1}^{\infty} a_n$. Definirajmo zaporedje $(s_n)_n$ kot $s_1 = a_1$, $s_2 = a_1 + a_2$, $s_3 = a_1 + a_2 + a_3$, …, $s_n = a_1 + a_2 + \ldots + a_n$, …, ki ga imenujemo* ***zaporedje delnih vsot*** *vrste $\sum_{n=1}^{\infty} a_n$.*

Delne vsote lahko uporabimo pri določanju, ali vrsta konvergira ali divergira.

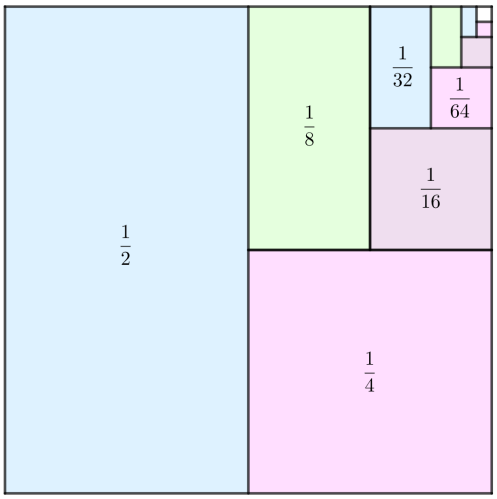
Definicija 3.3. *Če zaporedje delnih vsot številske vrste konvergira/divergira, potem rečemo, da* ***vrsta konvergira/divergira****. Limiti zaporedja delnih vsot pravimo* ***vsota vrste****.*

3.1 Geometrijska vrsta

Definicija 3.4. *Geometrijska vrsta je vrsta oblike $\sum_{n=0}^{\infty} aq^n$, kjer sta $a, q \in \mathbb{R}$.*

Če je $|q| < 1$, vrsta konvergira in ji lahko priredimo vsoto, ki je enaka $S = \frac{a}{1-q}$. V nasprotnem primeru vrsta divergira. Poglejmo si nekaj primerov geometrijskih vrst.

Če je $q = -\frac{1}{2}$, dobimo vrsto $1 - \frac{1}{2} + \frac{1}{4} - \frac{1}{8} + \frac{1}{16} - \frac{1}{32} + \ldots + (-1)^n \frac{1}{2^n} + \ldots$, ki ima vsoto $\frac{2}{3}$. Če za q izberemo 2, dobimo vrsto $1 + 2 + 4 + 8 + 16 + 32 + \ldots + n^2 + \ldots$, ki divergira.



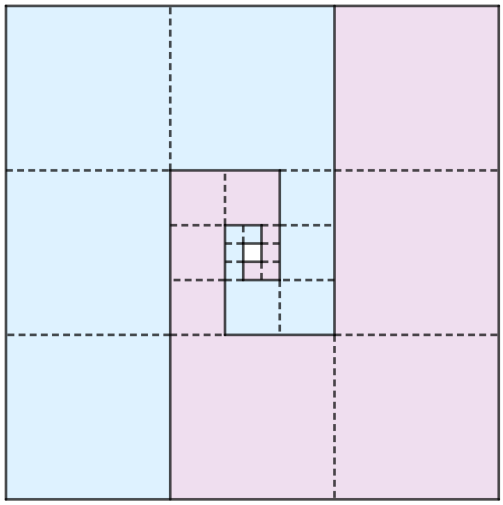
Slika 1: Grafična predstavitev geometrijske vrste za $q = \frac{1}{2}$.

Slika 1 prikazuje vrsto $\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \frac{1}{32} + \frac{1}{64} + \ldots + \frac{1}{2^n} + \ldots = 1$.
Slika 2 prikazuje vrsto $\frac{1}{3} + \frac{1}{9} + \frac{1}{27} + \frac{1}{81} + \ldots + \frac{1}{3^n} + \ldots = \frac{1}{2}$.

3.2 Vrste z nenegativnimi členi

Ker so vsi členi vrste nenegativni, je zaporedje delnih vsot naraščajoče. Iz izreka 2.1 sledi naslednja trditev.

Trditev 3.1. *Vrsta z nenegativnimi členi konvergira natanko tedaj, ko je zaporedje njenih delnih vsot navzgor omejeno.*



Slika 2: Grafična predstavitev geometrijske vrste za $q = \frac{1}{3}$.

Za lažje ugotavljanje konvergentnosti ali divergentnosti vrste lahko uporabimo primerjalni kriterij.

Izrek 3.1 (Primerjalni kriterij)**.** *Naj bosta* $\sum_{n=1}^{\infty} a_n$ *in* $\sum_{n=1}^{\infty} b_n$ *vrsti z nenegativimi členi, za kateri velja* $0 \leq a_n \leq b_n$ *za vse* $n \in \mathbb{N}$*.*

1. *Če* $\sum_{n=1}^{\infty} b_n$ *konvergira, potem tudi* $\sum_{n=1}^{\infty} a_n$ *konvergira.*
2. *Če* $\sum_{n=1}^{\infty} a_n$ *divergira, potem tudi* $\sum_{n=1}^{\infty} b_n$ *divergira.*

Dokaz. Definirajmo s_n kot n-to delno vsoto vrste $\sum_{n=1}^{\infty} a_n$ in t_n kot n-to delno vsoto vrste $\sum_{n=1}^{\infty} b_n$. Ker sta $\sum_{n=1}^{\infty} a_n$ in $\sum_{n=1}^{\infty} b_n$ vrsti z nenegativnimi členi, sta zaporedji $(t_n)_n$ in $(s_n)_n$ naraščajoči.

1. Vrsta $\sum_{n=1}^{\infty} b_n$ konvergira, zato konvergira tudi zaporedje $(t_n)_n$. Sledi, da je to zaporedje navzgor omejeno z mejo $M \in \mathbb{R}$. Iz pogoja vemo, da je $s_n \leq t_n$, zato ima tudi $(s_n)_n$ zgornjo mejo M. Sledi, da je $(s_n)_n$ navzgor omejeno zaporedje, torej je po izreku 2.1 konvergentno in vrsta $\sum_{n=1}^{\infty} a_n$ konvergira.
2. Ker vrsta $\sum_{n=1}^{\infty} a_n$ divergira, divergira tudi zaporedje $(s_n)_n$ in je zato navzgor neomejeno. Iz pogoja sledi, da je $s_n \leq t_n$, zato je tudi $(t_n)_n$ navzgor neomejeno, torej je po izreku 2.1 divergentno. Sledi, da vrsta $\sum_{n=1}^{\infty} b_n$ divergira.

□

3.3 Absolutna in pogojna konvergenca

Definicija 3.5. *Dana je vrsta* $\sum_{n=1}^{\infty} a_n$*. Če je* $\sum_{n=1}^{\infty} |a_n|$ *konvergentna, pravimo, da je vrsta* $\sum_{n=1}^{\infty} a_n$ ***absolutno konvergentna****.*

Primer absolutno konvergentne vrste je vrsta

$$\sum_{n=0}^{\infty} a_n = 1 - \frac{1}{2} + \frac{1}{4} - \frac{1}{8} + \frac{1}{16} - \frac{1}{32} + \ldots + (-1)^n \frac{1}{2^n} + \ldots$$

Definicija 3.6. *Dana je številska vrsta* $\sum_{n=1}^{\infty} a_n$*. Če je vrsta* $\sum_{n=1}^{\infty} a_n$ *konvergentna, ni pa absolutno konvergentna, je* ***pogojno konvergentna****.*

Vrsta

$$\sum_{n=1}^{\infty} a_n = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \frac{1}{5} - \frac{1}{6} + \ldots + (-1)^{n-1} \frac{1}{n} + \ldots$$

je pogojno konvergentna, saj konvergira proti $\ln 2$, vrsta

$$\sum_{n=1}^{\infty} |a_n| = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \ldots + \frac{1}{n} + \ldots$$

pa je t.i. harmonična vrsta, ki je znana divergentna vrsta.

Izrek 3.2 (Leibnitzov kriterij za alternirajoče vrste)**.** *Naj bo a_n padajoče zaporedje z limito 0. Potem vrsta $\sum_{n=1}^{\infty}(-1)^n a_n$ konvergira.*

Preverimo, ali je vrsta $1-\frac{1}{2}+\frac{1}{3}-\frac{1}{4}+\frac{1}{5}-\frac{1}{6}+\ldots+(-1)^{n-1}\frac{1}{n}+\ldots$ konvergentna. Ker je zaporedje $1, \frac{1}{2}, \frac{1}{3}, \ldots, \frac{1}{n}, \ldots$ padajoče in ima limito 0, je naša vrsta konvergentna.

4 Preureditve vrst

Definicija 4.1. *Naj bo $\sum_{n=1}^{\infty} a_n$ številska vrsta in naj bo $\pi\colon \mathbb{N} \to \mathbb{N}$ bijektivna funkcija. Vrsto $a_{\pi(1)} + a_{\pi(2)} + a_{\pi(3)} + \ldots + a_{\pi(n)} + \ldots$ imenujemo* ***preureditev vrste*** *$\sum_{n=1}^{\infty} a_n$.*

Zanima nas, koliko je vsota vrste, če vrstni red njenih členov med seboj premešamo.

Izrek 4.1. *Naj bo $\sum_{n=1}^{\infty} a_n$ absolutno konvergentna vrsta in $\pi\colon \mathbb{N} \to \mathbb{N}$ bijektivna preslikava. Potem vrsta $\sum_{n=1}^{\infty} a_{\pi(n)}$ konvergira in velja*

$$\sum_{n=1}^{\infty} a_{\pi(n)} = \sum_{n=1}^{\infty} a_n.$$

Če je vrsta absolutno konvergentna, s preureditvijo vrstnega reda členov torej ne vplivamo na vsoto vrste. To pa ne velja za pogojno konvergentne vrste.

Izrek 4.2. *Naj bo $\sum_{n=1}^{\infty} a_n$ pogojno konvergentna vrsta. Potem za vsak $A \in \mathbb{R}$ obstaja bijektivna preslikava $\pi\colon \mathbb{N} \to \mathbb{N}$, da je $\sum_{n=1}^{\infty} a_{\pi(n)} = A$. Še več, obstajata tudi bijektivni preslikavi $\pi_1, \pi_2\colon \mathbb{N} \to \mathbb{N}$, da je $\lim_{m\to\infty} \sum_{n=1}^{m} a_{\pi_1(n)} = \infty$ in $\lim_{m\to\infty} \sum_{n=1}^{m} a_{\pi_2(n)} = -\infty$.*

Dokaz. Predpostavimo lahko, da noben od členov v vrsti ni enak 0. Naj bo $(s_n)_n$ zaporedje delnih vsot vrste $\sum_{n=1}^{\infty} a_n$, torej

$$s_n = a_1 + a_2 + a_3 + \ldots + a_n.$$

Naj bodo p_1, p_2, …, p_k, … zaporedoma vsi členi zaporedja $(a_n)_n$, za katere velja $a_n > 0$, in naj bodo q_1, q_2, …, q_m, … zaporedoma nasprotne vrednosti vseh členov zaporedja $(a_n)_n$, za katere velja $a_n < 0$.

Naj $p_{k(n)}$ označuje n-to delno vsoto vrste $\sum_{i=1}^{\infty} p_i$, sestavljeno iz natanko tistih členov, ki so tudi med prvimi n členi vrste $\sum_{i=1}^{\infty} a_i$.

$$p_{k(n)} = p_1 + p_2 + p_3 + \ldots + p_k.$$

Podobno definiramo tudi $q_{m(n)}$.

$$q_{m(n)} = q_1 + q_2 + q_3 + \ldots + q_m.$$

Opazimo, da velja $k + m = n$, zato je

$$t_n = |a_1| + |a_2| + |a_3| + \ldots + |a_n| = p_{k(n)} + q_{m(n)}.$$

Označimo $\sum_{k=1}^{\infty} p_k$ z (1) in $\sum_{m=1}^{\infty} q_m$ z (2). Dokažimo, da obe vrsti divergirata. Ločimo dva primera.

Recimo, da (1) in (2) konvergirata. Sledi, da $(t_n)_n$ konvergira, ker je razlika konvergentnih zaporedij, kar vodi v protislovje, saj smo predpostavili, da vrsta $\sum_{k=1}^{\infty} a_n$ ni absolutno konvergentna.

Recimo, da (1) konvergira, (2) pa divergira. Velja

$$s_n = p_1 + p_2 + \ldots + p_k - q_1 - q_2 - \ldots - q_m = p_{k(n)} - q_{m(n)}.$$

Torej je $q_{m(n)} = p_{k(n)} - s_n$. Zaradi konvergence zaporedij $(p_{k(n)})_n$ in $(s_n)_n$ bi moralo konvergirati tudi zaporedje $(q_{m(n)})_n$. Pridemo do protislovja, ker smo predpostavili, da $(q_{m(n)})_n$ divergira. Če (1) divergira in (2) konvergira, se zgodi podobno.

Vrsta $\sum_{n=1}^{\infty} a_n$ konvergira, zato zaporedje $(a_n)_n$ konvergira proti 0. Sledi, da tudi podzaporedji $(p_n)_n$ in $(q_n)_n$ konvergirata proti 0.

Naj bo $A \in \mathbb{R}$. Poglejmo, kako moramo preoblikovati vrsto, da bo njena vsota enaka A. Ker je vrsta $\sum_{n=1}^{\infty} p_n$ divergentna, obstaja najmanjše tako število $k_1 \in \mathbb{N}$, da je

$$p_1 + p_2 + p_3 + \ldots + p_{k_1} > A.$$

Podobno obstaja najmanjše tako število $m_1 \in \mathbb{N}$, da je

$$p_1 + p_2 + p_3 + \ldots + p_{k_1} - q_1 - q_2 - q_3 - \ldots - q_{m_1} < A.$$

Nadaljujemo na isti način.

Ker je limita $\lim_{n\to\infty} p_{k(n)} = 0$ in $\lim_{n\to\infty} q_{m(n)} = 0$, ima vrsta po konstrukciji vrednost A.

□

5 Zaključek

Ob ponovni obravnavi vrste iz uvoda lahko sedaj rečemo, da je dana vrsta pogojno konvergirala, saj nam je uspelo s preureditvijo vrste dobiti dve različni vsoti. Ugotovili smo, da se pri preureditvi absolutno konvergentne vrste vsota ohrani, nasprotno pa lahko pogojno konvergentno vrsto preuredimo tako, da za vsoto dobimo poljubno realno število ali $\pm\infty$.

Literatura

[1] Zapiski predavanj predmeta Analiza I prof. dr. Barbare Drinovec Drnovšek (Univerza v Ljubljani, Fakulteta za matematiko in fiziko, študijsko leto 2023/2024).

[2] J. Globevnik, M. Brojan, *Analiza I*, 2012, dostopno na: `https://users.fmf.uni-lj.si/globevnik/skripta.pdf`

Neskončnost množic

Eva Bračun, Ema Franko, Timotej Potočnik
Mentorica: *Katarina Grilj*

Povzetek

V članku ponovimo osnovne pojme funkcij, s pomočjo katerih primerjamo moči neskončnih množic. Dokažemo, da zaradi Cantorjevega izreka o potenčnih množicah obstaja neskončno različnih neskončnosti. S pomočjo lastnosti slik množic dokažemo Cantor-Schröder-Bernsteinov izrek.

1 Uvod

Neskončnost je zanimiv a nenavaden koncept. Ljudje si jo predstavljajo na različne načine. Mnogi ob besedi neskončnost najprej pomislijo na vesolje, drugi na premice in ravnine, medtem ko nekaterim na misel pade neskončno sovraštvo do predmeta slovenščine. Mi pa se bomo osredotočili na primerjavo moči neskončnih množic in raziskovanje različnih neskončnosti.

2 Ponovitev osnovnih pojmov funkcij

Preden se poglobimo v neskončnost množic, se spomnimo osnovnih pojmov in lastnosti funkcij.

Definicija 2.1. *Naj bosta A in B množici. Funkcija $f\colon A \to B$ je:*

- ***injektivna**, če poljubna različna elementa iz A preslika v različna elementa iz B,*
- ***surjektivna**, če je vsak element iz B slika vsaj enega elementa iz A,*
- ***bijektivna**, če je injektivna in surjektivna.*

Če je funkcija $f\colon A \to B$ bijektivna, je vsak element $y \in B$ slika natanko enega elementa $x \in A$. Njena inverzna funkcija $f^{-1}\colon B \to A$ je potem definirana s predpisom $f^{-1}(y) = x$. Za inverzno funkcijo velja $f^{-1}(f(a)) = a$ za vsak $a \in A$ in $f(f^{-1}(b)) = b$ za vsak $b \in B$. Vemo, da je funkcija bijektivna natanko takrat, ko obstaja njena inverzna funkcija. Za dokaz bijektivnosti funkcije je torej dovolj dokazati obstoj inverzne funkcije.

Trditev 2.1. *Če je funkcija bijektivna, je njena inverzna funkcija prav tako bijektivna.*

Dokaz. Naj bo $f\colon A \to B$ bijektivna funkcija in $x,\ y \in B$. Predpostavimo, da velja $f^{-1}(x) = f^{-1}(y)$. Iz tega sledi $f(f^{-1}(x)) = f(f^{-1}(y))$. Ker je f^{-1} inverzna funkcija od f, velja $x = y$. S tem smo dokazali, da sta sliki dveh elementov enaki le, če sta elementa enaka. Funkcija f^{-1} je torej injektivna.

Dokažimo še surjektivnost. Izberimo poljubni element $a \in A$. Ker velja $f^{-1}(f(a)) = a$, je f^{-1} surjektivna, saj smo našli element iz množice B, ki se slika v element a. Ker je funkcija f^{-1} injektivna in surjektivna, je tudi bijektivna. □

Definirajmo še kompozitum funkcij in dokažimo nekaj njegovih osnovnih lastnosti.

Definicija 2.2. *Naj bodo A, B in C množice ter $f\colon A \to B$ in $g\colon B \to C$ funkciji.* ***Kompozitum funkcij** f in g je funkcija s predpisom*

$$x \mapsto g(f(x)),$$

ki slika iz množice A v množico C. Označimo jo z $g \circ f$.

Trditev 2.2. *Naj bosta $f\colon A \to B$ in $g\colon B \to C$ funkciji. Če sta f in g:*

- *injektivni, je tudi $g \circ f$ injektivna,*
- *surjektivni, je tudi $g \circ f$ surjektivna,*
- *bijektivni, je tudi $g \circ f$ bijektivna.*

Dokaz. Najprej predpostavimo, da sta f in g injektivni funkciji. Naj bosta $x,\ y \in A$ taka elementa, da velja $(g \circ f)(x) = (g \circ f)(y)$. Po definiciji kompozituma je to enako $g(f(x)) = g(f(y))$. Zaradi injektivnosti funkcije g velja $f(x) = f(y)$. Ker je tudi funkcija f injektivna, sledi $x = y$.

Nato predpostavimo, da sta f in g surjektivni funkciji. Izberemo poljuben $c \in C$. Zaradi surjektivnosti funkcije g vemo, da obstaja nek element $b \in B$, ki ga g slika v c, torej $g(b) = c$. Prav tako zaradi surjektivnosti f vemo, da obstaja nek element $a \in A$, za katerega velja $f(a) = b$. Posledično kompozitum $g \circ f$ preslika element a v c.

Kot zadnje predpostavimo, da sta f in g bijektivni funkciji. Ker za kompozitum $g \circ f$ velja, da je injektiven in surjektiven, je tudi bijektiven. □

3 Moč množic

Moč množice lahko definiramo kot število njenih elementov, vendar je s preštevanjem mogoče primerjati le množice s končnim številom elementov. S pomočjo spodnjih definicij pa bomo lahko primerjali še moči množic z neskončnim številom elementov. Najprej si poglejmo, kdaj imata množici enako moč.

Definicija 3.1. *Množici A in B imata **enako moč**, kadar obstaja bijektivna preslikava $f\colon A \to B$. Množici, ki imata enako moč, sta **ekvipolentni**, kar označimo z $|A| = |B|$.*

S pomočjo lastnosti inverzne funkcije in kompozituma, ki smo jih dokazali v prejšnjem razdelku, lahko dokažemo naslednje trditve.

- Če velja $|A| = |B|$, velja tudi $|B| = |A|$, saj je inverzna funkcija f^{-1} bijektivna.
- Če veljata enakosti $|A| = |B|$ in $|B| = |C|$, velja tudi $|A| = |C|$ zaradi bijektivnosti kompozituma $g \circ f$, ki slika iz množice A v C.
- Enakost $|A| = |A|$ velja, saj je funkcija, ki vsak element $x \in A$ preslika vase, bijektivna.

Definicija 3.2. *Moč množice A je **manjša ali enaka moči** množice B, če obstaja injektivna preslikava $f\colon A \to B$.*

*Moč množice A je **manjša** od moči množice B, če obstaja injektivna preslikava $f\colon A \to B$, ampak ne obstaja bijektivna preslikava iz množice A v množico B.*

4 Moči neskončnih množic

V tem poglavju želimo ugotoviti, ali so moči različnih neskončnih množic enake ali se razlikujejo.

Najprej primerjamo moč množice naravnih števil $\mathbb{N}$ z močjo množice naravnih števil, ki ji dodamo število 0. Tako množico označimo z $\mathbb{N}_0$.

Trditev 4.1. *Moč množice naravnih števil je enaka moči množice $\mathbb{N}_0$*

Dokaz. Definiramo funkcijo $f\colon \mathbb{N} \to \mathbb{N}_0$ s predpisom $f(n) = n - 1$. Da bi dokazali, da imata množici enako moč, je dovolj preveriti, da je ta funkcija bijektivna.

Najprej preverimo injektivnost. Izberemo poljubna elementa $n,\ m \in \mathbb{N}$, za katera velja $f(n) = f(m)$. Uporabimo predpis funkcije, da enačbo preoblikujemo v $n - 1 = m - 1$. Enačbo uredimo in dobimo $n = m$, torej je funkcija f injektivna.

Nato preverimo surjektivnost. Izberemo poljuben element $a \in \mathbb{N}_0$. Iščemo element iz $\mathbb{N}$, ki ga funkcija f preslika v a. Ugotovimo, da velja $f(a + 1) = a$. S tem smo dokazali surjektivnost. Ker je f injektivna in surjektivna, je bijektivna.

Poiščemo še inverz funkcije f. Na podlagi predpisa osnovne funkcije določimo, da je njen predpis $f^{-1}(n) = n + 1$. Preverimo lahko, da velja $f(f^{-1}(n)) = n$. □

Primerjamo še moč množice naravnih števil z močjo množice sodih naravnih števil. S tem smo množici $\mathbb{N}$ odstranili neskončno število elementov.

Trditev 4.2. *Množica sodih naravnih števil ima enako moč kot množica naravnih števil.*

Dokaz. Naj bo A množica sodih naravnih števil. Definiramo $f\colon \mathbb{N} \to A$ s predpisom $f(n) = 2n$. Da dokažemo bijektivnost funkcije f, moramo dokazati injektivnost in surjektivnost.

Injektivnost preverimo z izbiro poljubnih elementov $n,\ m \in \mathbb{N}$, za katera velja $f(n) = f(m)$. S pomočjo predpisa funkcije preoblikujemo enačbo v $2m = 2n$. Enačbo uredimo in dobimo $n = m$. S tem smo dokazali injektivnost funkcije f.

Surjektivnost funkcije f dokažemo tako, da izberemo poljuben element $x \in A$ in iščemo element iz $\mathbb{N}$, ki ga bo funkcija f preslikala v x. Iz predpisa sklepamo, da je $f(\frac{x}{2}) = x$. Ker je x sodo število, vemo, da je $\frac{x}{2}$ naravno število. Funkcija f je torej surjektivna. □

Primerjamo še moč množice $\mathbb{N}$ z množico celih števil $\mathbb{Z}$. S tem smo množici $\mathbb{N}$ dodali neskončno število elementov.

Trditev 4.3. *Moč množice naravnih števil je enaka moči množice celih števil.*

Dokaz. Naravna in cela števila razporedimo v vrsto na spodaj prikazan način.

1	2	3	4	5	6	7	...
0	1	-1	2	-2	3	-3	...

Na podlagi tega želimo definirati funkcijo $f\colon \mathbb{N} \to \mathbb{Z}$. Zapišemo ustrezni predpis.

$$f(n) = \begin{cases} \frac{n}{2}; & \text{če } n \text{ sod,} \\ -\frac{n-1}{2}; & \text{če } n \text{ lih.} \end{cases}$$

Injektivnost preverimo z izbiro poljubnih elementov $n,\ m \in \mathbb{N}$, za katera velja $f(n) = f(m)$. Dokaz moramo ločiti na tri primere.

1. Če sta n in m soda, zanju zaradi predpisa velja $\frac{n}{2} = \frac{m}{2}$. Enačbo uredimo in dobimo $n = m$.
2. Če sta n in m liha, zanju po predpisu velja $-\frac{n-1}{2} = -\frac{m-1}{2}$. Enačbo uredimo in dobimo $n = m$.
3. Če je n sod in m lih, velja $\frac{n}{2} = -\frac{m-1}{2}$. Ko enačbo uredimo, dobimo $n - 1 = -m$. Leva stran enačbe je večja ali enaka 0, desna pa je manjša od 0, zato pridemo do protislovja. Takšna elementa torej ne obstajata.

Ker mora vedno veljati $n = m$, je funkcija f injektivna.

Dokažimo še surjektivnost. Naj bo $x \in \mathbb{Z}$ poljuben element. Ločimo tri primere:

1. Če je $x = 0$, se element 1 slika v x.
2. Če je $x > 0$, velja $f(2x) = x$.
3. Če je $x < 0$, ugotovimo, da je $f(-2x + 1) = x$.

S tem, da smo poiskali ustrezne elemente, ki se slikajo v x, smo dokazali surjektivnost. Ker je funkcija f injektivna in surjektivna, je bijektivna. Množici $\mathbb{N}$ in $\mathbb{Z}$ imata torej enako moč. □

Definicija 4.1. *Množica je* ***štev no neskončna****, če ima enako moč kot množica naravnih števil.*

Ugotovili smo, da so množice $\mathbb{N}_0$, $\mathbb{Z}$ in množica vseh sodih naravnih števil štev no neskončne. Zdaj nas zanima, če obstajajo še kakšne druge neskončnosti.

5 Moč množice realnih števil

Dokazali bomo, da množica realnih števil ni številno neskončna in je večja od množice naravnih števil. To pomeni, da ne obstaja bijektivna preslikava med množico naravnih števil in množico realnih števil. Za to bomo uporabili Cantorjev diagonalni dokaz.

Izrek 5.1. *Množica naravnih števil* $\mathbb{N}$ *ima manjšo moč od množice realnih števil* $\mathbb{R}$.

Dokaz. Očitno je, da obstaja injektivna funkcija iz naravnih v realna števila. Že npr. $f_1(x) = x$ slika iz naravnih v realna števila (saj so naravna števila podmnožica realnih števil) in dveh različnih elementov ne slika v enak element. Sledi, da je $|\mathbb{N}| \leq |\mathbb{R}|$.

Če želimo dokazati, da velja $|\mathbb{N}| \neq |\mathbb{R}|$, moramo dokazati, da ne obstaja bijektivna funkcija iz naravnih v realna števila. Funkcija je bijektivna, če je injektivna in surjektivna hkrati, torej je dovolj, da dokažemo, da ne obstaja surjektivna funkcija.

Predpostavimo, da je $f\colon \mathbb{N} \to \mathbb{R}$ surjektivna. To pomeni, da bo za vsako realno število obstajalo neko naravno število, ki se bo slikalo vanj.

Da bi prišli do protislovja, je dovolj, da najdemo realno število x, ki ni v zalogi vrednosti funkcije f. Število x določimo po naslednji metodi. V številu $f(1)$ vzamemo prvo števko za decimalno vejico in jo primerjamo s številom tri. Če je drugačna od tri, naj bo $d_1 = 3$, če pa je enaka tri, naj bo $d_1 = 4$. Podobno za vsak $n \in \mathbb{N}$ v številu $f(n)$ pogledamo n-to števko za decimalno vejico in jo primerjamo s številom 3. Če je različna od tri, naj bo $d_n = 3$, če pa je enaka tri, naj bo $d_n = 4$. Definiramo število $x = 0.d_1d_2d_3....$ Za vsak $n \in \mathbb{N}$ nam torej d_n predstavlja n-to števko za decimalno vejico števila x.

Število x se od $f(1)$ razlikuje vsaj na prvem mestu za decimalno vejico, od $f(2)$ vsaj na drugem, od $f(3)$ vsaj na tretjem itd. Za vsak $n \in \mathbb{N}$ se torej x od $f(n)$ razlikuje vsaj na n-tem mestu za decimalko. Posledično ni enako nobenemu številu v zalogi vrednosti. Prišli smo do protislovja, funkcija f torej ni surjektivna, kar pomeni, da ni bijektivna. Ker ne obstaja bijektivna funkcija $f\colon \mathbb{N} \to \mathbb{R}$, množici $\mathbb{N}$ in $\mathbb{R}$ nimata enake moči. □

Za primer si vzamimo funkcijo, katere funkcijske vrednosti prvih 4 naravnih števil so zapisane spodaj.

$$\begin{aligned} f(1) &= 0.47302... \\ f(2) &= 5.13263... \\ f(3) &= 2.09273... \\ f(4) &= 1.75392... \\ &\dots \end{aligned}$$

Po naši metodi bomo tako dobili število x, ki se začne z

$$0.3433...$$

Omenimo še, da je bilo število tri, s katerim smo primerjali števke izbrano naključno, in bi lahko izbrali tudi kakšno drugo strategijo spreminjanja števk.

6 Cantorjev izrek

Za končno množico A z n členi je moč njene potenčne množice kar 2^n. Različne podmnožice namreč dobimo tako, da se za vsak element odločimo ali je v podmnožici ali pa ga ni. Za vsak element imamo torej dve možnosti. Tako je vseh podmnožic $2 \cdot 2 \cdot \ldots \cdot 2$ (n-krat število dvojk) oziroma 2^n. Za vsak $n \in \mathbb{N}$ vemo, da je $2^n > n$, torej za poljubno končno množico A velja $|\mathcal{P}(A)| > |A|$. Dokažimo še, da to velja tudi za neskončne množice.

Izrek 6.1 (Cantorjev izrek)**.** *Za poljubno množico* A *velja, da je moč njene potenčne množice večja od moči množice same*

$$|\mathcal{P}(A)| > |A|.$$

Dokaz. Dokaz je sestavljen iz dveh korakov. Najprej dokažemo, da je množica manjša ali enaka svoji potenčni množici, v drugem koraku pa dokažemo, da nista enako močni. Tako sledi, da je množica strogo manjša od svoje potenčne množice.

1. Najprej dokažimo, da je $|A| \leq |\mathcal{P}(A)|$. Pokazati moramo torej obstoj injektivne preslikave
$$f\colon A \to \mathcal{P}(A).$$
Tem pogojem zadostuje funkcija f, ki vsakemu elementu v množici A priredi podmnožico A, v kateri je samo ta element. Za vsak $x \in A$ namreč vemo, da je $\{x\} \in \mathcal{P}(A)$.
Preverimo, da je funkcija f injektivna. Naj bosta $x,\ y \in A$ taka elementa, da velja $f(x) = f(y)$. Iz predpisa funkcije f sledi $\{x\} = \{y\}$, torej je $x = y$. S tem smo dokazali
$$|A| \leq |\mathcal{P}(A)|.$$
2. Dokažimo še, da je $|A| \neq |\mathcal{P}(A)|$. Predpostavimo, da sta množici enako močni. To pomeni, da obstaja bijektivna preslikava $f\colon A \to \mathcal{P}(A)$. Naj bo S taka podmnožica množice A, ki vsebuje vse elemente x iz A, ki se slikajo v tako množico $f(x)$, da element sam ni v njej. Velja torej
$$S = \{x \in A \mid x \notin f(x)\}.$$
Vzamimo tak $a \in A$, da velja
$$f(a) = S.$$
   (a) Če je $a \in S$, potem po zgoraj dani definiciji $f(a) = S$ velja, da $a \in f(a)$. Element a se torej slika v podmnožico, ki a vsebuje. Po definiciji množice S in ker smo predpostavili, da $a \in S$, vemo, da a ni v $f(a)$. Pridemo torej do protislovja.
   (b) Obravnavamo še primer, ko $a \notin S$. Po definiciji S se a slika v podmnožico, ki tudi sama vsebuje a, velja torej $a \in f(a)$. Ker je $f(a) = S$, spet pridemo do protislovja.

   Pokazali smo torej, da ne more obstajati tak a, ki se slika v S. Ker je $S \in \mathcal{P}(A)$, je S tak element $\mathcal{P}(A)$, ki ni slika nobenega elementa iz A. Funkcija ni surjektivna, torej tudi ne bijektivna. Ker ne obstaja bijektivna preslikava med množicama, nista enako močni.

V dveh korakih smo torej dokazali, da je poljubna množica A strogo manjša od njene potenčne množice.

□

Velja torej, da ima potenčna množica vsake množice večjo moč kot množica sama
$$|\mathcal{P}(A)| > |A|.$$
Posledično obstaja neskončno različnih neskončnosti, saj lahko vedno vzamemo potenčno množico predpostavljeno največje množice in tako dobimo še večjo množico.

7 Slike množic

Ekvipolenco množic smo dokazovali z iskanjem bijektivnih preslikav med množicami. Ker pa je včasih lažje najti dve injektivni preslikavi, bomo dokazali Cantor-Schröder-Bernsteinov izrek. Najprej poglejmo, kaj je to slika množice in dokažimo lastnost slike množice injektivne funkcije, ki jo bomo uporabili pri dokazu izreka.

Definicija 7.1. *Naj bosta A in B množici, $f\colon A \to B$ funkcija ter $S \subseteq A$.* ***Slika podmnožice*** *S je množica $f_*(S) = \{f(x) \mid x \in S\}$.*

Trditev 7.1. *Naj bosta A in B množici, $f\colon A \to B$ injektivna funkcija ter X in Y poljubni podmnožici množice A. Potem je slika podmnožice X brez slike podmnožice Y enaka sliki podmnožice X brez Y. Velja torej*
$$f_*(X)\backslash f_*(Y) = f_*(X\backslash Y).$$

Dokaz. Enakost množic bomo dokazali v dveh korakih. Najprej bomo dokazali, da je poljuben element $z \in f_*(X)\backslash f_*(Y)$ tudi v množici $f_*(X\backslash Y)$, v drugem koraku pa še obratno.

1. Za poljuben element $z \in f_*(X)\backslash f_*(Y)$ vemo, da obstaja nek $a \in X$, za katerega velja $f(a) = z$. Ker $z \notin f_*(Y)$, vemo, da a ne more biti v množici Y. Sledi, da je $a \in X\backslash Y$, torej zares velja $z \in f_*(X\backslash Y)$.
2. Za poljuben element $z \in f_*(X\backslash Y)$ pa vemo, da obstaja nek a, ki je element X, da velja $z = f(a)$ in $a \notin Y$. Sledi, da je $z \in f_*(X)$. Zaradi injektivnosti mora a biti edini element, ki se slika v z, torej z ni v množici $f_*(Y)$. Sledi, da je $z \in f_*(X)\backslash f_*(Y)$.

□

8 Cantor-Schröder-Bernsteinov izrek

Lastnost slik podmnožic, ki smo jo spoznali v prejšnjem razdelku, najprej uporabimo, da dokažemo naslednjo lemo.

Lema 8.1. *Če sta A_1 in B_1 množici, za kateri velja $B_1 \subseteq A_1$ in $|A_1| \leq |B_1|$, je $|A_1| = |B_1|$.*

Dokaz. Naj bosta A_1 in B_1 množici, za kateri velja $B_1 \subseteq A_1$ in $|A_1| \leq |B_1|$. Zaradi $|A_1| \leq |B_1|$ vemo, da obstaja injektivna funkcija $f\colon A_1 \to B_1$. Naj bo $C_1 = A_1 \backslash B_1$.

Za vsak $n \in \mathbb{N}$, kjer je $n \geq 2$, definiramo:

$$A_n = f_*(A_{n-1}), \qquad B_n = f_*(B_{n-1}), \qquad C_n = A_n \backslash B_n.$$

Za vsak $n \in \mathbb{N}$ po definiciji velja $f_*(C_n) = f_*(A_n \backslash B_n)$. Ker je funkcija f injektivna, po trditvi 7.1 vemo:

$$f_*(A_n \backslash B_n) = f_*(A_n) \backslash f_*(B_n) = A_{n+1} \backslash B_{n+1} = C_{n+1}.$$

Zaradi injektivnosti funkcije f je torej slika množice C_n za vsak $n \in \mathbb{N}$ enaka množici C_{n+1}. Definiramo množico $C = \bigcup_{n\in\mathbb{N}} C_n$ in funkcijo $g\colon A_1 \to B_1$ s predpisom

$$g(x) = \begin{cases} f(x); & x \in C, \\ x; & x \notin C. \end{cases}$$

Zdaj želimo dokazati, da je funkcija g bijektivna. Najprej dokažimo, da je injektivna. Naj bosta x in y taka elementa iz množice A_1, da velja $g(x) = g(y)$.
Imamo 3 možnosti:

1. Najprej si pogledamo primer, ko sta $x,\ y \in C$, torej velja $f(x) = f(y)$. Ker je f injektivna funkcija, vemo, da je $x = y$.
2. Če velja $x,\ y \notin C$, potem zaradi predpisa funkcije g vemo $x = y$.
3. V primeru, da je $x \in C$ in $y \notin C$, vemo, da obstaja nek $n \in \mathbb{N}$, tako da je $x \in C_n$. Dokazali smo že, da potem velja $f(x) \in C_{n+1}$. Ker pa $y \notin C$ in $f(x) \in C$ ter hkrati zaradi predpisa funkcije g velja $f(x) = y$, smo prišli do protislovja.

S tem smo dokazali, da je funkcija g injektivna. Zdaj bomo dokazali še, da je surjektivna.
Naj bo z poljuben element v množici B_1. Ločimo 2 primera:

1. Če je $z \in C$, obstaja tak $n \in \mathbb{N}$, kjer je $n \geq 2$, da je $z \in C_n$. Dokazali smo že, da je $f_*(C_{n-1}) = C_n$. Iz predpisa funkcije g sklepamo, da velja $g_*(C_{n-1}) = C_n$. Obstaja torej tak $x \in C_{n-1}$, da je $g(x) = z$.
2. Če $z \notin C$, iz predpisa funkcije g sledi $g(z) = z$.

To nam pove, da je funkcija g surjektivna. Tako smo našli bijektivno funkcijo, s katero dokažemo lemo. □

Torej, če si izberemo množici A_1 in B_1 za kateri velja $B_1 \subseteq A_1$ in $|A_1| \leq |B_1|$, vemo, da za ti množici velja tudi $|A_1| = |B_1|$

Izrek 8.1 (Cantor-Schröder-Bernstein)**.** *Naj bosta A in B množici. Če obstajata injektivni preslikavi $f\colon A \to B$ in $g\colon B \to A$, potem obstaja bijektivna preslikava iz množice A v množico B*

V jeziku moči množic nam izrek torej pove, da če $|A| \leq |B|$ in $|B| \leq |A|$, potem je $|A| = |B|$.

Dokaz. Izberemo si injektivni funkciji $f\colon A \to B$ in $g\colon B \to A$.
Nato definiramo novo funkcijo $h\colon B \to g_*(B)$ s predpisom

$$h(x) = g(x).$$

Ker je funkcija g injektivna, je tudi funkcija h injektivna. Prav tako vemo, da je h surjektivna, saj slika v $g_*(B)$. Tako smo našli bijektivno funkcijo, ki slika iz B v $g_*(B)$, zato velja

$$|B| = |g_*(B)|.$$

Dovolj je torej dokazati

$$|g_*(B)| = |A|.$$

Pri tem želimo uporabiti lemo, zato preverimo ali množici zadostujeta pogojema iz leme.

1. Pogoj $g_*(B) \subseteq A$ je izpolnjen.
2. Preveriti moramo, če je pogoj $|A| \leq |g_*(B)|$ izpolnjen. Najprej si pogledamo kompozitum funkcij

$$h \circ f \colon A \to g_*(B).$$

Vemo, da je ta kompozitum injektiven, ker je kompozitum dveh injektivnih funkcij.

Če uporabimo lemo, vemo, da je $|A| = |g_*(B)|$.
Torej velja tudi

$$|A| = |g_*(B)| = |B|.$$

□

S pomočjo tega izreka primerjajmo še moč množice naravnih števil $\mathbb{N}$ z močjo množice pozitivnih racionalnih števil $\mathbb{Q}^+$.

Trditev 8.1. *Moč množice naravnih števil je enaka moči množice pozitivnih racionalnih števil.*

Dokaz. Najprej poiščemo injektivno funkcijo $f \colon \mathbb{N} \to \mathbb{Q}^+$. Temu ustreza kar funkcija s predpisom $f(n) = n$. Poiskati moramo še injektivno funkcijo $g \colon \mathbb{Q}^+ \to \mathbb{N}$. Vemo, da lahko vsak element iz $\mathbb{Q}^+$ na enoličen način zapišemo kot ulomek $\frac{m}{n}$, kjer sta $n,\ m \in \mathbb{N}$ tuji si števili. Definiramo funkcijo g s predpisom $g(\frac{m}{n}) = 2^m \cdot 3^n$.

Dokažimo, da je funkcija g injektivna. Naj bodo $a, b, c, d \in \mathbb{N}$ taka števila, da sta a in b tuji si števili ter c in d tuji si števili. Prav tako naj velja $g(\frac{a}{b}) = g(\frac{c}{d})$. Po predpisu funkcije enačbo preoblikujemo v $2^a \cdot 3^b = 2^c \cdot 3^d$. Ker sta števili na levi in desni strani enačbe enaki, morata imeti enak praštevilski razcep. Posledično velja $a = c$ in $b = d$, torej je $\frac{a}{b} = \frac{c}{d}$.

Ker smo našli injektivni funkciji $f \colon \mathbb{N} \to \mathbb{Q}^+$ in $g \colon \mathbb{Q}^+ \to \mathbb{N}$, po Cantor-Schröder-Bernsteinovem izreku vemo, da je $|\mathbb{N}| = |\mathbb{Q}^+|$.

□

9 Zaključek

Čeprav se nam ideja o različnih velikostih neskončnosti morda zdi nenavadna, saj si že neskončnost samo težko predstavljamo, smo se v članku ukvarjali s številnimi in neštevnimi neskončnostmi. Ugotovili smo, da obstaja več različnih neskončnosti, kar smo dokazovali z obstoji bijektivnih preslikav med množicami. Prav tako smo dokazali Cantorjev izrek in z njegovim diagonalnim dokazom ugotovili, da ima množica realnih števil večjo moč kot množica naravnih števil. Na koncu smo dokazali še Cantor–Schröder–Bernsteinov izrek, s pomočjo katerega lahko lažje dokazujemo obstoj bijektivnih preslikav med množicami.

Literatura

[1] A. Bauer, *Logika in množice*, 2022, dostopno na `https://www.andrej.com/zapiski/MAT-LMN-2022/lmn.pdf`

[2] Zapiski predavanj predmeta Logika in množice prof. dr. Alexa Simpsona (Univerza v Ljubljani, Fakulteta za matematiko in fiziko, študijsko leto 2023/2024)

Shorov algoritem

Aleksander Kalacun, Matjaž Meža, Jakob Žorž
Mentor*: Tim Milanez*

Povzetek

Spoznamo kvantni algoritem za faktorizacijo števil, imenovan Shorov algoritem, ki, vsaj v teoriji, po časovni zahtevnosti premaga še najhitrejši do sedaj znan klasični algoritem. V prvem delu razložimo klasični del algoritma, ki temelji na osnovah teorije števil, v drugem delu pa se spoprimemo še s kvantnim delom algoritma, kjer spoznamo temelje kvantne mehanike in kvantnega računanja, ki so zasnovani okoli linearne algebre.

1 Uvod

Šifriranje večine medmrežnih komunikacijskih poti danes deluje na podlagi RSA algoritma, ki omogoča varen in zaseben prenos informacij med različnimi uporabniki medmrežja. Algoritem sloni na dejstvu, da zmorejo računalniki hitro izračunati produkt dveh praštevil (šifriranje), medtem ko razcep tekšnega števila terja ogromno časa (dešifriranje), zato imamo RSA algoritem za varnega. Ob rodu kvantnega računalništva pa se je varnost te enkripcije postavila pod vprašaj, ko je leta 1995 ameriški matematik Peter Schor pretresel svet kriptografije in predstavil nov algoritem za faktorizacijo števil, zasnovan na konceptih kvantne mehanike. Z njim je, vsaj v teoriji, možno številu N, ki je produkt dveh praštevil, poiskati prafaktorje v

$$O((\log N)^2(\log\log N))$$

časa, kar je znatno hitrejše od najbolšega do sedaj znanega klasičnega algoritma, ki ima časovno zahtevnost [1]

$$O(e^{1.9(\log N)^{\frac{1}{3}}(\log\log N)^{\frac{2}{3}}}).$$

V delu predstavimo omenjeni Shorov algoritem, kjer sledimo [2].

2 Klasični del algoritma

Naj $\mathbb{Z}_n$ označuje množico števil $\{0, 1, 2, \ldots, n-1\}$, v kateri seštevamo in množimo po modulu n. Dva elementa a, b v tej množici sta enaka, kar pišemo kot $a \equiv b \bmod n$ in pravimo, da je a **kongruenten** b **po modulu** n, če velja $n|a-b$. To se zgodi natanko tedaj, ko imata števili isti ostanek pri deljenju z n.

Po Bezoutevi lemi ima element $x \in \mathbb{Z}_n$ multiplikativni inverz v $\mathbb{Z}_n$, tj. tak $y \in \mathbb{Z}_n$, da velja $xy \equiv 1 \bmod n$, natanko tedaj, ko je y tuj n. Podmnožico elementov, ki imajo multiplikativni inverz v $\mathbb{Z}_n$, označimo z $\mathbb{Z}_n^*$. Množica $\mathbb{Z}_n^*$ vsebuje natanko $\varphi(n)$ elementov, kjer φ označuje Eulerjevo totientsko funkcijo.

Želeli bi rešiti naslednji problem. Dano je število

$$N = pq,$$

za katerega vemo, da je produkt dveh praštevil p in q. Ob znani vrednosti N bi želeli hitro izračunati faktorja p in q. Če je N sod, potem je zagotovo eden od praštevilskih faktorjev enak 2, torej lahko predpostavimo, da je N lih. Če sta p in q enaka in je torej N kvadrat praštevila, se lahko hitro in z visoko natančnostjo izračuna koren od števila N in s tem p, torej lahko nadalje še predpostavimo, da sta p in q različna.

Vzemimo naključno število

$$1 < y < N.$$

Če imata N in y skupen faktor, smo končali, saj je $\gcd(N, y)$ v tem primeru enak enemu izmed faktorjev p, q in najmanjši skupni večkratnik dveh števil se s pomočjo Evklidovega algoritma da hitro izračunati. V nasprotnem primeru sta si N in y tuji in je $y \in \mathbb{Z}_N^*$, torej ima multiplikativni inverz v $\mathbb{Z}_N$. Ker je množica $\mathbb{Z}_N$ končna, se členi v zaporedju $1, y, y^2, \ldots$ elementov v $\mathbb{Z}_N$ ponavljajo, zato obstajata neki potenci $0 \leq l < k$, da velja

$$y^k \equiv y^l \bmod N \qquad \text{oziroma} \qquad y^{k-l} \equiv 1 \bmod N.$$

Naj bo $r \geq 1$ najmanjše takšno število, da velja

$$y^r \equiv 1 \bmod N.$$

Recimo, da smo imeli „srečo“ in da je r sodo število. Potem lahko razcepimo

$$y^r - 1 \equiv (y^{\frac{r}{2}} + 1)(y^{\frac{r}{2}} - 1) \equiv 0 \bmod N.$$

Po minimalnosti r število N ne deli $y^{\frac{r}{2}} - 1$, zato si $y^{\frac{r}{2}} + 1$ in N zagotovo nista tuja. Recimo, da smo imeli „izredno srečo“ in da poleg sodosti r tudi N ne deli $y^{\frac{r}{2}} + 1$. Potem velja

$$1 < \gcd(y^{\frac{r}{2}} + 1, N) < N,$$

torej je $\gcd(y^{\frac{r}{2}} + 1, N)$ enak enemu izmed prafaktorjev in smo končali.

Da zgornji algoritem uspe, smo potrebovali dve predpostavki: r je sod in $N \nmid y^{\frac{r}{2}} + 1$. Verjetnost, da naključno izbrano število y, ki je tuje N, zadošča tema predpostavkama, nam podaja naslednji izrek.

Izrek 2.1. *Recimo, da je N lih in da ima k praštevilskih faktorjev. Potem vsebuje množica*

$$\{y \in \mathbb{Z}_N^* \mid \textit{red } r \textit{ števila } y \textit{ je sod in } y^{r/2} + 1 \not\equiv 0 \bmod N\}$$

vsaj

$$\varphi(N)\left(1 - \frac{1}{2^{k-1}}\right)$$

elementov.

V našem primeru je $k = 2$, od koder sledi, da imamo „izredno srečo“ v vsaj polovici primerov. Edini časovno zahtevni korak v zgornjem algoritmu je izračun r, ki ga klasični računalnik ne more hitro izračunati. Tukaj pa nam pa na pomoč lahko priskočijo kvantni računalniki.

3 Uvod v linearno algebro

3.1 Vektorski prostori

V tem razdelku bomo razširili pojme vektorja, skalarja in baze, ki jih že poznamo iz srednje šole.

Definicija 3.1. ***Kompleksni vektorski prostor z bazo*** $e_1, \ldots, e_n$ *je množica*

$$V = \{\lambda_1 e_1 + \cdots + \lambda_n e_n \mid \lambda_1, \ldots, \lambda_n \in \mathbb{C}\},$$

ki je opremljena z operacijama

(1) seštevanja:

$$\begin{aligned}&(\lambda_1 e_1 + \cdots + \lambda_n e_n) + (\mu_1 e_1 + \cdots + \mu_n e_n)\\ &= (\lambda_1 + \mu_1)e_1 + \cdots + (\lambda_n + \mu_n)e_n \quad \textit{za } \lambda_1, \ldots, \lambda_n, \mu_1, \ldots, \mu_n \in \mathbb{C}, \textit{ in}\end{aligned}$$

(2) množenja s skalarjem:

$$\lambda \cdot \left(\sum_{i=1}^{n} \mu_i e_i\right) = \sum_{i=1}^{n} (\lambda \mu_i) e_i \quad \textit{za } \lambda, \mu_1, \ldots, \mu_n \in \mathbb{C}.$$

Številu n, tj. številu elementov v bazi, pravimo **dimenzija** *vektorskega prostora V.*

Kompleksni vektorski prostor z bazo $\{e_1, \ldots, e_n\}$ bomo označevali tudi kot $\mathbb{C}[\{e_1, \ldots, e_n\}]$.

Definicija 3.2. *Naj bosta V in W kompleksna vektorska prostora s končno bazo. Preslikava $L\colon V \to W$ je* ***linearna****, če velja*

(1) $L(x+y) = L(x) + L(y)$ za vsaka $x, y \in V$ in

(2) $L(\lambda x) = \lambda L(x)$ za vsak $x \in V$ in $\lambda \in \mathbb{C}$.

Enako se lahko definira tudi **realen vektorski prostor z bazo** in linearno preslikavo med realnima vektorskima prostoroma, kjer v definiciji zamenjamo vsako ponovitev množice $\mathbb{C}$ z množico $\mathbb{R}$.

Poljuben vektor $x \in V = \mathbb{C}[\{e_1, \ldots, e_n\}]$ lahko razpišemo po bazi

$$x = \sum_{i=1}^{n} \lambda_i e_i.$$

Linearna preslikava L slika x v

$$L(x) = L(\lambda_1 e_1) + \cdots + L(\lambda_n e_n) = \sum_{i=1}^{n} \lambda_i L(e_i).$$

Torej je L določena že s tem, kam slika bazne vektorje $e_1, \ldots, e_n$. Razpišimo $L(e_i)$ po bazi

$$L(e_i) = \sum_{j=1}^{n} a_{ij} e_j,$$

kjer so $a_{ij} \in \mathbb{C}$. Po prejšnjem razmisleku je L natanko določena z izbiro skalarjev $(a_{ij})_{i,j\in\{1,\ldots,n\}}$, ki jih zapišemo v tabelo, kot je prikazano spodaj

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}.$$

Takšnemu zapisu pravimo **matrika**. Po zgornjem postopku lahko vsaki linearni preslikavi priredimo matriko. Izkaže se, da je takšen zapis linearnih preslikav zelo priročen. Na primer, če želimo izračunati, kam linearna preslikava L slika nek vektor $x \in V$, moramo ta vektor najprej razviti po bazi $x = \sum_{i=1}^{n} \lambda_i e_i$, kar zapišemo kot

$$x = \begin{bmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{bmatrix},$$

nato pa poračunati vsote $\mu_i = \sum_{j=1}^{n} a_{ij}\lambda_j$ in jih zapisati v rezultat

$$L(x) = \begin{bmatrix} \mu_1 \\ \mu_2 \\ \vdots \\ \mu_n \end{bmatrix}.$$

Zgled 3.1. *Naj bo $L\colon \mathbb{R}^2 \to \mathbb{R}^2$ preslikava, ki zamenja koordinati*

$$L(x, y) = (y, x).$$

Po definiciji se da preveriti, da je L linearna preslikava med realnima vektorskima prostoroma $\mathbb{R}^2$ s standardno bazo $e_1 = (1, 0),\ e_2 = (0, 1)$. Pripadajoča matrika je

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

3.2 Vektorski prostori s skalarnim produktom

Standardni skalarni produkt vektorjev v prostoru $\mathbb{R}^3$, ki ga poznamo že iz srednje šole, je definiran kot

$$(x_1, x_2, x_3) \cdot (y_1, y_2, y_3) = x_1y_1 + x_2y_2 + x_3y_3.$$

Njegova uporabnost se je pokazala pri izračunu kotov med vektorji. Ta koncept bi radi definirali tudi na bolj splošnih vektorskih prostorih, kar naredimo na sledeči način.

Definicija 3.3. ***Skalarni produkt*** *na kompleksnem vektorskem prostoru V je preslikava*

$$\langle \cdot, \cdot \rangle \colon V \times V \to \mathbb{C},$$

ki zadošča naslednjim lastnostim.

(i) $\langle v_1 + v_2, w \rangle = \langle v_1, w \rangle + \langle v_2, w \rangle$ *za vsak* $v_1, v_2, w \in V$.

(ii) $\langle \lambda v, w \rangle = \lambda \langle v, w \rangle$ *za vsak* $v, w \in V$ *in* $\lambda \in \mathbb{C}$.

(iii) $\langle w, v \rangle = \overline{\langle v, w \rangle}$ *za vsak* $v, w \in V$.

(iv) $\langle v, v \rangle \geq 0$ *za vsak* $v \in V$ *in* $\langle v, v \rangle = 0$ *natanko tedaj, ko je* $v = 0$.

Število $\sqrt{\langle x, x \rangle}$ *bomo označevali z* $\|x\|$ *in mu pravili* **norma** *vektorja* x.

Iz zgornjih lastnosti sledi, da je skalarni produkt linearen v prvem faktorju in „poševno linearen“ v drugem faktorju, tj. velja

$$\langle v, \lambda_1 w_1 + \lambda_2 w_2 \rangle = \overline{\lambda_1} \langle v, w_1 \rangle + \overline{\lambda_1} \langle v, w_1 \rangle \text{ za vsak } v, w_1, w_2 \in V \text{ in } \lambda \in \mathbb{C}.$$

Zgled 3.2. *Na kompleksnem vektorskem prostoru $\mathbb{C}^n$ lahko skalarni produkt definiramo z naslednjo formulo*

$$\langle (z_1, \ldots, z_n), (w_1, \ldots, w_n) \rangle = z_1\overline{w_1} + \cdots + z_n\overline{w_n}.$$

Enostavno se da preveriti, da zgornji predpis res zadošča vsem lastnostim od (i) do (iv).

Kvantna mehanika dovoljuje le zelo specifične linearne preslikave, ki ohranjajo normo.

Definicija 3.4. *Linearna preslikava $U \colon V \to W$ med vektorskima prostoroma je* ***unitarna****, če velja*

$$\|Ux\| = \|x\| \text{ za vsak } x \in V.$$

Zgled 3.3. *Premislimo, kako izgledajo unitarne preslikave $U \colon \mathbb{R}^2 \to \mathbb{R}^2$ v realnem vektorskem prostorom $\mathbb{R}^2$ s standardno bazo $e_1 = (1, 0)$, $e_2 = (0, 1)$. Linearno preslikavo U lahko predstavimo z matriko*

$$U = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

Po unitarnosti imata vektorja e_1 in

$$Ue_1 = \begin{bmatrix} a \\ c \end{bmatrix}$$

enako normo, torej mora veljati

$$1 = a^2 + c^2.$$

Podobno imata tudi vektorja e_2 in Ue_2 enako normo, od koder sledi

$$1 = b^2 + d^2.$$

Potem obstajata takšni števili $\varphi \in [0, 2\pi)$ in $\theta \in [0, 2\pi)$, da velja $a = \cos\varphi$, $c = \sin\varphi$ in $b = \cos\theta$, $d = \sin\theta$. Enako normo pa morata imeti tudi vektorja

$$\begin{bmatrix} 1 \\ 1 \end{bmatrix} \quad in \quad \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix},$$

zato velja

$$2 = (a + b)^2 + (c + d)^2.$$

Desna stran zgornje enačbe pa je enaka $2 + 2(ab + cd)$*, zato dobimo*

$$ab + cd = 0,$$

oziroma

$$\cos(\varphi - \theta) = \cos\varphi\cos\theta + \sin\varphi\sin\theta = 0.$$

Torej je $\varphi - \theta \in \{\frac{\pi}{2}, \frac{3\pi}{2}\}$*. Če je* $\theta = \varphi - \frac{\pi}{2}$*, dobimo matriko*

$$U = \begin{bmatrix} \cos\varphi & \sin\varphi \\ \sin\varphi & -\cos\varphi \end{bmatrix}, \tag{1}$$

če pa je $\theta = \varphi - \frac{3\pi}{2}$*, dobimo matriko*

$$U = \begin{bmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{bmatrix}. \tag{2}$$

Pokazali smo torej, da so vse unitarne matrike ene izmed zgornjih dveh matrik. Matrike oblike 2 predstavljajo ravno rotacije okoli izhodišča za kot φ*.*

Definicija 3.5. *Naj bo* V *vektorski prostor s skalarnim produktom. Sistem vektorjev* $v_1, \ldots, v_n$ *je* ***ortonormiran****, če velja* $\langle v_i, v_j\rangle = 0$ *za vsak* $i \neq j$ *in* $\|v_i\| = 1$ *za vsak* i*.*

3.3 Tenzorski produkt

Naslednja definicija nam omogoča iz dveh vektorskih prostorov V dimenzije n in W dimenzije m konstruirati vektorski prostor dimenzije $n \cdot m$.

Definicija 3.6. ***Tenzorski produkt*** *vektorskih prostorov* V *z bazo* $e_1, \ldots, e_n$ *in* W *z bazo* $f_1, \ldots, f_m$ *je vektorski prostor* $V \otimes W$ *z bazo* $e_i \otimes f_j$*,* $i \in \{1, \ldots n\}$*,* $j \in \{1, \ldots m\}$*, da za vsaka* $v, v' \in V$ *in* $w, w' \in W$ *ter vse skalarje* λ *velja*

(i) $(v + v') \otimes w = v \otimes w + v' \otimes w$*,*

(ii) $v \otimes (w + w') = v \otimes w + v \otimes w'$*,*

(iii) $\lambda v \otimes w = (\lambda v) \otimes w = v \otimes (\lambda w)$*.*

Naj bosta $A\colon V_1 \to W_1$ in $B\colon V_2 \to W_2$ linearni preslikavi. Ti nam inducirata linearno preslikavo na tenzorskem produktu $A \otimes B\colon V_1 \otimes V_2 \to W_1 \otimes W_2$, ki je na baznih vektorjih definirana kot

$$(A \otimes B)(x \otimes y) = Ax \otimes By.$$

Zgled 3.4 (Walsh-Hadamardova preslikava)**.** *Naj bo* $V_1 = \mathbb{C}[\mathbb{Z}_2]$ *in* $W_1\colon V_1 \to V_1$ *linearna preslikava s pridruženo matriko*

$$W_1 = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}.$$

To je ravno matrika oblike 1 pri vrednosti $\varphi = \frac{\pi}{4}$*, torej je* W_1 *unitarna. Za* $n \in \mathbb{N}$ *označimo*

$$V_n = \underbrace{V_1 \otimes \ldots \otimes V_1}_{n\text{-krat}}.$$

Preslikavo

$$W_n = \underbrace{W_1 \otimes \ldots \otimes W_1}_{n\text{-krat}}\colon V_n \otimes V_n \to V_n \otimes V_n$$

imenujemo ***n*-ta Walsh-Hadamardova preslikava***. Njen matrični zapis dobimo induktivno na sledeči način. Matrični zapis* W_n *dobimo s pomočjo matričnega zapisa* W_{n-1}*, tako da koeficient* a_{ij} *v matričnem zapisu* W_{n-1} *zamenjamo z matriko* $a_{ij} \cdot W_1$*. Tako je na primer*

$$W_2 = \begin{bmatrix} \frac{1}{\sqrt{2}}W_1 & \frac{1}{\sqrt{2}}W_1 \\ \frac{1}{\sqrt{2}}W_1 & -\frac{1}{\sqrt{2}}W_1 \end{bmatrix} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{bmatrix}.$$

4 Kvantno računalništvo

4.1 Temelji kvantne fizike

Preden lahko začnemo naštevati postulate, moramo ustaliti notacijo, ki se jo v kvantni fiziki uporablja. Kot zahteva **Diracov zapis**, bomo vektorje ψ pisali kot $|\psi\rangle$. Uporabili bomo tudi t.i. **bra-ket** notacijo, ki skalarni produkt dveh vektorjev $|\psi\rangle$, $|\varphi\rangle$ označi kot $\langle\psi|\varphi\rangle$.

Postulat 4.1. ***Kvantni sistem*** *je podan s kompleksnim vektorskim prostorom $\mathcal{H}$ z ortonormirano bazo $|\psi_1\rangle, \ldots, |\psi_n\rangle$ in začetnim enotskim vektorjem $|\psi\rangle \in \mathcal{H}$. Enotskim vekotorjem v $\mathcal{H}$ pravimo* ***stanja****. Baznim vektorjem $|\psi_1\rangle, \ldots, |\psi_n\rangle$ pravimo* ***osnovna stanja****.*

Vsako stanje x lahko zapišemo kot **superpozicijo** osnovnih stanj

$$x = \lambda_1|\psi_1\rangle + \cdots + \lambda_n|\psi_n\rangle,$$

kjer velja

$$\begin{aligned} 1 &= \|x\|^2 \\ &= \left\langle \sum_{i=1}^{n} \lambda_i|\psi_i\rangle, \sum_{j=1}^{n} \lambda_j|\psi_j\rangle \right\rangle \\ &= \sum_{i=1}^{n}\sum_{j=1}^{n} \lambda_i\overline{\lambda_j}\langle\psi_i|\psi_j\rangle \\ &= \sum_{i=1}^{n} |\lambda_i|^2. \end{aligned}$$

Na primer, za kvantni sistem lahko vzamemo spin elektrona, ki je lahko v osnovnih stanjih $|\uparrow\rangle$ (gor) ali $|\downarrow\rangle$ (dol), za začetno stanje pa superpozicijo teh dveh osnovnih stanj

$$|\psi\rangle = \frac{1}{\sqrt{2}}\,|\uparrow\rangle + \frac{1}{\sqrt{2}}\,|\downarrow\rangle. \tag{3}$$

Postulat 4.2. *Pri razvoju kvantnega sistema lahko stanja spreminjajo zgolj unitarne preslikave.*

Ker je Walsh-Hadamardova preslikava W_1 unitarna, jo lahko uporabimo na stanju 3, ki nam ga slika v stanje

$$|\uparrow\rangle.$$

Opazimo, da se je superpozicija osnovnih stanj preslikala v osnovno stanje. Temu pojavu pravimo *interferenca.*

Postulat 4.3. *Če je sistem v stanju $\sum_{i=1}^{n} \lambda_i|\psi_i\rangle$, bomo ob meritvi izmerili bazno stanje ψ_i z verjetnostjo $|\lambda_i|^2$, stanje sistema pa se bo kolabiralo (kolapsiralo) v izmerjeno stanje.*

Če merimo stanje 3, bomo v polovici primerov izmerili, da ima elektron spin gor, v drugi polovici primerov pa, da ima elektron spin dol.

Postulat 4.4. *Kvantni sistem, ki ga dobimo z združitvijo kvantnih sistemov s prostorom stanj $\mathcal{H}_1$ in $\mathcal{H}_2$ ter začetnima stanjema $|\psi\rangle$ in $|\varphi\rangle$, je podan s prostorom stanj $\mathcal{H}_1 \otimes \mathcal{H}_2$ in začetnim stanjem $\psi \otimes \varphi$. Če je združen sistem v stanju*

$$\sum_{i=1}^{n} \lambda_i|e_i\rangle \otimes |\psi_i\rangle,$$

kjer so e_i osnovna stanja sistema $\mathcal{H}_1$ in $\psi_i \in \mathcal{H}_2$ enotski vektorji, potem ob meritvi prvega sistema z verjetnostjo $|\lambda_i|^2$ izmerimo stanje e_i, sistem pa se kolabira v stanje

$$|e_i\rangle \otimes |\psi_i\rangle.$$

4.2 Primerjava klasičnega računalnika s kvantnim

Klasični računalnik računa z **biti**, ki so lahko ali v stanju 0 ali v stanju 1, torej elementi $\mathbb{Z}_2$. Kvantni računalnik računa s **kubiti**, ki tvorijo kvantni sistem z osnovnimi stanji $|0\rangle$ in $|1\rangle$, tj. $\mathbb{C}[\mathbb{Z}_2]$. Poljubno stanje kubita je potem superpozicija teh dveh osnovnih stanj

$$\lambda_1|0\rangle + \lambda_2|1\rangle,$$

kjer $|\lambda_1|^2 + |\lambda_2|^2 = 1$. Če klasični računalnik deluje na n bitih, je njegov **register** (**spomin**) enak $\mathbb{Z}_2^n$, torej velikosti 2^n. Ko imamo kvantni računalnik z n kubiti, je njegov register enak n-ternemu tenzorskemu produktu

$$V_n = \underbrace{\mathbb{C}[\mathbb{Z}_2] \otimes \cdots \otimes \mathbb{C}[\mathbb{Z}_2]}_{n\text{-krat}} = \mathbb{C}[\underbrace{\mathbb{Z}_2 \otimes \cdots \otimes \mathbb{Z}_2}_{n\text{-krat}}].$$

Poleg 2^n osnovnih stanj vsebuje kvantni register še torej vse linearne kombinacije teh osnovnih stanj.

Račun na klasičnem računalniku je preslikava

$$f\colon \mathbb{Z}_n \to \mathbb{Z}_m$$

med dvema registroma. **Kvantni račun** na kvantnem računalniku je unitarna preslikava

$$U\colon V_n \to V_n$$

med dvema registroma z *enakim* številom kubitov.

Zgled 4.1 (NOT vrata)**.** *Klasična NOT vrata so predstavljena z računom $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$, ki ima predpis*

$$f(k) = 1 - k.$$

Kvantna NOT vrata pa predstavlja matrika

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

ki zamenja osnovni stanji $|0\rangle$ in $|1\rangle$.

V splošnem lahko vsak klasični račun $f\colon \mathbb{Z}_n \to \mathbb{Z}_m$ simuliramo na kvantnem računalniku, in sicer z linearno preslikavo

$$U_f\colon V_n \otimes V_m \to V_n \otimes V_m,$$

ki ima na baznih stanjih predpis

$$U_f(x \otimes y) = x \otimes (y + f(x)).$$

Izkaže se, da je ta preslikava unitarna, zato tvori kvantni račun. Račun f lahko iz nje povrnemo preko razvoja

$$U_f(x \otimes |\underbrace{0 \cdots 0}_{n\text{-krat}}\rangle) = x \otimes f(x)$$

in projiciranjem na drugi register.

5 Iskanje periode funkcije

5.1 Kvantna Fourierova transformacija

Orodje, ki nam bo prišlo prav pri kvantnem delu algoritma, je t.i. kvantna Fourierova transformacija. Fiksirajmo neko naravno število n. Za vsako celo število k definiramo funkcijo $\chi^k\colon \mathbb{Z} \to \mathbb{C}$ s predpisom

$$\chi^k(x) = e^{\frac{2\pi i k x}{n}}.$$

Definicija 5.1. *Naj bo V vektorski prostor z ortonormirano bazo $|0\rangle, |1\rangle, \ldots, |n-1\rangle$.* ***Kvantna Fourierova transformacija*** *na V je linearna preslikava $\mathcal{F}\colon V \to V$, ki bazni vektor $|x\rangle$ slika v*

$$\mathcal{F}|x\rangle = \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} \chi^k(x)|k\rangle.$$

Če želimo v prihodnje kvantno Fourierjevo transformacijo uporabiti na kakšnem kvantnem sistemu, se moramo najprej prepričati, da je ta preslikava unitarna.

Trditev 5.1. *Preslikava $\mathcal{F}$ je unitarna.*

Dokaz. Za bazni vektor $|x\rangle$ velja

$$\begin{aligned}\|\mathcal{F}|x\rangle\|^2 &= \langle \mathcal{F}|x\rangle, \mathcal{F}|x\rangle\rangle \\ &= \left\langle \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} \chi^k(x)|k\rangle, \frac{1}{\sqrt{n}} \sum_{l=0}^{n-1} \chi^l(x)|l\rangle \right\rangle \\ &= \frac{1}{n} \left\langle \sum_{k=0}^{n-1} \chi^k(x)|k\rangle, \sum_{l=0}^{n-1} \chi^l(x)|l\rangle \right\rangle.\end{aligned}$$

Po lastnostih skalarnega produkta je to enako

$$\frac{1}{n} \sum_{k=0}^{n-1} \sum_{l=0}^{n-1} \chi^k(x)\overline{\chi^l(x)}\langle k|l\rangle.$$

Nadalje se po ortonormiranosti baze zgornja vsota poenostavi do

$$\frac{1}{n} \sum_{k=0}^{n-1} \chi^k(x)\overline{\chi^k(x)} = \frac{1}{n} \sum_{k=0}^{n-1} 1 = 1 = \||x\rangle\|^2.$$

Ker $\mathcal{F}$ slika ortonormirano bazo $\{|0\rangle, |1\rangle, \ldots, |n-1\rangle\}$ v ortonormiran sistem, dokazana enakost velja tudi za splošen vektor. □

Pri kvantnem delu algoritma bomo potrebovali še naslednji rezultat.

Lema 5.1. *Naj bo V vektorski prostor z bazo $\mathbb{Z}_n$. Naj bo $f \in V$, ki jo gledamo kot funkcijo $f\colon \mathbb{Z}_n \to \mathbb{C}$, ki slika i v koeficient pred baznim vektorjem $|i\rangle$ v razvoju f po bazi. Recimo, da je f periodična funkcija s periodo r in da $r \mid n$. Potem velja*

$$\mathcal{F}(f)(k) = \begin{cases} \frac{\sqrt{n}}{r} \sum_{s=0}^{r-1} f(s)\chi^k(s), & \text{če } k \equiv 0 \bmod \frac{n}{r} \\ 0, & \text{sicer.} \end{cases}$$

Dokaz. Velja

$$\begin{aligned}\mathcal{F}(f)(k) &= \frac{1}{\sqrt{n}} \sum_{x=0}^{n-1} f(x)\chi^x(k) \\ &= \frac{1}{\sqrt{n}} \sum_{q=0}^{\frac{n}{r}-1} \sum_{s=0}^{r-1} f(qr+s)\chi^k(qr+s).\end{aligned}$$

Po periodičnosti funkcije f in multiplikativnosti funkcije χ^k dobimo

$$\begin{aligned}&\frac{1}{\sqrt{n}} \sum_{q=0}^{\frac{n}{r}-1} \sum_{s=0}^{r-1} f(s)\chi^k(qr)\chi^k(s) \\ &= \frac{1}{\sqrt{n}} \sum_{s=0}^{r-1} f(s)\chi^k(s) \sum_{q=0}^{\frac{n}{r}-1} \chi^k(qr).\end{aligned}$$

Če k ne deli $\frac{n}{r}$, potem je $\chi^k(qr) \neq 1$ za vsak $q = 0, \ldots, \frac{n}{r} - 1$ in po formuli za geometrijsko vrsto velja

$$\sum_{q=0}^{\frac{n}{r}-1} \chi^k(qr) = \frac{e^{2\pi ik} - 1}{e^{\frac{2\pi irk}{n}} - 1} = 0.$$

Sicer je $\chi^k(qr) = 1$ za vsak $q = 0, \ldots, \frac{n}{r} - 1$ in velja

$$\sum_{q=0}^{\frac{n}{r}-1} \chi^k(qr) = \frac{n}{r},$$

kar dokaže lemo.

□

5.2 Kvantni del algoritma

Vrnimo se sedaj k našemu začetnemu algoritmu. V drugem poglavju smo problem izračuna prafaktorjev števila

$$N = pq$$

prevedli na problem iskanja najmanjšega števila r, da velja

$$y^r = 1 \bmod N$$

za nek $y \in \mathbb{Z}_N^*$. To pa je ekvivalentno iskanju periode funkcije $f\colon \mathbb{Z}_N \to \mathbb{Z}_N$ s predpisom

$$f(k) = y^k \bmod N.$$

Označimo njeno periodo z r. Naj bo n takšno število, da je

$$2^{n-1} < N \leq 2^n.$$

V nadalje bomo enačili N z 2^n, kar lahko storimo, saj se bo končni rezultat le malo razlikoval od pravega.

Začnimo z dvema n-registroma $V_n \otimes V_n$ v začetnem stanju $|0\rangle \otimes |0\rangle$.

(1) Na prvem registru uporabimo Walsh-Hadamardovo preslikavo W_n in dobimo

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \otimes |0\rangle.$$

Dobljeno stanje nato preslikamo z U_f, kar nam da

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \otimes |f(x)\rangle.$$

(2) Sedaj opazimo drugi register, kar nam da neko vrednost y_0 in nam kolabira stanje v

$$\frac{1}{\sqrt{|f^{-1}(y_0)|}} \sum_{x \in f^{-1}(y_0)} |x\rangle \otimes |y_0\rangle.$$

Ker je f periodična, obstaja natanko eno število $0 \leq x_0 < r$, da je $f(x_0) = y_0$. Če označimo $K = \frac{N}{r}$, je zgornje stanje v prvem registru potem enako

$$\frac{1}{\sqrt{K}} \sum_{q=0}^{K-1} |x_0 + qr\rangle =$$
$$\sum_{x=0}^{N-1} \psi(x)\, |x\rangle,$$

kjer je

$$\psi(x) = \begin{cases} \frac{1}{\sqrt{K}}; & \text{če } r \mid x - x_0 \\ 0; & \text{sicer.} \end{cases}$$

Po definiciji je ψ periodična s periodo r.
(3) Na prvem registru sedaj uporabimo kvantno Fourierjevo transformacijo in po prejšnji lemi pridemo do stanja (po definiciji funkcije velja $r \mid N$)

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \chi^{\frac{sN}{r}}(x_0) \left| \frac{sN}{r} \right\rangle \otimes |y_0\rangle.$$

(4) Za konec opazimo to stanje v prvem registru, kar nam vrne vrednost c, ki je večkratnik števila $\frac{N}{r}$. Ker je bila vrednost y_0 naključna, je $c = \frac{sN}{r}$ za naključen $s \in \{0, \dots r-1\}$, oziroma, $\frac{c}{N} = \frac{s}{r}$. Preko zapisa ulomka $\frac{c}{N}$ v okrajšani obliki $\frac{c'}{N'}$ in upoštevanja enakosti

$$c'r = sN'$$

ugotovimo, da je r večkratnik števila N'. Ta korak ponavljamo, dokler nismo zadostno gotovi, da je največji skupni večkratnik dobljenih vrednosti res perioda r funkcije f.

Literatura

[1] J. P. Buhler, H. Lenstra in C. Pomerance, *Factoring integers with the number field sieve*, v: The development of the number field sieve (ur. A. K. Lenstra), Lecture Notes in Mathematics, Springer, Berlin, 2006, str. 50–94.

[2] C. Pittet, *Mathematical aspects of Shor's algorithm*, 2013, dostopno na `https://cel.hal.science/cel-00963668/document`.

Domneve

Blaž Peter Brunšek, Jure Kreže, Val Sajko
Mentor: *Jan Genc*

Povzetek

Skupina človeških raziskovalcev se je zaradi nesreče z raketo zbudila na neznanem planetu. Sumijo, da je Mars, vendar niso prepričani. Kako lahko uporabijo svoje znanje statistike, da ugotovijo, če so na Marsu ali ne?

1 Uvod

Blaise Pascal, John Conway, Jurij Vega in Viktor Vagner so bili na potovanju z raketo po vesolju. Žal je raketo izdelalo podjetje Boeing in so bili zelo skopi. Približno 400.000 kilometrov stran od Zemlje je zaradi neplačanih programerjev detektor prenehal delovati. Vsi so vdihnili poseben plin, ki ga je izumil Jakob Bernoulli za potnike, ki jim je zmanjkalo hrane, in zaspali za neznano število ur.

Ko so se zbudili, so se znašli na neznanem planetu v nepremikajoči se raketi. Sistem za avtopilot je deloval, vendar se je med pristankom toliko opreme pokvarilo, da navigacija ni delovala. Vedeli niso niti ne, koliko časa so spali. Niso mogli ugibati, kaj je bila njihova razdalja od doma.

»Aja!« je vzkliknil Conway, ki se je že parkrat potepal po vesolju, »sumim, da smo na Marsu... Veliko Marsovcev vidim in okolica mi izgleda znana.«

Pascal, ki nikoli ni rad tvegal, mu je odgovoril: »To bi bilo treba preveriti. Moramo nekoga vprašati ali analizirati prst. Če smo na Marsu, bomo veliko lažje prišli nazaj domov, sicer imamo pred nami veliko dela.«

Nekaj časa so hodili naokrog in opazovali okolico. Našli so se v Marsovski metropoli, Škofji Loki, in se sprehajali po trgovinah. Trgovci niso govorili znanega jezika.

»Nemogoče,« doda Vagner, ki je tako zelo dolgo čakal na odgovor, ker so njegove kognitivne sposobnosti linearno padale med urami slabega spanca in je bil precej mentalno omejen, »ne govorijo slovenščine in naša orodja za analizo so pokvarjena. Nekako drugače moramo ugotoviti, kje smo.«

Vsi so rahlo paničarili, vendar so po dolgem sprehodu okrog Škofje Loke približno vrnili svoje kognitivne sposobnosti na 10 %. Zaradi izboljšane kognicije se je Vega spomnil, da ima sumljivo obsežno znanje nezemljanske zakonodaje po celotni Rimski cesti, in razglasil: »Aha! Marsovci so zelo slavno ksenofobični! Ne dopuščajo več kot 20 % populacije nemarsovcev. Lahko bi jih anketirali in ugotovili, če je več kot 20 % nemarsovcev!«

Vsi so se, kljub sumu nezakonitih poslov z nezemljani s strani Vega, strinjali in začeli sestavljati anketo.

Ta trenutek se je Pascal spomnil, da Marsovci vidijo najbolje od vseh vrst v vesolju, in tako za njih pripravil pregled vida.

Pascal je hodil po Celju, ki je rdéč, vendar je barva pretirano izgovorjena (vsi vedno vlečejo é, ko jo izgovorijo), in anketiral prebivalce. Uspešno je anketiral 1000 prebivalcev, preden so mu prepovedali nadaljnje delovanje, in se vrnil k raketi.

Ko je Pascal našel svoje prijatelje, jim je sporočil žalostne novice: »Žal je 23% nemarsovcev. Ne vem, kje smo.« Vagner, ki je nekaj časa spal in je imel boljše kognitivne sposobnosti kot ostali, je komentiral: »To ni nujno. Statistično bi lahko vseeno samo imel slab vzorec. Moramo izračunati, kolikšna je verjetnost, da smo na Marsu!«

Vsi so bili zelo zadovoljeni z njegovim predlogom in začeli razmišljati. Problem je, da so se spomnili le najbolj osnovnih konceptov v statistiki in verjetnosti. Na srečo so eni najpametnejših ljudi v zgodovini, zato so se odločili, da bodo izpeljali to, kar lahko z uporabo logike. Sčasoma so se njihove kognitivne sposobnosti vračale in so prišli do rešitve. Tedaj je vprašanje, ali so lahko prepričani, če so na Marsu?

2 Neodvisnost dogodkov

Neodvisnost je v verjetnostnem računu in stohastiki odnos med dvema dogodkoma. Dogodka sta neodvisna, če pojav prvega ne povzroči večje verjetnosti nastopa drugega dogodka. Oziroma če pojav enega dogodka ne vpliva na izid drugega in obratno. Velja torej naslednja definicija:

Definicija 2.1. *Dogodek A je neodvisen od B, če je $P(A|B) = P(A)$.*

Definicija 2.2. *Dogodka A in B sta neodvisna, če zanju velja*

$$P(A \cap B) = P(A) \cdot P(B).$$

Definirajmo sedaj neodvisnost poljubnega končnega števila dogodkov.

Definicija 2.3. *Dogodki $A_1,\ A_2,\ \ldots,\ A_n$ so neodvisni, če je*

$$P(A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}) = P(A_{i_1}) \cdots P(A_{i_k})$$

za vsak $k \in \{1, 2, \ldots, n\}$ in za poljubna naravna števila

$$1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant n.$$

Posplošimo še definicijo na neskončno množico dogodkov oblike $\{A_1,\ A_2,\ \ldots\}$.

Definicija 2.4. *Dogodki $A_1,\ A_2,\ \ldots$ so neodvisni, če je njihova poljubna končna podmnožica neodvisna.*

Zgled 2.1. *Vržemo 5 standardnih kock. Kolikšna je verjetnost, da pri vsaj eni pade šestica? To nalogo rešimo z osnovnim izrekom o kombinatoriki in definicijo verjetnosti. Po definiciji neodvisnosti dogodkov lahko izračunamo nasprotni dogodek, da šestica ne pade, in njegova verjetnost je*

$$P(A) = \frac{5^5}{6^5}.$$

Če verjetnost tega dogodka odštejemo od 1, dobimo verjetnost želenega dogodka

$$P(B) = 1 - \frac{5^5}{6^5}.$$

Ker so meti kock neodvisni, lahko verjetnost nasprotnega dogodka izračunamo tudi kot produkt petih verjetnosti, da na eni kocki ne pade šestica, torej

$$P(B) = 1 - \left(\frac{5}{6}\right)^5.$$

Opazimo torej, da si lahko računanje verjetnosti večih sočasnih neodvisnih dogodkov preoblikujemo v računanje posamičnih verjetnosti, kar je ponavadi lažje rešiti.

3 Slučajne spremenljivke

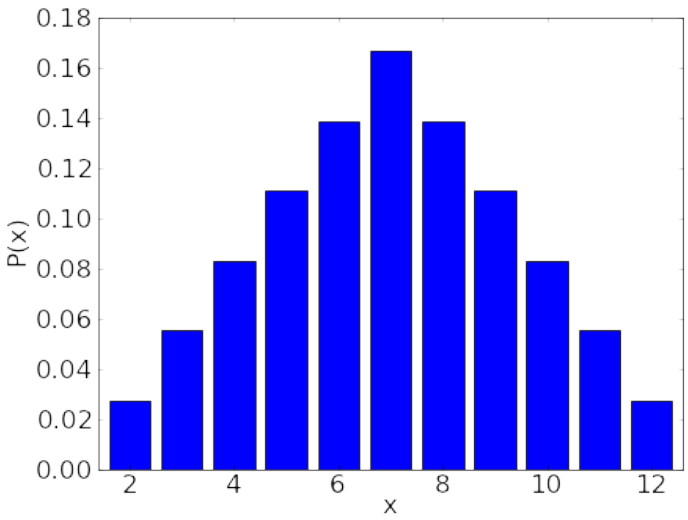
Poglejmo si zelo neformalno definicijo slučajnih spremenljivk.

Definicija 3.1. *Slučajne spremenljivke so števila, ki naključno nastanejo pri izvajanju poskusa.*

Sicer slučajnih spremenljivk formalno ne bomo definirali, jih bomo pa razložili s primerom.

Zgled 3.1. *Zamislimo si, da izvajamo poskus, v katerem večkrat vržemo dve igralni kocki. Primer slučajne spremenljivke je številska vrednost, ki bi jo lahko opazovali - na primer vsota pik na igralnih kockah ob posameznem metu.*

Za boljšo predstavo o naravi poskusa si lahko pomagamo s histogramom - grafom porazdelitve verjetnosti izidov za posamezne vrednosti slučajne spremenljivke.
Še en od znanih primerov porazdelitve slučajne spremenljivke je Bernoullijeva porazdelitev.



Slika 1: Histogram porazdelitve verjetnosti za posamezen izid poskusa. Na vodoravni osi so vrednosti naše slučajne spremenljivke označene z X (vsota pik na igralnih kockah), na navpični pa verjetnost izida.

Definicija 3.2. *Če ima neka slučajna spremenljivka X naslednjo porazdelitev*

- *zavzame vrednost 1 z verjetnostjo p,*
- *zavzame vrednost 0 z verjetnostjo $1 - p$,*

potem pravimo, da ima X ***Bernoullijevo porazdelitev****, kar zapišemo kot*

$$X \sim \text{Bernoulli}(p).$$

Primer poskusa in slučajne spremenljivke, ki je porazdeljena Bernoullijevo, je lahko število padlih grbov po nekaj metih kovanca. Izbrana slučajna spremenljivka lahko namreč zavzame vrednost 1 z verjetnostjo $0,5$ (če pade grb) in vrednost 0 z verjetnostjo $0,5$ (če ne pade grb). V tem primeru je kovanec pošten, lahko pa bi imeli verjetnost $0,3$, da pade grb, in verjetnost $0,7$, da ne pade grb.

3.1 Zvezne porazdelitve

Porazdelitev se razlikuje od prejšnjih v primeru, da izidi slučajne spremenljivke zavzamejo nek interval. Definicija je naslednja.

Definicija 3.3. *Slučajna spremenljivka X ima* **zvezno porazdelitev***, če obstaja nenegativna funkcija $f_X \colon \mathbb{R} \to [0, \infty]$, tako da je*

$$P(X \in (a, b)) = \int_a^b f_X(x)\, dx.$$

Tej funkciji pravimo **gostota slučajne spremenljivke**.

Opazimo, da bo X res porazdelitev, ko velja

$$\int_{-\infty}^{\infty} f_X(t)\, dt = 1.$$

Verjetnost, da zvezna slučajna spremenljivka zavzame vrednost na danem intervalu, je po definiciji določenega integrala enaka kar ploščini pod grafom funkcije gostote na podanem intervalu. Sedaj si bomo ogledali posebne primere zveznih porazdelitev, ki bodo uporabni kasneje v članku.

3.1.1 Normalna porazdelitev

Definicija 3.4. *Rečemo, da ima X **normalno porazdelitev** s parametroma μ in $\sigma^2 > 0$, če je njena gostota*

$$f_X(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-\mu)^2}{2\sigma^2}}.$$

To označimo kot $X \sim N(\mu, \sigma^2)$.

Opazimo, da je funkcija gostote te funkcije simetrična glede na os $x = \mu$, saj velja $f_X(\mu - t) = f_X(\mu + t)$. Izkaže se tudi, da je število σ enako razdalji med μ in točkama prevoja grafa funkcije gostote.

Normalna porazdelitev je odvisna od dveh parametrov: μ in σ, vendar kasneje bomo opazili, da si lahko računanje s poljubno normalno porazdelitvijo preoblikujemo s pomočjo preprostih relacij, ki veljajo med normalnimi porazdelitvami. V naslednjem razdelku definiramo posebno različico normalne porazdelitve. Na njo se bomo v nadaljevanju večkrat navezali. S pomočjo povezav med normalnimi porazdelitvami bomo uspeli računanje s poljubno normalno porazdelitvijo preoblikovati v računanje s to različico, saj zanjo poznamo zanesljive hitre metode zelo natančnih izračunov.

3.1.2 Standardizirana normalna porazdelitev

Če za parametra normalne porazdelitve vzamemo kar $\mu = 0$ in $\sigma = 1$, dobimo naslednjo porazdelitev.

Definicija 3.5. *Normalna porazdelitev je **standardizirana**, če velja*

$$Z \sim N(0, 1).$$

3.1.3 Porazdelitvena funkcija

Definicija 3.6. ***Porazdelitvena funkcija*** $F_X : \mathbb{R} \to [0, 1]$ *je definirana z naslednjim predpisom*

$$F_X(x) := P(X \leqslant x).$$

Torej porazdelitvena funkcija je funkcija porazdelitve slučajne spremenljivke X, ki nam pove verjetnost, da je vrednost slučajne spremenljivke manjša ali enaka argumentu x. Izračuna se z naslednjim integralom

$$F_X(t) = \int_{-\infty}^{t} f_X(x)\, dx.$$

3.1.4 Funkcija Φ

Definicija 3.7. *Za standardizirano normalno porazdelitev*

$$Z \sim N(0, 1)$$

je porazdelitvena funkcija označena z naslednjim zapisom

$$F_Z(x) = \Phi(x).$$

Velja torej

$$\Phi(t) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{t} e^{-\frac{x^2}{2}}\, dx.$$

Zapišimo trditev, ki nam bo pomagala v nadaljevanju.

Trditev 3.1. *Verjetnost, da vrednost slučajne spremenljivke $Z \sim N(0, 1)$ leži na intervalu (a, b), lahko izračunamo kot*

$$P(Z \in (a, b)) = \Phi(b) - \Phi(a).$$

Dokaz. Verjetnost, da vrednost slučajne spremenljivke Z leži na intervalu (a, b), je po definiciji

$$P(Z \in (a, b)) = \int_a^b f_Z(x)\,dx.$$

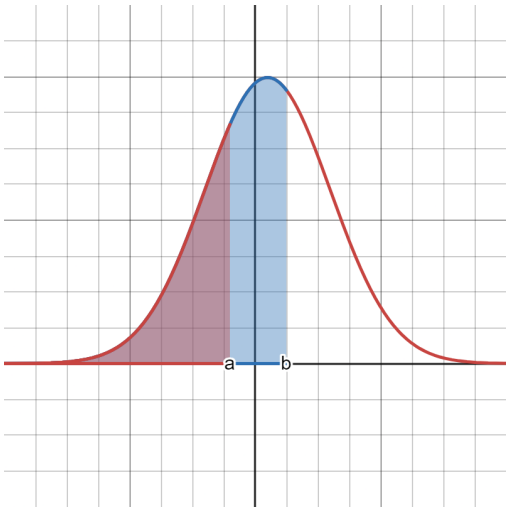
Ta integral se da razbiti na dva z upoštevanjem pravil o spremembi mej pri seštevanju oz. odštevanju integralov

$$\int_a^b f_Z(x)\,dx = \int_{-\infty}^b f_Z(x)\,dx - \int_{-\infty}^a f_Z(x)\,dx.$$

V tej enačbi sta integrala na desni strani po definiciji enaka $\Phi(b)$ in $\Phi(a)$, torej se lahko enačba zapiše kot

$$P(Z \in (a, b)) = \Phi(b) - \Phi(a).$$

□



Slika 2: Izračun vrednosti slučajne spremenljivke na intervalu.

Izrek 3.1. *Velja enakost*

$$\Phi(\infty) = 1.$$

Ker funkcijskih vrednosti funkcije Φ ne moremo na hitro računati na pamet, se ponavadi računa z njo z uporabo preglednice, na kateri so označeni pari argumentov in vrednosti funkcije Φ.

3.2 Povezava med normalnimi porazdelitvami

Kljub temu da so morda različne normalne spremeljivke normalne, so njihove normalne krivulje postavljene na različnih mestih na abscisni osi in so bolj ali manj sploščene. Te krivulje je najbolje pretvoriti v standardizirano normalno porazdelitev, za katero poznamo razpredelnico vrednosti.

Pri tem si lahko pomagamo s sledečima izrekoma.

Izrek 3.2. *Če sta X in Y neodvisni slučajni spremenljivki ter velja, da je $X \sim N(a, b^2)$ in $Y \sim N(c, d^2)$, je*

$$X + Y \sim N(a + c, b^2 + d^2).$$

Izrek 3.3. *Naj bo $X \sim N(\mu, \sigma^2)$ slučajna spremenljivka, potem velja*

$$aX + b \sim N(a\mu + b, a^2\sigma^2).$$

Standard Normal Probabilities

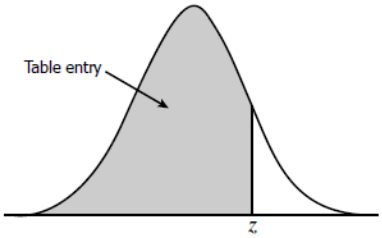


Table entry for z is the area under the standard normal curve to the left of z.

z	.00	.01	.02	.03	.04	.05	.06	.07	.08	.09
0.0	.5000	.5040	.5080	.5120	.5160	.5199	.5239	.5279	.5319	.5359
0.1	.5398	.5438	.5478	.5517	.5557	.5596	.5636	.5675	.5714	.5753
0.2	.5793	.5832	.5871	.5910	.5948	.5987	.6026	.6064	.6103	.6141
0.3	.6179	.6217	.6255	.6293	.6331	.6368	.6406	.6443	.6480	.6517
0.4	.6554	.6591	.6628	.6664	.6700	.6736	.6772	.6808	.6844	.6879
0.5	.6915	.6950	.6985	.7019	.7054	.7088	.7123	.7157	.7190	.7224
0.6	.7257	.7291	.7324	.7357	.7389	.7422	.7454	.7486	.7517	.7549
0.7	.7580	.7611	.7642	.7673	.7704	.7734	.7764	.7794	.7823	.7852
0.8	.7881	.7910	.7939	.7967	.7995	.8023	.8051	.8078	.8106	.8133
0.9	.8159	.8186	.8212	.8238	.8264	.8289	.8315	.8340	.8365	.8389
1.0	.8413	.8438	.8461	.8485	.8508	.8531	.8554	.8577	.8599	.8621
1.1	.8643	.8665	.8686	.8708	.8729	.8749	.8770	.8790	.8810	.8830
1.2	.8849	.8869	.8888	.8907	.8925	.8944	.8962	.8980	.8997	.9015
1.3	.9032	.9049	.9066	.9082	.9099	.9115	.9131	.9147	.9162	.9177

Slika 3: Tabela vrednosti funkcije Φ.

Dokaz. Označimo $Y = aX + b$. Opazimo s pomočjo preurejanja neenačbe v argumentu, da je

$$F_Y(y) = P(Y \leqslant y) = P(aX + b \leqslant y) = P\left(X \leqslant \frac{y-b}{a}\right) = F_X\left(\frac{y-b}{a}\right).$$

Ker je

$$F_X(x) = \int_{-\infty}^{x} f_X(x)\,dx,$$

velja po osnovnem izreku analize $F_X'(x) = f_X(x)$. Zato lahko izračunamo

$$\begin{aligned} f_Y(y) = F_Y'(y) &= \\ &= F_X'\left(\frac{y-b}{a}\right) \cdot \frac{1}{a} = \\ &= \frac{1}{a\sigma\sqrt{2\pi}} \cdot e^{-\frac{\left(\frac{y-b}{a}-\mu\right)^2}{2\sigma^2}} = \\ &= \frac{1}{a\sigma\sqrt{2\pi}} \cdot e^{-\frac{(y-b-a\mu)^2}{2a^2\sigma^2}}, \end{aligned}$$

kar pomeni, da je $Y \sim N(a\mu + b, a^2\sigma^2)$.

□

Oglejmo si uporabo teh izrekov na dveh zgledih.

Zgled 3.2. *Naj bosta X in Y slučajni spremenljivki, za kateri velja, da je $X \sim N(0,1)$ in $Y = aX + b$. Izračunajmo verjetnost $P(Y \leqslant t)$.*

$$P(Y \leqslant t) = P(aX + b \leqslant t) = P\left(X \leqslant \frac{t-b}{a}\right) = \Phi\left(\frac{t-b}{a}\right).$$

Torej v splošnem bo veljalo, da lahko povežemo poljubno normalno porazdelitev s standardizirano normalno porazdelitvijo, kot vidimo v zgledu 3.

Zgled 3.3. *Naj bo $X \sim N(\mu, \sigma^2)$ slučajna spremenljivka. Izračunajmo a in b tako, da bo $aX + b \sim N(0, 1)$. Dokazali smo že, da velja*

$$aX + b \sim N(a\mu + b, a^2\sigma^2) = N(0, 1).$$

Enačimo argumente:

$$a\mu + b = 0,$$
$$a^2\sigma^2 = 1$$

in iz dobljenih enačb izpostavimo parametra a in b.

$$a = \frac{1}{\sigma}$$
$$b = -\frac{\mu}{\sigma}$$

S tema enačbama lahko poljubno normalno porazdelitev pretvorimo v standardizirano normalno.

3.3 Pričakovana vrednost

Razložimo motivacijo za vpeljavo pričakovane vrednosti na zgledu. Zamislimo si, da igramo igro na srečo. Pri tej igri imamo na mizi 5 ploščic označenih z 1, ploščico označeno z 2, ploščico označeno s 3, ploščico označeno z D (dvojno) in 4 ploščice označene s S (stop). Skupno torej 12 ploščic. Na začetku jih obrnemo in premešamo. Igralec ploščice obrača od leve proti desni, dokler ne naleti na ploščico označeno s S. Ob koncu igre dobi izplačilo, ki je enako vsoti števil, ki jih vidimo na mizi. Če je med ploščicami, ki jih lahko vidimo, ploščica z oznako D, je izplačilo enako dvakratniku vsote števil, ki jih vidimo.

Smiselno bi se bilo vprašati, koliko bi bili pripravljeni plačati za igranje te igre, da bi lahko tudi ocenili, če je takšno igro smiselno večkrat igrati (če želimo imeti dobitek). Zanima nas torej pričakovano izplačilo igre oziroma pričakovana vrednost tega poskusa.

Izračunamo lahko povprečje izplačila za čim večje število odigranih iger, ki bi ustrezalo največjemu smiselnemu plačilu. Naj slučajna spremenljivka X označuje vsoto vidnih številk na mizi, ki določa izplačilo ob igri. Denimo, da lahko dobimo n različnih izplačil x_1, x_2, ..., x_n, potem bi plačali

$$\frac{x_1 \cdot (\text{št. ponovitev } x_1) + x_2 \cdot (\text{št. ponovitev } x_2) + \ldots + x_n \cdot (\text{št. ponovitev } x_n)}{\text{št. ponovitev poskusa}},$$

to pa lahko zapišemo kot

$$x_1 \cdot \frac{\text{št. ponovitev } x_1}{m} + \cdots + x_n \cdot \frac{\text{št. ponovitev } x_n}{m} =$$
$$= x_1 \cdot P(X = x_1) + \ldots + x_n \cdot P(X = x_n),$$

kjer smo z m označili število ponovitev poskusa. To nas motivira, da definiramo pričakovano vrednost.

Definicija 3.8. *Naj bo X slučajna spremenljivka z vrednostmi v_1, v_2, ..., v_n. Pričakovana vrednost slučajne spremenljivke X je*

$$E(X) = \sum_{i=1}^{n} v_i \cdot P(X = v_i).$$

Definicija 3.9. *Naj bo X slučajna spremenljivka z vrednostmi v_1, v_2, ... Pričakovana vrednost slučajne spremenljivke X je*

$$E(X) = \sum_{i=1}^{\infty} v_i \cdot P(X = v_i).$$

Če je slučajna spremenljivka X porazdeljena zvezno, uporabimo naslednjo definicijo.

Definicija 3.10. *Če je X zvezna slučajna spremenljivka, je pričakovana vrednost spremenljivke X*

$$E(X) = \int_{-\infty}^{\infty} v \cdot f_X(v)\, dv.$$

Sedaj bomo določili pričakovano vrednost za nas najpomembnejših dveh porazdelitev.

Trditev 3.2. *Pričakovana vrednost slučajne spremenljivke, ki je porazdeljena* Bernoulli(p)*, je enaka $E(X) = p$.*

Dokaz. Naj bo

$$X \sim \text{Bernoulli}(p).$$

Dokaza se lahko lotimo z zgornjo formulo za izračun pričakovane vrednosti. Upoštevamo tudi, da pri Bernoullijevi porazdelitvi nastopa vrednost 1 z verjetnostjo p in vrednost 0 z verjetnostjo $1 - p$

$$E(X) = 1 \cdot p + 0 \cdot (1 - p)$$

in dobimo

$$E(X) = p.$$

□

Trditev 3.3. *Pričakovana vrednost slučajne spremenljivke, ki ima porazdelitev $N(\mu, \sigma^2)$, je enaka μ.*

Dokaz. Naj bo slučajna spremenljivka X porazdeljena normalno. Gre za zvezno porazdelitev, torej uporabimo definicijo pričakovane vrednosti zvezne slučajne spremenljivke

$$E(X) = \int_{-\infty}^{\infty} v \cdot f_X\, dv.$$

V našem primeru torej računamo

$$E(X) = \int_{-\infty}^{\infty} \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-\mu)^2}{2\sigma^2}} \cdot v\, dv.$$

$$\begin{aligned} E(X) &= \int_{-\infty}^{\infty} \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-\mu)^2}{2\sigma^2}} \cdot v\, dv = \\ &= \frac{1}{\sigma\sqrt{2\pi}} \int_{-\infty}^{\infty} e^{-\frac{(x-\mu)^2}{2\sigma^2}} \cdot v\, dv = \\ &= \frac{1}{\sigma\sqrt{2\pi}} \left(\int_{-\infty}^{\infty} e^{-\frac{(x-\mu)^2}{2\sigma^2}} \cdot (v - \mu)\, dv + \int_{-\infty}^{\infty} \mu e^{-\frac{(x-\mu)^2}{2\sigma^2}}\, dv \right) \end{aligned}$$

Na tej točki za lažje računanje levega integrala določimo $-(v-\mu)^2 = m$ kot novo spremenljivko. Desni integral lahko pomnožimo (novo spremenljivko uvedemo le za računanje levega integrala) z ulomkom pred oklepajem in iz njega izpostavimo konstanto μ ter ga preoblikujemo v

$$\mu \cdot \int_{-\infty}^{\infty} \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-\mu)^2}{2\sigma^2}}\, dv.$$

Tu lahko opazimo, da integriramo porazdelitveno funkcijo (v našem primeru normalno porazdelitveno funkcijo) po celotni realni osi, kar pa je po definiciji enako 1. Vrednost desnega integrala pomnoženega z ulomkom pred oklepajem je torej kar $\mu \cdot 1 = \mu$.

Po uvedbi nove spremenljivke pa se levi integral preoblikuje v določen integral, ki ima za spodnjo mejo

$$\lim_{v \to -\infty} -(v - \mu)^2 = -\infty,$$

za zgornjo mejo pa prav tako

$$\lim_{v \to \infty} -(v - \mu)^2 = -\infty.$$

Integral na levi je torej določen integral z isto spodnjo in zgornjo mejo in je zato enak 0. Sedaj lahko vidimo, da je pričakovana vrednost normalno porazdeljene slučajne spremenljivke enaka

$$E(X) = 0 + \mu = \mu.$$

□

Poglejmo, kako na zgledu izračunati pričakovano vrednost. Zanimiv in praktičen primer je uporaba teoretične različice sodobne pečice, katere ideja je bila zasnovana prav na Marsu.

Zgled 3.4. *Pečica začne ob koncu peke piskati in iz praktičnih razlogov jo je možno ugasniti samo s pritiskom na gumb, kadar je število piskov enako 2^n, kjer je $n \in \mathbb{N}_0$, torej kadar je število piskov enako $1, 2, 4, 8, \ldots$ Iz drugih praktičnih razlogov pa se z vsakim pritiskom na ta gumb pečica ugasne z verjetnostjo $p = 0,5$. Zanima nas, kolikokrat bomo najverjetneje pritisnili na gumb, da se bo pečica ugasnila.*

Označimo slučajno spremenljivko - število vseh piskov pečice - kot X. Opazimo, da je verjetnost, da pečico ugasnemo po številu sekund, ki ni potenca števila 2, enaka 0. Uporabimo formulo za izračun pričakovane vrednosti

$$E(X) = \sum_{i=1}^{\infty} i \cdot P(X = i) = \sum_{k=0}^{\infty} 2^k \cdot \left(\frac{1}{2^{k+1}}\right) = \sum_{k=0}^{\infty} \frac{1}{2},$$

vendar ta vsota pa očitno nima končne vrednosti, zato sklepamo, da se pečica nikoli ne izključi.

3.4 Varianca

Definirajmo še eno količino, ki bo koristna za poglavje, ki sledi:

Definicija 3.11. Varianca *slučajne spremenljivke X je*

$$\mathrm{var}(X) = E(X^2) - E(X)^2.$$

Poglejmo si dva primera varianc. Najprej za Bernoullijevo porazdelitev.

Izrek 3.4. *Če je X slučajna spremenljivka, za katero velja $X \sim \mathrm{Bernoulli}(p)$, je $\mathrm{var}(X) = p(1-p)$.*

Dokaz. Najprej opazimo, da velja

$$\mathrm{var}(X) = E(X^2) - E(X)^2 = E(X^2) - p^2,$$

Za slučajno spremenljivko X^2 velja

$$X^2 = \begin{cases} 1^2, & \text{z verjetnostjo } p, \\ 0^2, & \text{z verjetnostjo } 1-p. \end{cases}$$

Torej je porazdelitev X^2 enaka porazdelitvi X. Iz tega sledi $E(X^2) = p$ oz.

$$\mathrm{var}(X) = p - p^2.$$

□

Druga pomembna varianca, ki jo bomo omenili, je varianca normalne porazdelitve. To bomo le navedli brez dokaza.

Izrek 3.5. *Če je $X \sim N(\mu, \sigma^2)$ slučajna spremenljivka, potem velja $\mathrm{var}(X) = \sigma^2$.*

4 Centralni limitni izrek

V tem poglavju se bo pokazala uporabna vrednost variance in pričakovane vrednosti. V ta namen navedimo naslednji izrek.

Izrek 4.1. ***Centralni limitni izrek*** *Naj bodo $X_1, X_2, \ldots$ neodvisne in enako porazdeljene slučajne spremenljivke, za katere velja $E(X_i) = \mu$ in $\mathrm{var}(X_i) = \sigma^2$. Za dovolj velike n velja*

$$X_1 + \cdots + X_n \dot{\sim} N(n\mu, n\sigma^2),$$

kjer $\dot{\sim}$ predstavlja približno porazdelitev.

Ta izrek nam pove, da se porazdelitev vsote slučajnih spremenljivk, ki so neodvisne in enako porazdeljene in za katere velja $E(X_i) = \mu$ in $\mathrm{var}(X_i) = \sigma^2$ približuje normalni porazdelitvi. Izrek je bolj natančen, ko se povečuje število slučajnih spremenljivk, ki jih seštevamo. Pri tem je X_i i-ta slučajna spremenljivka. Centralni limitni izrek se pogosto uporablja skupaj s standardizacijo na naslednji način.

Trditev 4.1. *Naj bo*

$$S_n := X_1 + \cdots + X_n$$

in naj bosta a in b taki realni števili, da velja

$$aS_n + b \dot{\sim} N(0, 1).$$

Tedaj velja

$$P(S_n \in (a, b)) = \Phi\left(\frac{b - n\mu}{\sigma\sqrt{n}}\right) - \Phi\left(\frac{a - n\mu}{\sigma\sqrt{n}}\right).$$

Dokaz. Centralni limitni izrek nam pove, da ima S_n porazdelitev

$$S_n \dot{\sim} N(n\mu, n\sigma^2).$$

S pomočjo zgleda 3.3 lahko najdemo taki števili c in d, da velja
$cS_n + d \dot{\sim} N(0, 1)$. To sta

$$c = \frac{1}{\sigma\sqrt{n}} \qquad \text{in} \qquad d = \frac{-\sqrt{n}\mu}{\sigma}.$$

Tedaj velja porazdelitev

$$\frac{1}{\sigma\sqrt{n}} \cdot (X_1 + \cdots + X_n) - \frac{\sqrt{n}\mu}{\sigma} \dot{\sim} N(0, 1),$$

ki jo postavimo na skupni imenovalec in dobimo

$$\frac{X_1 + \cdots + X_n - n\mu}{\sigma\sqrt{n}} \dot{\sim} N(0, 1).$$

Po tem preoblikovanju velja, da je verjetnost enaka

$$P\left(\frac{S_n - n\mu}{\sigma\sqrt{n}} \in \left(\frac{a - n\mu}{\sigma\sqrt{n}}, \frac{b - n\mu}{\sigma\sqrt{n}}\right)\right) = \Phi\left(\frac{b - n\mu}{\sigma\sqrt{n}}\right) - \Phi\left(\frac{a - n\mu}{\sigma\sqrt{n}}\right).$$

□

4.1 Domneve

Za rešitev začetnega problema bomo morali spoznati še nekaj osnov statistike. Poglejmo si, kaj so domneve. Zamislimo si, da z eksperimentom želimo določiti informacijo o nekem parametru (recimo parametru o porazdelitvi). Včasih imamo za ta parameter že kakšno idejo, recimo, da je kovanec pošten. To je **ničelna domneva** in jo označimo s H_0. Če je opazovanje eksperimenta preveč neskladno s H_0, H_0 **zavrnemo**, sicer pa rečemo, da **odstopanja niso statistično dovolj značilna (za zavrnitev)**.
Negacijo H_0 označimo s H_1 in jo imenujemo **alternativna domneva**. Če H_0 zavrnemo, sprejmemo H_1. Domneve H_0 nikoli ne sprejmemo, saj bi morda v drugem vzorcu našli protiprimer (dovolj je en za zavrnitev). Torej če želimo

sprejeti H_0, raje za ničelno domnevo postavimo H_1 in jo zavrnimo. Postopek odločitve se imenuje preizkus. Preizkus ustreza stopnji tveganja α, če

$$P(H_0 \text{ zavrnemo} \mid H_0 \text{ velja}) \leqslant \alpha.$$

Po tem sprejmemo končno odločitev, α pa si vnaprej določimo glede na to, kako majhno tveganje za napako pri našem končnem sklepu želimo (manjši α pomeni manjše tveganje). Na podlagi izbrane stopnje tveganja in zgornje neenačbe določimo območje intervala za naš parameter, kjer se zavrne H_0 in nastalemu območju rečemo **zavrnitveno območje**. Z drugimi besedami: če je vrednost slučajne spremenljivke po izvedenem preizkusu v zavrnitvenem območju, našo domnevo zavrnemo. Torej lahko določimo neko zavrnitveno območje oziroma interval, na primer (c, ∞). To bi pomenilo, da če je vrednost slučajne spremenljivke večja od c, našo domnevo zavrnemo.
Oglejmo si še verjetnost

$$P(H_0 \text{ zavrnemo} \mid H_1 \text{velja}) = 1 - \beta.$$

To število imenujemo **moč preizkusa**, vendar na podlagi njega ne določamo zavrnitvenega območja, a je vseeno dobro, da je čim višji. Nanj lahko gledamo kot na stranski produkt preizkusa.

5 Rešitev začetnega problema

Conway je predlagal, da so imeli dovolj izrekov in definicij za rešitev njihovega problema. Določil je, da so želeli biti vsaj 95 % prepričani, da so oz. niso na Marsu. Začel je svoj dokaz z določitvijo stopnje tveganja

$$\alpha = 0,05.$$

Njegova ničelna domneva H_0 je, da so na Marsu. Začel je z določevanjem slučajne spremenljivke

$$X_i = \begin{cases} 1, & \text{če } i\text{-ti anketiranec ni marsovec,} \\ 0, & \text{če } i\text{-ti anketiranec je marsovec.} \end{cases}$$

Ker ta slučajna spremenljivka zavzema le vrednosti 0 in 1, je Vega predlagal, da gre za Bernoullijevo porazdelitev. Tedaj je zapisal

$$X_i \sim \text{Bernoulli}(p).$$

Vagner je začel računati zavrnitveno območje. Vnaprej ve, da je oblike (c, ∞). S c smo označili največjo vrednost spremenljivke, za katero naše domneve še ne zavrnemo. Ravnamo se po neenačbi

$$P(H_0 \text{ zavrnejo} \mid H_0 \text{ je pravilna}) \leqslant \alpha.$$

Za pravilnost ničelne domneve določi, da je na Marsu 20 % nemarsovcev, saj je to mejna vrednost deleža nemarsovcev, določena z marsovsko zakonodajo, in bo račun veljaven tudi za vse druge možne pravilne vrednosti. To preoblikuje v

$$\begin{aligned} &P\left(\frac{X_1 + \cdots + X_{1000}}{1000} > c \mid H_0 \text{ je pravilen}\right) = \\ &= P\left(\frac{X_1 + \cdots + X_{1000}}{1000} > c \mid p = 0,2\right) = \\ &= P(X_1 + \cdots + X_{1000} > 1000c \mid p = 0,2) = \\ &= P(X_1 + \cdots + X_{1000} \in (1000c, \infty) \mid p = 0,2). \end{aligned}$$

Na tej točki je Pascal določil vrednosti za μ in σ z uporabo lastnosti Bernoullijeve distribucije in variance. Ugotovil je, da je $\mu = p$ in da je

$$\sigma = \sqrt{\text{var}(X_i)} = \sqrt{p(1-p)} = \frac{2}{5}.$$

Sledil je izračun

$$\begin{aligned} &P(X_1 + \cdots + X_{1000} \in (1000c, \infty) \mid p = 0,2) = \\ &= 1 - \Phi\left(\frac{1000c - 1000\mu}{\sigma\sqrt{1000}}\right) = \\ &= 1 - \Phi\left(\frac{1000c - 1000 \cdot 0,2}{\sqrt{1000} \cdot 0,4}\right). \end{aligned}$$

Pri tem so upoštevali, da je vrednost funkcije Φ na levi enaka 1, saj gre za vrednost integrala porazdelitvene funkcije po celotni realni osi. Conway ve, da enakost

$$P(X_1 + \cdots + X_{1000} \in (1000c, \infty) \mid p = 0,2) = \alpha$$

poišče ravno pravi c, saj bodo primeri stroge neenakosti dali manjša zavrnitvena območja (podmnožice pravega). Postavi in preoblikuje enačbo

$$1 - \Phi\left(\frac{1000c - 1000 \cdot 0,2}{\sqrt{1000} \cdot 0,4}\right) = \alpha,$$
$$\Phi\left(\frac{1000c - 1000 \cdot 0,2}{\sqrt{1000} \cdot 0,4}\right) = 0,95.$$

Vega je pogledal na svojo tabelo z vrednostmi inverzne funkcije Φ, ki jo nosi povsod, saj je zelo poznana in uporabna v vsakdanjem življenju, ter našel vrednost argumenta za $\Phi(x) = 0,95$. Izvedel je, da mora veljati

$$\frac{1000c - 1000 \cdot 0,2}{\sqrt{1000} \cdot 0,4} = 1,64$$

oz. $c \approx 0,22$. Iz tega sledi, da je zavrnitveno območje približno interval $(0'22, \infty)$. Njihov eksperiment vrne vrednost $0,23 \in (0'22, \infty)$. Torej sklepajo, da niso na Marsu, saj morajo ničelno domnevo zavrniti.

Literatura

[1] John A. Rice: *Mathematical Statistics and Data Analysis*, tretja izdaja. Brooks/Cole, 2006

Kirchoffov izrek

Manca Ernst, Primož Markovič, Teja Zabukovec
Mentor: *Matija Likar*

Povzetek

V članku predstavimo problem štetja vpetih dreves v grafu. Izpeljemo Kirchoffov izrek, ki povezuje število vpetih dreves v grafu z lastnimi vrednostmi sosednostne matrike grafa. Izrek uporabimo na primeru hiperkocke.

1 Uvod

Poglejmo si naslednji kombinatorični problem. Na Marsu se je zgodil šokanten dogodek. Na planet je priletel asterokubid, ki je zaradi Marsove unikatne atmosfere zavzel obliko kocke. Ugotovili smo, da se na njegovih ogliščih nahaja dragocena ruda, svoje rudniške rove pa lahko napeljemo le po robovih te kocke. Zaradi finančnih omejitev želijo skopati sistem rovov, tako da bo za vsak par vozlišč obstajala le ena pot. Lotijo se kopanja, a kmalu ugotovijo, da imajo veliko izbir, kakšen sistem rovov izbrati. Začnejo se prepirati o vseh možnih poteh in že nameravajo pripraviti anketo z vsemi povezavami, da bi se ljudstvo lahko odločilo za najboljše, vendar hitro ugotovijo, da ne vejo, koliko je sploh vseh možnih sistemov rovov, ki jih lahko izkopljejo. Možnosti je bilo tako veliko, da so med debato čisto pozabili na kamnine in začeli razmišljati le še o štetju takih sistemov.

2 Grafi in vpeta drevesa

K problemu bomo pristopili preko spektralne teorije grafov. Za začetek si poglejmo nekaj osnovnih pojmov teorije grafov, s katerimi formaliziramo svoj kombinatorični problem.

Definicija 2.1. ***Graf*** $G = (V, E)$ *je urejen par, kjer je*

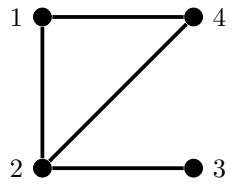
- $V = \{v_1, \ldots, v_p\}$ *neprazna množica* ***vozlišč*** *ali* ***točk*** *grafa,*
- $E = \{e_1, \ldots, e_q\}$ *pa množica* ***povezav*** *med njimi. Vsaka povezava je določena z množico dveh vozlišč, ki jo povezuje.*

Kocko v našem uvodnem problemu lahko modeliramo kot graf, tako da vzamemo njena oglišča za množico vozlišč. Dve vozlišči pa v grafu povežemo natanko tedaj, ko ju povezuje rob kocke. V nadaljevanju bomo še privzeli, da je med dvema vozliščema največ ena povezava, vozlišče pa ne sme imeti povezave same nase. Privzeli bomo tudi, da je množica vozlišč končna. Z izrazom $v_i \sim_G v_j$ bomo označili, da sta vozlišči v_i in v_j povezani v grafu G. Vozliščema, ki ju neka povezava povezuje, bomo rekli **krajišči** te povezave.

Primer 2.1. *Imamo graf* $G = (V, E)$ *z vozlišči* $V = \{1, 2, 3, 4\}$ *in povezavami* $E = \{(1, 2), (2, 3), (2, 4), (1, 4)\}$.

Poglejmo si še nekaj lastnosti grafov, ki nam bodo pomagali pri problemu. **Stopnja vozlišča** $d(v)$ je število povezav v grafu, ki imajo vozlišče v za eno izmed svojih krajišč. Graf je **d-regularen**, če ima vsako vozlišče v grafu stopnjo d. Stopnje vozlišč v zgornjem primeru grafa so prikazane v spodnji tabeli.

Zaporedje vozlišč $v_1 v_2 \ldots v_n$ v grafu imenujemo **sprehod**, če $v_i \sim_G v_{i+1}$ za $i = 1, \ldots, n-1$. Grafu pravimo, da je **povezan**, če za poljuben par vozlišč obstaja sprehod, ki se začne v enem in konča v drugem vozlišču. Graf v zgornjem primeru, je povezan.



Slika 1: Graf na štirih vozliščih.

vozlišče v	**stopnja vozlišča** $d(v)$
1	2
2	3
3	1
4	2

Tabela 1: Stopnje vozlišč v zgornjem primeru grafa.

Grafe pa lahko med sabo tudi množimo. Naj bosta $G = (V_1, E_1)$ in $H = (V_2, E_2)$ grafa. Njun produkt $G \times H = (V, E)$ definiramo kot

- $V = V_1 \times V_2 = \{(v_1, v_2) | v_1 \in V_1, v_2 \in V_2\}$,
- $E = \left\{ \{(u, v), (u', v')\} \,\middle|\, u, u' \in V_1,\ v, v' \in V_2, \begin{array}{c} (u = u') \wedge (v \sim_H v'), \\ \text{ali} \\ (u \sim_G u') \wedge (v = v') \end{array} \right\}$.

Naj bosta $G = (V, E)$ in $H = (V', E')$ grafa. Pravimo, da je H **podgraf** grafa G, če velja $V' \subseteq V$ in $E' \subseteq E$. Poseben tip podgrafa je **vpeti podgraf**, ki vsebuje vsa vozlišča prvotnega grafa, oz. $V' = V$.

Spoznajmo še nekaj vrst grafov, ki se pogosto pojavljajo.

- **Polni graf** ali **klika** K_n je graf z n vozlišči, kjer je vsako vozlišče povezano z vsemi ostalimi. Tako ima klika $\frac{n(n-1)}{2}$ povezav in je $(n-1)$-regularna.
- **Pot** P_n je graf z n vozlišči, kjer povežemo med sabo vozlišče i in vozlišče $i+1$ za $i \in \{1, 2, \ldots, n-1\}$.
- **Cikel** C_n je graf z n vozlišči, kjer povežemo med sabo vozlišče i in vozlišče $i+1$ za $i \in \{1, 2, \ldots, n-1\}$ ter tudi prvo in zadnjo vozlišče $(1, n)$, da dobimo 2-regularen graf. Če nek graf vsebuje cikel kot podgraf, pravimo da ima graf cikel, oz. da je cikličen. V nasprotnem primeru pravimo, da je graf acikličen.
- **Hiperkocka** $H_n = (V, E)$ je graf, ki je produkt n-tih poti P_2. Tako ima graf 2^n vozlišč in $2^{n-1} \cdot n$ povezav, s čimer dobimo n-regularen graf.

Poglejmo si še eno lemo, ki nam bo prišla prav v nadaljevanju.

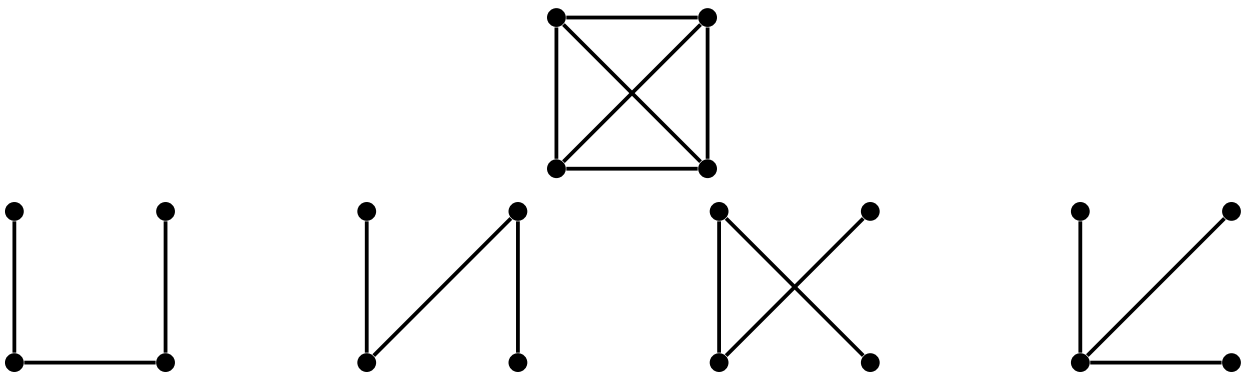
Lema 2.1. *Če graf nima cikla, potem ima vsaj eno vozlišče s stopnjo* 1*.*

Dokaz. Izberimo si poljubno vozlišče v grafu in se premikamo po povezavah, tako da se nikoli ne vrnemo na vozlišče, od koder smo prišli. Ker graf nima cikla, ne bomo nikoli prišli na isto vozlišče dvakrat, torej bomo morali sčasoma priti do nekega vozlišča, iz katerega ne bomo mogli nadaljevati, saj je krajišče le ene povezave. Tako vozlišče ima stopnjo 1. □

Vrsta grafa, ki se pojavi v našem problemu, je drevo.

Definicija 2.2. *Grafu $G = (V, E)$ rečemo **drevo**, če je povezan in nima ciklov. Vozliščem v drevesu, ki imajo stopnjo* 1*, pravimo **listi**.*

Za reševanje kombinatoričnih problemov je koristno poznati še nekaj ekvivalentnih pogojev, kdaj je graf drevo.



Slika 2: Graf K_4 in njegovih 16 vpetih dreves (izvzemši rotacije in zrcaljenja).

Lema 2.2. *Naj bo G graf z n vozlišči. Naslednje izjave so ekvivalente*

(a) graf G je drevo,

(b) graf G je povezan in ima $n-1$ povezav,

(c) graf G nima cikla in ima $n-1$ povezav,

(d) med vsakim parom vozlišč v G obstaja natanko ena pot.

Dokaz. Dokazali bomo le ekvivalentnost izjav (a) in (c), ostale pare pa lahko bralec poskusi dokazati sam. Najprej dokažimo, da izjava (a) implicira izjavo (c). Po definiciji drevesa naš graf nima ciklov, tako da je prvi pogoj zadoščen. Drugi pogoj pokažemo z indukcijo na številu vozlišč n. Baza indukcije $n = 1$ je očitna. Sedaj predpostavimo, da ima drevo z $n-1$ vozlišči $n-2$ povezav, želimo pa dokazati, da ima drevo z n vozlišči $n-1$ povezav. Po lemi 2.1 si lahko izberemo en list drevesa in ga odstranimo skupaj s povezavo, ki ga povezuje s preostankom grafa. Tako dobimo graf z $n-1$ vozlišči. S tem zagotovo ne bomo ustvarili novih ciklov. Ker smo odstranili list, nobeni drugi dve vozlišči v prvotnem grafu nista bili povezani preko njega, zato bodo vsa preostala vozlišča ostala povezana. Torej je nastali graf drevo z $n-1$ vozlišči. Po indukcijski predpostavki ima to drevo $n-2$ povezav. Ker smo odstranili eno povezavo, ima prvotno drevo $n-1$ povezav, kar zaključuje indukcijo.

Dokažimo še implikacijo v drugo smer. Spomnimo, da želimo dokazati, da je naš graf povezan in nima ciklov. Druga lastnost je seveda očitna. Naj bo G acikličen graf z $n-1$ povezavami. Po lemi 2.1 mu lahko, podobno kot prej, odstranimo neko vozlišče s stopnjo 1 skupaj s povezavo, ki ga povezuje s preostankom grafa. Dobimo acikličen graf G' z $n-2$ povezavami, ki je po naši indukcijski predpostavki drevo, torej je povezan. Želimo dokazati, da je tudi graf G povezan. To drži, saj iz grafa G' dobimo G tako, da dodamo eno vozlišče in povezavo nanj. Dodano vozlišče je povezano z nekim vozliščem v G' in posledično tudi z vsemi ostalimi vozlišči v G'. Torej je G povezan. Sledi, da je G res drevo, kar zaključuje indukcijo. □

Definicija 2.3. ***Vpeto drevo*** *je vpet podgraf, ki je drevo.*

Če pogledamo četrto izmed ekvivalentnih definicij drevesa, vidimo, da želimo v uvodnem problemu prešteti vpeta drevesa grafa kocke H_3. K takemu problemu je težko pristopiti na naiven kombinatoričen način, zato bomo v nadaljevanju vpeta drevesa grafa prešteti z uporabo linearne algebre. Lažji kombinatorični problem je prešteti vsa vpeta drevesa klike. Na sliki 2 so prikazana vpeta drevesa klike K_4. V splošnem bomo število vpetih dreves v grafu G označili s $\kappa(G)$.

3 Linearna algebra

Spoznali bomo nekaj ključnih izrekov iz linearne algebra, ki nam bodo koristili pri uvodnem problemu. Predpostavili bomo, da je bralec seznanjen z osnovnimi koncepti, kot so vektor, matrika, transponirana matrika in produkt dveh matrik. Bralec lahko osveži svoje znanje s [1]. Vrednost v i-ti vrstici j-tega stolpca matrike A bomo označili z $[A]_{ij} = a_{ij}$. Začnimo z definicijo permutacije, preko katere bomo definirali determinanto matrike.

Definicija 3.1. ***Permutacija*** *σ je bijekcija na množici $\{1, \ldots, n\}$. Množico vseh permutacij n elementov označimo s S_n.*

Spomnimo, da na množici z n elementi obstaja $n!$ permutacij. Permutacijo lahko zapišemo na več načinov, enega izmed njih smo si ogledali v naslednjem primeru.

Primer 3.1. *Za množico $\{1, 2, 3, 4\}$ se eno izmed permutacij lahko zapiše kot*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix},$$

kjer so v prvi vrstici elementi v običajnem vrstnem redu, v drugi vrstici pa vrednosti v katere se ti elementi slikajo. To lahko splošneje zapišemo kot

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}.$$

Potrebovali bomo še dve lastnosti permutacije. **Število inverzij** permutacije $\mathrm{inv}(\sigma)$ je število parov (i, j), kjer sta $i < j$ in $\sigma(j) < \sigma(i)$. **Signatura** permutacije $\mathrm{sgn}(\sigma) = (-1)^{\mathrm{inv}(\sigma)}$. Za permutacijo σ iz prvega primera sta taka para $(1, 2)$ in $(1, 3)$ iz česar sledi, da je $\mathrm{inv}(\sigma) = 2$.

3.1 Determinanta matrika

Definicija 3.2. *Determinanta matrike $A \in \mathbb{R}^{n \times n}$ je*

$$\det A = \sum_{\sigma \in S_n} \left(\mathrm{sgn}(\sigma) \prod_{i=1}^{n} a_{i\sigma(i)} \right).$$

Zgled 3.1. *Izpišimo determinanto splošne matrike za $n = 2$ in $n = 3$.*

$$\det \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} = a_{11}a_{22} - a_{12}a_{21}$$

$$\det \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{12}a_{21}a_{33} - a_{11}a_{23}a_{32} - a_{13}a_{22}a_{31}$$

Ker je število permutacij množice z n elementi enako $n!$, je tak način računanja determinante nepraktičen. Bolj običajno je računati determinanto z razvojem po vrstici ali stolpcu.

Izrek 3.1. *Ekvivalentno lahko determinanto matrike A definiramo preko razvoja po vrsticah ali po stolpcih*

$$\begin{aligned} \det A &= \sum_{k=1}^{n} (-1)^{k+1} a_{1k} \det A_{1k} \\ &= \sum_{k=1}^{n} (-1)^{k+1} a_{k1} \det A_{k1}, \end{aligned}$$

kjer je A_{ij} matrika, ki smo ji odvzeli i-to vrstico in j-ti stolpec. Omenimo še, da izrek drži, tudi ko namesto prve vrstice ali prvega stolpca opazujemo poljubno vrstico ali poljuben stolpec.

Dokaz izreka lahko bralec najde v [1], mi pa bomo dokazali, da definiciji sovpadata pri razvoju matrike 3×3 po prvi vrstici.

Zgled 3.2.

$$\begin{aligned} \det \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} &= a_{11} \cdot (a_{22}a_{33} - a_{23}a_{32}) - a_{12} \cdot (a_{21}a_{33} - a_{23}a_{31}) + a_{13} \cdot (a_{21}a_{32} - a_{22}a_{31}) \\ &= a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{12}a_{21}a_{33} - a_{11}a_{23}a_{32} - a_{13}a_{22}a_{31} \end{aligned}$$

Transponirana matrika neke matrike $A \in \mathbb{R}^{n\times m}$ je matrika $A^T \in \mathbb{R}^{m\times n}$, ki jo dobimo tako, da zamenjamo vrstice in stolpce matrike A, natančneje $[A^T]_{ij} = [A]_{ji}$. Bralca spomnimo še na nekaj uporabnih lastnosti pri računanju determinante.

Lema 3.1. *Naj bo $A \in \mathbb{R}^{n\times n}$ matrika. Zanjo veljajo naslednje lastnosti*

(a) $\det A^T = \det A$,

(b) če v A menjamo dve sosednji vrstici, se predznak determinante spremeni,

(c) če ima A vrstico samih ničel, potem je $\det A = 0$,

(d) če ima A dve enaki vrstici, potem je $\det A = 0$,

(e) če je A trikotna matrika, torej je $a_{ij} = 0$ za vse $i > j$, potem je $\det A = \prod_{i=1}^{n} a_{ii}$,

(f) $\det(-A) = (-1)^n \cdot \det A$,

(g) če poljubni vrstici v A prištejemo poljubno drugo vrstico v A se determinanta matrike ne spremeni.

Dokaz. Dokazali bomo le prvo izmed lastnosti. Dokaze ostalih lahko bralec poišče v [1]. Zaradi prve lastnosti veljajo preostale tudi če zamenjamo izraz vrstica z izrazom stolpec.
Prvo lastnost bomo dokazali z indukcijo po n. Baza indukcije $n = 1$ očitno velja, saj je taka matrika enaka sebi transponirani matriki. Za splošen n determinanto A^T razpišemo z razvojem po vrstici in uporabimo definicijo transponirane matrike ter indukcijsko predpostavko za podmatrike velikosti $(n-1)\times(n-1)$. Dobimo vsoto, ki je enaka determinanti matrike A preko razvoja po stolpcu.

$$\begin{aligned}
\det A^T &= \sum_{k=1}^{n} (-1)^{k+1} [A^T]_{1k} \det(A^T_{1k}) \\
&= \sum_{k=1}^{n} (-1)^{k+1} [A]_{k1} \det(A_{k1}) \\
&= \sum_{k=1}^{n} (-1)^{k+1} [A]_{k1} \det(A_{k1}) \\
&= \det A
\end{aligned}$$

□

Lema 3.2. *Naj bo $(k_1, \ldots, k_m)$ m-terica različnih celih števil med 1 in n ter naj bo $B \in \mathbb{R}^{n\times m}$. Z $B_{k_1,\ldots,k_m}$ označimo matriko B, v kateri vzamemo le vrstice $k_1, \ldots, k_m$ v tem vrstnem redu. Naj bo $(j_1, \ldots, j_m)$ enaka m-terica, vendar v naraščajočem vrstnem redu. Potem velja*

$$\det(B_{k_1,\ldots,k_m}) = \operatorname{sgn}(k_1, \ldots, k_m) \cdot \det(B_{j_1,\ldots,j_m})$$

Zgoraj smo s $\operatorname{sgn}(k_1, \ldots, k_m)$ označili signaturo permutacije na množici $\{j_1, \ldots, j_m\}$, ki slika element j_i v k_i.

Lema 3.3. *(Cauchy-Binetova formula) Naj bosta $A \in \mathbb{R}^{m\times n}$ in $B \in \mathbb{R}^{n\times m}$ matriki. Če je $n < m$, je* $\det(AB) = 0$, *sicer pa je*

$$\det(AB) = \sum_{\substack{S\subseteq\{1,\ldots,n\} \\ |S|=m}} \det A[S] \cdot \det B[S].$$

V zgornjem izrazu $A[S]$ označuje matriko A, v katerem obdržimo le stolpce z indeksi v množici S, istem vrstnem redu kot v originalni matriki. Podobno, $B[S]$ označuje matriko B, v kateri ohranimo le ustrezne vrstice.

Dokaz. Uporabimo definicijo determinante in nato še definicijo produkta matrik

$$\begin{aligned}
\det(AB) &= \sum_{\sigma\in S_m} \operatorname{sgn}(\sigma) \prod_{i=1}^{m} [AB]_{i\sigma(i)} \\
&= \sum_{\sigma\in S_m} \operatorname{sgn}(\sigma) \prod_{i=1}^{m} \left(\sum_{k=1}^{n} [A]_{ik} [B]_{k\sigma(i)} \right).
\end{aligned}$$

Permutacijo σ lahko razpišemo kot m-terico $(l_1, \ldots, l_m)$, kjer je $l_i = \sigma(i)$. Prav tako lahko razvijemo produkt vsot v izrazu

$$\begin{aligned}
&\sum_{1\le l_1,\ldots,l_m\le m} \operatorname{sgn}(l_1,\ldots,l_m)\left(\sum_{k=1}^{n}[A]_{1k}[B]_{k\sigma(1)}\right)\cdots\left(\sum_{k=1}^{n}[A]_{mk}[B]_{k\sigma(m)}\right)\\
&= \sum_{1\le l_1,\ldots,l_m\le m} \operatorname{sgn}(l_1,\ldots,l_m) \sum_{1\le k_1,\ldots,k_m\le n} [A]_{1k_1}\cdots[A]_{mk_m}\cdot[B]_{k_1 1}\cdots[B]_{k_m l_m}\\
&= \sum_{1\le l_1,\ldots,l_m\le m} \operatorname{sgn}(l_1,\ldots,l_m) \sum_{1\le k_1,\ldots,k_m\le n} \left(\prod_{i=1}^{m}[A]_{ik_i}\right)\left(\prod_{i=1}^{m}[B]_{k_i l_i}\right).
\end{aligned}$$

V zgornjem izrazu prvič seštevamo po vseh m-tericah $(l_1, \ldots, l_m)$, drugič pa po vseh m-tericah $(k_1, \ldots, k_m)$. Vrstni red teh dveh seštevanj lahko menjamo, člene tipa $[A]_{ik_i}$ pa lahko nesemo pred drugo vsoto

$$\begin{aligned}
&\sum_{1\le k_1,\ldots,k_m\le n}\ \sum_{1\le l_1,\ldots,l_m\le m} \operatorname{sgn}(l_1,\ldots,l_m)\left(\prod_{i=1}^{m}[A]_{ik_i}\right)\left(\prod_{i=1}^{m}[B]_{k_i l_i}\right)\\
&= \sum_{1\le k_1\ldots k_m\le n}\left(\prod_{i=1}^{m}[A]_{ik_i}\right)\sum_{1\le l_1\ldots l_m\le m} \operatorname{sgn}(l_1,\ldots,l_m)\left(\prod_{i=1}^{m}[B]_{k_i l_i}\right).
\end{aligned}$$

Desno stran izraza prepoznamo kot determinanto matrike B, v kateri obdržimo le vrstice $k_1, \ldots, k_m$, v tem vrstnem redu. Tako matriko bomo označili z $B_{k_1,\ldots,k_m}$.

$$\sum_{1\le k_1\ldots k_m\le n} [A]_{1k_1}\ldots[A]_{mk_m}\cdot\det(B_{k_1,\ldots,k_m})$$

Naj bo $(j_1, \ldots, j_m)$ urejena m-terica vrednosti iz $(k_1, \ldots, k_m)$ v nepadajočem vrstnem redu. Signaturo m-terice $(k_1, \ldots, k_m)$ definiramo preko števila inverzij m-terice (števila indeksov $i < j$, kjer je $k_i < k_j$). Signatura m-terice je -1, če je število inverzij liho, in 1, če je število inverzij sodo. Po lemi 3.2 vidimo, da je $\det(B_{k_1,\ldots,k_m}) = \operatorname{sgn}(k_1, \ldots, k_m)\det(B_{j_1,\ldots,j_m})$, torej

$$\sum_{1\le k_1,\ldots,k_m\le n} [A]_{1k_1}\ldots[A]_{mk_m}\cdot\operatorname{sgn}(k_1,\ldots,k_m)\cdot\det(B_{j_1,\ldots,j_m}).$$

Namesto, da seštevamo po vseh m-tericah $(k_1, \ldots, k_m)$, lahko iteriramo po vseh urejenih m-tericah $(j_1, \ldots, j_m)$ in njihovih permutacijah

$$\begin{aligned}
&\sum_{1\le j_1\le\cdots\le j_m\le n} \det(B_{j_1,\ldots,j_m})\sum_{\sigma\in S_m} sgn(\sigma)\prod_{i=1}^{m}[A]_{ij_{\sigma(i)}}\\
&= \sum_{1\le j_1\le\cdots\le j_m\le n} \det(B_{j_1,\ldots,j_m})\det(A_{j_1,\ldots,j_m})\\
&= \sum_{\substack{S\subseteq\{1,\ldots,n\}\\ |S|=m}} \det A[S]\cdot\det B[S],
\end{aligned}$$

kjer smo v zadnjih korakih prepoznali determinanto matrike A, v kateri obdržimo le stolpce, ki ustrezajo m-terici $(j_1, \ldots, j_m)$, in upoštevaje 3.1 (d) vzeli v poštev le tiste m-terice $(j_1, \ldots, j_m)$, ki imajo paroma različne vrednosti. □

Iz zgornje leme sledi znana posledica izreka za kvadratne matrike. Naj bosta $A, B \in \mathbb{R}^{n\times n}$, potem je namreč $\det(AB) = \det A\cdot\det B$.

3.2 Lastna vrednost in lastni vektor

Povzemimo še nekaj ključnih definicij in izrekov iz linearne algebra, ki jih bomo koristili v nadaljevanju.

Lema 3.4. *Naj bo $A \in \mathbb{R}^{n\times n}$. Enačba $A \cdot v = \mathbf{0}$, kjer $\mathbf{0}$ označuje stolpični vektor z n ničlami in je neznanka vektor v, ima netrivialno rešitev natanko tedaj, ko je* $\det(A) = 0$.

Definicija 3.3. *Real število λ je **lastna vrednost** matrike $A \in \mathbb{R}^{n\times n}$, če obstaja neničelni vektor $v \in \mathbb{R}^n$, imenovan **lastni vektor**, tako da je $Av = \lambda \cdot v$. Izrazu* $\det(tI_n - A)$ *pravimo karakteristični polinom matrike A. Označimo ga s $p_A(t)$. V izrazu smo z I_n označili **identično matriko** dimenzije n. To je matrika, kjer je $a_{ij} = 1$ natanko tedaj, ko je $i = j$.*

Lema 3.5. *Matrika $A \in \mathbb{R}^{n\times n}$ ima lastno vrednost λ natanko tedaj, ko je $p_A(\lambda) = 0$.*

Dokaz. Po definiciji lastne vrednosti matrike obstaja neki neničelni vektor v, tako da je $Av = \lambda v = \lambda I_n v$. Enačbo lahko preuredimo v $\lambda I_n v - Av = 0$. Zaradi distributivnosti lahko vektor v izpostavimo in dobimo $(\lambda I_n - A)v = 0$. Vektor v je po predpostavki neničelni, zato je po lemi 3.4 velja $\det(\lambda I_n - A) = 0$, kar po definiciji karakterističnega polinoma velja, če in samo če je $p_A(\lambda) = 0$. □

4 Število vpetih dreves v grafu

Vrnimo se sedaj k prvotnem problemu. V splošnem nas zanima število vpetih dreves v nekem grafu. Najprej si bomo ogledali, kako lahko ta problem prevedemo na linearno algebro. Za to je treba svojemu grafu prirediti **orientacijo**, oziroma smer povezav. To pomeni, da vsaki povezavi med parom vozlišč določimo začetno in končno vozlišče. V nadaljevanju bomo videli, da lahko za rešitev problema izberemo poljubno orientacijo.

Definicija 4.1. *Naj bo $G = (V, E)$ graf s p vozlišči in q povezavami. Grafu lahko definiramo naslednje matrike.*

- ***Sosednostna matrika** $A(G)$ je matrika $\mathbb{R}^{p\times p}$, kjer je $[A(G)]_{ij}$ število povezav med vozliščema v_i in v_j. Ob naših predpostavkah je to število lahko le* 0 *ali* 1*, kjer je slednje mogoče samo, če $i \neq j$.*
- ***Incidenčna matrika** $M(G)$ je matrika $\mathbb{R}^{p\times q}$, za katero velja*

$$[M(G)]_{ij} = \begin{cases} -1, & \text{če ima povezava } e_j \text{ začetek v vozlišču } v_i, \\ 1, & \text{če ima povezava } e_j \text{ konec v vozlišču } v_i, \\ 0, & \text{če vozlišče } v_i \text{ ni krajišče povezave } e_j. \end{cases}$$

- ***Laplaceova matrika** $L(G)$ je matrika $\mathbb{R}^{p\times p}$, za katero velja*

$$[L(G)]_{ij} = \begin{cases} -m_{ij}, & \text{kadar } i \neq j, \\ d(v_i), & \text{kadar } i = j. \end{cases}$$

pri čemer z $d(v_i)$ označimo stopnjo vozlišča v_i in z m_{ij} število povezav med vozliščema v_i in v_j, neodvisno od njihove orientacije.

Ker je mogoče vsakemu grafu prirediti tovrstne matrike, lahko kombinatorični problem štetja vpetih dreves na grafu prevedemo na linearno algebro. Kjer je nedvoumno, o katerem grafu govorimo, bomo te tri matrike na kratko označili z A, M in L. Algebraično bomo dokazali Kirchhoffov izrek o številu vpetih dreves na grafu in tako tudi prišli do rešitve problema za hiperkocko H_n. Za dokaz izreka potrebujemo še naslednje leme.

Lema 4.1. *Naj bosta $M \in \mathbb{R}^{p\times q}$ incidenčna matrika in $L \in \mathbb{R}^{p\times p}$ Laplaceova matrika istega grafa. Potem je $MM^T = L$.*

Dokaz. Dimenziji MM^T in L sta očitni enaki. Treba je še dokazati le, da je $[MM^T]_{ij} = [L]_{ij}$ za vsaka indeksa $i, j \in \{1, 2, \ldots, p\}$. Po definiciji množenja matrik velja

$$\begin{aligned} [MM^T]_{ij} &= \sum_{k=1}^{q} [M]_{ik}[M^T]_{kj} \\ &= \sum_{k=1}^{q} [M]_{ik}[M]_{jk}. \end{aligned}$$

Zdaj ločimo primera, ko je $i \neq j$ oziroma $i = j$.

1. Če velja $i \neq j$ in želimo, da $[M]_{ik}[M]_{jk} \neq 0$, morata biti vozlišči v_i in v_j povezani. Po definiciji incidenčne matrike ena od vrednosti $[M]_{ik}$ in $[M]_{jk}$ pri nekem $k \in \{1, 2, \ldots, q\}$ zavzema vrednost -1, druga pa 1, torej je produkt $[M]_{ik}[M]_{jk}$ enak -1. Vsota $\sum_{k=1}^{q}[M]_{ik}[M]_{jk}$ je potem enaka nasprotni vrednosti števila povezav med vozlišči v_i in v_j, kar ustreza definiciji Laplaceove matrike L.
2. Če velja $i = j$, je
$$[M]_{ik}[M]_{jk} = [M]_{ik}^2,$$
iz česar sledi
$$[MM^T]_{ii} = \sum_{k=1}^{q}[M]_{ik}^2.$$
Za vozlišče v_i, ki sovpada s k-to povezavo, je vrednost $[M]_{ik}^2$ enaka 1, sicer pa 0. Potem je vsota $\sum_{k=1}^{q}[M]_{ik}^2$ enaka stopnji vozlišča $d(v_i)$ in je
$$[MM^T]_{ii} = d(v_i),$$
kar tudi ustreza definiciji Laplaceove matrike in zaključuje dokaz. □

Lema 4.2. *Naj bo G d-regularen graf s p vozlišči.*

1. *Velja $L(G) = dI_p - A(G)$.*
2. *Če ima matrika $A(G)$ lastne vrednosti $\lambda_1, \lambda_2, \ldots, \lambda_p$, potem ima matrika $L(G)$ lastne vrednosti $d - \lambda_1, d - \lambda_2, \ldots, d - \lambda_p$.*

Dokaz.

1. Če identično matriko I_p pomnožimo s skalarjem d, dobimo matriko
$$dI_p = \begin{bmatrix} d & 0 & \ldots & 0 \\ 0 & d & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & d \end{bmatrix}$$
in izraz $dI_p - A(G)$ je potem enak
$$\begin{bmatrix} d & 0 & \ldots & 0 \\ 0 & d & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & d \end{bmatrix} - \begin{bmatrix} 0 & a_{12} & \ldots & a_{1p} \\ a_{21} & 0 & \ldots & a_{2p} \\ \vdots & \vdots & \ddots & \vdots \\ a_{p1} & a_{p2} & \ldots & 0 \end{bmatrix} = \begin{bmatrix} d & -a_{12} & \ldots & -a_{1p} \\ -a_{21} & d & \ldots & -a_{2p} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{p1} & a_{p2} & \ldots & d \end{bmatrix}.$$
Vrednosti na diagonali matrika $dI_p - A(G)$ so enake d, kar je ravno stopnja vozlišča v_i. Vse ostale vrednosti a_{ij}, za katere $i \neq j$, so enake nasprotnim vrednostim elementov matrike $A(G)$, torej je razlika matrik $dI_p - A(G)$ ravno Laplaceova matrika $L(G)$ grafa G.
2. Naj bosta λ_i lastna vrednost in v_i lastni vektor matrike $A(G)$. Vemo, da velja $\lambda_i v_i = A(G)v_i$ in $L(G) = dI_p - A(G)$, iz česar sledi
$$\begin{aligned} L(G)v_i &= (dI_p - A(G))v_i \\ &= dv_i - A(G)v_i \\ &= (d - \lambda_i)v_i. \end{aligned}$$
Potem je $d - \lambda_i$ lastna vrednost in v_i lasten vektor matrike $L(G)$, kar zaključuje dokaz. □

Definicija 4.2. *Naj bo $G = (V, E)$ graf in $M(G)$ njegova incidenčna matrika.* ***Reducirana incidenčna matrika*** *$M_0(G)$ je matrika $M(G)$, ki ji odstranimo zadnjo vrstico.*

Lema 4.3. *Naj bo G povezan graf s p vozlišči in q povezavami in naj bo S podmnožica $p - 1$ povezav. Potem je*
$$\det M_0[S] = \begin{cases} \pm 1, & \text{če povezave v } S \text{ tvorijo vpeto drevo in} \\ 0, & \text{če povezave v } S \text{ ne tvorijo vpetega drevesa,} \end{cases}$$
kjer $M_0[S]$ označuje matriko M_0, v kateri obdržimo le stolpce, ki ustrezajo povezavam iz S.

Dokaz. Naj bo M incidenčna matrika grafa G in naj bo $e_k \in E$ neka povezava, ki ima v_p za eno izmed krajišč. Naj bo $M_0[S]$ matrika, katere množica povezav S tvori vpeto drevo T.krajišče Vemo, da elementi m_{ij} matrike $M_0[S]$ zavzemajo vrednosti ± 1, če predstavljajo konce oziroma začetke povezav v S, ali 0, če ne tvorijo nobene povezave.

Matriki $M_0[S]$ odstranimo stolpec, ki ustreza povezavi e_k, ter vrstico, ki ustreza drugemu krajišču povezave e_k in dobimo matriko $M_0'[S] \in \mathbb{R}^{(p-2)\times(p-2)}$. Determinanto matrike $M_0[S]$ izračunamo z razvojem po stolpcu. Vse vrednosti v vrstici in stolpcu, ki smo ju odstranili, razen tiste, ki določa začetek oziroma konec povezave e, so enake 0, zato velja enakost

$$\det M_0[S] = \pm \det M_0'[S].$$

Ko matriki $M_0[S]$ odstranimo stolpec in vrstico, odstranimo povezavo e_k in združimo vozlišči, ki ju e_k povezuje, ter tako dobimo drevo T'. Potem lahko z indukcijo dokažemo, da je $\det M_0' = \pm 1$, iz česar res sledi $\det M_0[S] = \pm 1$.

Obravnavajmo še primer, ko množica povezav S ne tvori vpetega drevesa. Po lemi 2.2(c) ta množica vsebuje usmerjene povezave $e_1, \ldots, e_r$, ki tvorijo cikel. Naj bo $v = [v_1, \ldots, v_{p-1}]$ neničelni vektor, definiran z

$$v_i = \begin{cases} 1, & \text{če med obhodom cikla prepotujemo povezavo } e_i \text{ v smeri njene usmeritve,} \\ -1, & \text{če med obhodom cikla prepotujemo povezavo } e_i \text{ v nasprotni smeri,} \\ 0, & \text{če povezave } e_i \text{ ne prepotujemo.} \end{cases}$$

Opazimo, da dobimo

$$M_0[S] \cdot v = 0.$$

Vektor v tukaj ne more biti ničelni vektor, saj mora cikel, katerega prepotujemo imeti vsaj tri povezave, iz česar po lemi 3.4 sledi

$$\det M_0[S] = 0.$$

□

V dokazu smo videli, da je determinanta matrike $M_0[S]$ neodvisna od izbire orientacije povezav v G. V nadaljevanju bomo uporabljali incidenčno matriko zgolj v kontekstu njene determinante, ki je sedaj dobro definirana. Sedaj lahko dokažemo Kirchhoffov izrek, ki nam pove število vpetih dreves na grafu. Dokaze nekaterih lem in posledic, ki jih bomo zaradi njihove malovažnosti izpustili, lahko bralec poišče v [3].

Izrek 4.1 (Kirchhoffov izrek)**.** *Naj bo G povezan graf in naj bo L njegova Laplaceova matrika. Z L_0 označimo Laplaceovo matriko L, ki smo ji vzeli zadnji stolpec in zadnjo vrstico. Potem je število vpetih dreves na grafu G enako*

$$\kappa(G) = \det L_0.$$

Dokaz. Po lemi 4.1 je $L = MM^T$, iz česar sledi $L_0 = M_0 M_0^T$. Determinanto matrike L_0 lahko potem izračunamo s pomočjo Cauchy-Binetove formule in lastnosti 3.1(a) ter dobimo

$$\begin{aligned} \det L_0 &= \sum_{\substack{|S|=p-1 \\ S\subseteq\{1,2,\ldots,q\}}} (\det M_0[S])(\det M_0^T[S]) \\ &= \sum_{\substack{|S|=p-1 \\ S\subseteq\{1,2,\ldots,q\}}} (\det M_0[S])^2. \end{aligned}$$

Zaradi leme 4.3 je $\det M_0[S] = \pm 1$, kadar povezave v S tvorijo vpeto drevo, oziroma je $\det M_0[S] = 0$, če povezave ne tvorijo vpetega drevesa. Sledi, da je v primeru, da povezave v S tvorijo vpeto drevo, $(\det M_0[S])^2 = 1$, in v nasprotnem primeru $(\det M_0[S])^2 = 0$, torej je res $\kappa(G) = \det L_0$. □

4.1 Število vpetih dreves na hiperkocki H_n

S pomočjo Kirchhoffovega izreka lahko potem rešimo začetni problem in izračunamo število vpetih dreves na hiperkocki H_n. Vemo, da je število vpetih dreves na grafu G enako $\kappa(G) = \det L_0$. Izkaže se, da lahko s pomočjo naslednje leme izrek poenostavimo tako, da za izračun števila vpetih dreves potrebujemo zgolj lastne vrednosti grafu prirejene sosednostne ali Laplaceove matrike.

Lema 4.4. *Naj bo $L \in \mathbb{R}^{p\times p}$ matrika, v kateri je vsota po vrsticah in stolpcih enaka 0 in L_0 matrika, ki nastane, če matriki L odstranimo zadnji stolpec in vrstico. Potem je koeficient pred t v karakterističnem polinomu* $\det(tI - L)$ *enak*

$$(-1)^{p-1}p \det L_0.$$

Dokaz. Naj bo $L \in \mathbb{R}^{p\times p}$ takšna matrika, da je vsota po vsaki vrstici in stolpcu v njej enaka 0. Izraz $tI - L$ je potem enak

$$tI - L = \begin{bmatrix} t - l_{11} & -l_{12} & \dots & -l_{1p} \\ -l_{21} & t - l_{22} & \dots & -l_{2p} \\ \vdots & \vdots & \ddots & \vdots \\ -l_{p1} & -l_{p2} & \dots & t - l_{pp} \end{bmatrix}.$$

Če k zadnji vrstici matrike $tI - L$ prištejemo ostale vrstice te matrike, bodo vse vrednosti v njeni zadnji vrstici enake t, saj je vsota po stolpcu v L enaka 0. Nato iz zadnje vrstice izpostavimo t in novo matriko označimo z $N(t)$. Ker prištevanje vrstic ne spremeni determinante matrike (lema 3.1(g)), je

$$\det(tI - L) = t \det N(t)$$

in koeficient pred t polinoma $\det(tI - L)$ je enak $\det N(0)$.

Potem k zadnjemu stolpcu matrike $N(0)$ prištejemo vse ostale stolpce. Opazimo, da so vrednosti v zadnjem stolpcu enake 0, razen zadnje, ki je enaka p. Če zdaj z razvojem po zadnjem stolpcu izračunamo determinanto te matrike, po lemi 3.1(f) dobimo

$$\det N(0) = p \det(-L_0) = p(-1)^{p-1} \det L_0,$$

iz česar sledi, da je koeficient enak $(-1)^{p-1}p \det L_0$. □

Posledica 4.1.

(a) Naj bo G povezan graf s p vozlišči, in naj bodo lastne vrednosti matrike $L(G)$ enake $\mu_1, \mu_2, \dots, \mu_p$, da velja $\mu_p = 0$.[1] *Potem je*

$$\kappa(G) = \frac{1}{p}\mu_1\mu_2 \cdots \mu_{p-1}.$$

(b) Naj bo G d-regularen graf in naj bodo $\lambda_1, \lambda_2, \dots, \lambda_p$, kjer je $\lambda_p = d$, lastne vrednosti matrike $A(G)$. Potem velja

$$\kappa(G) = \frac{1}{p}(d - \lambda_1)(d - \lambda_2) \cdots (d - \lambda_{p-1}).$$

Ker je hiperkocka n-regularen graf, potrebujemo za izračun števila njej vpetih dreves zgolj lastne vrednosti njene sosednostne matrike, kar imenujemo **spekter** grafa. Računanja lastnih vrednosti kocke H_3 se lahko bralec loti sam, v splošnem pa bomo za izračun spektra hiperkocke potrebovali naslednjo lemo, ki je pa ne bomo dokazali.

Lema 4.5. *Naj bosta G in H grafa s sosednostnima matrikama $A(G)$ in $A(H)$. Če imata matriki $A(G)$ in $A(H)$ zaporedoma lastne vrednosti $\alpha_1, \dots, \alpha_m$ ter $\beta_1, \dots, \beta_n$, ima matrika $A(G \times H)$ mn lastnih vrednosti oblike*

$$\{\alpha_i + \beta_j \mid i \in \{1, 2, \dots, m\} \text{ in } j \in \{1, 2, \dots, n\}\}.$$

Hiperkocka H_n je enaka kartezičnemu produktu

$$H_n = \underbrace{P_2 \times \cdots \times P_2}_{\text{n-krat}},$$

pri čemer je P_2 pot z dvema vozliščema, katere sosednostna matrika ima lastni vrednosti $\lambda_1 = 1$ in $\lambda_2 = -1$. Iz tega sledi, da ima H_n natanko 2^n lastnih vrednosti tipa $2i$, kjer je $i \in \{-n, \dots, n\}$ in se vsaka pojavi $\binom{n}{i}$-krat. Če to vstavimo v enačbo iz posledice 4.1(b), dobimo

[1] Bralec se lahko prepriča, zakaj ima matrika $L(G)$, kjer je vsota po vrsticah 0, zmeraj lastno vrednost $\mu_p = 0$. Podobno velja za matriko $A(G)$, kjer imamo, da je vsota po vrsticah d, kar nam zagotavlja lastno vrednost $\lambda_p = d$.

$$\begin{aligned}\kappa(H_n) &= \frac{1}{2^n}\prod_{i=1}^{2^n}(n-\lambda_i)\\ &= \frac{1}{2^n}\prod_{i=1}^{n}(2i)^{\binom{n}{i}}\\ &= 2^{2^n-n-1}\prod_{i=1}^{n} i^{\binom{n}{i}}\end{aligned}$$

in s tem tudi število vpetih dreves poljubne hiperkocke H_n.

Če se vrnemo k prvotnemu problemu pa ugotovimo, da je število vpetih dreves v kocki enako 384. Za konec pa v tabeli 2 navedimo še nekaj vrednosti za majhne n.

n	$\kappa(H_n)$
1	1
2	4
3	384
4	42467328
5	$\sim 2.08 \times 10^{19}$

Tabela 2: Število vpetih dreves v hiperkocki H_n za $n \leq 5$.

5 Zaključek

Prvoten kombinatorični problem štetja sistemov rovov asterokubida smo prevedli na problem štetja vpetih dreves v kocki. S pomočjo Kirchoffovega izreka smo ta problem rešili za splošen povezan graf ob predpostavki, da poznamo lastne vrednosti njegove Laplaceove matrike oz. njegov spekter, če gre za d-regularen graf. Tega smo za hiperkocko tudi izračunali in ugotovili, da se bodo MaRSovci pošteno namučili z evalvacijo vseh 384 možnih sistemov rovov asterokubida.

Literatura

[1] Artin, M. (2011). Algebra. Addison-Wesley Longman.

[2] Juvan, M., Potočnik, P. (2000). Teorija grafov in kombinatorika: primeri in rešene naloge.

[3] Stanley, R. P. (2011). Enumerative combinatorics: Cambridge University Press.

Teorija kodiranja in Hammingov kod

Vaj Filej, Janoš Ivanec
Mentor: *Juš Kocutar*

Povzetek

Obravnavane so osnove teorije kodiranja. Definirani so linearni kodi, dimenzija in minimalna razdalja. Predstavljen je Hammingov kod in kako je z njim povečana verjetnost pravilno poslanih sporočil.

1 Uvod

Želimo modelirati, kako lahko pošiljamo sporočila v resničnem življenju. Vsako sporočilo pretvorimo v zaporedje simbolov, ki so 0 ali 1. Pošiljatelj pošlje zaporedje preko nekega kanala in prejemnik ga dobi. V resničnem življenju se pri prenosu sporočila skozi vsak kanal lahko zgodijo napake. To pomeni, da se kakšen simbol spremeni iz 0 v 1, ali pa, da ga ne moremo določiti. Ideja teorije kodiranja je, da sporočilu, ki ga želimo poslati, dodamo nekaj bitov in s tem poskrbimo, da niso vse oblike sporočil dovoljene.

Poglejmo problem na preprostem primeru. Recimo, da želimo poslati sporočilo štirih bitov in vemo, da je verjetnost, da se vsak bit pokvari, enaka p. Predpostavimo tudi, da je verjetnost, da se en bit pokvari, neodvisna od tega, ali se drugi pokvarijo. Sledi, da je verjetnost, da se celo sporočilo štirih bitov prenese pravilno, enaka $(1-p)^4$. Za $p = 4\%$ to pomeni, da je verjetnost, da bo celotno sporočilo pravilno, enaka $\approx 85\%$. Naš cilj je, s čim manj dodanih bitov, povečati verjetnost pravilno prenesenega sporočila.

2 Osnovne definicije

2.1 Kodi

Najprej bomo definirali množico vseh možnih zaporedij neke dolžine. Elementu množice $\{0,1\}$ pravimo **bit**.

Definicija 2.1. *Označimo s $\mathbb{F}_2^n$ množico vseh možnih zaporedij dolžine n, kjer je n naravno število, s členi v $\{0,1\}$. Velja torej*

$$\mathbb{F}_2^n = \{(a_1, a_2, a_3, \ldots, a_n) : \ a \in \{0,1\}, \ n \in \mathbb{N}\}.$$

Za množico dovoljenih simbolov (t.i. abecedo) bi si namesto $\{0,1\}$ lahko izbrali poljubno množico, na primer slovensko abecedo $\{A, B, \ldots, Z, \check{Z}\}$. Dva razloga, zakaj si izberemo množico z dvema elementoma, sta, da je to najmanjše število simbolov, ki naredi zanimivo množico zaporedij dolžine n. Drugi razlog je, da sta 0 in 1 osnovna simbola v računalništvu, od koder izvirajo praktični problemi, ki so motivirali razvoj teorije kodiranja.

Na množici bitov $\{0,1\}$ definiramo operacijo seštevanja s predpisi

$$\begin{aligned} 1+1 &= 0, \\ 1+0 &= 1, \\ 0+1 &= 1, \\ 0+0 &= 0. \end{aligned}$$

Ta operacija je enaka operaciji seštevanja ostankov po modulu 2, ali pa logičnim vratom XOR. Lahko preverimo, da je zgornje seštevanje asociativno in komutativno.

Seštevanje na množici $\{0,1\}$ lahko prenesemo na množico $\mathbb{F}_2^n$ tako, da seštevamo komponente. Za poljubna elementa

$$x = (a_1, a_2, \ldots, a_n),\ y = (b_1, b_2, \ldots, b_n) \in \mathbb{F}_2^n$$

definiramo njuno vsoto kot

$$x + y = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n).$$

Definicija 2.2. ***Kod*** *C je podmnožica množice $\mathbb{F}_2^n$.*

Namen definicije „koda“ je, da predstavlja množico vseh *dovoljenih* zaporedij bitov. Zato, da lahko prejemnik sporočila zazna ali popravi potencialne napake, ki so nastale pri prenosu sporočila skozi kanal, je bistveno, da dovoljena zaporedja niso vsi elementi $\mathbb{F}_2^n$. Če bi vsa sporočila dolžine n bila dovoljena, bi prejemnik sporočila mislil, da so bila dejansko poslana sporočila z napakami.

Namesto $(a_1, a_2, \ldots, a_n)$ bomo elemente množice $\mathbb{F}_2^n$ pisali kot $a_1a_2\ldots a_n$; na primer $(1,0,1) = 101$. Zaporedje $00\ldots00$ bomo pogosto označili kar s simbolom 0 in bo razvidno iz konteksta, ali mislimo na zaporedje z ničlami ali bit 0.

V naslednjem primeru bomo vzeli $n = 3$ in si ogledali kod $C \subset \mathbb{F}_2^3$, kjer je

$$\mathbb{F}_2^3 = \{000, 001, 010, 011, 100, 101, 110, 111\},$$

$$C = \{000, 011, 101, 110\}.$$

Opazimo lahko, da je v zgornjemu kodu C zadnji bit v zaporedju enak vsoti prvih dveh bitov po prej definiranem seštevanju na množici $\{0,1\}$. Zaradi tega pravila je število vseh elementov v kodu enako $2 \cdot 2 = 4$, saj imamo dve možnosti za vsakega od prvih bitov, tretji pa je z njima že določen.

2.2 Hammingova razdalja

Poskusimo definirati razdaljo med dvema poljubnima zaporedjema v množici $\mathbb{F}_2^n$. Želimo, da sta si dve zaporedji blizu, če imata več enakih bitov na enakih mestih v zaporedju. To lahko storimo s pomočjo Hammingove razdalje, ki primerja dve zaporedji in zazna vsa mesta v zaporedjih, v katerih se razlikujeta. Razdalja je potem enaka številu vseh mest, v katerih se razlikujeta.

Definicija 2.3. *Za poljubna elementa $x = a_1a_2\ldots a_n$ in $y = b_1b_2\ldots b_n \in \mathbb{F}_2^n$ definiramo* ***Hammingovo razdaljo*** *$d(x,y)$ kot*

$$d(x,y) = |\{i :\ a_i \neq b_i,\ 1 \leq i \leq n\}|.$$

Za Hammingovo razdaljo velja trikotniška neenakost.

Izrek 2.1 (Trikotniška neenakost)**.** *Naj bodo $x, y, z \in \mathbb{F}_2^n$. Potem velja*

$$d(x,y) \leq d(x,z) + d(z,y).$$

Dokaz. Naj bodo $x = a_1a_2\ldots a_n,\ y = b_1b_2\ldots b_n$ in $z = c_1c_2\ldots c_n$. Trdimo, da velja

$$\{i :\ a_i \neq b_i\} \subseteq \{j :\ a_j \neq c_j\} \cup \{k :\ b_k \neq c_k\}.$$

Denimo, da imata x in y različna bita na mestu l, torej $l \in \{i;\ a_i \neq b_i\}$. Potem velja, da ima zaporedje z na mestu l različen bit ali od x ali od y. V nasprotnem primeru bi imeli vsi trije elementi enak bit na mestu l, kar vemo, da ne drži. Zato velja naslednja veriga neenakosti

$$\begin{aligned} d(x,y) &= |\{i :\ a_i \neq b_i\}| \\ &\leq |\{j :\ a_j \neq c_j\} \cup \{k :\ b_k \neq c_k\}| \\ &\leq |\{j :\ a_j \neq c_j\}| + |\{k :\ b_k \neq c_k\}| \\ &= d(x,z) + d(z,y), \end{aligned}$$

kar smo želeli dokazati. □

Na primer, zaporedji $10000, 10011 \in \mathbb{F}_2^5$ se razlikujeta v dveh bitih, in sicer na četrtem in petem mestu, zato je njuna Hammingova razdalja enaka

$$d(10000, 10011) = 2.$$

Na poseben način bomo poimenovali razdaljo do zaporedja $00\ldots00$.

Definicija 2.4. ***Težo*** *zaporedja $w \in \mathbb{F}_2^n$, ki jo označimo z $|w|$, definiramo kot Hammingovo razdaljo med zaporedjem, ki ima vse člene 0, in zaporedjem w, torej*

$$|w| = d(0, w).$$

2.3 Minimalna razdalja

Minimalna razdalja koda je najmanjša možna razdalja med dvema različnima elementoma koda. Koncept minimalne razdalje je pomemben, ker bo igral vlogo pri številu napak, ki jih lahko kod zazna ali popravi. Večja kot je minimalna razdalja, več jih lahko popravi.

Definicija 2.5. *Naj bo $C \subset \mathbb{F}_2^n$ kod.* ***Minimalna razdalja*** *koda C je najmanjša možna razdalja d med poljubnima različnima elementoma $x, y \in C$, torej*

$$d = \min\{d(x, y) : \ x \neq y, \ x, y \in C\}.$$

Rečemo, da lahko kod $C \subset \mathbb{F}_2^n$ *popravi* m napak, če lahko prejemnik sporočila ob predpostavki, da se je zgodilo največ m napak, točno določi, katero sporočilo je bilo poslano. Podobno pravimo, da lahko kod $C \subset \mathbb{F}_2^n$ *zazna* l napak, če lahko prejemnik sporočila ob predpostavki, da se je zgodilo največ l napak, določi, da se je pri prenosu sporočila zgodila napaka.

Izrek 2.2. *Naj bo $C \subset \mathbb{F}_2^n$ kod z minimalno razdaljo d. Največje število napak, ki jih kod C lahko zazna, je $d-1$. Največje število napak, ki pa jih lahko popravi, je $\left\lfloor \frac{d-1}{2} \right\rfloor$.*

Dokaz. Najprej dokažimo, da lahko kod popravi $\left\lfloor \frac{d-1}{2} \right\rfloor$ napak. Predpostavimo, da je napak največ $\left\lfloor \frac{d-1}{2} \right\rfloor$. Radi bi pokazali, da lahko vsakemu zaporedju z, ki ima največ toliko napak, priredimo enoličen element koda, ki je temu sporočilu najbližji. To sporočilo je tisto, ki ga je pošiljatelj poslal, preden je prišlo v kanal.

Enoličnost takega elementa iz koda lahko dokažemo s protislovjem. Recimo da za dva različna elementa x, y v kodu velja

$$d(x, z) \leq \left\lfloor \frac{d-1}{2} \right\rfloor \quad \text{in} \quad d(y, z) \leq \left\lfloor \frac{d-1}{2} \right\rfloor.$$

Po definiciji minimalne razdalje velja $d \leq d(x, y)$. Dobimo naslednjo verigo neenakosti

$$\begin{aligned} d &\leq d(x, y) \\ &\leq d(x, z) + d(z, y) \\ &\leq \left\lfloor \frac{d-1}{2} \right\rfloor + \left\lfloor \frac{d-1}{2} \right\rfloor \\ &\leq \frac{d-1}{2} + \frac{d-1}{2} \\ &= d - 1. \end{aligned}$$

Sledi, da velja $d \leq d-1$, kar je protislovje, zato obstaja največ en element koda C, ki je zaporedju z najbližji.

Naslednje, kar bomo pokazali, je, da lahko ob predpostavki največ $d-1$ napak, zaznamo, ali se je zgodila napaka.

Recimo, da prejemnik prejme sporočilo $z \in \mathbb{F}_2^n$ in ve, da se je zgodilo največ $d-1$ napak. Če zaporedje z ni v kodu, prejemnik ve, da se je zgodila napaka. Če pa element z je v kodu, pa je nemogoče, da je bilo dejansko poslano neko drugo sporočilo iz koda, saj bi potem razdalja med poslanim in prejetim sporočilom bila manjša ali enako $d-1$, kar je manj od minimalne razdalje. Idejno to preprosto pomeni, da ne moremo „skočiti“ od enega kodnega sporočila do drugega.

□

2.4 Linearni kodi

Sedaj bomo definirali posebne vrste kodov, ki jih bomo obravnavali do konca članka.

Definicija 2.6. ***Linearen kod*** *$C \subset \mathbb{F}_2^n$ je kod z lastnostjo, da za poljubna $x, y \in C$ velja $x + y \in C$.*

Definicija pravi, da če dva elementa iz koda C seštejemo, potem bo tudi njun seštevek element kode. Njihova prednost je, da lahko iz majhnega števila baznih elementov sestavimo poljubni element koda z uporabo seštevanja. Primer linearnega koda je $C \subset \mathbb{F}_2^4$ z elementi $C = \{0000, 0011, 1100, 1111\}$. Če seštejemo elementa $\{0011\}$ in $\{1100\}$, dobimo $\{1111\}$, ki je v kodu.
Primer koda, ki ni linearen, je $C = \{10, 01\}$, saj elementa $10 + 01 = 11$ ni v tem kodu.

Izkaže se, da pri linearnem kodu za določitev minimalne razdalje ni potrebno primerjati vsakega elementa z vsakim, temveč je dovolj primerjati en element z vsemi.

Izrek 2.3. *Naj bo $C \subset \mathbb{F}_2^n$ linearen kod. Potem je minimalna razdalja koda C enaka*

$$d = \min\{|z| : \ z \in C, \ z \neq 0\}.$$

Dokaz. Po definiciji obstajata različna elementa $u = u_1u_2 \cdots u_n$ in $v = v_1v_2 \cdots v_n, \in C$, za katera velja $d(u, v) = d$. Prištejemo elementoma u in v poljuben element $w = w_1w_2 \dots w_n \in \mathbb{F}_2^n$ in izračunajmo $d(u + w, v + w)$.

Opazimo, da za poljubno koordinato i velja $u_i = v_i$, če in samo če je $u_i + w_i = v_i + w_i$, zato sta množici $\{i : \ a_i \neq b_i\}$ in $\{j : \ a_j + w_j \neq b_j + w_j\}$ enaki in po definiciji velja $d(u, v) = d(u + w, v + w)$.

Če izberemo $w = v$, vemo, da je $u + v$ element C, saj je kod C linearen. Vemo torej naslednje

$$d = d(u, v) = d(u + v, v + v) = d(u + v, 0).$$

Sklepamo, da je minimalna razdalja enaka teži elementa $u + v$ iz C, kar smo želeli dokazati. □

Za primer vzamimo naslednji linearen kod $C \subset \mathbb{F}_2^3$

$$C = \{000000, 111111, 111000, 000111\}; \quad |111000| = 3.$$

Minimalna razdalja je po izreku 2.3 enaka najmanjši teži elementa koda C. Hitro preverimo, da je najmanjša teža elementa koda C enaka 3, zato je minimalna razdalja koda C enaka 3.

2.5 Dimenzija

Izkaže se, da linearni kodi ne morejo imeti poljubne velikosti, ampak da je njihova velikost vedno potenca števila 2.

Izrek 2.4. *Naj bo $C \subset \mathbb{F}_2^n$ linearni kod. Potem velja $|C| = 2^k$ za neko naravno število $0 \leq k \leq n$.*

Dokaz. Definirajmo kod $C' \subset \mathbb{F}_2^{n-1}$ kot kod, ki ga sestavljajo zaporedja iz prvih $n - 1$ bitov koda C. Kod C' je linearen, saj ima enake lastnosti kot kod C, samo da pozabimo na zadnji bit. Na C' lahko gledamo kot sliko preslikave $\pi \colon \mathbb{F}_2^n \to \mathbb{F}_2^{n-1}$, ki slika element $(a_1, a_2, \dots, a_{n-1}, a_n)$ v element $(a_1, a_2, \dots, a_{n-1})$. Obravnavamo lahko dve možnosti.

1. Če je zožitev preslikave π na C injektivna, potem velja $|C'| = |C|$.
2. Zožitev preslikave π na C ni injektivna. V kodu C sta potem po definiciji različna elementa u in v, za katera velja $u = t_1t_2 \dots t_{n-1}0$ in $v = t_1t_2 \dots t_{n-1}1$. Ker je C linearen kod je njuna vsota $u + v = 00 \cdots 001$ v C. Po definiciji C' za vsak $w \in C'$ obstaja vsaj en element iz C, ki ga π slika v w. Velja tudi, da za vsak $w \in C'$ obstajata največ dva elementa iz C, ki se slikata v w, saj je prvih $n - 1$ bitov že določenih, zadnji pa je lahko ali 0 ali 1.

   Trdimo, da za vsak $w \in C'$ obstajata natanko dva elementa $z_1, z_2 \in C$, ki ju π slika v w. V kodu C je element $00 \cdots 001$ in kod C je linearen. Če torej za $z \in C$ velja $\pi(z) = w$, potem je drugi element iz C, ki se slika v w, enak $z + 00 \cdots 001$.

   Zato je v kodu C natanko dvakrat toliko elementov kot v kodu C'.

Vemo torej, da je moč množice C' enaka

$$|C'| = \begin{cases} |C|; & \pi|_C \text{ je injektivna,} \\ \frac{1}{2}|C|; & \pi|_C \text{ ni injektivna.} \end{cases}$$

Postopek lahko ponovimo na kodu C', saj je kod C' linearen in ima dolžino $n-1$. Nato postopek ponovimo še $(n-1)$-krat. V zadnjem koraku dobimo kod, ki je enak $\{0\}$ ali $\{0,1\}$. Moč teh množic je enaka 1 ali 2, obe sta potenci 2, v vsakem koraku pa smo ali obdržali moč prejšnje množice ali pa jo razpolovili. Zato je moč prvotnega koda C enaka potenci števila 2.

□

Definicija 2.7. *Naj bo $C \subset \mathbb{F}_2^n$ linearen kod. Vemo, da je število elementov v kodu $C = 2^k$ za nek $k \in \mathbb{N}_0$. Eksponentu k pravimo* ***dimenzija*** *koda C.*

Za poljuben linearen kod definirajmo dimenzijo, ki je enaka eksponentu v potenci števila 2, ki nastopa v njeni moči. Lahko jo interpretiramo tudi kot število mest, ki jih zavzame sporočilo pri prenosu. Za primer lahko vzamemo naslednji linearen kod

$$C \subset \mathbb{F}_2^n, \quad C = \{0000, 0011, 1100, 1111\}.$$

Število elementov v C je 4, torej je dimenzija enaka 2.

Definicija 2.8. *Linearnemu kodu $C \subset \mathbb{F}_2^n$ z minimalno razdaljo d in dimenzijo k pravimo $[n, k, d]$-kod.*

3 Primeri kodov

3.1 Sodi kod

Definicija 3.1. ***Sodi kod*** *$E \subset \mathbb{F}_2^n$ je kod, ki vsebuje vsa zaporedja iz $\mathbb{F}_2^n$ s sodo težo, torej*

$$E = \{u \in \mathbb{F}_2^n : \ |u| \text{ je sodo število}\}.$$

Izrek 3.1. *Za vsak $n \in \mathbb{N}$ je sodi E kod linearen kod.*

Dokaz. Naj bosta $x, y \in E$ poljubna elementa. Želimo, dokazati, da je $x + y$ v E, kar po definiciji pomeni, da je $|x + y|$ sodo število.

Označimo število vseh mest v zaporedju, kjer ima zaporedje x bit 1 in zaporedje y bit 0, z a ter označimo število mest, kjer ima x bit 0 in y bit 1, z b. Nato dobimo

$$|x| = a + c,$$

$$|y| = b + c,$$

kjer c označuje število mest, na katerih imata x in y hkrati bit 1. Obe števili $|x|$ in $|y|$ sta sodi. Preštejemo število enic v $x + y$. Ugotovimo, da je to natanko $|x + y| = a + b$. To velja, ker se na vseh c mestih, kjer imata oba x in y bit 1, tisto mesto sešteje v 0.

Parnost števila $a + b$ je enaka parnosti $a + b + 2c = (a + c) + (b + c) = |x| + |y|$, ki pa je vsota dveh sodih števil po predpostavki in zato sodo število. Zato velja, da je $|x + y|$ sodo število s čimer smo pokazali, da je sodi kod E linearen kod. □

Primer sodega koda je $C \subset \mathbb{F}_2^3$,

$$C = \{000, 011, 101, 110\}.$$

Za $n \geq 2$ velja, da je minimalna razdalja sodega koda enaka $d = 2$, ker vedno obstaja element teže 2. Dimenzija k pa je za $n \geq 1$ enaka $n - 1$. To lahko vidimo, tako da pogledamo preslikavo

$$f \colon \mathbb{F}_2^n \to \mathbb{F}_2^n, \quad u \to u + 100\ldots00.$$

Opazimo, da je preslikava f bijektivna in da slika elemente s sodo Hammingovo težo v elemente z liho Hammingovo težo, in obratno.

Vemo torej, da je za $n \geq 2$ sodi kod vedno $[n, n-1, 2]$-kod, kar z uporabo izreka 2.2 pravi, da lahko vedno zaznamo največ eno napako, popraviti pa jih ne moremo.

3.2 Hammingov kod

Hammingov kod ima sedem bitov. Prvi štirje biti v njegovih zaporedjih so poljubni, naslednji trije pa so biti za določitev parnosti. Poljuben element H je oblike $d_1d_2d_3d_4p_1p_2p_3$, kjer so zadnji trije biti podani z naslednjimi enačbami

$$\begin{aligned} p_1 &= d_1 + d_2 + d_4, \\ p_2 &= d_1 + d_3 + d_4, \\ p_3 &= d_2 + d_3 + d_4. \end{aligned}$$

Pokazali bomo, da je Hammingov kod linearen kod, in določili njegovo minimalno razdaljo in dimenzijo.

Izrek 3.2. *Hammingov kod je linearen kod.*

Dokaz. Naj bosta $x = a_1a_2a_3a_4p_1p_2p_3 \in H$ in $y = b_1b_2b_3b_4q_1q_2q_3 \in H$ poljubna elementa. Želimo pokazati, da je $x + y$ element H. Prvi štirje biti vsote $x + y$ so enaki $a_1 + b_1, \ldots, a_4 + b_4$ in so lahko poljubni. Dejstvo, da so zadnji trije primerne oblike, pa je posledica komutativnosti in asociativnosti seštevanja na $\{0, 1\}$. Na primer, bit na petem mestu vsote $x + y$ je enak

$$\begin{aligned} p_1 + q_1 &= (a_1 + a_2 + a_4) + (b_1 + b_2 + b_4) \\ &= (a_1 + b_1) + (a_2 + b_2) + (a_4 + b_4), \end{aligned}$$

kar je natanko enako vsoti prvega, drugega in četrtega mesta vsote zaporedji $x + y$. Sklepanje ponovimo še za šesti in sedmi bit in ugotovimo, da je $x + y$ po definiciji element H. □

Izrek 3.3. *Hammingov kod H je $[7, 4, 3]$-kod.*

Dokaz. Po definiciji je $n = 7$. Dimenzija k je enaka 4, ker so prvi štirje biti poljubni, zadnji trije pa so točno določeni glede na prve štiri, torej je vseh elementov koda natanko $2 \cdot 2 \cdot 2 \cdot 2 = 16 = 2^4$.

Vemo, da je H linearen kod, zato lahko minimalno razdaljo d določimo z najmanjšo težo vseh 16 elementov koda. Vemo da je d največ 3, ker imamo v H element 1000110. Preveriti moramo vse elemente v kodu, ki imajo na prvih štirih mestih največ dva bita enaka 1. Ugotovimo, da je teža vseh takšnih elementov 3 ali 4. Zato je minimalna razdalja d natanko 3. □

Zadnji presenetljiv rezultat, ki nakazuje na uporabnost Hammingovega koda, je, da lahko H vedno popravi največ eno napako. To se na prvi pogled zdi presentetljivo, ker nismo niti podvojili števila vseh bitov prvotnega sporočila, ki je dolgo štiri bite. Velja namreč, da prvi štirje biti predstavljajo sporočilo, zadnji trije pa so dodatek.

Izrek 3.4. *Hammingov kod H lahko zazna 2 napaki in popravi 1.*

Dokaz. Uporabimo izrek 2.2 in dejstvo, da je minimalna razdalja $d = 3$, zato je $d - 1 = 2$ in $\left\lfloor \frac{d-1}{2} \right\rfloor = 1$. □

Sedaj lahko poskusimo rešiti problem iz uvoda. Želimo torej poslati sporočilo štirih bitov. Naj bo verjetnost, da se pri prenašanju sporočila en bit pokvari, enaka p in predpostavimo, da je verjetnost neodvisna od drugih bitov. Izračunajmo, kolikšna je verjetnost, da pravilno prenesemo sporočilo, če sporočilo prenesemo v Hammingovem kodu.

Verjetnost, da je celotno sporočilo brez napak, je $(1 - p)^7$, kar je manj kot $(1 - p)^4$ za sporočilo brez dodatka. Vendar so zdaj sprejemljiva tudi vsa sporočila, ki imajo natanko eno napako, ker jo lahko popravimo. Verjetnost da se bit pokvari pri poljubnem mestu je $p(1 - p)^6$, torej je skupna verjetnost pravilnega sporočila enaka

$$(1 - p)^7 + 7p(1 - p)^6.$$

Če vstavimo $p = 4\%$ kot v uvodu, sedaj verjetnost, da lahko prenesemo pravilno sporočilo, naraste na kar 97%. Torej nam je uspelo z uporabo Hammingovega koda povečati verjetnost pravilno poslanega sporočila iz 85% na 97%. Verjetnost je še veliko boljša za manjše p.

4 Zaključek

Predstavili smo problem napak pri prenašanju podatkov, sestavljenih iz zaporedij bitov. Definirali smo koncept koda in linearnega koda. Nato smo definirali dimenzijo koda, ki meri velikost dejanskega sporočila in minimalne razdalje, od katere je odvisno število napak, ki jih lahko zaznamo ali popravimo. Na koncu smo predstavili sodi kod in Hammingov kod. Slednji lahko zmeraj popravi eno napako, kljub temu, da niti ne podvojimo velikost sporočila.

Literatura

[1] J. Top, *Security & Codes*, dostopno na `https://www.rug.nl/staff/steffen.muller/security-and-codes-updated.pdf`

Vsote kvadratov

Lovro Kastelic, Marsela Supé Vide, Tija Vidmar
Mentor*: Izak Jenko*

Povzetek

V članku smo raziskovali, katera naravna števila so predstavljiva – jih je mogoče zapisati kot vsoto dveh popolnih kvadratov. Osredotočili smo se predvsem na praštevila. Definirali smo kongruentnost ter podrobno pojasnili in dokazali mali Fermatov izrek. Predstavljivost praštevil smo predstavili geometrijsko s pomočjo krilatih kvadratov. Dokazano smo nato uporabili za odgovor na vprašanje o predstavljivosti sestavljenih naravnih števil.

1 Uvod

Za vse so krivi Francozi. Mogoče se sprašujete, kaj imajo Francozi skupnega z vsotami dveh kvadratov, vendar vam zagotavljamo, da boste kmalu izvedeli, zakaj sta Fermat in Pascal pomembna.

Vsote dveh kvadratov predstavljajo zanimiv matematični koncept, ki spada v matematično področje, imenovano teorija števil. Že antični matematiki so se ukvarjali s to temo, ki se je skozi zgodovino razvila v eno najbolj fascinantnih področij matematike.

Definicija 1.1. *Pravimo, da je število $n \in \mathbb{N}$* ***predstavljivo****, če ga lahko zapišemo kot vsoto dveh popolnih kvadratov, torej če obstajata taki celi števili $x,\ y \in \mathbb{Z}$, da je*

$$n = x^2 + y^2.$$

Opomba 1.1. *Celo število je* popoln kvadrat*, če je oblike k^2 za neko celo število $k \in \mathbb{Z}$. V nadaljevanju bomo zavoljo jedrnatosti pridevnik* popoln *pogosto izpuščali in popolne kvadrate imenovali samo kvadrati.*

Poglejmo naravna števila do 20 in jih poskusimo zapisati kot vsoto dveh kvadratov. Ugotovimo, da tak zapis ni mogoč za vsa števila, kot nas prepriča tabela 1. Naiven način, kako za naravno število n preverimo, ali je predstavljivo ali ne, je sledeč. Zapišemo si vse kvadrate pozitivnih celih števil, ki so manjši ali enaki n, in si ogledamo njihove razlike od n. Če je kakšna od teh razlik popoln kvadrat, smo našli zapis števila n kot vsoto dveh kvadratov in je torej predstavljivo, sicer pa ni predstavljivo. Na primer popolni kvadrati manjši ali enaki številu 19 so 0, 1, 4, 9 in 16, njihove razlike do 19 pa so zaporedoma 19, 18, 15, 10 in 3. Ker nobeno od teh *ni* popoln kvadrat, število 19 ni predstavljivo.

Tabela 1: Števila kot vsote dveh kvadratov.

$1 = 1^2 + 0^2$	$6 \neq$	$11 \neq$	$16 = 4^2 + 0^2$
$2 = 1^2 + 1^2$	$7 \neq$	$12 \neq$	$17 = 4^2 + 1^2$
$3 \neq$	$8 = 2^2 + 2^2$	$13 = 3^2 + 2^2$	$18 = 3^2 + 3^2$
$4 = 2^2 + 0^2$	$9 = 3^2 + 0^2$	$14 \neq$	$19 \neq$
$5 = 2^2 + 1^2$	$10 = 3^2 + 1^2$	$15 \neq$	$20 = 4^2 + 2^2$

Tekom tega članka bomo spoznali izrek, ki nam bo brez intenzivnega računanja povedal, kdaj je naravno število n predstavljivo, če le poznamo njegov praštevilski razcep.

1.1 Produkt kot vsota dveh kvadratov

Prvo splošno opazko o predstavljivih številih povzame naslednja trditev, ki pove, da je produkt predstavljivih števil spet predstavljivo število.

Trditev 1.1. *Če lahko dve naravni števili $n = x^2 + y^2$ in $m = z^2 + w^2$ napišemo kot vsoto dveh kvadratov, lahko tudi njun produkt zapišemo kot vsoto dveh kvadratov.*

Dokaz. Izračunamo

$$\begin{aligned} n \cdot m &= (x^2 + y^2)(z^2 + w^2) \\ &= x^2z^2 + x^2w^2 + y^2z^2 + y^2w^2 \\ &= x^2z^2 + x^2w^2 + y^2z^2 + y^2w^2 + 2xyzw - 2xyzw \\ &= (xz + yw)^2 + (xw - yz)^2. \end{aligned}$$

V tretji vrstici smo prišteli in odšteli $2xyzw$ in s tem dopolnili po dva člena iz druge vrstice do dveh popolnih kvadratov. □

2 Osnove teorije števil

2.1 Praštevila

Eden izmed najbolj osnovnih objektov v teoriji števil so *praštevila*. Praštevilo je naravno število večje od 1, katerega edina delitelja sta 1 in število samo. Njihovo pomembnost poudarja znameniti osnovni izrek aritmetike.

Izrek 2.1 (Osnovni izrek aritmetike)**.** *Vsako naravno število večje od* 1 *je produkt praštevil, ki je enoličen do vrstnega reda faktorjev natančno.*

V luči našega osnovnega problema, bomo znali s pomočjo faktorizacije odločiti o predstavljivosti sestavljenih števil, ko ugotovimo, katera praštevila so predstavljiva.

2.2 Osnovni izrek o deljenju

Spomnimo se osnovnega izreka o deljenju.

Izrek 2.2 (Osnovi izrek o deljenju)**.** *Naj bosta a in b poljubni celi števili, pri čemer $b \neq 0$. Če delimo a z b, potem obstajata celi števili q in ostanek r, da velja*

$$a = q \cdot b + r.$$

Ostanek je vedno večji ali enak 0 *in manjši od delitelja* ($0 \leq r < b$).

Številoma q in r iz zgornjega izreka pravimo *količnik* in *ostanek*. Naslednja trditev nam pove, da sta ti dve količini enolično določeni s številoma a in b, zato je na primer smiselno govoriti o *ostanku števila a pri deljenju z b*.

Trditev 2.1. *Za vsak par $a,\ b \in \mathbb{Z}$ sta števili q in r iz zgornjega izreka o deljenju enolična.*

Dokaz. Če bi za par $a,\ b \in \mathbb{Z}$ obstajal še en par $q',\ r' \in \mathbb{Z}$, za katerega je

$$a = q'b + r' \quad \text{in} \quad 0 \leq r' < b,$$

bi lahko število a zapisali na dva načina

$$q \cdot b + r = a = q' \cdot b + r'.$$

S preurejanjem enačbe dosežemo

$$(q - q')b = r' - r.$$

Ker je $|r' - r| < b$, sledi

$$|q - q'| < 1.$$

Števili q in q' sta celi, zato se slednje lahko to zgodi le, če sta enaki. Od tod sklepamo tudi $r = r'$. □

Definicija 2.1. *Če vzamemo števili $a,\ b \in \mathbb{Z}$, potem število b **deli** število a, ko obstaja število $k \in \mathbb{Z}$, da je*

$$a = k \cdot b.$$

*Pravimo tudi, da je število a **večkratnik** števila b. To označimo z $b \mid a$. Kadar število b* ne *deli a, pišemo tudi $b \nmid a$.*

Opazimo, da število b deli število a natanko tedaj, ko je ostanek a pri deljenju z b enak 0.

Trditev 2.2. *Denimo, da za $n \in \mathbb{N}$ in $a,\ b \in \mathbb{Z}$ velja $n \mid a$ in $n \mid b$, potem velja*

$$n \mid ab \quad in \quad n \mid a + b.$$

Dokaz. Zapišimo $a = a_0 n$ in $b = b_0 n$, kjer sta $a_0,\ b_0 \in \mathbb{Z}$. Potem lahko produkt teh števil zapišemo kot

$$\begin{aligned} ab &= a_0 b_0 n^2 \\ &= (a_0 b_0 n)n, \end{aligned}$$

iz česar je razvidno, da $n \mid ab$. Podobno velja tudi za vsoto dveh števil

$$\begin{aligned} a + b &= a_0 n + b_0 n \\ &= (a_0 + b_0)n, \end{aligned}$$

kar potrdi, da $n \mid a + b$. □

2.3 Kongruence

V nadaljevanju želimo računati z ostanki, kar formaliziramo z vpeljavo pojma *kongruentnosti* števil.

Definicija 2.2. *Dve števili $a,\ b \in \mathbb{Z}$ sta **kongruentni** po modulu n, kadar velja*

$$n \mid a - b.$$

To označimo z

$$a \equiv b \bmod n.$$

Trditev 2.3. *Kongruentni števili imata pri deljenju z n isti ostanek.*

Dokaz. Če imamo dve števili $a = q_1 n + r_1$ in $b = q_2 n + r_2$, kjer je $n \in \mathbb{N}$, potem lahko njuno razliko zapišemo kot

$$\begin{aligned} a - b &= q_1 n + r_1 - q_2 n - r_2 \\ &= (q_1 - q_2)n + (r_1 - r_2). \end{aligned}$$

Če iz te enačbe izoliramo razliko ostankov, ugotovimo, da je sestavljena iz razlike dveh celih števil, ki sta deljivi z n.

$$\begin{aligned} r_1 - r_2 &= (a - b) - (q_1 - q_2)n \\ &= k \cdot n - (q_1 - q_2)n \end{aligned}$$

Število $a - b$ namreč lahko zapišemo kot večkratnik števila n, kar pomeni, da obstaja $k \in \mathbb{Z}$, da je $a - b = k \cdot n$. Tako ugotovimo, da $n \mid r_1 - r_2$. Ker pa sta oba ostanka manjša od n in brez škode za splošnost predpostavimo še $r_2 \leq r_1$, je možno le, da sta ostanka enaka, torej $r_1 = r_2$. □

Naslednja trditev je zelo pomembna, saj nam bo v nadaljevanju bistveno poenostavila računanje s kongruencami.

Trditev 2.4. *Imejmo po dva para kongruentnih celih števil $a \equiv a' \bmod n$ in $b \equiv b' \bmod n$, pri čemer je $n \in \mathbb{N}$. Potem velja*

$$a + b \equiv a' + b' \bmod n \quad in \quad ab \equiv a'b' \bmod n.$$

Dokaz. Kadar sta števili kongruentni po modulu n, število n deli njuno razliko. Torej lahko v našem primeru zapišemo

$$a - a' = n \cdot v \quad \text{in} \quad b - b' = n \cdot u,$$

za neka $u,\ v \in \mathbb{Z}$. Trdimo, da je $a + b \equiv a' + b' \bmod n$. Poglejmo njuno razliko

$$\begin{aligned} a + b - (a' + b') &= a - a' + b - b' \\ &= nv + nu \\ &= n \cdot (v + u). \end{aligned}$$

Torej $n \mid a + b - (a' + b')$, kar dokaže želeno.

Dokažimo še drugi del trditve, ki pravi, da je $ab \equiv a'b' \bmod n$. Poglejmo razliko zmnožkov

$$\begin{aligned} ab - a'b' &= ab - a'b' - a'b + a'b \\ &= b(a - a') + a'(b - b') \\ &= b \cdot nv + a' \cdot nu \\ &= n \cdot (bv + a'u). \end{aligned}$$

V prvi vrstici smo odšteli in prišteli isto količino $a'b$ in po izpostavljanju ustreznih členov dobili, da $n \mid ab - a'b'$, kar pokaže zatrjeno. □

3 Krilati kvadrati

Sedaj smo pripravljeni za izrek, ki pove, katera praštevila so predstavljiva. Presenetljivo in precej zvito bomo izrek dokazali z uporabo geometrije. Vpeljali bomo t. i. *krilate kvadrate* in preučili njihovo obnašanje in povezavo s predstavljivostjo praštevil. Sledili bomo dokazu iz knjige [1, Chapter 4], ki ga je našel moskovski matematik Alexander Spivak.

Izrek 3.1. *Naj bo $p \in \mathbb{N}$ praštevilo.*

1. *Če velja $p = 2$ ali $p \equiv 1 \bmod 4$, potem je p mogoče zapisati kot vsoto dveh kvadratov.*
2. *Če je $p \equiv 3 \bmod 4$, praštevila p ni mogoče zapisati kot vsoto dveh kvadratov.*

Dokaz. Drugi del izreka je mnogo lažje dokazati kot prvega, zato začnimo z njim. Potrebujemo le lastnosti računanja s kongruencami iz trditve 2.4.

Trditev pokažimo s protislovjem. Recimo, da je preštevilo p predstavljivo, torej je $p = x^2 + y^2$ za neka $x,\ y \in \mathbb{Z}$. Če na to enakost pogledamo po modulu 4, dobimo

$$3 \equiv x^2 + y^2 \bmod 4. \tag{1}$$

Z izračunom kvadratov števil 0, 1, 2 in 3 (to so vsi možni ostanki celega števila pri deljenju s 4) vidimo, da je ostanek kvadrata pri deljenju s 4 lahko le 0 ali 1. Desna stran enačbe (1) torej zavzame le vrednosti 0, 1 ali 2 in *ne* 3. Predpostavka o predstavljivosti praštevila p je torej neresnična, zato p ni mogoče zapisati kot vsoto dveh kvadratov.

Lotimo se še prvega dela. Definirajmo množico

$$S = \{(x, y, z) \in \mathbb{N}^3 \mid 4xy + z^2 = p\}.$$

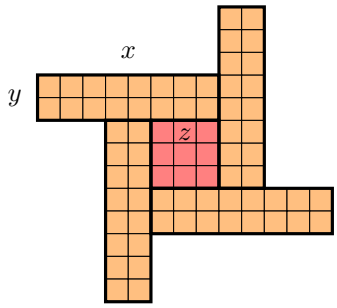
Najprej opazimo, da je množica S neprazna. Po predpostavki je namreč $p \equiv 1 \bmod 4$, zato obstaja $k \in \mathbb{N}$, da je $p = 4k + 1$, torej je $(k, 1, 1) \in S$.

Po opazovanju enačbe

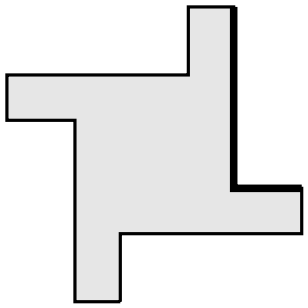
$$4xy + z^2 = p \tag{2}$$

ugotovimo, da lahko vsako od treh spremenljivk (zelo grobo) navzgor omejimo s p. Ker vse spremenljivke zavzamejo vrednosti med naravnimi števili, je tako rešitev enačbe (2) le končno mnogo. Množica S je torej končna.

Sedaj pokažimo, da je moč množice S liha. Naj bo $(x, y, z) \in S$ poljubna rešitev. Tej rešitvi lahko priredimo *krilati kvadrat*, ki je sestavljen iz osrednjega kvadrata, ki ima stranico dolžine z in štirih pravokotnikov z dolžinama



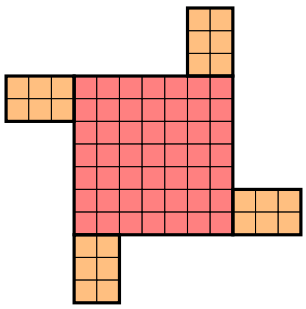
Slika 1: Krilati kvadrat.



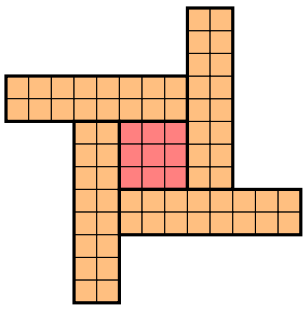
Slika 2: Oblika krilatega kvadrata.

stranic x in y, pri čemer se vsi štirje pravokotniki stikajo s sredinskim kvadratom v stranici dolžine x, kot je prikazano na sliki 3.

Vsaka od rešitev $(x, y, z) \in S$ tako določa en podobnostni razred krilatih kvadratov (zrcalna slika krilatega kvadrata namreč podaja isto rešitev). Iz vsakega od razredov izberemo tistega, ki ima kotni L v desnem nekonveksnem oglišču vsaj tako visok kot širok (ta je označen na sliki 3). Velja pa tudi obratno, iz vsakega krilatega kvadrat lahko razberemo trojico $(x, y, z) \in \mathbb{N}^3$, tako da preberemo dolžine stranic kvadrata in pravokotnikov, ki ga sestavljajo. Trojica potem zadošča enačbi $4xy + z^2 = p$, saj je to natanko ploščina krilatega kvadrata, zato pripada S. Množico S lahko tako identificiramo z množico vseh krilatih kvadratov, ki imajo kotni L v desnem nekonveksnem oglišču vsaj tako visok kot širok.



(2, 3, 7)

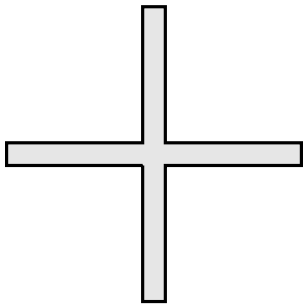


(8, 2, 3)

Slika 3: Dva različna krilata kvadrata za praštevilo $p = 73$ z enako obliko.

Oblika krilatega kvadrata je lik v ravnini, ki ga definira krilati kvadrat, odvisen pa je le od robne krivulje, ki ga obdaja. Oblika krilatega kvadrata s slike 3 je prikazana na sliki 3. Za vsako obliko krilatega kvadrata dobimo bodisi en bodisi dva krilata kvadrata. Na sliki 3 imamo dva različna krilata kvadrata z enako obliko.

Po dva krilata kvadrata oz. trojici iz množice S dobimo iz vsake oblike krilatih kvadratov, razen pri eni in sicer tisti, ki ima kotni L enako visok kot širok (ta je prikazana na sliki 3).



Slika 4: Oblika krilatega kvadrata, ki ima kotni L enako širok kot visok.

Če $(x, y, z) \in S$ pripada krilatemu kvadratu, katerega oblika ima to lastnost, velja $x = z$. Od tod lahko faktoriziramo $p = 4xy + z^2 = x(4y + x)$. Toda p je praštevilo, zato je $x = 1$, kajti za naravni števili x in y je $4y + x > 0$. Opazimo, da ta krilati kvadrat pripada natanko trojici $(1, k, 1)$, ki izhaja iz dejstva, da lahko zapišemo $p = 4k + 1$. Vsaki od oblik krilatih kvadratov lahko torej priredimo dva krilata kvadrata, le eni pa samo enega. To pomeni, da je S množica z liho močjo.

Dokaz izreka zaključimo z definicijo še enega parjenja krilatih kvadratov. To dosežemo s funkcijo $f\colon S \to S$ definirano s predpisom

$$f(x, y, z) = (y, x, z).$$

Očitno f slika v množico S, saj je (x, y, z) rešitev enačbe $4xy + z^2 = p$ natanko tedaj, ko je (y, x, z) rešitev. Funkcija f tako popari trojico (x, y, z) s trojico (y, x, z). Ker pa je moč množice S liha, mora f vsaj eno od rešitev popariti samo s seboj, kar pomeni, da je ta oblike (x, x, z). Ta trojica nazadnje pokaže, da je praštevilo p predstavljivo kot vsota dveh kvadratov, saj dobimo zapis

$$p = (2x)^2 + z^2.$$

□

4 Števila, ki so vsota dveh kvadratov

Sedaj raziščimo še, kako se predstavljivost praštevil posploši na predstavljivost ostalih sestavljenih števil.

4.1 Mali Fermatov izrek

V nadaljevanju bo koristno poznati mali Fermatov izrek. Za dokaz bomo potrebovali binomski izrek in eno lastnost binomskega simbola, zato najprej raziščimo ta dva koncepta.

Definicija 4.1. *Za naravni števili $n \in \mathbb{N}$ in $0 \leq k \leq n$ je **binomski simbol** definiran kot*

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

Opomba 4.1. *Kombinatorično binomski simbol $\binom{n}{k}$ šteje, na koliko načinov lahko iz množice z n elementi izberemo podmnožico s k elementi.*

Če pogledamo Pascalov trikotnik, lahko binomski simbol $\binom{n}{k}$ najdemo v n-ti vrstici kot k-ti element te vrstice, pri tem pa pazimo, da prvo število v vrstici štejemo kot 0-ti element.

Primer 4.1. *Recimo, da nas zanima, na koliko načinov lahko iz množice z močjo 5 izberemo podmnožico moči 3. Pogledamo četrto število v peti vrstici Pascalovega trikotnika, ter vidimo, da je rezultat 10. Pravilnost lahko preverimo tudi z računom*

$$\binom{5}{3} = \frac{5!}{3!(5-3)!} = \frac{20}{2} = 10.$$

$n=0$ 1
$n=1$ 1 1
$n=2$ 1 2 1
$n=3$ 1 3 3 1
$n=4$ 1 4 6 4 1
$n=5$ 1 5 10 10 5 1
$n=6$ 1 6 15 20 15 6 1
$n=7$ 1 7 21 35 35 21 7 1

Slika 5: Pascalov trikotnik.

Izrek 4.1 (Binomski izrek)**.** *Za polinoma v spremenljivkah x in y velja enakost*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

Binomski izrek, nam pomaga pri razčlenitvi dvočlenika na poljubno stopnjo. Ugotovimo, da koeficiente v razvoju najdemo v n-ti vrstici Pascalovega trikotnika.

Lema 4.1. *Naj bo $p \in \mathbb{N}$ praštevilo in $0 < k < p$. Potem $p \mid \binom{p}{k}$.*

Dokaz. Binomski simbol $\binom{p}{k}$ je vedno celo število in ga lahko zapišemo tudi kot

$$\binom{p}{k} = \frac{p \cdot (p-1) \cdots (p-k+1)}{k \cdot (k-1) \cdots 2 \cdot 1}.$$

V imenovalcu so vsi faktorji manjši od p, ki je praštevilo, zato $k!$ deli produkt $(p-1)\cdots(p-k+1)$, kar pomeni, da je $\frac{(p-1)\cdots(p-k+1)}{k!}$ celo število. Od tod sledi, da $p \mid \binom{p}{k}$. □

Pravkar dokazano je seveda razvidno tudi v Pascalovem trikotniku 5, če pogledamo vrstice pri $n = 2,\ 3,\ 5,\ 7$.

Lema 4.2 (Brucove sanje)**.** *Naj bosta $a,\ b \in \mathbb{Z}$ in $p \in \mathbb{N}$ praštevilo. Tedaj velja*

$$(a+b)^p \equiv a^p + b^p \bmod p.$$

Dokaz. Po binomskem izreku vemo, da je

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k}.$$

Lema 4.1 nam pove, da je $\binom{p}{k} \equiv 0 \bmod p$ za vse $0 < k < p$, zato po modulu p v zgornji vsoti ostaneta le prvi in zadnji člen, pri indeksih $k = 0$ in $k = p$. Sledi

$$(a+b)^p \equiv a^p + b^p \bmod p.$$

□

Izrek 4.2 (Mali Farmatov izrek)**.** *Naj bo $p \in \mathbb{N}$ praštevilo in $a \in \mathbb{Z}$, potem velja*

$$a^p \equiv a \bmod p.$$

Dokaz. Najprej omenimo, da se je dovolj omejiti na $0 \le a < p$, saj ima vsako celo število ostanek pri deljenju s p vsebovan v množici $\{0, \ldots, p-1\}$. Izrek dokažimo z matematično indukcijo.

Za $a = 0$ in $a = 1$, je trditev očitna. Denimo torej, da je $(a-1)^p \equiv a-1 \bmod p$ in pokažimo, da velja $a^p \equiv a \bmod p$. Zapišemo lahko

$$a^p \equiv ((a-1)+1)^p \equiv (a-1)^p + 1^p \bmod p,$$

kjer drugo kongruenco zagotavlja lema 4.2. Po indukcijski predpostavki tedaj sledi

$$(a-1)^p + 1^p \equiv a - 1 + 1 \equiv a \bmod p,$$

kar dokaže želeno. □

Izrek bomo še malenkost izboljšali, v ta namen se spomnimo, kdaj je funkcija injektivna in surjektivna. Funkcija $g\colon S \to S$ je *injektivna*, kadar za vsaka $x,\ y \in S$ iz $g(x) = g(y)$, sledi $x = y$. Z drugimi besedami je funkcija g injektivna, kadar za neki $y \in S$ obstaja največ en $x \in S$, ki se z g slika v y. Funkcija $g\colon S \to S$ je *surjektivna*, kadar za vsak $y \in S$ obstaja neki $x \in S$, ki se z g slika vanj. Funkcija g je torej surjektivna natanko takrat, ko je za vsak $y \in S$ rešljiva enačba $g(x) = y$.

Lema 4.3. *Naj bo S končna množica in $g\colon S \to S$ injektivna preslikava, potem je g surjektivna.*

Dokaz te leme ni zahteven, a ga bomo kljub temu izpustili.

Trditev 4.1. *Naj bo $p \in \mathbb{N}$ praštevilo. Za vsak $a \in \mathbb{Z}$, kjer $p \nmid a$, obstaja neki $b \in \mathbb{Z}$, za katerega velja*

$$ab \equiv 1 \bmod p.$$

Dokaz. Naj bo $Z_p = \{0, 1, ..., p-1\}$, ki predstavlja ostanke po modulu p. Potem naj bo funkcija $f\colon Z_p \to Z_p$ podana s predpisom $f(x) = ax \bmod p$. Pokažimo, da je f injektivna.

Naj bosta $x,\ y \in Z_p$ poljubna in denimo, da velja $f(x) = f(y)$. Potem drži

$$ax \equiv ay \bmod p.$$

Od tod sledi, da $p \mid a(x-y)$. Ker vemo, da p ne deli a, sklepamo, da $p \mid x - y$. Slednje pomeni $x \equiv y \bmod p$, ker pa x in y ležita v Z_p, torej sta že ostanka, imamo tudi enakost $x = y$.

Množica Z_p je končna, zato lahko uporabimo lemo 4.3. Po pravkar dokazanem je f injektivna, zato je tudi surjektivna. Obstaja torej $b \in Z_p$, da je $f(b) = 1 \bmod p$, kar pomeni, da b zadošča kongruenci

$$ab \equiv 1 \bmod p.$$

□

Sledi manjša izboljšava malega Fermatovega izreka, dokaz katere je uporaba izreka 4.2 in trditve 4.1.

Izrek 4.3. *Naj bo $p \in \mathbb{N}$ praštevilo in $a \in \mathbb{Z}$, tako da $p \nmid a$. Tedaj velja*

$$a^{p-1} \equiv 1 \bmod p.$$

Dokaz. Ker p ne deli a, obstaja $b \in \mathbb{Z}$, da velja $ab \equiv 1 \bmod p$. Če kongruenco $a^p \equiv a \bmod p$ z obeh strani pomnožimo z b, dobimo

$$a^p b \equiv ab \bmod p.$$

Torej imamo $a^{p-1} \equiv a^{p-1}ab \equiv a^p b \equiv ab \equiv 1 \bmod p$, kar dokaže želeno. □

Zgled 4.1. *Kakšen je ostanek števila 17^{341} pri deljenju s 5? Vemo, da lahko 17 zapišemo kot $17 = 3 \cdot 5 + 2$, kar pomeni, da ima 17 pri deljenju s 5 ostanek 2, torej je $17 \equiv 2 \bmod 5$. To pomeni, da velja $17^{341} \equiv 2^{341} \bmod 5$. Ker 5 ne deli 2, po izboljšavi malega Fermatovega izreka velja*

$$2^4 \equiv 1 \bmod 5.$$

Slednje je preprosto opaziti tudi s kratkim računom. Dalje sklepamo, da velja

$$2^{341} \equiv 2^{85 \cdot 4 + 1} \equiv (2^4)^{85} \cdot 2 \equiv 2 \bmod 5.$$

To pomeni, da je $17^{341} \equiv 2 \bmod 5$.

Preden lahko odgovorimo na prvotno vprašanje, vpeljimo še pojem *reda* nekega elementa po modulu preštevila p.

Definicija 4.2. *Naj bo praštevilo $p \in \mathbb{N}$ in $a \in \mathbb{Z}$. Poleg tega naj velja $p \nmid a$. Definirajmo* ***red*** *elementa a po modulu p kot* najmanjše *naravno število $r \in \mathbb{N}$, za katerega velja*

$$a^r \equiv 1 \bmod p.$$

Trditev 4.2. *Imejmo praštevilo $p \in \mathbb{N}$, število $a \in \mathbb{Z}$ in denimo, da drži $p \nmid a$. Naj bo $r \in \mathbb{N}$ red elementa a. Če za $m \in \mathbb{N}$ velja $a^m \equiv 1 \bmod p$, potem $r \mid m$.*

Dokaz. Zaradi osnovnega izreka o deljenju vemo, da obstajata $q,\ t \in \mathbb{Z}$, za kateri velja $0 \leq t < r$ in

$$m = qr + t.$$

S tem lahko preoblikujemo $a^m \equiv 1 \bmod p$ v $a^{qr+t} \equiv 1 \bmod p$, kar je enako tudi $(a^r)^q \cdot a^t \equiv 1 \bmod p$. Po naši definiciji je $a^r \equiv 1 \bmod p$. Dobimo $1^q \cdot a^t \equiv 1 \bmod p$. Ker je r najmanjše število za katerega $a^r \equiv 1 \bmod p$, mora biti $t = 0$. Ker pa je t ostanek pri deljenju m s številom r, velja $r \mid m$. □

4.2 Glavni izrek

Najprej dokažimo pomožno lemo, ki bo koristna pri dokazu glavnega izreka.

Lema 4.4. *Vzemimo praštevilo $p \in \mathbb{N}$. Če je $x^2 \equiv -1 \bmod p$, kjer je $x \in \mathbb{Z}$, potem je $p = 2$ ali pa je $p \equiv 1 \bmod 4$.*

Dokaz. Predpostavimo, da je $p > 2$ in pokažimo, da je red elementa x po modulu p enak 4.

Očitno je $x^4 \equiv 1 \bmod p$. Red elementa x ne more biti 1, saj bi moralo držati $x \equiv 1 \bmod p$, kar pa ne more biti res, saj $1^2 \not\equiv -1 \bmod p$. Prav tako red ne more biti 2, saj vemo $x^2 \equiv -1 \not\equiv 1 \bmod p$. S protislovjem pokažimo še, da tudi 3 ni red elementa x. Predpostavimo, da je 3 red elementa x po modulu p. Potem velja

$$x^3 \equiv 1 \bmod p.$$

Z upoštevanjem predpostavke $x^2 \equiv -1 \bmod p$, sledi

$$1 \equiv x^3 \equiv x \cdot x^2 \equiv -x \bmod p.$$

Toda potem je $x^2 \equiv (-x)^2 \equiv 1 \bmod p$, kar je v nasprotju s predpostavko, saj $1 \not\equiv -1 \bmod p$.

Najmanjše naravno število $r \in \mathbb{N}$, za katerega je $x^r \equiv 1 \bmod p$, je tako $r = 4$, ki je torej red elementa x po modulu p.

Posebej opomnimo, da velja $p \nmid x$, saj bi v nasprotnem imeli $x \equiv 0 \bmod p$ in tako tudi $x^2 \equiv 0 \bmod p$, kar nasprotuje predpostavki leme. Zato lahko uporabimo izboljšavo malega Fermatovega izreka 4.3, ki nam pove, da je $x^{p-1} \equiv 1 \bmod p$. Po trditvi 4.2, tako dobimo, da $4 \mid p-1$. Od tod sledi $p - 1 \equiv 0 \bmod 4$. Po preureditvi te kongruence pa dobimo $p \equiv 1 \bmod 4$, kar dokaže našo trditev. □

Kako zdaj vse te izreke povežemo na naše vprašanje, katera naravna števila je mogoče zapisati kot vsoto dveh kvadratov? Uporabili bomo osnovni izrek aritmetike, ki pravi, da lahko vsako naravno število zapišemo kot produkt praštevil. Poleg tega pa bo koristno tudi dejstvo, da lahko z izjemo števila 2 praštevila razdelimo v dve skupini, in sicer na praštevila, ki so kogruentna 1, in tista, ki so kongruenta 3 po modulu 4. Sedaj smo pripravljeni za glavni izrek.

Izrek 4.4. *Recimo, da je n poljubno naravno število, $p_1, \ldots, p_k$ in $q_1, \ldots, q_m$ pa njegovi različni praštevilski faktorji, pri čemer za vse i in j velja*

$$p_i \equiv 1 \bmod 4 \quad \text{in} \quad q_j \equiv 3 \bmod 4.$$

Zapišimo

$$n = 2^t \cdot p_1^{e_1} \ldots p_k^{e_k} \cdot q_1^{f_1} \ldots q_m^{f_m}, \tag{3}$$

za neka naravna števila $t \in \mathbb{N}_0$, $e_1, \ldots, e_k \in \mathbb{N}$ in $f_1, \ldots, f_m \in \mathbb{N}$.

Tedaj je število n predstavljivo kot vsota dveh kvadratov, če in samo če so vsi eksponenti f_j sodi.

Dokaz. ($\Leftarrow$) V začetku članka smo že opazili, da lahko število napišemo kot vsoto kvadratov dveh števil, kadar lahko to storimo za vsa števila v neki njegovi faktorizaciji. To pove trditev 1.1. Poglejmo, zakaj so vsi faktorji iz faktorizacije (3) predstavljivi.

Začnimo z 2. Če je eksponent t sod, je oblike $t = 2u$ za neki $u \in \mathbb{N}_0$. Potem je 2^t kvadrat nekega števila in zato tudi predstavljiv, saj velja

$$2^{2u} = (2^u)^2 + 0^2.$$

Če pa je eksponent t lih, je oblike $t = 2u + 1$ za neki $u \in \mathbb{N}$, in velja

$$2^{2u+1} = 2 \cdot (2^u)^2 = (2^u)^2 + (2^u)^2,$$

ki je vsota dveh kvadratov.

Za praštevila p_i smo v izreku 3.1 dokazali, da jih lahko vedno zapišemo kot vsoto dveh kvadratov, praštevila q_j pa se pojavijo s sodimi eksponenti, zato so že sami kvadrati in zato predstavljivi. Sledi, da je n predstavljivo.

($\Rightarrow$) Sedaj denimo, da je n mogoče zapisati kot vsoto dveh kvadratov

$$n = x^2 + y^2 \quad \text{za } x,\ y \in \mathbb{Z}$$

in pokažimo, da so vsi eksponenti f_j sodi.

Naj bo q eno od praštevil q_j iz praštevilskega razcepa števila n. Pokažimo, da $q^2 \mid n$. Slednje bomo dokazali tako, da pokažemo, da $q \mid x$ in $q \mid y$.

Predpostavimo, da $q \nmid x$. Naj bo $z \in \mathbb{Z}$ tako, da bo veljalo $xz \equiv 1 \bmod q$. Praštevilo q je delitelj n, zato je $n \equiv 0 \bmod q$. Potem velja

$$0 \equiv z^2 n \equiv z^2 x^2 + z^2 y^2 \equiv 1 + (zy)^2 \bmod q.$$

Če to preuredimo, dobimo $(zy)^2 \equiv -1 \bmod q$. Lema 4.4 nam pove, da je $q \equiv 1 \bmod 4$. Toda, ker smo predpostavili $q \equiv 3 \bmod 4$ pridemo v protislovje. Po enakem postopku lahko dokažemo tudi $q \mid y$.

Ker velja $q \mid x$ in $q \mid y$, mora veljati tudi

$$\left(\frac{x}{q}\right)^2 + \left(\frac{y}{q}\right)^2 = \frac{n}{q^2}.$$

Vidimo, da je število $\frac{n}{q^2}$ možno zapisati kot vsoto dveh kvadratov, zato lahko ta postopek nadaljujemo in na vsakem koraku opazimo, da v primeru, ko praštevilo q z $q \equiv 3 \bmod 4$ deli n, tudi q^2 deli n. Torej imajo vsi prafaktorji q_j v praštevilskem razcepu n sode eksponente, tj. f_j so vsi sodi. □

5 Zaključek

V članku smo se spraševali, kaj mora držati, da lahko neko poljubno naravno število zapišemo kot vsoto kvadratov dveh celih števil. Naprej nam je to uspelo dokazati za poljubno praštevilo, za katerega je bilo potrebno samo, da ima pri deljenju s 4 ostanek 1, oz. $p \equiv 1 \bmod 4$. Od tod smo nazadnje izpeljali, da lahko število zapišemo kot vsoto dveh kvadratov, če in samo če lahko to naredimo za vse prafaktorje, ki ga sestavljajo in imajo tisti, ki jih ne moremo samih po sebi zapisati kot vsoto dveh kvadratov, sodo potenco.

Literatura

[1] M. Aigner, G. M. Ziegler, *Proofs from THE BOOK*, 6th edition Springer, Berlin, 2018.

[2] *Fermatov mali izrek*, v: Wikimedie, S. P. (2022, August 23). Fermatov mali izrek. Wikipedija, Prosta Enciklopedija. `https://sl.wikipedia.org/wiki/Fermatov_mali_izrek`

[3] K. Šivic, *Funkcije in funkcijske enačbe*, `https://www.dmfa.si/Tekmovanja/MaSSA/Dokumenti/funkcijske_predavanje.pdf`

Popolna števila

Adam Bürmen, Ekaterina Chizhova
Mentor: *Nino Cajnkar*

Povzetek

Najprej so definirana popolna števila, nato so obravnavana soda in liha popolna števila. Ugotovljena je potrebna oblika sodih popolnih števil. Raziskana so liha popolna števila in ugotovljeno je, da njihove rešitve ne poznamo. Raziskani so pogoji, ki veljajo za liha popolna števila.

1 Uvod

Morda vam je kakšno število všeč, morda imate najljubše število, morda se vam kakšno celo zdi popolno. Na srečo so matematiki že v grških časih določili, katera števila so popolna, da si vam ni treba beliti glave s takšnimi težkimi odločitvami. Danes poznamo prvih nekaj sodih popolnih števil, nismo pa še odkrili, koliko jih je. Za razliko od sodih popolnih števil, o lihih ne vemo niti, ali obstajajo. Zaradi svoje preprostosti in visoke težavnosti je to eden izmed najbolj znanih odprtih problemov v matematiki.

2 Popolna števila

Laično lahko definiramo popolna števila kot taka števila, katerih seštevek vseh deliteljev je dvakrat večji kot število samo. Ta definicija je na začetku raziskovanja popolnih števil služila svojemu namenu, dokler ni Euler v srednjem veku iznašel sigma funkcije in revolucioniral nadaljnje delo na problemu.

Definicija 2.1. ***Seštevek deliteljev*** *oziroma* ***sigma funkcija*** *je funkcija $\sigma : \mathbb{N} \to \mathbb{N}$ s predpisom*

$$\sigma(n) = \sum_{d|n} d.$$

Definicija 2.2. ***Popolna števila*** *so naravna števila, za katera velja*

$$\sigma(n) = 2n.$$

Definicija 2.3. ***Pravi delitelji*** *števila $n \in \mathbb{N}$ so vsa taka števila $d \in \mathbb{N}$, za katera velja $d \mid n$ in $1 < d < n$.*

Definicija 2.4. *Rečemo, da je število n* ***deficitno*** *ali* ***nezadostno****, če velja $\sigma(n) < 2n$, in* ***obilno****, če je $\sigma(n) > 2n$. Števili, katerih vsota pravih deliteljev je enaka, se imenujeta* ***prijateljski števili****, večja množica takšnih števil pa se imenuje* ***družabno število****. Število, ki je prijateljsko samo sebi, je popolno število. Popolno število je tudi družabno število s periodo 1.*

V naslednjem izreku bomo dokazali, da je funkcija seštevka deliteljev **multiplikativna**.

Izrek 2.1. *Za naravni števili m in n z $gcd(m, n) = 1$, velja*

$$\sigma(mn) = \sigma(m) \cdot \sigma(n).$$

Dokaz. Naj bodo $1, d_1, d_2, \cdots, d_k$ delitelji n ter $1, t_1, t_2, \cdots, t_j$ delitelji m. Po definiciji velja

$$\sigma(n)\sigma(m) = (1 + d_1 + \cdots + d_k)(1 + t_1 + \cdots + t_j).$$

Ko vsoti deliteljev zmnožimo, bo vsak dobljeni člen v vsoti delitelj mn. Ker sta si m in n tuji, se bodo na desni strani enačbe pojavili vsi delitelji mn, saj lahko poljubnega zapišemo kot zmnožek enega delitelja m in delitelja n. Zaradi tujosti m in n se ne bo noben člen ponovil dvakrat, torej je izraz enak $\sigma(mn)$. Zato je sigma funkcija res multiplikativna. □

Izrek 2.2. *Naj bo $N = \prod_{i=1}^{k} p_i^{\alpha_i}$ praštevilski razcep števila N, kjer so p_i njegovi praštevilski delitelji in α_i potenca i-tega praštevilskega delitelja v razcepu. Potem je*

$$\sigma(n) = \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}.$$

Dokaz. Po izreku 1 sledi

$$\sigma\left(\prod_{i=1}^{k} p_i^{\alpha_i}\right) = \prod_{i=1}^{k} \sigma(p_i^{\alpha_i}) = \prod_{i=1}^{k} (1 + p_i + \cdots + p_i^{\alpha_i}) = \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1},$$

kjer smo v drugi neenakosti upoštevali dejstvo, da

$$\sigma(p^\alpha) = 1 + p + ... + p^{\alpha-1} + p^\alpha.$$

□

Lema 2.1. *Naj bo N naravno število in μ pravi delitelj števila N. Potem velja*

$$\sigma(\mu) < \sigma(N).$$

Še več, velja tudi

$$\frac{\sigma(\mu)}{\mu} < \frac{\sigma(N)}{N}.$$

Dokaz. Najprej izračunamo $\sigma(N)/N$

$$\frac{\sigma(N)}{N} = \frac{1}{N} \sum_{d|N} d = \frac{1}{N} \sum_{d|N} \frac{N}{d} = \sum_{d|N} \frac{1}{d}.$$

Ker je μ pravi delitelj N, bo veljalo, da je vsak delitelj μ tudi delitelj N, zato z uporabo zgornje enakosti lahko dokažemo željen rezultat

$$\frac{\sigma(N)}{N} > \frac{\sigma(\mu)}{\mu}.$$

Ker je μ pravi delitelj N, so vsi delitelji μ tudi delitelji N, ker pa tudi N deli samega sebe, nujno sledi $\sigma(\mu) < \sigma(N)$ in dokazali smo tudi prvo neenakost. □

Posledica 2.1. *Če je N popolno število, potem velja*

$$\sum_{d|N} \frac{1}{d} = 2.$$

2.1 Soda popolna števila

Med nekaj prvimi sodimi popolnimi števili so 6, 28, 496, 8128. Poznamo le končno mnogo sodih popolnih števil.

Izrek 2.3 (Cataldi-Fermat)**.** *Če je $2^n - 1$ praštevilo za neko naravno število n, bo n tudi praštevilo.*

Dokaz. Denimo, da lahko zapišemo $n = rs$ za $r, s \in \mathbb{N}$, za katera velja $r, s > 1$

$$2^{rs} - 1 = (2^r)^s - 1 = (2^r - 1)(1 + 2^r + \cdots + (2^r)^{s-1}).$$

Potem velja, da $2^n - 1$ ni praštevilo, kar nas pripelje do protislovja, ki dokaže izrek. □

Definicija 2.5. *Praštevila oblike $2^n - 1$ imenujemo **Mersennova praštevila**.*

Izrek 2.4. *Za vsako Mersennovo praštevilo $2^n - 1$ je število $2^{n-1}(2^n - 1)$ sodo popolno število.*

Dokaz. Izrek bomo dokazali z uporabo dejstva, da za vsako praštevilo p velja, da je $\sigma(p) = p + 1$. Z uporabo izreka o multiplikativnosti velja

$$\sigma(2^{n-1}(2^n - 1)) = \sigma(2^{n-1})\sigma(2^n - 1) = (2^n - 1)2^n = 2(2^{n-1}(2^n - 1)).$$

□

Trenutno (17. julij 2024) poznamo le 47 Mersennovih praštevil in s tem tudi 47 sodih popolnih števil. Ne ve se, ali obstaja neskončno število popolnih števil.

Izrek 2.5 (Evklid-Eulerjev izrek)**.** *Vsako sodo popolno število se lahko zapiše v obliki*

$$2^{n-1}(2^n - 1),$$

kjer je n naravno število in $2^n - 1$ praštevilo.

Dokaz. Dano sodo popolno število zapišimo kot $N = 2^{n-1}m$, kjer sta $n, m \in \mathbb{N}$ in m ni sodo število. Po izreku o multiplikativnosti izračunamo

$$\sigma(N) = 2N = 2^n m = \sigma(2^{n-1})\sigma(m) = (2^n - 1)\sigma(m).$$

Sledi $2^n - 1 \mid m$, torej lahko zapišemo $m = q(2^n - 1)$, za naravno število q. Če je $q = 1$ smo končali, zato predpostavimo $q > 1$. Med delitelji števila m bodo tako števila $1, 2^n - 1, q$ in m. Sedaj bomo omejili vrednost $\sigma(m)$ in poiskali protislovje

$$\sigma(m) \geq 1 + 2^n - 1 + q + (2^n - 1)q = 2^n(q + 1),$$
$$\frac{m}{\sigma(m)} \leq \frac{(2^n - 1)q}{2^n(q + 1)} = \frac{2^n - 1}{2^n} \cdot \frac{q}{q + 1} < \frac{2^n - 1}{2^n}.$$

Vendar iz enakosti $2^n m = (2^n - 1)\sigma(m)$ sledi $\frac{m}{\sigma(m)} = \frac{2^n - 1}{2^n}$, kar je protislovje, torej je $q = 1$. □

Izrek 2.6. *Če je $N = 2^{n-1}(2^n - 1)$ popolno število in $N \neq 6$, potem je*

$$N = 1^3 + 3^3 + \cdots + (2^{(n-1)/2)} - 1)^3.$$

Dokaz. Vemo, da velja

$$\sum_{i=1}^{n} i^3 = \frac{(n(n + 1))^2}{4}.$$

Če zdaj vstavimo $N = 2^{(n-1)/2}$ za nek lih n, dobimo željen rezultat. □

Izrek 2.7. *Vsako popolno sodo število ima zadnjo števko v desetiškem zapisu* 6 *ali* 8*.*

Dokaz. Vemo, da je vsako sodo popolno število oblike

$$2^{n-1}(2^n-1),$$

kjer je 2^n-1 praštevilo in je posledično iz prejšnjega izreka tudi n praštevilo. Torej je n liho število, in lahko zapišemo $n=4m+1$ ali $n=4m+3$ za neki $m\in\mathbb{N}$. Če je $n=4m+1$, potem je

$$\begin{aligned}2^{n-1}(2^n-1)&=2^{4m}(2^{4m+1}-1)=16^m(2\cdot 16^m-1)\\&\equiv 6^m(2\cdot 6^m-1)\equiv 6(2\cdot 6-1)\equiv 6\cdot 1\equiv 6 \pmod{10}.\end{aligned}$$

Če je $n=4m+3$, potem je

$$\begin{aligned}2^{n-1}(2^n-1)&=2^{4m+2}(2^{4m+3}-1)=16^m\cdot 4(2\cdot 16^m\cdot 8-1)\\&\equiv 6^m\cdot 4(2\cdot 6^m\cdot 8-1)\equiv 6\cdot 4(6\cdot 8-1)\equiv 4\cdot 7\equiv 8 \pmod{10}.\end{aligned}$$

Torej smo dokazali, da ima vsako popolno sodo število zadnjo števko v desetiškem zapisu 6 ali 8. □

3 Liha popolna števila

Ne ve se ali obstajajo liha popolna števila. Kljub številnim ugotovljenim potrebnim pogojem še nismo razvozlali problema obstoja lihih popolnih števil. Če obstaja liho popolno število, mora biti večje od 10^{3000}. Poleg tega mora imeti tudi vsaj 8 različnih prafaktorjev (in vsaj 11, če ni deljivo s 3), ter mora biti vsaj en prafaktor večji od 107, dva prafaktorja večja od 104 in trije prafaktorji večji od 100.

Zapisali bomo nekaj pogojev za liha popolna števila, ki zaradi zapletenosti dokazov ne bomo dokazali.

Trditev 3.1. *Euler je pokazal, da ima liho popolno število N obliko*

$$N=p^{4\lambda+1}q^2,$$

za neko $\lambda\in\mathbb{N}$, praštevilo p oblike $4k+1$ in praštevilo q oblike $4r+1$.

Dokaz. Dokaz je prepuščen kot vaja bralcu. □

Izrek 3.1 (Touchard (1953))**.** *Če liho popolno število obstaja, mora biti oblike $12k+1$ ali $36k+9$.*

Nadalje je še za vsako liho popolno število z r prafaktorji in $0<i<6$ Kishore leta 1981 dokazal zgornje meje za majhne faktorje lihih popolnih števil. Pokazal je namreč, da velja $p_i<2^{2^{i-1}}(r-i+1)$.

Trditev 3.2. *Naj bo N liho popolno število s k različnimi prafaktorji in naj bo*

$$P=\prod_{p\mid n}p.$$

Potem je

$$N<P^{2^k}-1.$$

Trditev 3.3. *Če je N liho popolno število s k prafaktorji, potem*

$$N<2^{4^k}.$$

4 Zaključek

Spoznali smo popolna števila, osrednjo temo enega izmed največjih odprtih problemov v matematiki, ter razna osnovna orodja iz teorije števil za reševanje takšnih problemov. Dokazali smo najpomembnejše izreke na tem področju, kot sta na primer Evklid-Eulerjev in Cataldi-Fermajev. Spoznali smo tudi, kaj so Mersennova praštevila in kako so povezana s popolnimi števili.

Literatura

[1] P. P. Nielsen, Odd Perfect Numbers Have at Least Nine Distinct Prime Factors, 22 Feb 2006. http://arxiv.org/abs/math.NT/0602485.

[2] Nielsen, P. Pace, An upper bound of odd perfect numbers.

[3] Eric W. Weisstein, Odd Perfect Number, `https://mathworld.wolfram.com/` (dostopano 19. 7. 2024).

[4] Perfect Number, Wikipedia, `https://en.wikipedia.org/w/Perfect_number` (dostopano 20. 7. 2024).

DRUŽABNI PROGRAM

Marsovski Estimathon

Izak Jenko, Matija Likar

Estimathon je razburljiva ekipna igra, ki združuje kviz s hitrim matematičnim razmišljanjem in ocenjevanjem. Cilj igre je v kratkem času čim natančneje oceniti intervale, v katerih leži numerični odgovor na vsako izmed zastavljenih vprašanj. Ekipe so pri tem nagrajene glede na število zadetkov in majhnost ustreznih intervalov, saj večji interval pomeni lažji zadetek. Na letošnjem taboru MaRS smo tekmovanje Estimathon tokrat organizirali drugič. Udeležilo se ga je 22 dijakinj in dijakov iz vse Slovenije.

Pravila igre

Tipična izvedba igre Estimathon traja 30 minut, v katerih vsaka od ekip sočasno rešuje 13 ocenjevalnih problemov, ki jih organizator pripravi vnaprej. Vsi problemi imajo točno rešitev, ki je pozitivno realno število, vsaka od ekip pa odgovor odda v obliki intervala s pozitivno zgornjo in spodnjo mejo $[\min, \max]$, za katerega meni, da vsebuje točno rešitev.

Pravimo, da je dani interval, ki ga odda ekipa, dober, če vsebuje točen odgovor. Število vseh točk neke ekipe izračunamo s formulo

$$\left(10 + \sum_{\text{dobri intervali}} \left\lfloor \frac{\max}{\min} \right\rfloor\right) \cdot 2^{13-(\text{št. dobrih intervalov})}.$$

Seštejemo torej spodnje cele dele razmerij zgornjih in spodnjih mej vseh dobrih intervalov. Recimo, da je pri nekem vprašanju s točnim odgovorom 1234 ekipa podala interval $[1000, 2500]$. Interval je dober, saj vsebuje točen odgovor, in bo k vsoti prispeval $\lfloor 2500/1000 \rfloor = \lfloor 2.5 \rfloor = 2$. Vsoti nato še prištejemo 10 in na koncu rezultat pomnožimo s tolikšno potenco števila 2, kot je imela ekipa nerešenih nalog ali slabih intervalov. Za vsak prazen ali napačen odgovor, se tako rezultat podvoji. Zmaga ekipa, ki zbere najmanjše število točk.

Za oddajo odgovorov ima vsaka ekipa na voljo 18 listkov, na katere zapiše ime svoje ekipe, številko problema, ki ga ocenjuje, ter krajišči intervala, torej zgornjo in spodnjo mejo svoje ocene rešitve danega problema. Za dani problem lahko tako ekipa odda več listkov z odgovori, vendar pa za rezultat vedno šteje zadnji oddani listek. Listke je možno oddajati tekom celotnih 30 minut igranja. Ves čas tekmovanja je razvidna tudi tabela rezultatov, ki se sproti posodablja. Prepovedana je uporaba računal, telefonov, interneta in ostalih zunanjih pripomočkov. Igra Estimathon je bila zasnovana leta 2013 v podjetju Jane Street. Več o Estimathonu lahko izvemo na povezavi `www.estimathon.com`.

Vprašanja in odgovori

Letošnji tekmovalci so si razbijali glave z naslednjimi 13 vprašanji, ki smo jih sestavljalci izbrali iz matematike, lokalne okolice CŠOD Planinka, popularne kulture in drugod.

1. Koliko kabin ima Pohorska vzpenjača?
2. Koliko je detektorjev dima v CŠOD Planinka?
3. Koliko je bilo uspešnih podaj Slovenije na letošnjem evropskem prvenstvu v nogometu?
4. Kolikšna je cestna razdalija od krožišča pri cerkvi v Spodnjih Hočah do CŠOD Planinka v enotah dolžine najdaljše stranice čokoladice Mars?
5. Število je perfektno, kadar je vsota njegovih pravih deliteljev enaka številu samemu. Za praštevilo p je Evklid dokazal, da je $2^{p-1}(2^p - 1)$ perfektno, če je le $2^p - 1$ praštevilo. Kaj je peto perfektno število?
6. Enotni delitelj števila n je delitelj d števila n, za katerega sta d in n/d tuji si števili. Koliko je parov (n, d), kjer je d enotni delitelj števila n, in je n naravno število med 1 in 100?
7. Koliko je skupno število registriranih avtobusov in miniavtobusov v Sloveniji?
8. Koliko je vseh osnovnih šol v občini Maribor?
9. Kolikšna je zračna razdalija med Plečnikovim spomenikom NOB v domačem kraju nogometaša Benjamina Šeška in vzpetino, ki so jo Rimljani poimenovail Mons Ocra, v kilometrih?
10. Koliko maseljcev piva lahko zlijemo v telo s prostornino enega barela?
11. Koliko ogledov imajo Joker Out Official na YouTube?
12. Koliko ton krompirja je Slovenija pridelala v letu 2023?
13. Koliko znaša vsota emšo treh organizatorjev letošnjega estimathona?

Bralce vabimo, da poskusijo odgovoriti na vseh 13 vprašanj, predno poiščejo rešitve v spodnji tabeli. Zaradi preprostosti so nekateri statistični podatki zaokroženi. Podatki so biti vzeti dne 14. 7. 2024.

vprašanje	1	2	3	4	5	6	7
odgovor	64	49	940	125.263	33.550.336	359	2.860
vprašanje	8	9	10	11	12	13	
odgovor	25	93	467	21.202.677	69.000	$5,43 \times 10^{12}$	

Rezultati in zaključek

Tekmovalci so se na Estimathonu odrezali nekoliko bolje kot lani. Pri vsakem izmed vprašanj je vsaj ena izmed ekip postavila *dober* interval, vendarle pa nobena izmed ekip ni znala rešiti vseh vprašanj. Najbolje je bilo reševano osmo vprašanja, ki so ga pravilno rešile vse ekipe, štirim pa je uspelo postaviti mejo, kjer je $\left\lfloor \frac{\max}{\min} \right\rfloor = 1$. Najtrši oreh je pa predstavljalo deveto, ki sta ga uspešno rešili le dve ekipi.

Lovoriko letošnjega Estimathona si je useplo priboriti ekipi Pak, ki je uspešno rešila 11 problemov in dosegla rezultat 116 točk. Tesno za petami jim je bila ekipa Makaroni in za njimi še Literani Štajerci. Obe ekipi sta pravilno rešili 9 problemov in osvojili 320 oziroma 432 točk. Organizacijsko ekipo letošnjega tekmovanja smo sestavljali Jan Genc, Izak Jenko in Matija Likar.

Slika 1: Udeleženci Estimathona v nestrpnem pričakovanju začetka tekmovanja

IZKUŠNJE UDELEŽENCEV

Izkušnje udeležencev

Manca Ernst, Jure Kreže, Marsela Supé Vide, Jakob Žorž

Marsela

Odločitev, da se letos udeležim tabora MaRS je bila definitivno ena izmed najboljših odločitev za poletne tabore do zdaj. Bila sem prijetno presenečena nad lepo dobrodošlico in super cimrami, prav tako pa je bilo delo na projektih zanimivo in koristno. Naučili smo se uporabljati LaTeX ter pridobivali znanja na področjih matematike, ki jih od prej ne poznamo toliko. Od predavanj mi je bila najbolj všeč glavna delavnica in večerno predavanje o bitnih računalnikih, saj je bila snov razložena tako, da je pritegnila pozornost in bila razumljiva.

Kot prva zmagovalka MaRSovskega morilca se mi je v spomin najbolj vtisnil „pokol“ na žar večeru. V eni noč mi je uspelo ubiti še zadnje tri kandidate, enega z zasedo in pomočjo ostalih mentorjev, druga dva pa v jedilnici, kjer sem Matiji (žar mojstru) najprej oskrbela manjšo opeklino, par minut kasneje pa še odskrbela iz igre. Spomnim se tudi branja MaRSovskega dnevnika cimram vsako jutro ter nadobudno spremljanje Instagrama za naše slike, ali pa ponočevanje z družabnimi igrami, da je naše navdušenje odzvanjalo po domu do poznih ur.

Tabor bi priporočala vsem matematičnim nadobudnežem, saj je res nepozabna izkušnja. Mentorji poskrbijo, da je vse super, jutranja telovadba ter pohod pa sta bila ravno prav za skupino nadobudnih matematikov.

MaRSa se bom zagotovo udeležila še naslednje leto, saj je bil ta tabor nepozaben.

Jure

Veš, da je tabor dober, ko spremeni tvojo študijsko izbiro in je spanec po njem kot udarec lokomotive.

Manifestacije dni s sumljivo visokimi razmerji energije proti spancu MaRSa niso omejene na ustanavljanje zadruge poštenih modrih kmetov v Avalonu (igranje družabnih iger), treniranje železnega želodca s preobilnimi količinami Cedevite (ustvarjanje notranjih šal) in odvisnosti od kart Jane Street (te karte so res dobre), ampak vključijo tudi pletenje najboljših prijateljstev, ki ostanejo tudi onkraj tabora in postanejo del tebe.

Na MaRS sem prišel kot fizik, ki je sovražil vsako idejo statistike, in odšel kot matematik na drugem prijavnem roku, ki vsepovsod, kjer nastopajo neodvisne in enako porazdeljene slučajne spremenljivke, vidi centralni limitni izrek. Tabor ima nepopisno moč vzbuditi ljubezen do raznih področij matematike, ki jih morda prej celo nisi maral.

Poleg izjemnih prijateljev, kvalitetnega znanja in neskončnih zalog Cedevite sem spoznal, da matematiki radi ostajajo fit. Vsak dan je bila neka fizična aktivnost, na kateri sem ali spoznal, da sem podpovprečen v igri med dvema ognjema (tolažim se s tem, da so drugi nadnaravno dobri), ali da se najboljše teme pogovorov razkrijejo med daljšimi pohodi.

Zadnji dan smo vsi opazovali svoje presenetljivo dobre izdelke in cenili svoje nove sposobnosti in znanja v matematiki, programu LaTeX in Pythonu, ko smo se žal morali posloviti. Čeprav teden mine bistveno prehitro, ostanejo nove izkušnje, prijateljstva in znanja za vedno, tega pa ti nihče ne more odvzeti.

Ko sem prišel domov, sem (po zelo potrebnih 18 urah spanca) pogledal nazaj na ta teden in vedel, da je bil pravilna izbira.

Manca

»Valovanje 3,« bi ob prihodu in tradicionalnem pozdravu izjavil veteranski igralec igre Codenames in ponosen udeleženec tabora MaRS, osrednjega poletnega dogodka vsakega ljubitelja matematike.

Čeprav na začetku letošnje avanture, ki je potekala v enem izmed delov Pohorja vseh časov, stari uživači Cedevite velikega števila elementov množice prišlekov nismo prepoznali, smo jih v končnem času vseeno predstavili grupi izbranih družabnih in drugih avalonskih iger. Medtem ko smo se nekateri poskušali spomniti vlog v Coupu (posebna

zahvala za Official Rule Book gre Percivalu Modremu iz Dupleka pri Aleksandriji), je zelo glasna aliansa Škofje Loke, ki po zadnjih informacijah ni touch, v ratu uspela pretentati celo visokotehnološke merilce petja (kot hobi).

Seveda pa na taboru nismo dopustili družabnim igram, da bi narekovale naš vsakdan; MaRS ne bi bil MaRS brez pisanja matematičnih člankov, ki se je brez težav zavleklo do novic v zgodnjih jutranjih urah. Eni ob kavi, drugi pa ob starani Cedeviti, smo se tako popotniki kot kockarji spoprijeli z zanimivimi matematičnimi temami in skozi projekte vztrajno urili svoje linearne sposobnosti. Naše urnike so zapolnile tudi delavnice in predavanja, med katerimi se je morda kdaj kakšen det zložo, a se večinoma nismo zašvicali ful.

Kljub izjemnemu programu, ki nas je spremljal ves teden, smo vsi težko pričakovali zadnji večer tabora. Takrat sta se zvrstila pustolovščina in piknik, na katerem so se nam pridružili tudi nekateri bivši udeleženci in nam morda celo poskusili ukrasti copat ali dva, pred našim pragom pa so se pozno ponoči prikazali tudi taki, ki so v želji po pravem MaRSovskem druženju prileteli naravnost iz angleške banje.

Kaj bi veteran in ponosen MaRSovec izjavil ob odhodu, ni znano, saj verjetno spi in nabira energijo za popravljanje članka, a po vsej verjetnosti bi skupaj z novimi prijatelji in vsem znanjem, ki ga je prejel na taboru, povzel nekega spreobrnjenega fizika: “Bil sem tam!”

Jakob

MaRSovska izkušnja je bila zelo pozitivna. Z besedami težko povzameš, zakaj si je ta tabor zaslužil poseben prostor v mojem srcu. Matematične aktivnosti skupaj z odlično družbo lepo zaokroži in izpolni to, kar bi tabor zares moral biti. Ljubezen do matematike, verjamem, da gojijo tudi mnogi drugi. Tista ideja o bolj splošni stvari, novega pogleda na problem, ki razjasni in zadane bistvo problema, pa naj bo to topologija, abstraktna algebra ali pa kaj drugega.

Na MaRSu se mi zdi, da se tak način mišljenja spodbuja in goji, ne samo od mentorjev do dijakov, temveč tudi med vrstniki, ki debatirajo in se spodbujajo, inspirirajo. Način učenja prof. Bašiča je bil še posebej učinkovit, saj smo namesto izrekov in dokazov delali primere in s tem počasi skozi intuicijo in iskanjem vzorca prišli do posplošitve - izreka. Motiviral nas je, da smo samo skozi konstrukcije razmislili o bolj splošni ideji in smo za izreke razumeli, zakaj kako so sploh nastali.

Poleg matematike smo seveda tudi počeli obmatematične posle, kot na primer Avalon, kjer smo se za preostanek dneva preobrazili v spletkarje in preračunljivce ali pa poštene modre kmete. Ko je ponoči ura odbila tri, smo odprli novice. Dlje kot smo se zabavali, bolj so padale naše linearne sposobnosti (po krivulji slovenske funkcije).

Zjutraj smo se zbudili utrujeni, a je jutranja telovadba poskrbela, da smo bili čez dan vsaj približno prisotni. Zjutraj smo se med drugim igrali tudi »med dvema ognjema«, kjer je bilo za nekatere zelo hitro konec veselice, saj jih je Primož izločil s svojimi natančnimi in hitrimi streli. Cedevita je bil tudi zelo pomemben del tabora. Poleg nacejanja omenjene pijače, smo na MaRSovski pustolovščini lani videli vzpon tako imenovanih »cedevita enjoyerjev«, ki so zmagali, in letošnji padec enako imenovane ekipe, ki je bila zadnja. MaRS je bila odlična izkušnja, saj je vsak dobil priložnost, da je spoznal matematične sovrstnike in stkal nova prijateljstva. Marsikdo je tudi spoznal bodoče sošolce ali pa spreobrnil kakšnega fizika v matematika.

PODPORNIKI

DMFA Slovenije

Društvo matematikov, fizikov in astronomov Slovenije je stanovska organizacija, ki združuje pedagoge, raziskovalce in študente. Ustanovljeno je bilo leta 1949. Društvo skrbi za popularizacijo matematike, fizike in astronomije med mladimi in v širši javnosti. Organizira tekmovanja iz znanja, ki se jih vsako leto udeleži več kot 100000 tekmovalcev. Organizira znanstvena srečanja in promovira znanstvene dosežke svojih članic in članov. Izdaja društveno glasilo Obzornik za matematiko in fiziko in Presek, list za mlade matematike, fizike, astronome in računalnikarje. Društvo aktivno deluje v mednarodnih združenjih na posameznih področjih in sodeluje z društvi, raziskovalnimi organizacijami in pedagoškimi inštitucijami v Sloveniji.

Zavarovalna skupina Sava

Zavarovalna skupina Sava je k strankam usmerjena, prilagodljiva in trajnostno naravnana zavarovalniška skupina s posli na več kot 110 zavarovalnih in pozavarovalnih trgih sveta. Skupina ponuja zavarovalne, pozavarovalne in pokojninske rešitve ter storitve upravljanja premoženja.
Matična družba Sava Re, d.d., zagotavlja pozavarovalne storitve več kot 450 partnerjem po vsem svetu. Z družbami je prisotna v šestih državah regije Adria in je tako ena večjih zavarovalniških skupin s sedežem v jugovzhodni Evropi. Bonitetni agenciji S&P Global Ratings in AM Best sta v letu 2023 Savi Re obnovili bonitetno oceno kreditne sposobnosti in finančne moči »A« s stabilno napovedjo. V letu 2023 je obseg poslovanja skupine znašal več kot 910 milijonov EUR, dobiček pa 65 milijonov EUR.

UL FMF

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

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:

Univerza v Mariboru

Fakulteta za naravoslovje
in matematiko

- **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.

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.

AFLabs

Smo mednarodno razvojno raziskovalno podjetje, ki se ukvarja z unikatnimi projekti, ki zahtevajo visoko raven tehničnega znanja, natančnosti, ekipnega dela, izkušenj in zanesljivosti.

3K IT

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 strastjo 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.

Dewesoft

Dewesoft je tu, da izzove in spremeni svet merilne tehnologije. Razvijamo testne in merilne rešitve, usmerjene k strankam, tako da vedno razmišljamo drugače in se potiskamo nad najvišje standarde. Vse se je začelo s preprosto zamislijo, ki je zdaj prerasla v globalni uspeh, saj ponuja merilne rešitve vodilnim svetovnim blagovnim znamkam.