



PRESEK

- KAKO Z MATEMATIKO DO NAJBOLJŠEGA ZASLUŽKA?
- POIZKUŠEVALNICA
- PENTOMINO
- NAGRADNA KRIŽANKA



ISSN 0351-6652



9 770351 665456

Sestavljanje koščkov

➤ Sestavljanje razbitih koščkov je težko samo po sebi, lahko pa si predstavljamo, da opravilo postane še težje, ko preteče tisoče let in se zamenja nekaj civilizacij. Arheologi, ki se soočajo s stotinami tisočev koščkov določenega najdišča, so se obrnili na matematiko, da jim pomaga pri ponovnem sestavljanju delcev. Koščke najprej digitalno skenirajo. Potem programska oprema uporablja geometrijo, kombinatoriko in statistiko, da rekonstruira starodavne ročne izdelke, celo če manjkajo mnogi delčki.

Matematika se uporablja tudi v drugih novih pristopih k arheologiji in paleontologiji: v natančnem kartografiranju zakopanih ladijskih razbitin in pri ponovni ustvaritvi gibanja dinozavrov. V takih in drugih podobnih primerih nam uspeh, morda paradoksalno, omogoči boljše razumevanje preteklosti. Naj gre za izboljšanje osnovnih tehnik, kot je to na primer trianguliranje, ali za zapletene objekte, kot so na primer parcialne diferencialne enačbe, matematični raziskovalci orjejo ledino pri razkrivanju starodavnih skrivnosti. ✕



POJASNILO: Gornji prispevek je prevod iz rubrike "The Mathematical Moments", ki jo objavlja Ameriško matematično društvo AMS na spletni strani www.ams.org/mathmoments.

➤ Presek

list za mlade matematike, fizike, astronome in računalnikarje
letnik 34, šolsko leto 2006/2007, številka 5

Uredniški odbor: Vladimir Batagelj, Tanja Bečan (jezikovni pregled), Mojca Čepič, Mirko Dobovišek (glavni urednik), Vilko Domajnko, Darjo Felda (tekmovanja), Bojan Golli, Andrej Guštin (astronomija), Marjan Jerman (matematika), Martin Juvan, Maja Klavžar (odgovorna urednica), Damjan Kobal, Andrej Likar (fizika), Matija Lokar, Franci Oblak, Marijan Prosen, Marko Razpet, Andrej Taranenko (računalništvo), Marija Vencelj, Matjaž Vencelj.

Dopisi in naročnine: DMFA-založništvo, Presek, Jadranska ulica 19, p. p. 2964, 1001 Ljubljana, telefon (01) 4766 553, 4232 460, telefaks (01) 2517 281.

Internet: www.presek.si

Elektronska pošta: presek@dmfa.si

Naročnina za šolsko leto 2006/2007 je za posamezne naročnike 16,69 EUR (3.999,59 SIT) – posamezno naročilo velja do preklica, za skupinska naročila učencev šol 14,61 EUR (3.501,14 SIT), posamezna številka 3,76 EUR (901,05 SIT), dvojna številka 6,89 EUR (1.651,12 SIT), stara številka 2,71 EUR (649,42 SIT), letna naročnina za tujino pa znaša 25 EUR.

Transakcijski račun: 03100-1000018787.

Devizna nakazila: SKB banka d.d. Ljubljana, Ajdovščina 4, 1513 Ljubljana, SWIFT (BIC): SKBASIX, IBAN: SI56 0310 0100 0018 787.

List sofinancirata Javna agencija za raziskovalno dejavnost Republike Slovenije ter Ministrstvo za šolstvo in šport

Založilo DMFA-založništvo

Oblikovanje, ilustracija in tehnično urejanje

Polona Šterk in Matjaž Čuk

Tisk Tiskarna Pleško, Ljubljana

Naklada 2100 izvodov

© 2007 Društvo matematikov, fizikov in astronomov Slovenije – 1665

Razmnoževanje ali reproduciranje celote ali posameznih delov brez poprejšnjega dovoljenja založnika ni dovoljeno.

Poština plačana pri pošti 1102 Ljubljana

NAVODILA SODELAVCEM PRESEKA ZA ODDAJO PRISPEVKOV

Presek objavlja poljudne in strokovne članke iz matematike, fizike, astronomije in računalništva. Poleg člankov objavlja prikaze novih knjig s teh področij in poročila z osnovnošolskih in srednješolskih tekmovanj v matematiki in fiziki. Prispevki naj bodo zanimivi in razumljivi širšemu krogu bralcev, učenec višjih razredov osnovnih šol in srednješolcem.

Članek naj vsebuje naslov, ime avtorja (oz. avtorjev) in sedež institucije, kjer avtor(ji) dela(jo). Slike in tabele, ki naj bodo oštevilčene, morajo imeti dovolj izčrpen opis, da jih lahko večinoma razumemo ločeno od besedila. Slike v elektronski obliki morajo biti visoke kakovosti (jpeg, tiff, eps, ...), velikosti vsaj 8 cm pri ločljivosti 300 dpi. V primeru slabše kakovosti se slika primerno pomanjša ali ne objavi. Avtorji člankov, ki želijo objaviti slike iz drugih virov, si morajo za to sami priskrbeti dovoljenje (copyright). Zaželeno velikost črk je vsaj 12 pt, razmak med vrsticami pa vsaj 18 pt.

Prispevke pošljite odgovorni urednici na naslov uredništva DMFA-založništvo, Uredništvo revije **Presek**, p. p. 2964, 1001 Ljubljana ali na naslov elektronske pošte presek@dmfa.si.

Vsak članek se praviloma pošlje vsaj enemu anonimnemu recenzentu, ki oceni primernost članka za objavo. Če je prispevek sprejet v objavo in če je besedilo napisano z računalnikom, potem uredništvo prosi avtorja za izvorno datoteko. Le-te naj bodo praviloma napisane v eni od standardnih različic urejevalnikov TeX oziroma LaTeX, kar bo olajšalo uredniški postopek.

Avtor se z oddajo članka strinja tudi z njegovo kasnejšo objavo v elektronski obliki na internetu.

Kazalo

■ MATEMATIČNI TRENUTKI

Sestavljanje koščkov 2

■ MATEMATIKA

Kako z matematiko do najboljšega zaslužka? (*Janez Povh*) 4-8
Številski sistemi (*Janko Bračič*) 9-11

■ FIZIKA

Kvantna kriptografija - Prvi del
- Kvantni bankovci (*Marko Žnidarič*) 12-15, 18
Kuhinjska poizkuševalnica-Kartezijev plavač (*Mojca Čepič*) 18-19
Kuhinjska poizkuševalnica-Kaj se zgodi pri soljenju ledu,
odgovor na nalogo iz prejšnje številke (*Mojca Čepič*) 20-21

■ ASTRONOMIJA

Tuji planeti - zgodovina odkrivanja (*Nikolaj Štritof*) 22-26

■ RAČUNALNIŠTVO

Pentomino (*Igor Pesek*) 27-30
Rešitvi nagradnih nalog 30

■ RAZVEDRILO

Nagradna križanka (*Marko Bokalič*) 16-17
Rešitev nagradne križanke Presek 34/4 18
Sudoku 25

■ TEKMOVANJA

6. tekmovanje dijakinj in dijakov srednjih poklicnih šol v
znanju matematike (*Dušanka Vrenčur*) 8-9
50. matematično tekmovanje srednješolcev Slovenije priloga
Šolsko tekmovanje iz znanja poslovne matematike
za bronasto priznanje priloga
Državno tekmovanje v poslovni matematiki 2006 priloga
Mednarodno matematično tekmovanje mest (Pomladanski krog) .. priloga

Kako z matematiko do najboljšega zaslužka?

JANEZ POVH

■ Veselje in težave sosedu Blaža

➔ Sosedu Blažu je res padla sekira v med. Natančneje, sreča ga je obiskala nepričakovano in mu prinesla 25.000 evrov. Za človeka, ki je prvič poskusil z igro na srečo, je ta loterijski dobiček res izjemna sreča.

A vsaka palica ima dva konca. Če je en konec dober, je drugi navadno manj prijeten. Tako je tudi pri Blažu. Druga plat zgodbe so hude skrbi, kaj narediti s srečnim dobitkom. Ker je pravi Gorenjec, hoče Blaž s tem denarjem čim boljje ravnati, da ga bo čez kako leto še več. Toda kako veliki dobiček oplemeniniti?

Novica o Blaževi sreči se je seveda hitro razširila, z njo pa vsaj tako hitro tudi krog njegovih prijateljev. V njegovi bližini se je začel kazati tudi znanec Polde, ki je vedno z nečim trgoval in je pogosto potreboval svež denar za reševanje stisk z zalogami. V tem času se je ukvarjal z lesom in si je spet ustvaril preveliko zalogo. Blažu je zato začel prigovarjati, naj mu posodi del denarja za eno leto, on pa mu za vsakih 1.000 evrov posojila čez eno leto namesto obresti da en kubik suhih bukovih drv (ki je tako na oko vreden 100 evrov). Blaž se bolj navdušuje za borzo. Izračunal je, da bi mu investicija v manj rizične sklade prinesla v naslednjem letu na vsakih 1.000 evrov še 90 evrov dobička.

Položaj je v resnici malce bolj zapleten. Ta znanec Polde je z Blaževo ženo v sorodu, tovrstne vezi pa je treba negovati (no, tudi suha drva bo potreboval, saj je nafta zelo draga), zato bi Poldetu posodil nekaj denarja (vsaj 3.000 evrov), vendar gotovo ne več kot 10.000 evrov. Po drugi strani pa naložba v vrednostne papirje jamči omenjen donos le, če je naloženi znesek večji od 10.000 evrov. Blaž ima precej več zaupanja v sklad kot v Poldeta, zato si želi, da je znesek, ki ga bo vložil v sklad, vsaj za 1.000 evrov večji od dvakratnika zneska, posojenega Poldetu. Za

nameček namerava Blaž izvesti še nekaj popravil na hiši, ki bodo stala do 3.000 evrov in jih tudi želi plačati z loterijskim dobitkom. Njegova žena bi bila ob vsem tem prav zadovoljna, če bo še kaj ostalo doma kar tako, za priboljšek.

Blaž si sedaj vneto prizadeva ugotoviti, kako naj razporedi nepričakovano dobljeni denar, da bi imel po enem letu največji dobiček, hkrati pa bi upošteval omenjene omejitve.

Če bi Blaž ne stremel po največjem dobičku, bi bil problem preprost. Poldetu bi posodil npr. 5.000 evrov, v sklad bi dal 15.000 evrov, preostalih 5 tisočakov pa bi porabil za popravilo hiše in zase. Čez eno leto bi s tem zaslužil 5 kubikov suhih drv in še $15 \cdot 90 = 1.350$ evrov pri skladu, kar bi bilo skupaj vredno 1.850 evrov. Ta rešitev je dobra (upošteva vse zahteve), žena bi bila gotovo zadovoljna, vendar verjetno ni optimalna (ne prinese največjega možnega dobička).

Blaž ve, da denar ne leži na cesti in da je treba varčevati takrat, ko imaš denar, in ne takrat, ko ti ga zmanjka. Torej hoče največji možni dobiček.

■ Zapišimo Blažev problem matematično

Poglejmo, kako bi opisani problem zapisali bolj matematično. Iščemo torej takšni vsoti, ki naj ju Blaž posodi Poldetu oziroma naloži v sklad, da bo zadoščeno vsem omejitvam, dobiček po enem letu pa bo največji. Zaradi preglednosti naj bodo vsote merjene v tisočakih. Označimo z x in y iskani vsoti (x je seveda vsota za Poldeta, merjena v tisoč evrov, y pa vsota za sklad). Zahtevo, da Poldetu posodi med 3.000 in 10.000 evrov, zapišemo kot $3 \leq x \leq 10$. Vsota, vložena v sklad, mora biti vsaj 10.000, kar pomeni $y \geq 10$. Ker mora biti y vsaj za 1.000 večji od dvakratnika x , to pomeni $y \geq 2x + 1$. Skupaj vloženi denar ne sme preseči 22.000 evrov, če hočemo, da še kaj ostane za priboljšek in za plačilo popravil na hiši. To seveda pomeni $x + y \leq 22$.

Ker x tisočakov, ki jih Blaž posodi Poldetu, pomeni pa enem letu x kubikov drv, vsak kubik pa je vreden 100 evrov, kar je 0,1 tisočaka, je skupni dobiček, ki ga bo Blaž prejel v enem letu, enak $0,1x + 0,09y$. Zgornji problem lahko torej zapišemo tako: poišči tak par števil (x, y) , da bo imela funkcija

$$\blacksquare \quad 0,1x + 0,09y$$

največjo vrednost med vsemi pari, ki zadoščajo pogojem

- $x + y \leq 22$
- $x \geq 3$
- $x \leq 10$
- $y \geq 10$
- $2x + 1 \leq y$.

■ Nekaj opomb k obravnavanemu problemu

V zgornjem problemu je funkcija dobička linearna (neznanki nastopata le kot x in y in ne kot npr. x^2 ali e^x ipd.), prav tako so vse neenačbe linearne. Tak problem, pri katerem iščemo ekstremno vrednost linearne funkcije (to funkcijo v splošnem imenujemo *namenska funkcija*), ki zadošča določenim linearnim neenačbam, imenujemo *problem linearne optimizacije* ali tudi *linearni program*. Z reševanjem tovrstnih problemov se ukvarja posebna disciplina uporabne matematike, imenovana *operacijsko raziskovanje*, katere začetek sega v obdobje druge svetovne vojne. V dobrih šestdesetih letih razvoja so bile razvite številne metode, s katerimi lahko rešimo linearne programe večje razsežnosti.

Študentje, ponekod pa tudi že dijaki, se učijo navadno grafično in simpleksno metodo. Prva je primerna predvsem za reševanje linearnih programov, kjer nastopata le dve spremenljivki, kot v našem primeru. Bralec lahko najde opis prve metode v nadaljevanju tega prispevka, za opis simpleksne metode pa priporočamo literaturo [1, 2, 4].

Simpleksna metoda, ki jo je leta 1947 v osnovni izvedbi predstavil Georg Dantzig, omogoča reševanje linearnih programov z več spremenljivkami. V desetletjih uporabe in nadaljnjega razvoja se je pokazalo, da je ta metoda v praksi izjemno učinkovita, in do predstavitve metod notranjih točk (prvo tovrstno metodo je leta 1984 predstavil indijski matematik Karmakar) ni imela nobene resne alternative (več o metodah notranjih točk za linearno programiranje lahko bralec najde v [3]).

Za izvajanje simpleksne metode in metod notranjih točk je smiselna uporaba računalnika. Na internetni strani¹ lahko bralec najde najaktualnejše računalniške programe za reševanje linearnih programov. Večina teh programov uporablja kombinacijo simpleksne metode in ene od izvedb metod notranjih točk. Analiza učinkovitosti teh programov, ki je





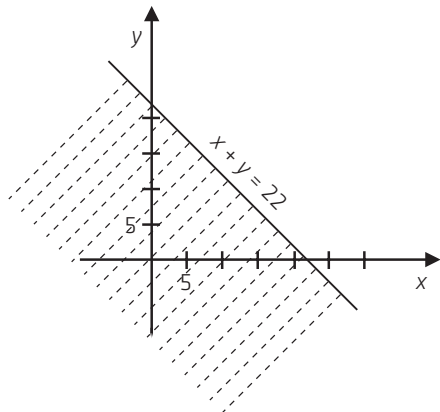
predstavljena na domači strani Hansa Mittelmann², pokaže, da večina računalniških programov lahko v nekaj minutah reši linearni program, kjer je nekaj 100.000 spremenljivk in nekaj 100.000 neenačb. Iz te domače strani lahko tudi sklepamo, da je med najučinkovitejšimi programski paket CPLEX³. Večina proizvajalcev nudi tudi brezplačno poskusno različico, kjer pa je velikost problema navadno omejena na okrog 1.000 spremenljivk in 1.000 neenačb.

Najhitrejši način za reševanje manjših linearnih programov je uporaba kakšnega interaktivnega spletnega programa, kot sta npr. programa na internetnih straneh <http://www-fp.mcs.anl.gov/otc/Guide/CaseStudies/simplex/index.html> (november 2006) in http://people.hofstra.edu/faculty/Stefan_Waner/RealWorld/simplex.html (november 2006). Bralec lahko z malce truda uporabi tudi dodatek Reševalec v programu Excel.

■ Rešimo matematični problem grafično

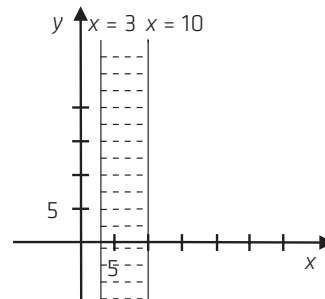
Linearni program, ki smo ga priredili Blaževemu problemu, ima le dve neznanki, zato ga je mogoče rešiti z grafično metodo. Pri tej metodi najprej predstavimo v ravnini vse točke (x, y) , ki zadoščajo vsem neenačbam. Nato premislimo, kako izgledajo v ravnini tiste točke, kjer ima namenska funkcija konstantno vrednost, in s pomočjo tega premisleka poiščemo tisto točko, kjer je dosežen optimum namenske funkcije.

Oglejmo si najprej, kako izgleda v ravnini množica točk (x, y) , katerih koordinati x in y zadoščata neenačbi $x + y \leq 22$. To so tiste točke, ki ležijo pod premico $x + y = 22$ (slika 1). Podobno so točke, katerih



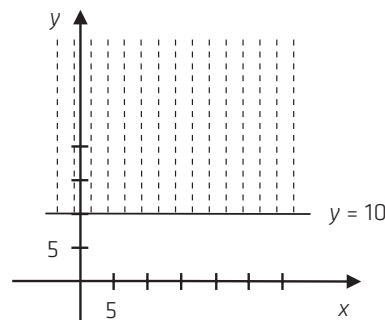
Slika 1. Rešitve neenačbe $x + y \leq 22$

koordinata x zadošča drugima dvema neenačbama, tiste, ki so med premicama $x = 3$ in $x = 10$ (slika 2).



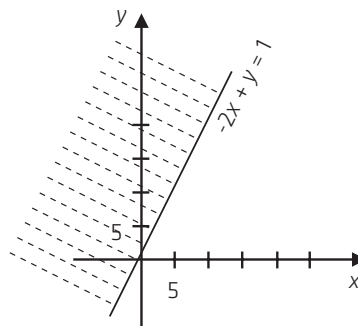
Slika 2. Rešitve neenačbe $3 \leq x \leq 10$

Točke, ki predstavljajo rešitve četrte neenačbe, so na sliki 3. Oglejmo si sedaj zadnjo neenačbo. Zapišemo



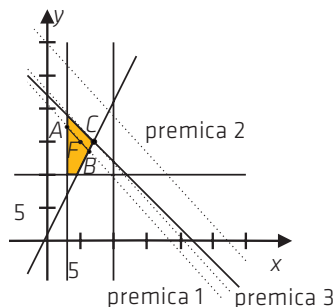
Slika 3. Rešitve neenačbe $y \geq 10$

jo lahko kot $-2x + y \geq 1$. Točke, ki predstavljajo njeno rešitev, so na eni strani premice $-2x + y = 1$. Ker par $x = 0, y = 5$ zadošča tej neenačbi, je prava stran premice tista, ki vsebuje to točko, torej zgornja stran (slika 4).



Slika 4. Rešitve neenačbe $-2x + y \geq 1$

Grafično predstavitev parov (x, y) , ki hkrati rešijo vse neenačbe, dobimo tako, da vzamemo presek ob-



Slika 5. Dopustna množica za naš linearni program

močij s slik 1-4. To območje je večkotnik, predstavljen na sliki 5. Katerakoli točka (x, y) iz tega večkotnika predstavlja za Blaža rešitev, ki ustreza vsem pogojem (neenačbam) in je torej dobra rešitev, ni pa nujno najboljša oziroma optimalna. Množico dobrih rešitev, ki jo predstavlja omenjeni večkotnik, imenujemo tudi *dopustna množica*. Rešitev $x = 5$ in $y = 15$ iz prejšnjega razdelka predstavlja točka F iz notranjosti dopustne množice.

Blažev problem bomo rešili, če bomo med vsemi dobrimi rešitvami našli optimalno, torej tako, pri kateri je namenska funkcija $0,1x + 0,09y$ največja.

Kot smo že ugotovili, ima v točki F ta funkcija vrednost 1,85. Poglejmo sedaj, če je še kakšna točka iz ravnine taka, da ima namenska funkcija tam vrednost 1,85. Vse take točke so ravno rešitve enačbe $0,1x + 0,09y = 1,85$, grafično pa jih predstavimo kot premico 1 na sliki 5. Presečišče te premice z dopustnim območjem je daljica AB , točke s te daljice pa pripadajo vsem tistim dopustnim parom (x, y) , pri katerih je dobiček enak 1,85.

Ker iščemo največji možni dobiček, se sedaj vprašajmo še, za katere točke (x, y) velja, da je dobiček $0,1x + 0,09y$ enak npr. 2,7? To so točke, ki na sliki 5 ležijo na premici 2. Vendar pa nobena od teh točk ne zadošča našim neenačbam, saj premica ne seka večkotnika dopustnih rešitev. Ne glede na to pa smo ugotovili pomembno lastnost: namenska funkcija ima na premicah, vzporednih s premico 1, ves čas enako vrednost. Če je vzporednica desno od premice 1, je ta vrednost večja od 1,85, sicer pa manjša. Iskanje dopustne rešitve (x, y) , pri kateri je dobiček največji, je torej enakovredno iskanju vzporednice, ki je od premice 1 najbolj oddaljena v desno, a še

vedno seka naš večkotnik. Tako vzporednico lahko dobimo, če premico 1 počasi vzporedno premikamo v desno tako daleč, da pridemo do zadnje točke večkotnika, t.j. do točke, ko z najmanjšim nadaljnjim vzporednim pomikom v desno premica ne seka več našega večkotnika.

Ugotovimo, da je taka skrajna vzporednica ravno premica 3, zadnja točka pa točka $C(7, 15)$, ki je presečišče premic $x + y = 22$ in $-2x + y = 1$. Koordinati te točke $x = 7$ in $y = 15$ sta tako najboljša rešitev linearnega programa, saj zadoščata vsem neenačbam in ima namenska funkcija pri njej največjo vrednost: $0,1 \cdot 7 + 0,09 \cdot 15 = 2,05$.

■ Analiza rešitve in nadaljnji zapleti

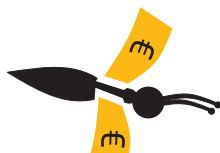
Postopek reševanja iz prejšnjega razdelka torej pove, naj Blaž posodi Poldetu 7.000 evrov, v sklad pa naj naloži 15.000 evrov. Za popravilo hiše in za približek mu ostane 3.000 evrov. Tako zasnovana naložba mu čez eno leto prinese sedem kubikov drv, kar je vredno 700 evrov, in 1.350 evrov, skupno torej 2.050 evrov. Rešitev je uporabna, saj ustreza vsem zahtevam, daje največji dobiček in je v praksi izvedljiva.

Seveda se pred izvedbo take naložbe lahko zaplete. Lahko se zgodi, da Polde namesto bukovih ponudi smrekova drva, ki so vredna manj. Prav tako se lahko zgodi, da žena ni zadovoljna s tem, da tako malo ostane doma, in hoče drugačno razporeditev denarja. Prva sprememba vpliva na namensko funkcijo, druga pa na neenačbe v linearnem programu. Oboje ima lahko za posledico drugačno optimalno rešitev. Analiza vpliva teh sprememb na optimalno rešitev se imenuje analiza občutljivosti in zahteva natančnejši vpogled v področje linearne optimizacije.

Seveda pa se lahko problem tudi razširi. Denimo, da Blaž razmišlja o vezavi dela sredstev na banki (donos je sicer majhen, varnost pa velika). V sedanjih razmerah je ta donos približno 30 evrov letno za vsakih naloženih 1.000 evrov. Če bi Blaž hotel dati na banko vsaj 3.000 evrov, bi dobil optimalno razporeditev svojega denarja kot rešitev naslednjega linearnega programa: poišči maksimum funkcije



- 1 <http://lionhrtpub.com/orms/surveys/LP/LP-survey.html>, november 2006
- 2 <http://plato.asu.edu/bench.html>, november 2006
- 3 <http://www.ilog.com/products/cplex/>, november 2006





$$0,1x + 0,09y + 0,03z$$

pri pogojih, da količine x , y in z zadoščajo neenābam

- $x + y + z \leq 22$
- $x \geq 3$
- $x \leq 10$
- $y \geq 10$
- $-2x + y \geq 1$
- $z \geq 3$.

Ta linearni program ima tri spremenljivke, zato bi grafiāno reševanje zahtevalo risanje in vzporedno premikanje ravnin v tridimenzionalnem prostoru. Ker je list papirja dvodimenzionalen, naši moŹgani pa teŹko iz dvodimenzionalne slike delajo dobre tridimenzionalne sklepe, je tovrstno reševanje teŹavno in lahko hitro vodi do napaānih rešitev. Tako si pomagamo z drugimi metodami, omenjenimi v razdelku 3. Z uporabo enega od interaktivnih spletnih programov dobimo naslednjo rešitev: $x = 6$, $y = 14$ in $z = 3$. Najveāji dobiāek je torej 1.950 evrov in je manjši kot v prejšnjem primeru, kar gre na raāun veāje varnosti, ki izhaja iz vezave sredstev na banki.

■ Zaključek

Linearno programiranje je doseglo med vsemi matematiānimi orodji v nematematiānih vedah verjetno najveājo popularnost. Čeprav Źivljenje navadno ni linearno, pa ga vsi radi poenostavljamo do te mere, da postane linearno, to pa potem omogoāa uporabo linearnega programiranja.

Iz prispevka sicer ni razvidno, kaj je BlaŹ na koncu storil, upamo pa, da je bralec prepoznal v opisanem pristopu naāin, kako lahko rešimo mnogo optimizacijskih problemov. Grafiāna metoda je gotovo zelo preprosta metoda za reševanje, a zaradi omejenosti na linearne programe z dvema spremenljivkama navadno ni uporabna. V prispevku omenjene metode notranjih toāek in simpleksna metoda so trenutno pravi naāin za reševanje veājih linearnih programov. Ker pa ima veāina bralcev dostop do interneta, je najenostavnejši naāin za reševanje linearnih programov kar uporaba spletnih reševalcev. Nekaj predlogov je podanih v razdelku 3, seveda pa lahko bralec sam vnese v enega od spletnih iskalnikov ključne besede *simplex method*, *linear programming* itd. Vi-

del bo, da je ponudba zelo velika in da so Źe prvi zadetki zelo uporabni.

■ Literatura

- [1] A. Vadal, *Rešeni problemi linearnega programiranja*, DrŹavna zaloŹba Slovenije, Ljubljana, 1972.
- [2] D. Hvalica, *Linearno programiranje in njegova uporaba*, Univerza v Ljubljani, Ekonomska fakulteta, 2005.
- [3] S. J. Wright, *Primal-dual interior-point methods*, SIAM, Philadelphia, 1997.
- [4] W. L. Winston, *Operations Research: Applications and Algorithms*, Duxbury Press, Belmont, CA, 1994. ☒

6. tekmovanje dijakinj in dijakov srednjih poklicnih Źol v znanju matematike

DUŠANKA VRENČUR

☛ Na Źolskem tekmovanju je letos tekmovalo 1757 tekmovalcev. Društvo matematikov, fizikov in astronomov Slovenije, Tehniški Źolski center v Kranju in Zavod RS za Źolstvo so bili 22. 4. 2006 organizatorji 6. drŹavnega tekmovanja v znanju matematike za 54 najboljših dijakinj in dijakov srednjih poklicnih Źol iz 32ih slovenskih poklicnih Źol. Med njimi je bilo podeljenih 17 zlatih priznanj. Na sveāani podelitvi je organizator prvim trem najbolje uvršāenim iz vsakega letnika podelil priznanja in praktiāne nagrade. Prejeli so jih:

1. NAGRADA

■ Prvi letnik

- TOMAŽ TREFALT, ŠC Krško – Srednja šola Sevnica

■ Drugi letnik

- GREGOR ZIDARIČ, ŠC Ptuj – Poklicna in tehniška strojna šola

■ Tretji letnik

- JOŽEF FLORJANČIČ, Kmetijska šola Grm Novo mesto

2. NAGRADA

■ Prvi letnik

- MATEJ ŠULIGOJ, TŠC Nova Gorica – Poklicna in tehniška strojna in prometna šola

■ Drugi letnik

- ĐANI ČAUŠ, TŠC Kranj

■ Tretji letnik

- MATIJA STRUGAR, TŠC Nova Gorica – Srednja lesarska in gradbena šola Nova Gorica

3. NAGRADA

■ Prvi letnik

- MIHA ANŽIČ, SŠ Domžale – Poklicna in strokovna šola

■ Drugi letnik

- MIHA JERAJ, ŠC Novo mesto – Srednja gradbena in lesarska šola

■ Tretji letnik

- BOŠTJAN MUNDA, Srednja gradbena šola Maribor ☒

Številski sistemi

JANKO BRAČIČ

➔ V 15. stoletju je uspešen nemški trgovec vprašal uglednega profesorja, na katero univerzo naj pošlje svojega sina, da bo le-ta dobro podučen o poslovnih zadevah. *Nemške univerze, mu odvrne profesor, so dovolj dobre, da se fant nauči seštevati in odštevati. Toda če želi obvladati tudi množenje in deljenje, bi moral iti na katero od italijanskih univerz.*

Preden se začnete smejati, naj povem, da so v 15. stoletju v Nemčiji števila še vedno zapisovali z rimskimi števkami. Poskusite sami zmnožiti, ali pa le sešteti, števila CCLXIV, MDCCCIX, DCL in MLXXXI, ne da bi jih prej zapisali v desetiškem številskem sistemu.

Računanje je tesno povezano s predstavitvijo števil, s katerimi računamo. Kot vidimo, so lahko osnovnejše računske operacije precej zapletene, če je predstavitev števil preveč zapletena. Veliko udobnejši za računanje kot zapis z rimskimi števkami so nekateri mestni številski sistemi.

Poglejmo najprej, kako zapisujemo števila v desetiškem sistemu. Na primer, s 54321 je predstavljeno število

$$5 \cdot 10^4 + 4 \cdot 10^3 + 3 \cdot 10^2 + 2 \cdot 10^1 + 1 \cdot 10^0.$$

Kot vidimo, je v tem zapisu zelo pomembno, na katerem mestu stoji posamezna številka. Namreč, iste številke zapisane v drugačnem vrstnem redu predstavljajo neko drugo število. Tako, na primer, predstavlja zapis 12345 število $1 \cdot 10^4 + 2 \cdot 10^3 + 3 \cdot 10^2 + 4 \cdot 10^1 + 5 \cdot 10^0$, ki seveda ni enako številu





$$5 \cdot 10^4 + 4 \cdot 10^3 + 3 \cdot 10^2 + 2 \cdot 10^1 + 1 \cdot 10^0.$$

Na splošno ima zapis realnega števila v desetiškem sistemu obliko

$$\dots d_3 d_2 d_1 d_0 . d_{-1} d_{-2} \dots,$$

pri čemer so d_i števke iz množice $\{0, 1, \dots, 9\}$. Vrednost posameznega mesta v zapisu določajo potence števila 10. Pri tem velikost potenc od leve proti desni pada. Pika v zapisu nam pove, kje se začnejo mesta, ki pripadajo potencom z negativnimi eksponenti. Zgornji zapis tako predstavlja število

$$\dots + d_3 \cdot 10^3 + d_2 \cdot 10^2 + d_1 \cdot 10^1 + d_0 \cdot 10^0 + d_{-1} \cdot 10^{-1} + d_{-2} \cdot 10^{-2} + \dots$$

Seveda število 10 lahko nadomestimo s poljubnim naravnim številom $b > 1$. Tako dobimo številski sistem z osnovo b . Na primer, ko je $b = 2$, vzamemo za množico števk $\{0, 1\}$ in govorimo o dvojiškem številskem sistemu; pri $b = 3$ in množici števk $\{0, 1, 2\}$ pa o trojiškem številskem sistemu itd. Pravzaprav pri izbiri osnove ni nujno, da se omejimo le na naravna števila, prav tako ni nujno, da je množica števk za vsako mesto ista. Splošni mestni številski sistem določata dve zaporedji: zaporedje mestnih vrednosti a_n in zaporedje množic števk za posamezno mesto, D_n . Poglejmo si nekaj primerov.

PRIMER 1. Naj bo $b \geq 2$ naravno število. Za vsako celo število n postavimo $a_n = b^n$ in $D_n = \{0, 1, \dots, b-1\}$. Ti zaporedji (a_n) in (D_n) določata običajni številski sistem z osnovo b . Sem spadajo torej dvojiški sistem, trojiški sistem itd. Predstavimo število sto v nekaterih od teh sistemov:

$$1100100_{(2)} = 400_{(5)} = 144_{(8)} = 100_{(10)} = 84_{(12)}.$$

V katerem sistemu je število predstavljeno, smo označili tako, da smo osnovo sistema zapisali v oklepaju kot indeks.

PRIMER 2. Označimo z (-3) številski sistem, ki ga določata zaporedji $a_n = (-3)^n$ in $D_n = \{-1, 0, 1\}$, pri čemer je n poljubno celo število. Primerjajmo zapis nekaterih števil v tem sistemu z zapisom v desetiškem sistemu. Na primer,

$$2_{(10)} = (-1)(-1)_{(-3)},$$

$$100_{(10)} = 1(-1)(-1)01_{(-3)} \text{ in}$$

$$(-1)10.0(-1)_{(-3)} = -15.1_{(10)}.$$

Tu smo s črto nad števkjo označili, da se števka periodično ponavlja. Premislite, katera števila so predstavljena z zapisom $100_{(-3)}, (-1)(-1)0101(-1)_{(-3)}, (-1).(-1)_{(-3)}$ in kako se v tem sistemu predstavi število $-1000_{(10)}$.

PRIMER 3. V številskem sistemu (n^2) naj mestne vrednosti določa zaporedje popolnih kvadratov $a_n = n^2$, pri čemer so indeksi le naravna števila. Torej je

a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	...
1	4	9	16	25	36	49	64	81	...

Za vsako mesto naj bo množica števk vedno ista, in sicer $\{0, 1, 2, 3\}$. Trdimo, da lahko v tem številskem sistemu zapišemo vsako naravno število. Res! Znameniti Lagrangeov izrek pravi, da lahko vsako naravno število zapišemo kot vsoto štirih ali manj popolnih kvadratov, kar celo pomeni, da v številskem sistemu (n^2) za zapis vsakega naravnega števila potrebujemo kvečjemu štiri neničelne števke. Zapiše prvih nekaj naravnih števil v tem sistemu bo bralka oziroma bralec zlahka poiskal sam/a. Za večja števila je potrebno nekoliko več dela. Tako se moramo kar nekoliko potruditi, da najdemo zapis $80_{(10)} = 1010012_{(n^2)}$, medtem ko ni težav z zapisom $81_{(10)} = 100000000_{(n^2)}$. Omenimo še, da v tem sistemu nekatera števila nimajo samo ene predstavitve. Na primer, velja

$$12_{(10)} = 3 \cdot 2^2 + 0 \cdot 1^2 = 30_{(n^2)}$$

$$12_{(10)} = 1 \cdot 3^2 + 0 \cdot 2^2 + 3 \cdot 1^2 = 103_{(n^2)}.$$

PRIMER 4. Zadnji zgled je tako imenovani *faktorialni številski sistem* (f) . Za vsako naravno število n je $n!$ označen produkt vseh naravnih števil od 1 do vključno z n . To število imenujemo *n faktorialno* (nekateri pravijo tudi *n faktulteta*). Tako je $1! = 1$, $2! = 1 \cdot 2 = 2$, $3! = 1 \cdot 2 \cdot 3 = 6$ itd. Na splošno, $n! = 1 \cdot 2 \cdot \dots \cdot (n-1) \cdot n$. V faktorialnem številskem sistemu so mestne vrednosti dane z zaporedjem $a_n = n!$:

a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	...
1	2	6	24	120	720	5040	40320	362880	...

Množica števk se od mesta do mesta spreminja: $D_n = \{0, 1, \dots, n\}$. Tako kot v prejšnjem zgledu tudi tu teče indeks n le po množici naravnih števil. V tem številskem sistemu lahko predstavimo vsako naravno število. To pomeni, da lahko vsako naravno število zapišemo v obliki

$$d_n \cdot n! + d_{n-1} \cdot (n-1)! + \dots + d_2 \cdot 2! + d_1 \cdot 1!,$$

pri čemer je $0 \leq d_k \leq k$ za vse indekse $k \in \{1, \dots, n\}$. Poglejmo, kako dano naravno število m zapišemo v faktorialnem sistemu. Števke $d_1, d_2, \dots$ dobimo tako, da število m najprej podelimo z 2. Dobimo količnik, označimo ga z m_1 in ostanek $d_1 \in \{0, 1\}$. Če je količnik m_1 različen od nič, ga delimo s 3. Pri tem deljenju dobimo količnik m_2 in ostanek $d_2 \in \{0, 1, 2\}$. S postopkom nadaljujemo, če je $m_2 \neq 0$: m_2 delimo s 4, da dobimo količnik m_3 in ostanek $d_3 \in D_3$. Vse skupaj ponavljamo tako dolgo, dokler ni nek količnik, recimo m_n , enak nič; ostanek je tedaj $d_n = m_{n-1} \in D_n$. Zdaj lahko zapišemo

$$m = d_n \cdot n! + \dots + d_2 \cdot 2! + d_1 \cdot 1! = d_n \dots d_2 d_1 (f).$$

Za vajo zapišimo število sto v faktorialnem številskem sistemu. Ker velja

$$\begin{aligned} 100 : 2 &= 50, & \text{ostane } 0 \\ 50 : 3 &= 16, & \text{ostane } 2 \\ 16 : 4 &= 4, & \text{ostane } 0 \\ 4 : 5 &= 0, & \text{ostane } 4, \end{aligned}$$

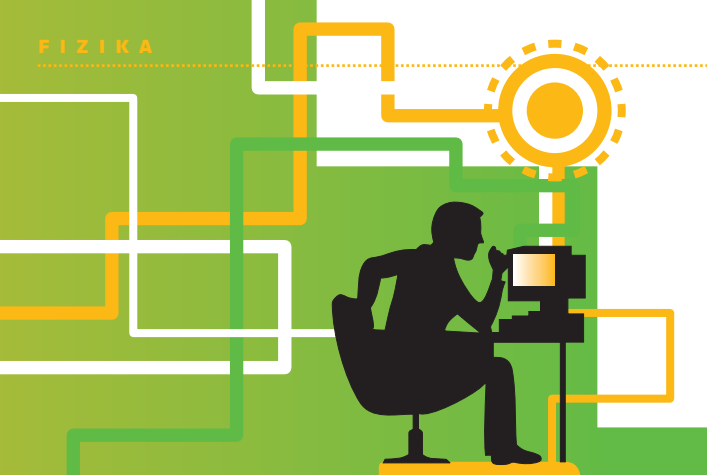
je $100_{(10)} = 4020_{(f)}$.

Kot kažejo navedeni zgledi, se lahko mestni številski sistemi precej razlikujejo med seboj. Vabim bralko oziroma bralca, da sam/a sestavi svoj številski sistem in ga razišče. Seveda, večina številskih sistemov v praksi ni uporabna, saj je lahko računanje v njih še bolj zahtevno kot pri zapisu z rimskimi številskami. Pomislite, na primer, da bi morali računati v sistemu iz tretjega zgleda, kjer mestne vrednosti določajo kvadrati naravnih števil. Tudi v faktorialnem številskem sistemu bi imeli težave z računanjem, vendar je ta sistem uporaben pri nekaterih drugih problemih, predvsem v kombinatoriki.

Zgodovina številskih sistemov je dolga in zanimiva. Začne se z Babilonci, ki so uporabljali številski sistem z osnovo 60. Kot verjetno že veste, izhaja

razdelitev ure na 60 minut in minute na 60 sekund prav iz šestdesetiškega sistema. Manj znano je, da v vsakdanjem življenju, recimo pri trgovanju, Babilonci niso uporabljali šestdesetiškega sistema, ampak so stvari kupčkali po deset, sto itd., kar pomeni, da so uporabljali desetiški številski sistem, tako kot že nekatere druge civilizacije v Mezopotamiji pred njimi. Številski sistem z osnovo 60 so uporabljali predvsem babilonski matematiki oziroma astronomi. Tudi druge stare civilizacije so se ukvarjale s številskimi sistemi. Omenimo Maje, ki so pred približno 2000 leti imeli zelo razvit dvajsetiški številski sistem. Desetiški številski sistem kot ga uporabljamo danes, je nastal okrog leta 600 v Indiji. Potem se je razširil na zahod do Perzije, kjer so ga prevzeli Arabci. V Evropi se je desetiški sistem pojavil okrog leta 1200. Da so ga sprejeli na celim kontinentu, je trajalo kar nekaj stoletij. ☘





Kvantna kriptografija

PRVI DEL - KVANTNI BANKOVCI

■ Kvantni bankovci

MARKO ŽNIDARIČ

☛ Stephen Wiesner in Charles Bennett sta se spoznala v času svojega dodiplomskega študija. Postala sta dobra prijatelja in ohranila stike tudi po končani fakulteti. Nekje v zgodnjih sedemdesetih, med enim izmed obiskov, je Wiesner navdušeno razlagal Bennettu o svoji novi ideji, kako narediti bankovce, ki bi jih bilo popolnoma nemogoče ponarediti. Ideja je bila zares "nora". Takšen super bankovec bi bil namreč kvantni bankovec. Kvantni bankovec bi imel vgrajene majhne kvantne delce, katerih obnašanje opisuje kvantna fizika. Ta pravi, da na kvantnih sistemih ni mogoče izvajati meritev, ne da bi jih pri tem vsaj majceno zmotili. Če želimo izvedeti, v katerem stanju je kvantni delec, moramo opraviti meritev, na primer tako, da na njega posvetimo s šibko svetlobo. Vendar pa delec po koncu meritve ne bo več v istem stanju kot pred njo, temveč bo naključno pristal v enem izmed stanj, ki ustrezajo vsem možnim izidom meritev. Kvantna fizika napove le verjetnosti, da delec najdemo v enem izmed teh možnih stanj, z drugimi besedami, napove verjetnosti, da pri meritvi dobimo določen rezultat, ne pa natančno, v katerem stanju ga bomo našli pri konkretni meritvi. Verjetnosti za posamezne izide meritev so natančno določene z začetnim stanjem, v katerem je bil delec, preden smo začeli z meritvijo. O tej naključnosti je Erwin Schrödinger, eden izmed pionirjev kvantne mehanike, izjavil: "Ni mi všeč in mi je žal, da sem imel karkoli opraviti z njo." Iz običajnega sveta makroskopskih teles smo namreč navajeni, da so stvari deterministične. Če poznamo stanje, v katerem je sistem, lahko natančno napovemo, kakšen bo rezultat meritve. V kvantnem svetu majhnih delcev je drugače. To, da kvantna fizika napove le verjetnosti, ne pa točnih izidov meritev, se morda na prvi pogled zdi, da je le hiba našega pomanjkljivega opisa na-

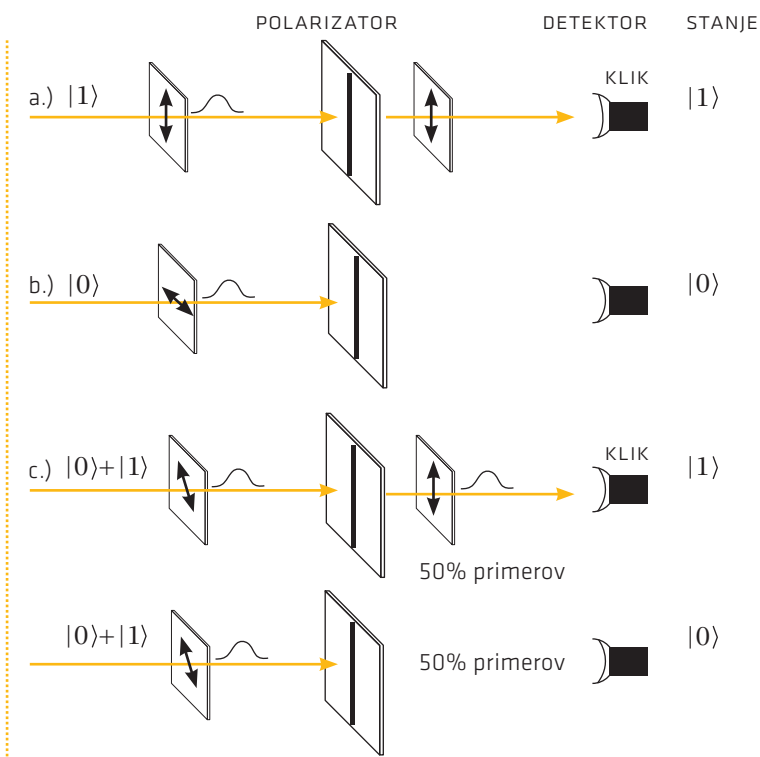
rave, torej kvantne mehanike. Vendar pa temu ni tako. Naj se nam to zdi še tako nenavadno, verjetnostim se ne da izogniti. Po kvantni meritvi je delec torej v drugem stanju kot pred njo. Natanko to lastnost kvantnih delcev pa je Wiesner izkoristil za zaščito kvantnega bankovca. Če bi hoteli izdelati dvojnik takšnega bankovca, z drugimi besedami ga ponarediti, bi morali izdelati tudi natančne kopije kvantnih delcev na tem bankovcu. Torej bi ponarejevalec moral izmeriti stanja, v katerih se ti delci nahajajo. Ker pa bi se ta stanja pri meritvi spremenila, bi to spremembo lahko zaznali in tako ugotovili, da dejansko gre za ponaredek. Ker je ta lastnost kvantnih delcev, da meritev vpliva na to, v katerem stanju bo delec po meritvi, ključna tako za kvantne bankovce kot za kvantno kriptografijo, si pogloblje oglejmo preprost primer.

Za kvantne delce bomo vzeli kar fotone, to je najmanjše nedeljive dele svetlobe. Fotoni so lahko v dveh osnovnih ortogonalnih stanjih, ki ju določa smer linearne polarizacije. Polarizacija fotona je dana kar s smerjo nihanja električnega polja. Običajna svetloba, npr. žarnice, je nepolarizirana. To pomeni, da so posamezni fotoni polarizirani v vseh možnih smereh. Če tako svetlobo pošljemo skozi posebno snov, imenovano polarizator, se le-ta polarizira. Polarizator ima namreč to lastnost, da prepušča le svetlobo s točno določeno smerjo polarizacije, npr. v navpični smeri. Svetlobo polarizirano v ortogonalni smeri, torej vodoravno, tak polarizator zadrži. Smer prepuščene svetlobe lahko seveda enostavno spremenimo tako, da polarizator zavrtimo za nek kot. Polarizator je npr. sestavni del vsakih spodobnih sončnih očal. V teh je polarizator obrnjen tako, da zadrži svetlobo polarizirano v vodoravni smeri. Ker je svetloba odbita od vodoravnih površin, npr. cest, v

večji meri polarizirana ravno v vodoravni smeri, nam to zmanjša neželeno bleščanje. Foton je lahko torej v dveh osnovnih stanjih, v takem z navpično smerjo polarizacije in v tistem z vodoravno smerjo polarizacije. Dogovorimo se, da bomo vodoravno polariziran foton označili simbolično z $|0\rangle$, navpično polariziran pa z $|1\rangle$ (nenavadna pisava ima določen pomen v kvantni teoriji, ki pa za nas ne bo pomemben). Ti dve stanji tvorita t.i. bazo, s katero lahko sestavimo foton, ki ima polarizacijo v poljubni smeri. Če polarizator obrnemo pod kotom 45° , tako da so prepuščeni fotoni polarizirani pod kotom 45° , lahko npr. te fotone opišemo kot enakomerno superpozicijo fotonov z navpično in vodoravno polarizacijo, simbolično torej kot $|0\rangle + |1\rangle$. Kako pa izmerimo polarizacijo fotona? Postopek je preprost (glej sliko 1). Če



želimo izmeriti, ali je foton v stanju $|0\rangle$ ali pa je v stanju $|1\rangle$, moramo tak foton poslati skozi polarizator, ki prepušča fotone z navpično polarizacijo. Če sedaj na detektorju fotonov, ki je postavljen za polarizatorjem, zaznamo foton, lahko upravičeno sklepamo, da je bil vhodni foton v stanju $|1\rangle$. Podobno, če detektor fotona ne zazna, sklepamo, da je bil foton v stanju $|0\rangle$, saj navpični polarizator popolnoma zadrži le fotone z vodoravno polarizacijo. Če je foton na začetku v stanju $|1\rangle$ (primer na sliki 1a) ali pa če je v stanju $|0\rangle$ (slika 1b), z interpretacijo meritve ni težav. Izmerjeno stanje fotona se ujema z začetnim stanjem. Stvari pa so drugačne, če je začetni foton polariziran pod kotom. Če je ta v stanju $|0\rangle + |1\rangle$, potem kvantni račun pokaže, da bo tak foton pola-



Slika 1. Meritev polarizacije fotona. V primeru (c) se izmerjeno stanje $|1\rangle$ ali $|0\rangle$ razlikuje od začetnega stanja $|0\rangle + |1\rangle$. Meritev je povzročila spremembo stanja.

rizator v polovici primerov prepustil, v polovici pa zadržal (slika 1c). Kateri izmed obeh primerov se bo zgodil pri konkretni meritvi, ni mogoče napovedati. To je naključnost kvantne mehanike! Sedaj tudi vidimo, da je v tem tretjem primeru detektirano stanje fotona ($|0\rangle$ ali $|1\rangle$) drugačno kot pa stanje fotona pred meritvijo. Natanko to pa bi izkoriščali kvantni bankovci. Fotoni v takšnem bankovcu bi bili polarizirani v naključnih smereh, ki bi bile znane le banki (nič seveda nismo povedali o tehnični izvedljivosti tega, da bi imeli v bankovcu "vgrajene" fotone). Da bi izdelal ponaredek, bi moral ponarejevalec izmeriti polarizacije fotonov. Pri npr. diagonalno polariziranem fotonu (primer iz slike 1c) bi glede na rezultat meritve v ponaredek vgradil foton z napačno polarizacijo $|0\rangle$ ali $|1\rangle$, ne pa $|0\rangle + |1\rangle$. To napako pa bi na banki lahko odkrili. Toliko o delovanju kvantnega bankovca.

No, Bennettu se je Wiesnerjeva ideja zdela zanimiva, tako da jo je sklenil predstaviti tudi širšemu občinstvu. Napisal je članek in ga poslal v objavo





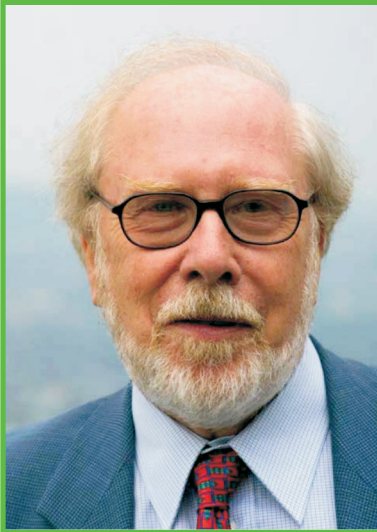
v strokovno računalniško revijo. Urednikom in recenzentom se je celotna zadeva na žalost zdela nekoliko manj zanimiva in članek so gladko zavrnil. V bran urednikom je verjetno na mestu omeniti, da je članek napisal fizik v tehničnem žargonu fizike, ki pa je bil verjetno popolnoma nerazumljiv tedanjim računalničarjem in matematikom. Da pa celotna zadeva ni tiho poniknila nekje v globinah zgodovine, se lahko zahvalimo Bennettu. Ta je s kvantnimi bankovci občasno "težil" različnim ljudem v upanju, da se bo komu vse skupaj vendarle zdelo zanimivo. Tako je preteklo kar nekaj let, dokler se ni Charles Bennett leta 1979 znašel na plaži v Porto Ricu. Na tej isti plaži je bil tudi Gilles Brassard, računalničar iz Montreala, ki se je ukvarjal s kriptografijo. Potrebno je sicer povedati, da se Bennett in Brassard nista hkrati znašla na tej plaži popolnoma po naključju. Oba sta bila namreč udeleženca kriptografske konference v San Juanu, vendar pa se osebno nista poznala. Kot se dogodka spominja Brassard, je nenadoma k njemu priplaval popoln neznanec in mu začel razlagati o kvantnih bankovcih. Brassardu se ideja o uporabi kvantne fizike za zaščito bankovca ni zdela popolnoma neumna. Osnovni princip sta z Bennetom hitro razširila na tedaj porajajočo se kriptografijo z javnimi ključi. Rodilo se je novo področje – kvantna kriptografija, ki jo lahko imamo tudi za začetnico kvantne informacijske teorije, širšega področja na stičišču fizike, matematike in računalništva, ki se ukvarja s kvantimi računalniki, kvantno teleportacijo ipd.

■ Klasični kriptografski postopki

Za srečanje Brassarda in Bennetta v San Juanu lahko rečemo, da sta bila oba ob pravem času na pravem mestu. Ob pravem času tudi zato, ker so le nekaj let prej, leta 1976, javno objavili prvi postopek za šifriranje z javnim ključem, imenovan Diffie-Hellmanov algoritem (glej tudi članek A. Jurišića, *Diffie-Hellmanov dogovor o ključu*, Presek 34(1) (2006/2007), str. 25-30). Izkazalo se je namreč, da je šifriranje z javnim ključem tisto pravo področje, kjer je mogoče z uporabo kvantne fizike narediti popolnoma nove sisteme šifriranja, ki so boljši kot pa obstoječi klasični sistemi. Pri vseh postopkih šifriranja bi radi rešili osnovni problem: poslati želimo skrivno sporočilo, pri tem pa obstaja možnost, da bo to sporočilo med potovanjem do naslovnika nekdo prebral. Ker že-

limo, da ostane vsebina sporočila kljub temu tajna, moramo pred pošiljanjem sporočilo šifrirati, prejemnik pa šifrirano sporočilo dešifrirati. Preprosti postopki šifriranja so zelo stari. Ponavadi so si jih omislili gospodje, ki so svoje besede imeli za dovolj pomembne, da so jih želeli zaupati le izbranim osebam, npr. poglavarji držav ali vojska. Vse do sedemdesetih let pa so bili znani le kriptografski sistemi z zasebnim ključem. Pri teh imata obe stranki, pošiljatelj sporočila Anja in prejemnik Boštjan, enako skrito geslo, imenovano ključ, ki ga uporabita pri šifriranju in dešifriranju. Ta ključ mora biti znan samo njima, saj je od tega odvisna varnost šifriranja. Preprost postopek šifriranja je, da npr. vsako črko abecede premaknemo za r mest oziroma, če črke predstavimo s številkami, da vsaki črki prištejemo r . V primeru $r = 1$ to pomeni, da gre $A \rightarrow B, B \rightarrow C, \dots$, in $Z \rightarrow A$. Pri dešifriranju enostavno vsaki črki odštejemo r . Vendar pa tak enostavni postopek šifriranja nudi le malo varnosti. Ker je naš ključ, torej skrito število r , dolg le en znak, je zaščito relativno enostavno zlomiti. Četudi ne poznamo pravega r , je različnih možnih vrednosti za r le toliko, kot je vseh črk v abecedi. Če torej za r preizkusimo vse možne vrednosti, bo hitro jasno, pri katerem r bomo ob dešifriranju dobili smiselno besedilo. Vidimo tudi, da bi k varnosti pripomoglo, če bi za različne dele besedila uporabili različne r -je, torej če bi imeli daljši ključ. Tako bi moral potencialni vlomilec preveriti veliko več različnih možnih kombinacij r -jev, preden bi našel pravo. Ta princip velja za prav vse šifrirne sisteme. Le-ti so tem bolj varni, tem daljši ključ imajo. Še več, Claude Shannon je pokazal, da je edini dokazano varni sistem šifriranja, torej tak, ki ga absolutno ni mogoče zlomiti, takšen, pri katerem je dolžina skritega ključa kar enaka dolžini besedila, ki ga želimo šifrirati. Torej, daljše kot je besedilo, daljši ključ potrebujemo. Povrhu vsega, ključ lahko uporabimo samo enkrat. Pri našem primeru šifriranja s premikom črk za r mest to pomeni, da moramo za vsako črko besedila uporabiti svoj r . Tak način šifriranja imenujemo Vernamovo šifriranje, po Gilbertu Vernamu, ki ga je odkril okoli leta 1918, ko je delal za ameriško vojsko. Kot smo že povedali, je Vernamovo šifriranje edini dokazano varni način šifriranja. Jasno je, da je Vernamovo šifriranje zelo potratno glede dolžine ključa. Zaradi tega se danes večinoma uporabljajo postopki s krajšimi ključi znani po kraticah DES, AES, IDEA. Glavna težava vseh sistemov z zasebnim ključem je

Nagradna križanka



				TEPTALNI STROJ NA SMUČIŠČU	OLGA CEHOVA	SLOVENSKI BIOKEMIČAR (VITO)	HRVAŠKA NAFTNA DRŽABA	443 km DOLG PRITOK VISLE	PREDVOJNI BRITANSKI MINISTRI IN PREMIER	AM. FIZIK IN KEMIČ NORVEŠK. RODU (LARS)	DELAVEC PRI VITLU	NACE SUMI	NEMŠKI PISATELJ (WOLF-GANG)	DUHOVNIK PRI PRIMITIVNIH LJUDSTVIH
	PARADOKSALNOST							8						
	INFORMACIJSKA VEDA													
	ENAKA SOGLASNIIKA			ZGODNOST ZEMLJA, GLEDE NA SVOJO OBLIKO								KATRAN NEKDANJI ALBANSKI DIKTATOR HOXHA		
	NATANČNO OMEJEN ČAS, DOLOČEN ZA KAJ						AMERIŠKA UNIVERZA V NEW HAVNU						POGOJNI VEZNIK	
	VODNI VRETNČARJI, KI DIHAJO S ŠKRIGAMI						IZGUBA VLAGE PRI USKLADIŠČENIH ŽIVILIH						KITARIST IN PEVEC HENDRIX	
	KVARNER-SKI OTOK					GIMNASTIKA Z ZAHTEVNIMI PRVINAMI	BRST			4				
	NEETIČNOST						PRIKRITJE RESNIČNIH PODATKOV							
									PESNIK FRITZ					
									ANTON AZBE					
AVTOR MARKO BOKALIC	NAVIDEZNO DOKAZOVANJE	USTVARJALEC SOFTVERA	SVETOVNI SPLET ČAPKOVA DRAMA O ROBOTOH			ZAVAROVALNIŠKI KALKULANT ORIENTAL. DVOREC						ZATOPEK NAS IMITATOR RAYA CHARLESA (UROŠ)		
ZLEPEK						REKA V JV. ISTRI					LJUBEZNOST, LJUBKOST LOM SVETLOBE		14	
					SENČNA POBOČJA		3			2. SOLMIZ. ZLOB. SL. SKLADATELJ (MATIJA)		IVAN CANKAR	JEZIK EVROPSKIH ŽIDOV. RAZVIT IZ NEMŠČINE	DRUŠTVENA PRISTOJBINA PRIJETEN VONJ
MESTO NA BOLIVJSKI VISOKI PLANOTI					AKONTACIJA									
STAREJŠI PROGRAMSKI JEZIK ZA TEHNIČ. PROBLEME						ENOCELIČNI MIKROORGANIZEM								
KRAJ NA ROBU LJUBLJAN. BARJA			GL. MESTO KUBE AMERIŠKI LOVEC NA KOZUHARJE					HRIBOVJE NA SZ BENINA V ZAHODNI AFRIKI	ČLAN POVELJ. NIŠKEGA OSEBJA, ČASTNIK					
RIBJA KOŠČICA			POMANJKANJE HRANE SESTANEK, RANDI						PROSOJNA MEGLICA AZIJSKA DRŽAVA V VOJNI	7		NEKDANJI BENEŠKI VLADAR		
PUSTOLOVSKI JUNAK IZ DŽUNGLE						RASTLIN. OPRIJEMAL. ORGAN. PROGRAM. JEZIK						PREDSTAVNIK SIMBOLIZMA SL. MATEM. (IVAN)		
VODJA ISLAMSKE SKUPNOSTI				LIKOVNI UMETNIK PTICA, KI TUDI PLAVA						ZAČIMBNA ZMES ZA NAMAKANJE DIVJACINE				
VRSTA TEKSTILNE VEZAVE		1			GRŠKI JONSKI OTOK, ZNAN PO ODISEJU			9		JUNAK IZ ŠPANSKEGA EPA MEDLA SVETLOBA	16		ČRKA P	PTIČ, KI SE RAD ŠOPIRI POLJE OB IGRISČU
BORIŠČE V RIMSKEM AMFITEATRU					ZNAK ZA SELEN			SPOJINA S KISIKOM				PROGRAM. JEZIK, IMENOVAN PO FR. MATEM. ČA - ? - ČA		
					IGRALEC HARRIS			PREDLOG						
										NAPRAVA, KI OJACI VHODNO VELIČINO				
	VELIKA POSODA ZA NAMAKANJE SADJA									LAHKO PRENOSLJIV PROGRAMSKI JEZIK			NAČIN OBRAVNAVANJA ALI ZDRAVLJENJA	
						PROGRAM. JEZIK, KI GA JE RAZVIL PENTAGON								

NAGRADNI RAZPIS

Črke iz označenih polj po vrsti zapišite na Preseku priloženo dopisnico, dodajte tudi svoje ime, priimek in naslov. Dopisnice pošljite na Presekov naslov (poština je že plačana) do 25. aprila 2007, ko bomo izžrebali tri nagrajence, ki bodo prejeli knjigo **Java za telebane**.

nekdo odkril tak algoritem, bi bila varnost celotnega interneta v trenutku v razsulu.

Pravzaprav tak algoritem že obstaja. Leta 1994 je Peter Shor odkril t.i. kvantni algoritem za faktorizacijo, pri katerem število korakov narašča le kot $T \sim N^3$, torej je veliko hitrejši kot najboljši klasični algoritem. S takšnim Shorovim algoritmom bi lahko faktorizirali velika števila v trenutku. Vendar pa potrebujemo za izvajanje Shorovega algoritma kvantni računalnik. Njegovo delovanje sicer lahko simuliramo na klasičnem namiznem računalniku, vendar je v tem primeru simulacija obupno počasna. Dobra novica za varnost interneta je ta, da znanstvenikom do sedaj še ni uspelo narediti kolikor toliko spodobnega kvantnega računalnika. Doslej jim je uspelo sestaviti le preprost majhen laboratorijski model, s katerim so faktorizirali število 15. Po mnenju večine, uporabnih kvantnih računalnikov ne bomo imeli še vsaj nekaj deset let, kljub temu pa so v principu resna grožnja šifrirnim postopkom z javnim ključem. Na srečo pa nam kvantna fizika, ki nam na eni strani s kvantnimi računalniki ruši varnost RSA, daje nov postopek šifriranja, to je t.i. kvantno kriptografijo. Pravzaprav ne gre za nov postopek šifriranja, temveč le za popolnoma varno izmenjavo ključa, ki se potem uporablja pri šifriranju z zasebnim ključem, npr. pri Vernamovem šifriranju.

Več o tem pa v nadaljevanju. ☒

Kartezijev plavač

➔ Kartezijev plavač je znana fizikalna igračka. Za tiste, ki igračke ne poznamo, lahko z njo izvedemo nekaj čarovnij. Za tiste, ki jo poznajo, jo lahko pripravimo tako, da se ne bo obnašala na običajen način. V času plastenke, ki ga živimo danes, je izdelava zelo enostavna (povzeli jo bomo po članku Gorazda Planinšiča, objavljenem v Physics education¹).



REŠITEV NAGRADNE KRIŽANKE PRESEK 34/4

➔ Za nagradno križanko iz prejšnje številke smo prejeli 18 pravih rešitev. Nagradno geslo se je glasilo **Jurij baron Vega**.

Izžrebani reševalci, Ana Canzutti iz Nove Gorice, Jože Pavlišič iz Črnomlja in Amela Rankanovič iz Sežane so razpisane nagrade prejeli po pošti. ☒

MOJCA ČEPIČ

■ Potrebujemo

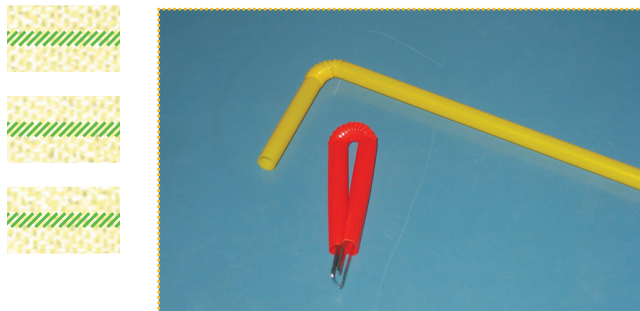
- prazna plastenka z zamaškom na navoj,
- slamica za pitje pijač s harmoniko za upogib (ali nekaj njih)
- papirne sponke ustrezne velikosti, da jih je mogoče potisniti v slamico,
- kozarec,
- voda.

Za izdelavo Kartezijevega plavača za poznavalce, torej za tiste, ki so se z njim že kdaj ukvarjali in ki jih želimo presenetiti, potrebujemo še nekaj velikih žlic kuhinjske soli.

Slamico za pitje pijač prepognemo na harmonikastem delu in jo odrežemo tako, da bosta ravna dela slamice enako dolga. S papirno sponko spnemo odprta konca slamice tako, da nastane slamica v obliki stisnjene črke U. Na sponko, ki odprta dela slamice spenja, nanizajmo nekaj sponk, ki delujejo kot utež. Kartezijev plavač dobro deluje le, če komaj plava. Nepotopljeni delež plavača mora biti majhen, zato ga moramo predhodno preizkusiti. V večji kozarec natočimo vodo in vanjo vržemo plavač. Če potone, snamemo sponko ali dve, če gleda slamica iz vode cm ali celo več, sponko ali dve dodamo. Ko smo s plavačem zadovoljni, ga spustimo v plastenko, zvrhano nalito z vodo, in privijemo zamašek. Plavač mora še vedno plavati pod zamaškom. Če pod pritiskom zamašek potone, ga vzamemo iz plastenke in mu snamemo eno papirno sponko. S plavačem se lahko začnemo igrati.

Poskusimo naslednje in odgovorimo na vprašanja:

- ▶ Kaj se zgodi s plavačem, če plastenko stisnemo?
- ▶ Kaj se zgodi s plavačem, če plastenko spet spustimo?
- ▶ Ali lahko potopimo plavača, če plastenko stisnemo na spodnjem delu?
- ▶ Ali je stisk plastenke odvisen od mesta na katerem plastenko stisnemo?
- ▶ Ali lahko obdržimo plavača na vnaprej izbrani globini dalj časa?
- ▶ Kakšni so vaši občutki, medtem ko plavač lebdi v sredini plastenke?



Sedaj pa se preizkusimo še s plavačem za poznavalce. Prazno plastenko napolnimo do polovice z vodo in dodajamo sol. Platenko ves čas stresajmo, da se sol stopi. Ko se sol neha topiti, pazljivo, ob robu rahlo nagnjene plastenke nalijmo čisto neslano vodo do vrha. Platenko čim manj premikajmo. Vanjo spustimo plavač iz prejšnjega poskusa in privijmo zamašek. Platenke s plavačem ne prestavljajmo, da ne premešamo tekočin, saj ostaja nasičena slana raztopina v spodnjem delu plastenke.

Poskusimo še naslednje:

- ▶ Ali lahko potopimo plavača do dna?
- ▶ Ali ga lahko obdržimo v neki globini na sredini plastenke?
- ▶ Ali je to sedaj lažje ali težje kot pri prejšnjem poskusu?
- ▶ Kakšni so sedaj vaši občutki med zadrževanjem plavača na stalni globini? ☒

1 G. Planinšič, M. Kos and R. Jerman, *Two-liquid Cartesian diver*, Phys. Educ. **39**, (2004), 58-64.

Kaj se zgodi pri soljenju ledu

ODGOVOR NA LOGE

MOJCA ČEPIČ

☉ Uredniki so me opozorili, da v navodilu za poskus iz prejšnje številke Preseka nikjer niso bili omenjeni ledeni kristali iz naslova. Bilo je namenoma, izidi poskusov so vendar uganka, kajne?

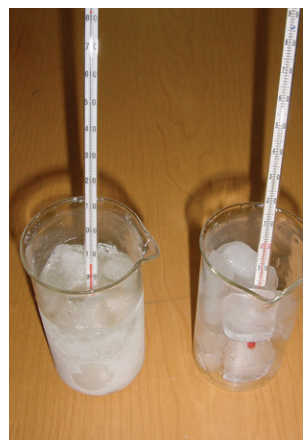
Poskus naj bi potekal takole:

- ▶ dva kozarca smo napolnili z ledenimi kockami iz zamrzovalnika ali, še bolje, z zdrobljenimi ledenimi kockami;
- ▶ v enega od kozarcev smo nasuli nekaj velikih žlic soli in pomešali;
- ▶ opazovali smo zunanost kozarcev, in če je bilo mogoče, merili temperaturo v mešanici ledu.

Opazovanje obeh kozarcev pokaže nekaj zanimivosti. Led v kozarcu brez soli se počasi tali, kozarec je hladen in na njem kondenzira voda iz ozračja. Izloča se v obliki vodnih kapljic, kar je znano vsakomur, ki se poleti rad hladi s kozarcem hladne limonade (slika – kozarec na levi).

Soljeni led se prav tako tali, a zunanost kozarca je drugačna. Na zunanji strani se nabirajo ledeni kristalčki. Lahko jih celo nastrgamo in naredimo majhen kupček "snega". To nakazuje, da mora biti temperatura mešanice ledu in soli nižja od 0°C , torej nižja od temperature, pri kateri se tali voda. Le tako je mogoče, da se vodni hlapi iz zraka izločijo v obliki ledenih kristalčkov. S termometrom lahko ta predvidevanja potrdimo.

Temperatura talečnega ledu je okoli 0°C , termometer pogosto pokaže stopinjo ali dve višjo temperaturo, ker se rado zgodi, da se termometer nahaja v bližini stene ali dna kozarca. Če zmes ledu in vode



Slika 1. V levem kozarcu je mešanica soli, ledu in slane vode, v desnem pa mešanica ledu in vode. Temperatura v levem kozarcu je okoli -15°C , v desnem pa okoli 0°C . Na levem kozarcu so se nabrali ledeni kristalčki, na desnem pa le kapljice vode (foto Goran Iskrič).

dobro premešamo in led še prevladuje, bo temperatura gotovo zelo blizu ničle.

Temperatura mešanice ledu, slane vode in še neraztopljene soli je precej nižja. Običajno namerimo okoli -15°C . Če poskus izvedemo obratno, da zamrzemo skoncentrirano slano raztopino in izmerimo, kdaj se začne taliti, je temperatura okoli -17°C . To temperaturo je Fahrenheit izbral kot izhodiščno temperaturo (torej 0 Fahrenheitov), ko je določal svojo temperaturno lestvico.

Ob tem opazovanju se pojavi mnogo zanimivih vprašanj. Kako to, da se s soljenjem spremeni temperatura tališča? Pri odgovoru nam pomaga kemija. Voda ima glede na svojo strukturo in molekulsko maso zelo visoko tališče in vrelišče. Molekularni plini, kot je npr. CO_2 , so pri 0°C še vedno v plinastem stanju, tališče pa je globoko pod ničlo. Mikroskopski procesi v snovi imajo nekaj skupnih imenovalcev. Molekule se "želijo" nahajati v zanje najugodnejših legah. To lahko ponazorimo s frnikolami, ki jih nasujemo v okrogel kozarec. Frnikole se prerazporedijo tako, da je težišče vseh frnikol skupaj kolikor mogoče nizko oziroma da je potencialna energija frnikol najmanjša. Če je frnikola ena sama, počiva natanko na najnižji točki kozarca z okroglim dnom. Zato se molekule poskušajo razporediti tako, da bodo čim tesneje skupaj zaradi privlačnih sil med njimi. Molekule pa se tudi gibljejo. V trdni snovi običajno nihajo okoli prej opisanih ugodnih leg, v tekočini in plinih pa se gibljejo naokoli in vrtijo. Kinetična energija, ki jo imajo molekule zaradi teh gibanj, je povezana s temperaturo. Čim večja je temperatura, tem večja je povprečna kinetična energija molekul in njih "želja" po gibanju.

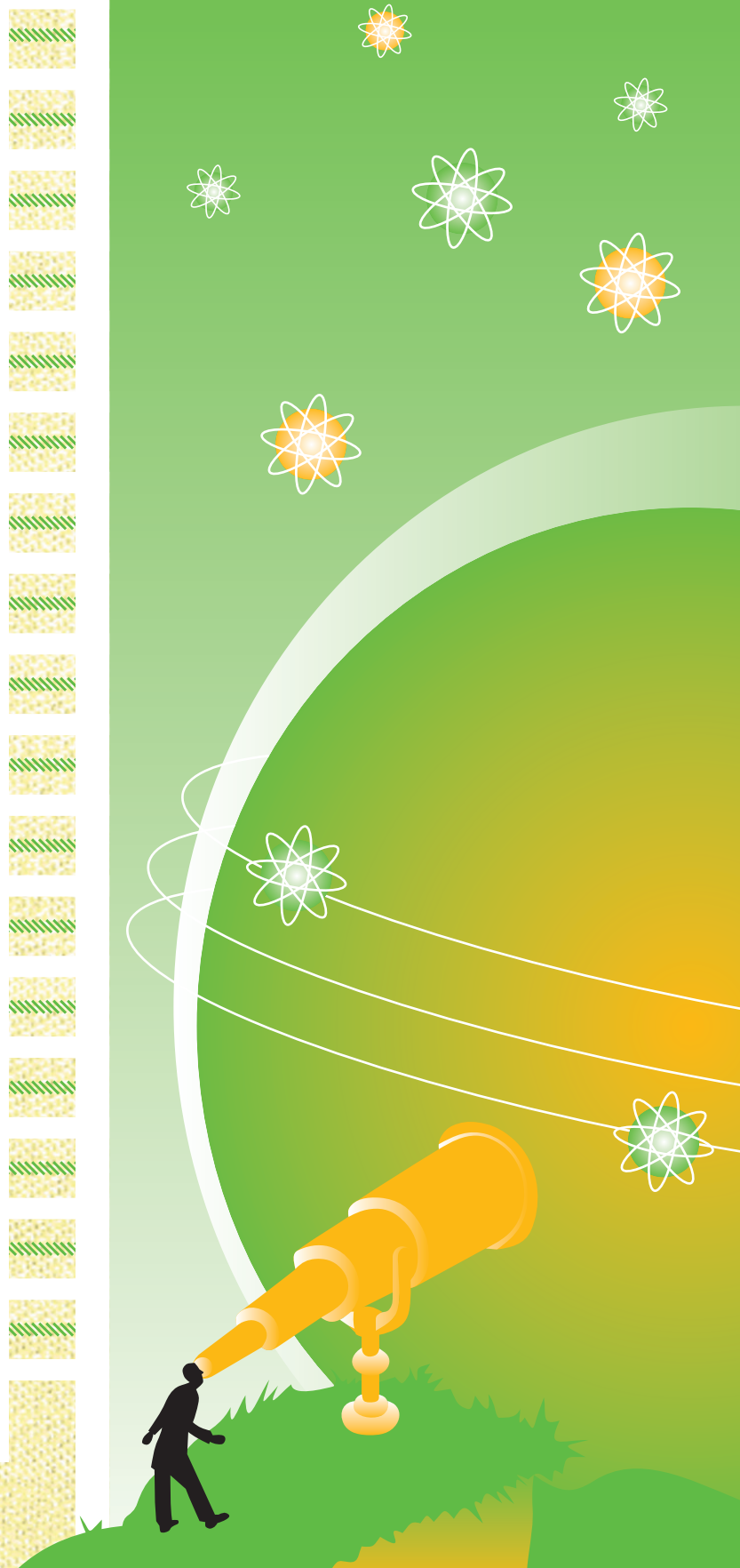
Zaradi obeh dogajanj je v vsaki snovi prisotna tekma med "željo" po gibanju in "željo" po najugodnejši legi, na katero pa najbolj vplivajo medmolekularne interakcije. Kadar ena "želja" prevlada nad drugo, se pojavi fazni prehod. Voda se stali pri segrevanju (povečevanju gibanja) ali zmrzne pri hlajenju (zmanjševanju gibanja). Na enak način lahko razložimo, zakaj voda izpari, če jo segrevamo (molekule se v plinu lažje gibljejo, ker zaradi velikih razdalj med njimi ne čutijo več privlačnih sil), oziroma kondenzira, če paro hladimo. V nekaterih snoveh se to zgodi pri natanko določeni temperaturi, pri temperaturi faznega prehoda, nekaterim snovem pa se lastnosti kar zvezno spremenijo iz trdnega v tekoče. Vosek ali maslo se najprej zmehča in pri višjih temperaturah teče, podobno poteka strjevanje voska.

Molekule vode tvorijo vodikove vezi, ki dodatno povezujejo molekule in preprečujejo prevelike razdalje med molekulami in "uničujejo" uresničevanje želje po gibanju. Zato je potrebna višja temperatura, da se led stali in se vodne molekule začno gibati. Šele ko se te vezi pretrgajo, voda izhlapi. Energijo za trganje vezi dovedemo s segrevanjem. Dodatek soli povezuje med molekulami spremeni tako, da se "želja po gibanju uresniči" že pri nižji temperaturi. Temperatura tališča se zniža. Zanimivo, na temperaturo vrelišča sol vpliva v nasprotni smeri, jo namreč zviša.

Sedaj lahko razumemo, zakaj pozimi solijo ceste. S soljenjem se tališče ledu zniža in pri isti temperaturi, ko bi čista voda bila še led, je slana voda še vedno le slana in nedrseča voda. Soljeni led se na mestih, kjer je sol, stali, saj molekule soli kemijsko reagirajo z molekulami vode v ledu in znižajo tališče. Led se naenkrat znajde pri temperaturi višji od tališča in se seveda začne taliti.

Še nekaj pri tem dogajanju je zanimivo. Zmešali smo sol s sobno temperaturo, led s temperaturo blizu ničle, nastala pa je mešanica s temperaturo -15°C , se pravi z nižjo temperaturo od obeh sestavin. Razlaga tega poskusa je predstavljala hud problem v času, ko so še menili, da je toplota podobna snovi, ki se med telesi izmenjuje in je ni mogoče uničiti ali ustvariti¹. A temu problemu bomo več časa posvetili kdaj drugič. ☒

¹ J. Güémez, C. Filches and M. Fiolhais, *Reproducing Black's experiments: freezing point depression and supercooling of water*, Eur. J. Phys. **23** (2002) 83–91.



Tuji planeti – zgodovina odkrivanja

NIKOLAJ ŠTRITOF

➔ “Ali obstaja mnogo svetov, ali obstaja samo eden?

To je eno najplemenitejših in navdušujočih vprašanj pri preučevanju narave.” Albert veliki (13. stoletje)

Ob koncu 20. stoletja je prišlo do pričakovanega odkritja planeta pri drugi zvezdi. Sedaj, na začetku 3. tisočletja, prehaja iskanje in raziskovanje eksoplanetov v zrelo obdobje. Do začetka leta 2007 so astronomi odkrili 209 planetov pri 184 zvezdah. Planete so odkrili celo pri pulzarjih. V tem sestavku bomo pregledali zgodovino raziskovanj planetov pri zvezdah podobnih Soncu.

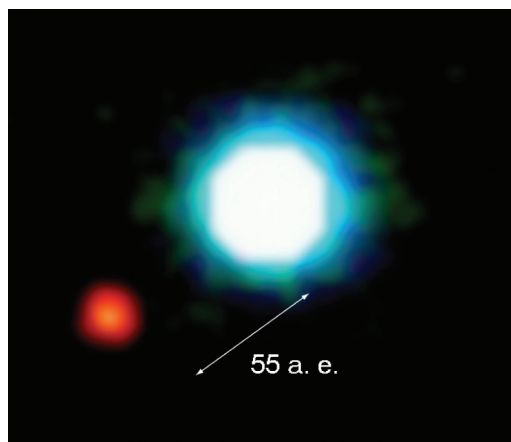
Že Epikur (341 – 270 pr. n. št.) je trdil: “Obstaja neskončno svetov, drugačnih in podobnih našemu.” Kar je v nasprotju z Aristotelom (384 – 322 pr. n. št.), ki je trdil: “Ne more biti več svetov kot en sam.” Filozofi in učenjaki so do konca srednjega veka v glavnem ugibali o obstoju drugih svetov, na primer Giordano Bruno (1548 – 1600). Prvi, ki se je dejansko lotil iskanja eksoplanetov, je bil Christian Huygens (1629 – 1695), pri čemer ni poznal oddaljenosti do zvezd. Njegovo iskanje je bilo seveda neuspešno.

Iskanja nevidnih spremljevalcev pri drugih zvezdah so se resno lotili šele v 19. stoletju. Tako je Bessel leta 1844 astrometrično zaznal nevidnega spremljevalca pri Siriju in kasneje pri Prokionu. Drugi astronomi mu niso verjeli. Dve leti kasneje je Bessel umrl. Resnica je prišla na dan leta 1862, ko je Alan Clark pri Siriju našel šibkega spremljevalca, za katerega se je v 20. stoletju izkazalo, da je bela pritlikavka.

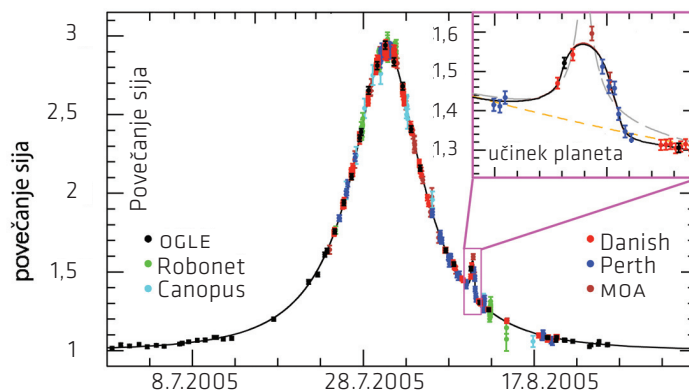
Astronomi so se v 20. stoletju z vse boljšimi teleskopi in z izboljšanimi fotografskimi tehnikami optimistično lotili iskanja eksoplanetov. Tako je leta 1943 ameriški astronom danskega rodu Kaj Aage Strand objavil, da njegova opazovanja zvezde 61 Laboda (61 Cyg) kažejo, da ima ena od zvezd spremljevalca z maso 16-krat večjo od Jupitra (M_J), česar kasneje niso potrdili. V tistem času se je močno povečalo zanimanje za gibanja bližnjih rdečih pritlikavk, na primer 70 Kačenosca (70 Oph) in seveda Barnardove zvezde, ki ima največje lastno gibanje in je druga najbližja zvezda. Z njo se je več kot pol stoletja ukvarjal Piet Van den Kamp, ki je postal neke vrste tragični junak. Od leta 1938 naprej je večkrat objavljaj odkritja spremljevalcev Barnardove zvezde, ki naj bi imeli različne mase, od 60 do $1,6 M_J$. Njegove trditve niso bile dokazane, nedvomno pa je veliko prispeval k razvoju astrometrije. Umrl je maja 1995, nekaj mesecev pred objavo prvega odkritja eksoplaneta.

Z razvojem tehnologij, predvsem računalništva v 70-ih in 80-ih letih 20. stoletja, je postal aktualen drug način lova na planete – spektroskopsko natančno merjenje radialnih hitrosti zvezd. V tem času je bilo iskanje tujih planetov tesno povezano s spektroskopskim iskanjem rjavih pritlikavk. Najbolj so si prizadevale skupine iz Kanade in Združenih držav Amerike, med njimi izstopata Geoffrey Marcy in Paul Butler z univerze San Francisco. Po svoji strogosti pri obravnavanju opazovanj je še posebej znan prvi. Zaradi njegovih proti analiz, s katerimi je “pobijal” možne kandidate za eksoplanete, je dobil nadimek “Dr. Smrt” (Dr Death).

Leta 1992 sta Alexander Wolszczan in Dale Frail



Slika 1. Mednarodna skupina astronomov je z 8,2-metrskim teleskopom VLT na evropskem južnem observatoriju ESO v bližini zvezde 2M1207A prvič neposredno posnela planet zunaj Osončja. Zvezda je od nas oddaljena približno 200 svetlobnih let, planet pa je od nje oddaljen 55-krat dlje, kot je Zemlja od Sonca, in ima približno 5-krat večjo maso od Jupitra. (Foto ESO)



Slika 2. Krivulja poteka sija pri mikrolečanju OGLE-2005-BLG-390. Bližnja zvezda, ki je zastrla bolj oddaljeno, je delovala kot gravitacijska leča in ji za nekaj tednov povečala sij. Ker pa okoli zvezde-leče kroži nevidni planet, je ta pustil odtis v krivulji (povečano v okvirčku). Različne vrste točk so meritve dogodka z različnimi teleskopi po svetu. (Ilustracija ESO)

objavila odkritje kar dveh planetov pri milisekundnem pulzarju PSR 1257+12. Sedaj vemo, da so tam trije planeti. Seveda je bilo to pomembno odkritje, vendar ni povzročilo velikega navdušenja. Pulzarji so nevtronske zvezde in ne "navadne" zvezde, kot je Sonce. Planeti pri pulzarjih so zelo posebni in ne nekaj, kar si ponavadi predstavljamo kot planet. Veliko znanja spektroskopije in tudi kanček sreče sta imela leta 1995 Švicarja Michel Mayor in Didier Queloz, ki sta končno spektroskopsko odkrila planet pri zvezdi 51 Pegaza (51 Pegasi). Presenečenje v laični in strokovni javnosti je bilo ogromno. Do tedaj smo si vedno predstavljali tuje planete zelo podobne našim. Toda 51 Peg b, kot je njegovo uradno ime, sodi v skupino planetov, ki jim sedaj pravimo vroči jupitri. To so planeti, ki 20-krat bliže od Zemlje krožijo okoli centralne zvezde, imajo maso približno 1 Jupitra in periodo od 1,2 do 5 dni. 51 Peg b ima periodo $P = 4,23$ dni, kroži na oddaljenosti $a = 0,052$ astronomske enote in ima najmanj maso $M = 0,47 M_J$.

Po tem odkritju so se kar vsule objave odkritij planetov, ne samo tako blizu centralne zvezde, temveč na zelo različnih oddaljenostih. Presenečenja so se kar vrstila, veliko tujih sistemov ima zelo ekscentrične planetne tirnice, nekateri imajo po dva ali tri planete orjake. Osončje je naravnost dolgočasno s svojimi skoraj

okroglimi tiri, izjema je Pluton, pa še ta ni več planet.

Poleg spektroskopske metode je eksoplanete mogoče odkrivati tudi drugače, na primer s fotometrično metodo. Če planet kroži blizu zvezde, je večja verjetnost, da gre navidezno prek ploščice zvezde. Ker je razmerje med polmerom zvezde in polmerom planeta približno 10 proti 1, sij zvezdi pade za približno 1 odstotek. Če skrbno merimo sij zvezde, lahko zaznamo tak padec sija. Iz tega lahko določimo polmer planeta. Prvič so tak padec zaznali leta 1999 pri zvezdi s spektroskopsko odkritim planetom HD 209458. Sedaj so odkrili ali dopolnilno opazovali 14 planetnih sistemov s fotometrično metodo.

Masa ukrivi prostor okoli sebe, kar opisuje splošna teorija relativnosti. Zaradi tega se oddaljeno vesoljsko telo obnaša podobno kot vinski kozarec na peclju, ki ukrivi oziroma leči svetlobo. Če opazujemo nekaj 10 milijonov zvezd, se lahko zgodi, da pride med nas in zvezdo v ozadju šibko telo – šibka zvezda z malo maso, rjava, rdeča, bela pritlikavka ali celo nevtronska zvezda ali črna luknja. Takrat to telo deluje kot gravitacijska leča in ojača svetlobo zvezde v ozadju. Iz oblike svetlobne krivulje je mogoče sklepati, ali je zvezda sama ali ima planet. S to metodo gravitacijskega lečenja so do sedaj od leta 2004 odkrili štiri planetne sisteme.





Doslej opisane metode so posredne, neposredno slikanje tujih planetov pa je zahtevna naloga. Astro-
nomom je doslej uspelo le enkrat neposredno videti
planet pri zvezdi 2M1207A.

Živimo v razburljivem času odkritij tujih planetnih
sistemov. V bližnji prihodnosti bomo zvedeli, kako
pogosti so planetni sistemi, kako in kje nastanejo,
koliko je planetov podobnih Zemlji ipd.

METODE ODKRIVANJA PLANETOV ZUNAJ OSONČJA - EKSOPLANETOV

Astrometrična metoda

Astrometrija je merjenje položaja zvezd. Prisotnost planeta, ki ga ni mogoče neposredno videti, se kaže v majhnih spremembah lege zvezde. Zvezda in planet namreč krožita okoli skupnega težišča, zato zvezda dela majhno elipso na nebu. Velikost elipse, ki jo zvezda zaradi planeta dela na nebu, je reda velikosti $1/1000$ ločne sekunde. Pod takim kotom vidimo kovanec za 1 evro na oddaljenosti 4600 kilometrov. Doslej so z astrometrično metodo s Hubblovim vesoljskim teleskopom dokazali obstoj planetov pri dveh zvezdah in jima hkrati določili tudi natančno maso. Oba planetna sistema so že prej odkrili s spektroskopsko metodo. Evropska vesoljska agencija ESA bo čez nekaj let izstrelila astrometrični satelit GAIA. Obetajo si bogato žetev odkritij planetnih sistemov.

sonca, šel navidezno prek njega, je 1 %. Torej na 100 takih sistemov pride eden, ki bi ga lahko fotometrično zaznali. Če bi, denimo, iz velike oddaljenosti opazovali prehod Zemlje prek Sonca, bi se njegov sij zmanjšal za $1/10000$ celotnega sija. To natančnost lahko dosežemo z vesoljskimi observatoriji, kjer opazovanje ne moti ozračje. Tako natančen je francoski satelit COROT, ki so ga izstrelili konec leta 2006. Tudi GAIA bo natančno merila sij zvezd.

Spletna stran: Enciklopedija ekstrasolarnih planetov – The Extrasolar Planets Encyclopaedia: <http://exoplanet.eu/>

To spletno stran že od leta 1996 ureja Jean Schneider iz pariškega observatorija. Stran je v angleščini.

Spektroskopska metoda

Zelo natančno merjenje radialne hitrosti zvezd s pomočjo Dopplerjevega pojava. Zvezda in planet krožita okoli skupnega težišča, tako naše Sonce kroži zaradi Jupitra okoli skupnega težišča po krogu s polmerom 750000 kilometrov v 12-ih letih. Opazovalec, ki bi z Dopplerjevim pojavom natančno meril hitrost Sonca, bi ugotovil, da se mu hitrost spreminja s periodo 12 let in amplitudo 12 m/s. Sedaj redno merijo hitrosti zvezd v smeri gledanja z natančnostjo od 1 m/s do 3 m/s. To pomeni, da so mase planetov, ki jih s to metodo ugotovijo, najmanjše možne mase za dani planet, saj naklonov tirov s tovrstnim opazovanjem ni mogoče določiti. Skupaj z astrometrično ali fotometrično metodo pa natančno določijo maso planetov ali drugih objektov. Doslej najmanjši, na ta način odkriti planet, ima maso samo nekaj mas Zemlje. Na tak način išče eksoplanete kak ducat skupin astronomov po vsem svetu.

Fotometrična metoda

Če gre planet med opazovalca in zvezdo, se navidezni sij zvezde zmanjša, tako kot se navidezno zmanjša sij zelo oddaljeni luči, če pred njo leti večja. Te metode opazovanja ali celo iskanja eksoplanetov se lahko lotijo tudi amaterski astronomi ali šolski krožek z nekoliko boljšo opazovalno opremo. Verjetnost, da gre vroč jupiter prek zvezde, je 10 %, torej na 10 sistemov z vročim jupitrom pride tak, ki povzroči padec sija za 1 %. Verjetnost, da bi planet, ki kroži na oddaljenosti 1 astronomske enote od svojega

Gravitacijsko mikrolečenje

Kot je znano iz splošne relativnostne teorije, masa ukrivi prostor-čas, zato se žarek v gravitacijskem polju ukrivi. Tako, denimo, majhna zvezda, deluje kot slaba leča, ki sliko izvira zvezde razbije na dve sliki in ju ojači. Sliki pri leči reda velikosti mase Sonca in oddaljenosti 10.000 svetlobnih let sta kakšno 1/1000 ločno sekundo narazen. Zato ju ne razločimo, ojačanje pa opazimo kot porast sija. Seveda je verjetnost, da se bosta zvezda izvir in zvezda leča poravnali v smeri našega gledanja, majhna. Zato astronomi opazujejo v smeri, kjer je veliko zvezd – proti centralni zadebelitvi Rimske ceste. Astronomi redno snemajo nekaj 10 milijonov zvezd in opazijo od 400 do 600 mikrolečenj na leto. Enostavna leča ima enostavno svetlobno krivuljo, če pa je leča dvojna zvezda, je krivulja zelo zapletena. Če ima zvezda leča planet, se to pozna kot odstopanje od enostavne krivulje enojne leče. Gravitacijsko lečenje je moč opazovati s skromnimi sredstvi, vendar je večino teh pojavov zaznanih v smeri jedra Galaksije v ozvezdju Strelec, ki je v naših krajih vedno nizko nad obzorjem.

Kaj je sploh planet?

Pred kratkim se je močno razvila debata o Plutonu in definiciji planetov. Astronomi so namreč odkrili več njemu podobnih in celo večjih teles, zato so ga prestavili med transneptunske objekte. To pa je le del debate o planetih. Pred nekaj desetletji so astronomi poznali rdeče pritlikavke kot najmanjše zvezde, najmanjše imajo maso 0,08 mase Sonca ali 80 mas Jupitra (M_J). V njihovih središčah potekajo jedrske reakcije, pri katerih se vodik pretvarja v helij, sprošča se energija in zato svetijo. Manjša telesa pa ne vzdržujejo dovolj visoke temperature in tlaka, da bi potekale te reakcije. Samo na →

Slikanje planetov

Planeti ne oddajajo lastne svetlobe. Vidimo jih zaradi odbite svetlobe, razen ko so zelo mladi in še vroči, ko sevajo infrardečo svetlobo. Torej so zelo šibki v primerjavi s centralnimi zvezdami. Razmerje sijev zvezde in mladega planeta je tipično 1 proti 1 milijarda. Poleg tega je navidezni kot, za katerega so planeti oddaljeni od svoje zvezde, majhen, v najboljšem primeru okoli ločne sekunde. Torej nas pri neposrednem opazovanju eksoplanetov moti svetloba zvezde in majhna oddaljenost planetov od zvezde. Do sedaj so astronomi posneli štiri kandidate, vendar so vsi mladi in še ni jasno, ali ne gre morda za rjave pritlikavke.

Sudoku

	a	b	c	d	e	f	g	h	i
A				3	6		9	5	
B	6								
C				2	8				
D	5		8				4		
E	7		3	1		4	5		9
F			9				1		3
G					9	2			
H									7
I		4	1		7	5			

→ Rešitev najdeš na strani 26



začetku njihovega življenja potekajo jedrske reakcije, ki pretvarjajo devterij in litij. Ko obeh zmanjka, se ta objekt zelo počasi ohlaja in še dolgo šibko sveti. Te objekte imenujemo rjave pritlikavke. V resnici niso rjave, so malce modrikaste zaradi molekul metana in vode v njihovih atmosferah. Pri masah pod $13 M_J$ pa še prej omenjene reakcije ne morejo poteci, zato imajo planeti največjo maso $13 M_J$. Glede spodnje meje pa ni jasno, kaj je planet, kar kaže primer Plutona. Nekateri predlagajo, da moramo ločiti objekte glede na njihov nastanek. ✖

REŠITEV SUDOKU S STRANI 25



	a	b	c	d	e	f	g	h	i
A	1	8	2	3	6	7	9	5	4
B	6	3	7	5	4	9	8	2	1
C	9	5	4	2	8	1	7	3	6
D	5	1	8	9	3	6	4	7	2
E	7	6	3	1	2	4	5	8	9
F	4	2	9	7	5	8	1	6	3
G	8	7	6	4	9	2	3	1	5
H	2	9	5	8	1	3	6	4	7
I	3	4	1	6	7	5	2	9	8

POPRAVEK IZ ČLANKA »DVE O LUNI«

Datum ščipa in čas vzida Lune
ob ščipu za leto 2007

3. januar	16.02
2. februar	17.23
4. marec	18.33
2. april	19.33
2. maj	20.43
1. junij	21.51
30. junij	21.29
30. julij	21.07
28. avgust	19.52
26. september	18.33
26. oktober	17.42
24. november	15.47
24. december	16.32

✚ V prejšnji številki Preseka je v tabeli o vzidih Lune ob ščipu (članek "Dve o Luni") prišlo do neljube napake. Datumi ščipov v letu 2007 so sicer pravilni, ure vzida pa so napačne. Za napako se avtor iskreno opravičuje. Tokrat objavljamo prave vrednosti.

Podatki veljajo za Ljubljano in so v srednjeevropskem času, med 25. marcem in 27. oktobrom pa v poletnem času. Za druge kraje po Sloveniji se časi od teh razlikujejo kvečjemu za +7 oz. -7 minut. Vir: Naše nebo 2007. ✖



Pentomino

IGOR PESEK

➤ Vsi poznamo računalniško igrico Tetris, ki jo lahko sedaj najdete tudi na nekaterih mobilnih telefonih. Za tiste, ki igre še ne poznate, naj jo na kratko opišemo. V tej igri imamo različne like, ki padajo z vrha zaslona in jih lahko premikamo vodoravno ter obračamo v obe smeri za 90° . Cilj igre je postavljati te like tako, da tvorimo vodoravne vrste, ki izginejo samo, ko je vrsta zapolnjena. Vsi liki v igri so sestavljeni iz štirih kvadratov, ki se stikajo z vsaj eno stranico drugega kvadrata. Če poskusimo narisati vse možne kombinacije štirih kvadratov in pri tem upoštevamo vse simetrije, ugotovimo, da je takšnih likov sedem.

Nekatere igre namesto štirih kvadratov uporabljajo pet kvadratov. Poglejmo, kaj zanimivega lahko odkrijemo.

■ Pentomino

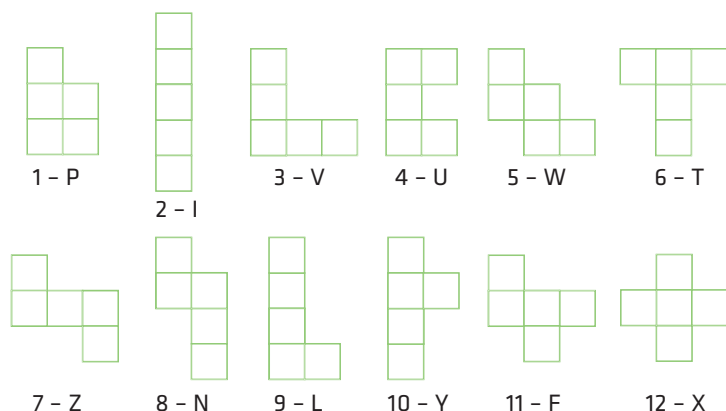
Likom, ki so sestavljeni iz štirih kvadratov, pravimo tetromini. Podobno likom, ki so sestavljeni iz petih kvadratov, pravimo pentomini. Konstruiramo jih s postavitvijo petih skladnih kvadratov na različne položaje v ravnini, tako da lik ostane povezan in je vsak kvadrat z vsaj eno stranico povezan z enim





od drugih kvadratov. Javnosti jih je prvič predstavil Solomon Golomb leta 1953 (več si lahko preberete v [3]) in od takrat so bili navdih mnogim družabnim igram in matematičnim problemom.

Obstaja dvanajst likov – pentominov, ki jih glede na obliko lahko poimenujemo s črkami latinske abecede, in sicer T, U, V, W, X, Y, Z, F, I, L, P in N. Zakaj ravno te črke? Če pogledamo like in pripadajoče črke, opazimo veliko podobnosti med njimi. Tu tiči glavni razlog za izbor teh črk. Kako vemo, da jih je res samo dvanajst in ne več? Držati se moramo dveh pravil. Prvič, če lahko kateri lik zavrtimo tako, da izgleda kot kak drug lik, potem ta dva lika nista različna. In drugič, če lahko lik zrcalimo preko navpične ali vodoravne osi in izgleda kot kak drug lik, potem lika nista različna. Z upoštevanjem teh dveh pravil dobimo dvanajst likov, ki so prikazani na sliki 1. V

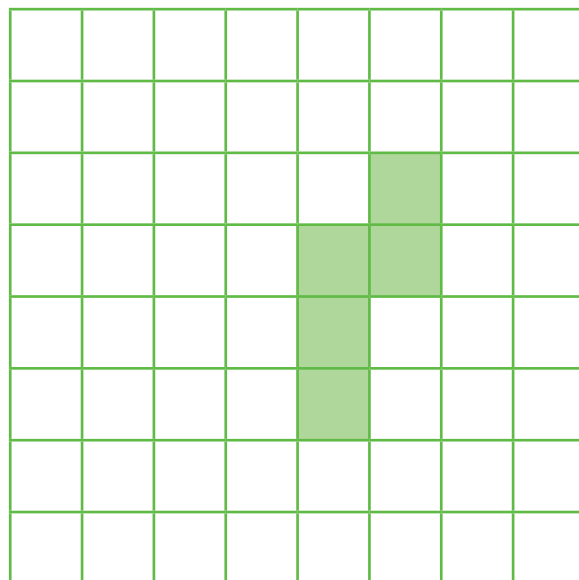


Slika 1. Vsi možni liki – pentomini

primeru, da upoštevamo tudi like, ki jih dobimo z vrtenjem ali zrcaljenjem, imamo na voljo 63 različnih likov. Nekateri liki imajo namreč samo eno obliko, npr. lik X, nekateri pa tudi več. Razmisli, kateri lik ima največ možnih oblik in zakaj.

Igre

Tetris temelji na likih, sestavljenih iz štirih skladnih kvadratov, imenovanih tetromini, obstajajo pa tudi igre, ki temeljijo na pentominih. Zelo znana je družabna igra, kjer imata oba igralca skupaj na voljo vseh 12 pentominov. Cilj igre je postavljati pentomine na igralno ploščo velikosti 8×8 tako, da naš soigralec v naslednji potezi na ploščo ne more



Slika 2. Zmagovalna prva poteza prvega igralca

več postaviti niti enega od preostalih pentominov. V [4] je dokazano, da lahko prvi igralec vedno zmagaja, če pravilno postavi prvi pentomino. Na sliki 2 je prikazana prva poteza prvega igralca, ki vodi do zmage. Razmisli, kako mora prvi igralec igrati v naslednjih potezah, da bo res zmagal, in ali obstaja še kakšna druga zmagovalna prva poteza.

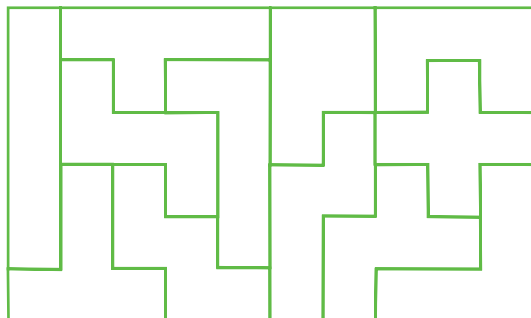


Slika 3. Družabna igra pokrivanja pravokotnika

Pri še eni bolj priljubljenih iger (slika 3) s pentomini pokrivamo pravokotnik, katerega ploščina meri 60 kvadratov. Zakaj ravno 60 kvadratov? Imamo dvanajst različnih pentominov, vsak je sestavljen iz petih kvadratov, kar pomeni, da lahko z njimi pokrijemo lik s ploščino 60 kvadratov. Obstajajo štirje različni pravokotniki s takšno ploščino, in sicer

6×10 , 5×12 , 4×15 in 3×20 kvadratov.

Poglejmo si rešitev za 6×10 predstavljeno na sliki 4. Hitro lahko ugotovimo, da to ni edina rešitev oziroma razporeditev likov v pravokotnik. Celo več, za



Slika 4. Rešitev problema postavitve pentominov v pravokotnik 6×10

pravokotnik velikosti 6×10 so ugotovili, da je vseh možnih rešitev kar 2339. Za podoben pravokotnik velikosti 5×12 obstaja nekaj manj rešitev, in sicer 1010. Da bi sami našli vse rešitve, bi potrebovali kar nekaj dni, zato si oglejmo, kako bi se težave lotili z uporabo računalnika.

Računalniška predstavitev in iskanje vseh rešitev

Če za reševanje problemov uporabljamo računalnik, moramo najprej razmisliti, kako predstaviti rešitev problema oziroma trenutno stanje rešitev. V našem primeru moramo pokriti pravokotnik, ki je sestavljen iz kvadratov. Ker je vsak kvadrat v pravokotniku na mestu, določenem z vrstico in stolpcem, je najprimernejša uporaba predstavitev z matriko oziroma, natančneje, z dvodimenzionalnim poljem. Vsak element v matriki predstavlja en kvadrat, ki bo nosil informacijo o tem, s katerim pentominom smo ga pokrili. Za zapis pentomina bomo uporabili kar črko, ki ga predstavlja. Na ta način bomo lahko hitro ugotovili način in uporabo likov. Če ta pristop uporabimo na primeru rešitve na sliki 4, dobimo rešitev v obliki polja na sliki 5.

Poglejmo, kako bi poiskali vse rešitve tega problema. Oštevilčimo polje oziroma njegove elemente z zaporednimi številkami, kot je prikazano na sliki 6.

I	Y	Y	Y	Y	P	P	U	U	U
I	Z	Y	L	L	P	P	U	X	U
I	Z	Z	Z	L	P	N	X	X	X
I	I	W	Z	L	N	N	F	X	V
I	T	W	W	L	N	F	F	F	V
T	T	T	W	W	N	F	V	V	V

Slika 5. Polje z rešitvijo problema na sliki 4

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60

Slika 6. Dvodimenzionalno polje z oštevilčenimi elementi

Tudi like označimo z zaporednimi številkami. Vsako oštevilčenje je dobro, mi bomo uporabili kar tisto s slike 1. Reševanje poteka tako, da v vsakem koraku našega preiskovanja poskusimo pokriti nepokriti element polja z najmanjšo zaporedno številko, in sicer z neuporabljenim likom, ki ima najmanjšo zaporedno številko. V prvem koraku torej postavimo predmet s številko 1 tako, da v polju pokrijemo element 1. Če uporabimo tudi like vrtenja in zrcaljenja, kot je prikazano na sliki 7, lahko lik 1 (v našem primeru lik P) postavimo v polje na šest različnih načinov. Ko je lik 1 postavljen v matriko, nadaljujemo z likom 2 in ga poskusimo postaviti v prvi naslednji nepokriti element z najmanjšo zaporedno številko. Pri takem preiskovanju upoštevamo vse oblike likov, kar pomeni, da imamo v resnici na voljo 63 likov in ne samo 12.

Če tako nadaljujemo, pridemo bodisi do rešitve





bodisi do nerešljivega položaja, ker naslednjega pentomina ne moremo več postaviti v pravokotnik. V primeru, ko smo našli rešitev, jo shranimo, v nasprotnem primeru, ko je situacija nerešljiva, pa zadnji lik poskusimo umestiti v vseh možnih oblikah, za kar uporabimo zrcaljenje in vrtenje. Če tudi to ne uspe, odstranimo predzadnji lik iz polja in ga poskusimo postaviti v drugi možni obliki. Nadaljujemo z zadnjim likom in ga ponovno poskušamo umestiti. Tako sistematično poskušamo z vsemi možnimi oblikami posameznih likov. Opozoriti velja, da vrstni red ni vedno enak. Nastopi lahko situacija, ko je lik, ki je bil v prejšnji postavitvi na n -tem mestu, sedaj na $n + 1$ mestu.

S takšnim preiskovanjem smo preizkusili vse like v vseh možnih pozicijah in oblikah ter tako dobili seznam vseh možnih rešitev danega problema. Takšnemu pristopu preiskovanja vseh možnih situacij pravimo tudi *iskanje z vračanjem*. Seveda ne preiskujemo sami, ampak pustimo, da to dela računalnik, ki je bil prvotno namenjen reševanju ravno takšnih problemov.

Zaključek

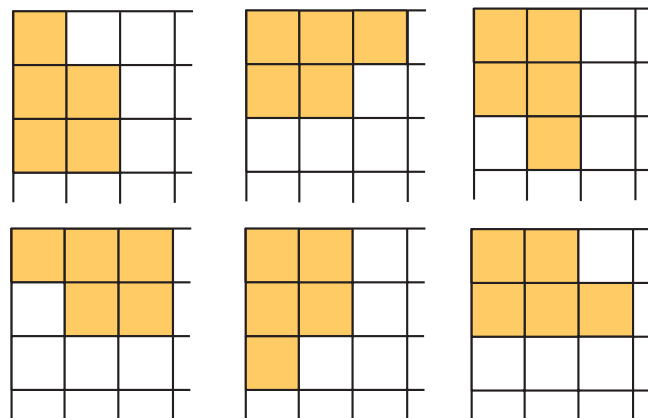
Spoznali smo zanimiv problem pentominov in njihove postavitve v pravokotnik velikosti 6×10 , ki ima kar 2339 možnih rešitev. Seveda to ni edini možen pravokotnik s 60 kvadrati. Zelo zanimiv je tudi pravokotnik velikosti 3×20 , ki ima samo dve rešitvi. Poskusite ju najti.

Nagradna naloga

Napišite program, ki za dane pravokotnike velikosti $m \times n$ poišče vse rešitve pokritja s pentomini. Vašo rešitev pošljite v uredništvo Preseka do 4. maja 2007. Naključno izžrebanega avtorja čaka lepa knjižna nagrada.

Literatura

- [1] <http://en.wikipedia.org/wiki/Pentomino>
- [2] V. Batagelj, *Pentomino*, Presek 2 (1974), str. 40–42.
- [3] S. W. Golomb, *Polyominoes: Puzzles, Patterns, Problems, and Packings*, Princeton Univ. Press, 1994.
- [4] H. K. Orman, *Pentominoes: A First Player Win*, Games of No Chance, 29 (1996), str. 339–344. ☒



Slika 7. Različne možne postavitve lika P

REŠITVI NAGRADNIH NALOG



☒ V drugi številki letošnjega Preseka smo v računalniški rubriki objavili nagradno nalogo. Potrebno je bilo napisati algoritem, ki se v obliki spirale sprehodi po kvadratni matriki. Za podrobnosti glejte omenjeno številko Preseka. Prejeli smo tri pravilne rešitve. Žreb je bil naklonjen ALEŠU BIZJAKU iz Jesenic na Dolenjskem, ki prejme knjigo **Java 2: Temelji programiranja založbe Pasadena**. Njegova rešitev bo objavljena na Presekovi domači strani.

V tretji številki letošnjega Preseka smo v računalniški rubriki objavili nagradno nalogo. Potrebno je bilo napisati algoritma, ki opišeta pot dveh prebivalcev planeta Tris, če želita obiskati drug drugega. Prejeli smo dve rešitvi, vendar je samo ena prejeta rešitev pravilno rešila obe zadani nalogi. Nagrajenec je NINO BAŠIČ iz Ljubljane, ki prejme knjigo **Java 2: Temelji programiranja založbe Pasadena**. Tudi njegova rešitev bo objavljena na Presekovi domači strani. ☒

Stare številke revije Presek so še vedno na voljo

Če želite dopolniti svojo zbirko revij Presek, so nekatere stare številke še vedno na voljo. Na spodnjem naslovu najdete seznam razpoložljivih števil in naročilnico:

<http://www.presek.si/staro.htm>

Za individualne naročnike revije Presek, člane DMFA, dijake in študente je cena stare številke 2,17 EUR (520,02 SIT), za vse ostale pa 2,71 EUR (649,42 SIT).

Izkoristite možnost dodatnih popustov pri večjem naročilu!

PRESEKOVA ZVEZDNA KARTA

Posodobljena zvezdna karta je zelo primeren pripomoček za šolske krožke iz astronomije in ostale ljubitelje opazovanja nočnega neba.

Pavla Ranzinger:

PRESEKOVA ZVEZDNA KARTA

2000,0

format:
54 × 58 cm

plastificirana
zložena

cena: 3,34 EUR
(800,40 SIT)



PRESEKOVE MAJICE

Za tople pomladne in poletne dni smo vam pripravili kakovostne bombažne majice s kratkimi rokavi z logotipom revije Presek.

velikost:
M, L ali XL
(opozarjamo, da
so majice velike!)

barva:
modra ali rdeča

cena: 5,22 EUR
(1.250,92 SIT)

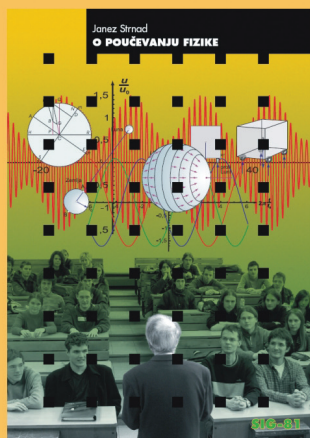


Individualni naročniki revije Presek, člani DMFA, dijaki in študentje imate ob naročilu pri DMFA-založništvo 20 % popusta na zgornje cene – izkoristite ga!

Dodatne informacije lahko dobite v uredništvu Preseka po telefonu (01) 4766 553 ali 4232 460.

Novosti v Knjižnici Sigma

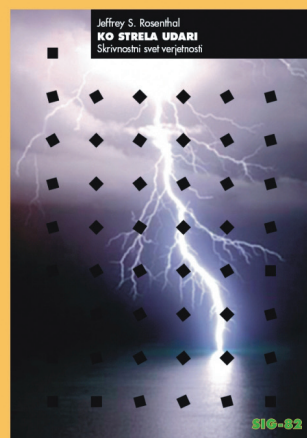
Že od leta 1959 nam Knjižnica Sigma prinaša poljudna in strokovna besedila za popularizacijo področij matematike, fizike, astronomije in računalništva. Vključuje tako zbirke nalog z različnih tekmovanj, dopolnilne učbenike, priročnike in drugo zanimivo branje domačih avtorjev, kot tudi nekaj prevodov znanih tujih avtorjev. Najnovejši dve knjižici sta izšli konec leta 2006.



Janez Strnad:
**O POUČEVANJU
FIZIKE**

320 strani
format 14 × 20 cm
mehka vezava

12,49 EUR
(2.993,10 SIT)



Jeffrey S. Rosenthal:
KO STRELA UDARI
Skrivnostni svet
verjetnosti

264 strani
format 14 × 20 cm
mehka vezava

12,49 EUR
(2.993,10 SIT)

Robert B. Banks:

**LEDENE
GORE,
PADAJOČE
DOMINE**
in druge prigode
iz uporabne
matematike

skupaj 348 strani
format 14 × 20 cm
mehka vezava

cena kompleta:
20,86 EUR (4.998,89 SIT)



Borut Zalar:
**TEŽIŠČA IN
VZTRAJNOSTNI
MOMENTI**

120 strani
format 14 × 20 cm
mehka vezava

8,35 EUR
(2.000,99 SIT)



Poleg omenjenih lahko v Knjižnici Sigma najdete še več kot 40 drugih del. Podrobnejše predstavitve so na spodnjem naslovu, kjer lahko vse knjige tudi naročite s popustom:

<http://www.knjiznica-sigma.si/>

Individualni naročniki revije Presek, člani DMFA, dijaki in študentje imate ob naročilu pri DMFA-založništvo 20 % popusta na zgornje cene – izkoristite ga!

Dodatne informacije lahko dobite v uredništvu Preseka po telefonu (01) 4766 553 ali 4232 460.