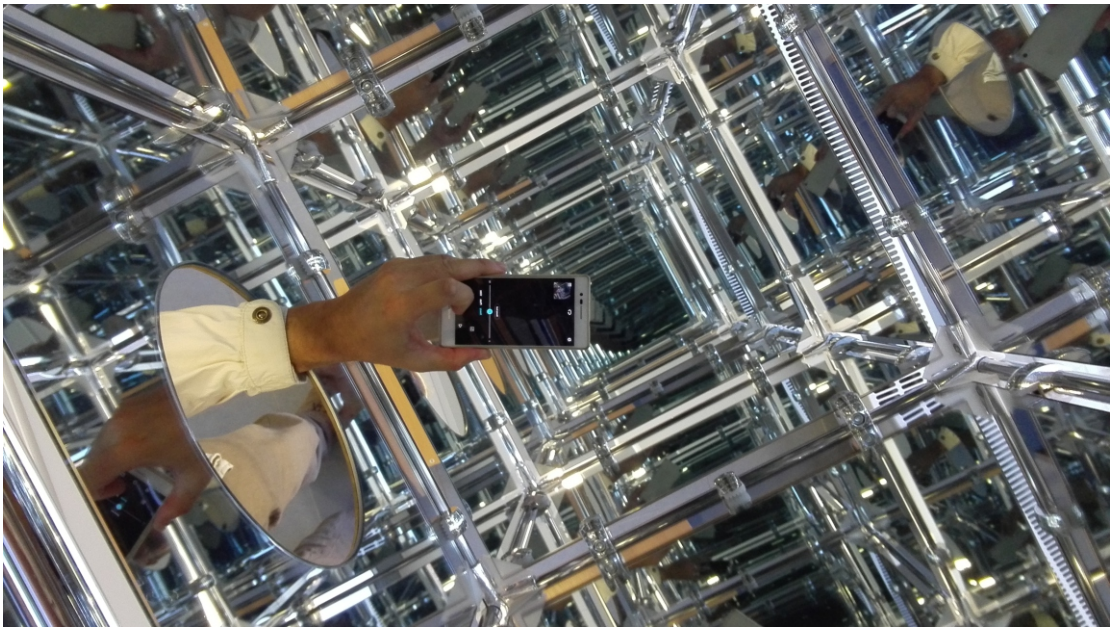
IZDAJA DRUŠTVO MATEMATIKOV, FIZIKOV IN ASTRONOMOV SLOVENIJE

ISSN 0473-7466

2020
Letnik 67
3

OBZORNIK ZA MATEMATIKO IN FIZIKO



OBZORNIK ZA MATEMATIKO IN FIZIKO

Glasilo Društva matematikov, fizikov in astronomov Slovenije
Ljubljana, MAJ 2020, letnik 67, številka 3, strani 81–120

Naslov uredništva: DMFA–založništvo, Jadranska ulica 19, p. p. 2964, 1001 Ljubljana **Telefon:** (01) 4766 633, 4232 460 **Telefaks:** (01) 4232 460, 2517 281 **Elektronska pošta:** zaloznistvo@dmfa.si **Internet:** http://www.obzornik.si/ **Transakcijski račun:** 03100–1000018787 **Mednarodna nakazila:** SKB banka d.d., Ajdovščina 4, 1513 Ljubljana **SWIFT (BIC):** SKBASI2X **IBAN:** SI56 0310 0100 0018 787

Jezikovno pregledal Grega Rihtar.
Računalniško stavila in oblikovala Tadeja Šekoranja.
Natisnila tiskarna COLLEGIUM GRAPHICUM v nakladi 1100 izvodov.

Člani društva prejemajo Obzornik brezplačno. Celoletna članarina znaša 24 EUR, za druge družinske člane in študente pa 12 EUR. Naročnina za ustanove je 35 EUR, za tujino 40 EUR. Posamezna številka za člane stane 3,99 EUR, stare številke 1,99 EUR.

DMFA je včlanjeno v Evropsko matematično društvo (EMS), v Mednarodno matematično unijo (IMU), v Evropsko fizikalno društvo (EPS) in v Mednarodno združenje za čisto in uporabno fiziko (IUPAP). DMFA ima pogodbo o recipročnosti z Ameriškim matematičnim društvom (AMS).

Revija izhaja praviloma vsak drugi mesec. Sofinancira jo Javna agencija za raziskovalno dejavnost Republike Slovenije iz sredstev državnega proračuna iz naslova razpisa za sofinanciranje domačih znanstvenih periodičnih publikacij.

Poštnina plačana pri pošti 1102 Ljubljana

NAVODILA SODELAVCEM OBZORNIKA ZA ODDAJO PRISPEVKOV

Revija Obzornik za matematiko in fiziko objavlja izvirne znanstvene in strokovne članke iz matematike, fizike in astronomije, včasih tudi kak prevod. Poleg člankov objavlja prikaze novih knjig s teh področij, poročila o dejavnosti Društva matematikov, fizikov in astronomov Slovenije ter vesti o drugih pomembnih dogodkih v okviru omenjenih znanstvenih ved. Prispevki naj bodo zanimivi in razumljivi širšemu krogu bralcev, diplomantov iz omenjenih strok.

Članek naj vsebuje naslov, ime avtorja (oz. avtorjev), sedež institucije, kjer avtor(ji) dela(jo), izvleček v slovenskem jeziku, naslov in izvleček v angleškem jeziku, klasifikacijo (MSC oziroma PACS) in citirano literaturo. Slike in tabele, ki naj bodo oštevilčene, morajo imeti dovolj izčrpen opis, da jih lahko večinoma razumemo tudi ločeno od besedila. Avtorji člankov, ki želijo objaviti slike iz drugih virov, si morajo za to sami priskrbeti dovoljenje (copyright). Prispevki so lahko oddani v računalniški datoteki PDF ali pa natisnjeni enostransko na belem papirju formata A4. Zaželena velikost črk je 12 pt, razmik med vrsticami pa vsaj 18 pt.

Prispevke pošljite odgovornemu uredniku ali uredniku za matematiko oziroma fiziko na zgoraj napisani naslov uredništva. Vsak članek se praviloma pošlje dvema anonimnima recenzentoma, ki morata predvsem natančno oceniti, kako je obravnavana tema predstavljena, manj pomembna pa je originalnost (in pri matematičnih člankih splošnost) rezultatov. Če je prispevek sprejet v objavo, potem urednik prosi avtorja še za izvorne računalniške datoteke. 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.

PROBLEM UČENJA Z NAPAKAMI IN SODOBNI KRIPTOSISTEMI

TILEN MARC

Fakulteta za matematiko in fiziko
Univerza v Ljubljani

Math. Subj. Class. (2020): 94A60, 68P25, 81P94

Sodobni kriptosistemi so osnovani na matematičnih problemih in njihova varnost je zagotovljena samo, dokler ne obstajajo algoritmi, ki bi te probleme učinkovito rešili. V članku predstavimo nedavno vpeljan algoritmičen problem učenja z napakami, ki se izkaže za izjemno uporabnega v kriptografiji, saj omogoča sestavo novih kriptosistemov z zanimivimi in uporabnimi lastnostmi. Taki kriptosistemi veljajo tudi za varne pred nasprotniki, ki imajo dostop do kvantnega računalnika, kar za večino drugih ne velja. Predstavljena sta kvantno varen kriptosistem z javnim ključem in kriptosistem, ki omogoča računanje na šifriranih podatkih, kar je znano pod imenom homomorfno šifriranje. Konstrukcija slednjega je bila odprt problem več desetletij in dosežena šele s pomočjo problema učenja z napakami.

PROBLEM OF LEARNING WITH ERRORS AND MODERN CRYPTOSYSTEMS

Modern cryptosystems are based on mathematical problems and their security is guaranteed only as long as there are no efficient algorithms solving these problems. We present a recently introduced algorithmic problem of learning with errors (LWE). The problem is crafted for the use in cryptography and allows to construct new cryptosystems with interesting and useful properties. Such cryptosystems are considered safe even against adversaries with access to quantum computers, which does not hold for most of the other systems. We explain how to construct two cryptosystems: a quantumly secure cryptographic scheme with public key, and a scheme that enables computation on encrypted data, known as homomorphic encryption. The construction of the latter was a long standing open problem and was solved only recently with the help of LWE problem.

Uvod

Problem učenja z napakami (ang. *learning with errors – LWE*) je vpeljal Regev v [4] kot nov algoritmičen problem in dokazal, da je vsaj tako težek kot nekateri drugi znani problemi. Članek je povzročil pravo revolucijo, saj je bilo v zadnjem desetletju napisanih na tisoče znanstvenih člankov, ki temeljijo na problemu LWE. Regev je bil leta 2018 za svoj prispevek nagrajen s prestižno Gödelovo nagrado, ki jo vsako leto podelijo za doprinos k teoretičnemu računalništvu.

Glavni razlog za priljubljenost problema LWE je njegova uporabnost v kriptografiji. Eden izmed osnovnih temeljev sodobne kriptografije je t. i. asimetrična kriptografija. Ta omogoča, da uporabnik izračuna svoj javni

ključ, s pomočjo katerega mu lahko vsakdo pošlje šifrirano sporočilo, ki ga lahko dešifrira le lastnik javnega ključa s pomočjo svojega skrivnega ključa. Taki kriptosistemi se dandanes uporabljajo v računalniški komunikaciji, bančništvu in praktično na vseh področjih, kjer je tajnost podatkov pomembna. Varnost asimetrične kriptografije temelji na predpostavki, da iz javnega ključa ne moremo izračunati skrivnega, saj bi v nasprotnem primeru lahko vsak dešifriral sporočila. Zato so kriptosistemi z javnim ključem osnovani na matematičnih problemih, za katere ne poznamo učinkovitih algoritmov za reševanje.

V praksi daleč najbolj uporabljana matematična problema sta t. i. problem razcepa naravnega števila in z njim povezan problem diskretnega logaritma. Problema, ki ju lahko uvrstimo na področje teorije števil, sta omogočila slavne kriptografske sheme, kot so RSA, ElGamalov sistem in DSA, pa tudi sodobnejše konstrukte, ki temeljijo na eliptičnih krivuljah. Največjo grožnjo vsem omenjenim tehnologijam predstavlja razvoj t. i. kvantnega računalnika in kvantnih algoritmov. Glavni razlog je, da je Shor že leta 1999 v [6] opisal kvantni algoritem, ki zmore v polinomskem času razbiti naravno število in poiskati diskretni logaritem. Torej obstaja algoritem, s katerim lahko s pomočjo kvantnega računalnika razbijemo skoraj vsak dandanes uporabljan kriptosistem z javnim ključem, vdremo v bančne račune itd. V trenutku pisanja članka kvantni računalniki že obstajajo, vendar je njihova zmogljivost še zelo omejena. Ali se bo to v prihodnje spremenilo, lahko samo ugibamo.

Problem LWE ne temelji na zgoraj omenjenih problemih in je zaenkrat varen pred kvantnimi računalniki, saj (trenutno) ne poznamo kvantnega algoritma, ki bi ga v polinomskem času uspel rešiti. Še več – kot bomo videli, je Regev dokazal, da je problem LWE vsaj tako težek kot nekateri problemi na t. i. rešetkah. Ti so poznani že dlje časa in veljajo za težke, zato je zaupanje v neobstoj polinomskih (kvantnih) algoritmov za reševanje problema LWE še večje.

V članku bomo predstavili enega izmed načinov, kako je mogoče sestaviti kriptosistem z javnim ključem, katerega varnost temelji na težavnosti problema LWE. Tak kriptosistem torej velja za kvantno varnega, razvoj tovrstnih kriptosistemov pa je ena izmed najpomembnejših tem sodobne kriptografije. To dokazuje tudi dejstvo, da v času pisanja članka poteka pomemben izbor ameriškega Nacionalnega inštituta za standarde in tehnologijo (NIST) [7] za določitev kvantnih kriptografskih standardov, ki se bodo uporabljali v bližnji prihodnosti. Večina shem, ki so se uvrstile v ožji izbor, temelji na problemu LWE ali njegovih izpeljankah.

Problem LWE poleg kvante varnosti kriptosistemov z javnim ključem prinaša tudi druge novosti. Tako lahko sestavimo nove kriptosisteme, katerih varnost temelji na težavnosti problema LWE, z lastnostmi, ki jih starejši

kriptosistemi ne omogočajo. Področje simetrične kriptografije omogoča šifriranje podatkov s pomočjo skrivnega ključa, tako da jih lahko dešifriramo samo ob poznavanju le-tega. Taki sistemi se uporabljajo za hitro prenašanje sporočil med uporabniki, ki so si izmenjali skrivni ključ, pa tudi za varno hrambo podatkov. V sodobnem svetu veliko podatkov hranimo v oblaku, in če želimo ohraniti osebne podatke varne, morajo biti taki podatki šifrirani. Poleg hrambe ponudniki omogočajo tudi urejanje, analizo, napovedi, priporočila in druge storitve, ki temeljijo na računanju s podatki. A če so podatki šifrirani, take storitve niso mogoče, saj ponudnik storitev v oblaku podatkov ne pozna. Želeli bi torej na videz nemogoče – računanje (in s tem vse storitve, ki smo jih vajeni) brez poznavanja podatkov. Čeprav opisano zveni kot sodobni problem, je bil izziv sestaviti kriptosistem, ki bi omogočal računanje s šifriranimi podatki, brez poznavanja le-teh, predlagan že leta 1978 v [5]. Tak kriptosistem imenujemo homomorfno šifriranje. Problem je bil dolgo časa odprt, dokler ni prvi tak sistem opisal Gentry v [3]. Objavljen kriptosistem je bil osnovan na problemu LWE in od njegove objave je bilo predlaganih več različic in izboljšav. Eno izmed teh bomo predstavili v članku.

Preostanek članka je strukturiran na naslednji način: v razdelkih Problem LWE in Težavnost problema LWE definiramo problem LWE in pokažemo, zakaj je to težek problem, v razdelku Kriptosistem z javnim ključem, osnovan na problemu LWE predstavimo kriptosistem z javnim ključem, ki temelji na problemu LWE, in ga nato v razdelku Homomorfno šifriranje nadgradimo v kriptosistem za homomorfno šifriranje. Da lahko to storimo, konstruiramo t. i. generator psevdonaključnih vektorjev s stranskimi vrati in razložimo, kako uporabiti dvojiško kodiranje pri konstrukciji.

Problem LWE

Začnimo s preprostim matematičnim problemom reševanja linearnih enačb. Naj bo p praštevilo in z $\mathbb{Z}_p$ označimo polje s p elementi. Torej, elementi $\mathbb{Z}_p$ so števila $\{0, 1, \ldots, p-1\}$, operaciji seštevanja in množenja pa izvajamo po modulu p. Naj bo $A \in \mathbb{Z}_p^{m \times n}$ poljubna matrika in $b \in \mathbb{Z}_p^m$ vektor za $m \geq n \geq 1$. Problem iskanja $x \in \mathbb{Z}_p^n$ v matrični enačbi nad $\mathbb{Z}_p$

$$Ax = b$$

ni težek, saj ga lahko rešimo z Gaussovo eliminacijo, četudi je p velik.

Otežimo zgornji problem z dodajanjem napake. Za vrednost $y \in \mathbb{Z}_p$ označimo $|y| = \min(y, p-y)$ in recimo, da je vrednost $y \in \mathbb{Z}_p$ *majhna*, če je vrednost $|y| = \min(y, p-y)$ občutno manjša od p: za vse uporabe v članku lahko bralec predpostavi, da je $|y|$ manjši od $\sqrt{p}$. Naj bo $e \in \mathbb{Z}_p^m$ vektor z majhnimi vrednostmi, torej je vrednost vsake komponente v e občutno

manjša od p. Naj bosta $A \in \mathbb{Z}_p^{m\times n}$ in $b \in \mathbb{Z}_p^m$ dana kot prej. Iskanje vrednosti x, da velja

$$Ax + e = b,$$

kjer je e neznan, je osnova problema učenja z napakami (LWE).

Oglejmo si zgornji problem nekoliko natančneje. Na prvi pogled je problem enostavnejši, saj imamo m linearnih enačb in $m+n$ neznank – neznana sta tako x kot e. V primeru, da je $m = n$, lahko izberemo $e = 0$ in rešimo $Ax = b$, kot v zgornjem primeru z Gaussovo eliminacijo. Problem postane težji, če je m večji kot n, saj nismo zadovoljni z vsako rešitvijo, ampak samo s tistimi, v katerih je e majhen. Reševanje problema s standardnimi metodami linearne algebre nam ne zagotavlja take rešitve. Na problem lahko pogledamo tudi drugače: podprostor vseh vektorjev $\{Ay \mid y \in \mathbb{Z}_p^n\}$ je največ n-dimenzionalni podprostor m-dimenzionalnega prostora $\mathbb{Z}_p^m$. Če želimo najti x, da velja $Ax + e = b$, potem moramo najti tak majhen e, da je $b - e \in \{Ay \mid y \in \mathbb{Z}_p^n\}$.

Definirajmo sedaj iskalni problem LWE natančneje. Da bo problem uporaben v kriptografiji, mora biti take narave, da lahko enostavno generiramo naključne vrednosti (recimo nove skrite in javne ključe), za katere je problem težek. Zato problem definiramo za naključne vrednosti, izbrane iz vnaprej določenih porazdelitev. Torej problema LWE ne bomo definirali za poljubne vrednosti A, x, e, b, ampak za naključne, kar je precej drugače od mnogih drugih algoritmičnih problemov, ki jih rešujemo za poljubne vhodne podatke. Razlog za tako definicijo je, da je marsikateri (tudi NP-poln) problem težek, če so vhodni podatki poljubni, vendar lahek za naključne.

Označimo s χ porazdelitev naključnih majhnih vektorjev, izbranih iz $\mathbb{Z}_p$ (v naslednjem razdelku bomo natančneje definirali, kako izbrati χ). Za vrednost (vektor, matriko itd.) x bomo rekli, da je izbrana enakomerno naključno, če so verjetnosti izbire vseh mogočih vrednosti enake.

Definicija 1. Naj bo p praštevilo, $m \geq n \geq 1$, $A \in \mathbb{Z}_p^{m\times n}$ enakomerno naključno izbrana matrika, $x \in \mathbb{Z}_p^n$ enakomerno naključno izbran vektor in $e \in \mathbb{Z}_p^n$ vektor, naključno izbran iz porazdelitve χ. Definirajmo $b \in \mathbb{Z}_p^m$ kot $b := Ax + e$. *Iskalni problem* $LWE_{n,m,p,\chi}$ je problem najti x, če poznamo samo A in b.

Pozoren bralec bi lahko opazil, da ima sistem $b = Ax+e$ lahko več rešitev. Spomnimo se – najti moramo tak majhen e, da je $b-e \in \{Ay \mid y \in \mathbb{Z}_p^n\}$. Če določimo parametre tako, da je m občutno večji od n, je po številu elementov prostor $\{Ay \mid y \in \mathbb{Z}_p^n\}$ občutno manjši od celega prostora. Intuicija nam zato pravi, da je verjetnost (za naključno izbrane A, x, e), da ima enačba več kot eno rešitev, majhna. Kot bomo videli, je za kriptografsko uporabo pomembno le, da je problem tako težek, da ne moremo najti nobene rešitve x, e, kjer je e majhen.

Težavnost problema LWE

V tem razdelku bomo definirali odločitveno verzijo problema LWE, natančneje določili porazdelitev χ, ki se uporablja za izbiro vektorja e, in predstavili pomemben rezultat glede težavnosti problema LWE.

Odločitveni problem LWE

Izkaže se, da je za kriptografsko uporabo prikladno, da definiramo *odločitveno* verzijo problema LWE.

Definicija 2. *Odločitveni problem* je problem, ki ima le dve možni rešitvi: 0 ali 1.

Torej, če želimo rešiti odločitveni problem, želimo izpeljati algoritem, ki za vhodne podatke vrne odgovor 0 ali 1. V primeru odločitvenega problema LWE je naloga razlikovati med vrednostmi, izbranimi iz dveh različnih porazdelitev.

Definicija 3. Naj bo p praštevilo, $m \geq n \geq 1$, $A \in \mathbb{Z}_p^{m \times n}$ enakomerno naključno izbrana matrika, $x \in \mathbb{Z}_p^n$ enakomerno naključno izbran vektor in $e \in \mathbb{Z}_p^m$ vektor, naključno izbran iz porazdelitve χ. Naj bo $b \in \mathbb{Z}_p^m$ definiran kot $b := Ax + e$ in $c \in \mathbb{Z}_p^m$ izbran iz enakomerne porazdelitve. *Odločitveni problem* $LWE_{n,m,p,\chi}$ je problem, katerega vhod je ena izmed vrednosti (A, b) ali (A, c), algoritem pa mora določiti, katera izmed vrednosti je bila vhod. Torej, algoritem prejme vrednost (A, z) in mora določiti, ali je vektor z vektor vrednosti enakomerne porazdelitve ali je z dobljen iz porazdelitve enačbe LWE.

Za razliko od iskalnega problema tukaj naloga ni, da dobimo (A, z) in poiščemo x, e, da velja $Ax + e = z$, ampak da lahko razločimo, ali je bil z naključno izbran prek izbire A, x, e, ali je preprosto vektor enakomerno naključnih vrednosti. Ti dve porazdelitvi seveda nista enaki; recimo, vektor z, izbran iz prve porazdelitve, je vedno tak, da obstaja rešitev enačbe $Ax + e = z$, kjer je e majhen, medtem ko za enakomerno naključen vektor z rešitev morda (in tudi zelo verjetno) ne obstaja. Izkaže se, da sta iskalni in odločitveni problem podobne težavnosti, saj lahko prevedemo enega na drugega [4]. Za uporabo v kriptografiji bi želeli, da je odločitveni problem LWE (in zato tudi iskalni) težek, torej da algoritem, ki bi deloval dovolj hitro in rešil problem pravilno v več primerih kot napačno, ne obstaja.

Definirajmo matematično, kaj pravzaprav mislimo, ko rečemo, da je odločitveni problem $\mathrm{LWE}_{n,m,p,\chi}$ težek. Označimo z $\Pr(X)$ verjetnost dogodka X. Za algoritem $\mathcal{A}$, ki rešuje odločitveni problem LWE, označimo z $\mathcal{A}(A, z)$ vrednost, ki jo vrne $\mathcal{A}$ ob vhodu (A, z).

Definicija 4. Naj bo $n > 0$ parameter in naj bo $m \geq n$, p praštevilo in χ porazdelitev, ki so lahko določeni v odvisnosti od n. Naj bosta (A, b) in (A, c) para, kjer je $b \in \mathbb{Z}_p^m$ definiran kot $b := Ax + e \in \mathbb{Z}_p^m$ in $c \in \mathbb{Z}_p^m$ enakomerno naključen, torej sta (A, b) in (A, c) generirana kot možna vhoda odločitvenega problema $\mathrm{LWE}_{n,m,p,\chi}$. *Predpostavka LWE* pravi, da za vsak polinomski algoritem $\mathcal{A}$, ki vrača 0 ali 1, velja

$$|\Pr(\mathcal{A}(A, b) = 1) - \Pr(\mathcal{A}(A, c) = 1)| < 2^{-Cn}$$

za neko konstanto $C > 0$.

Predpostavka LWE pravi, da ne obstaja algoritem, ki bi mu v polinomskem času uspelo razlikovati (torej vrniti 0 ali 1) med naključnima vhodoma odločitvenega problema $\mathrm{LWE}_{n,m,p,\chi}$ bolje kot z eksponentno majhno verjetnostjo. Intuitivno to v neformalnem jeziku pomeni, da če predpostavka LWE drži in izračunamo $b = Ax + e$ z naključno izbranimi A, x, e, potem se b zdi kot enakomerno naključen vektor. Če predpostavka LWE drži, potem bomo rekli, da je $b = Ax + e$ *računsko neločljiv* od enakomerno naključnega vektorja.

Definicija vsebuje verjetnosti, da algoritem vrne pravilno ali napačno odločitev, saj je problem definiran na naključnih podatkih in bi lahko naključno sprejemal odločitve. Da bi bolje razumeli definicijo, si oglejmo preveč preprost algoritem za reševanje odločitvenega problema LWE. Recimo, da algoritem $\mathcal{B}$ problem reši tako, da preprosto vrže kovanec in izbere 0 ali 1. Seveda tak algoritem ne bi bil preveč uporaben. Oglejmo si vrednost:

$$|\Pr(\mathcal{B}(A, b) = 1) - \Pr(\mathcal{B}(A, c) = 1)| = \left|\frac{1}{2} - \frac{1}{2}\right| = 0.$$

Slednje lahko razumemo tako, da tak algoritem ne bi uspel razlikovati pravilne odločitve od napačne. Če predpostavka LWE drži, potem vsak algoritem, ki bi deloval v polinomskem času, ne bi deloval veliko bolje, kot da vržemo kovanec.

V nadaljevanju razdelka bomo razložili, za kakšne parametre n, m, p, χ se verjame, da predpostavka LWE drži.

Diskretna Gaussova porazdelitev

Do sedaj smo vprašanje, kako izbrati m, p, χ, da bo predpostavka LWE smiselna, pustili odprto. V tem podrazdelku bomo opisali, kako izbrati porazdelitev χ, s katero izberemo vektor e v $Ax + e$.

Definicija 5. *Diskretna Gaussova porazdelitev* D_σ, ki ima vrednosti v $\mathbb{Z}$, je taka porazdelitev, da je za vsak $x \in \mathbb{Z}$ verjetnost izbire x enaka $Ce^{-\frac{x^2}{2\sigma^2}}$,

kjer je $\sigma > 0$ in C taka konstanta, da se verjetnosti vseh dogodkov seštejejo v 1.

Z $\bar{D}_\sigma$ označimo diskretno Gaussovo porazdelitev, ki ima vrednosti v $\mathbb{Z}_p$, ki jih dobimo tako, da izberemo $y \in \mathbb{Z}$ iz D_σ in izračunamo $\bar{y} = (y \bmod p) \in \mathbb{Z}_p$.

Verjetnost izbire vrednosti iz D_σ, katerih absolutna vrednost je večja od σ, eksponentno hitro pada. Če je σ občutno manjši kot praštevilo p, bodo tudi absolutne vrednosti števil, generiranih z D_σ, z zelo veliko verjetnostjo občutno manjše od p. To pomeni, da bodo vrednosti y, generirane z $\bar{D}_\sigma$, majhne. Torej, vrednost $\min(y, p - y)$ bo občutno manjša od p. Take vrednosti želimo v problemu LWE.

Problemi na rešetkah

V tem podrazdelku bomo odgovorili, kako izbrati preostale parametre problema $\mathrm{LWE}_{n,m,p,\chi}$ s pomočjo v uvodu omenjenega rezultata Regeva [4]. Najprej potrebujemo dve definiciji:

Definicija 6. Naj bodo $v_1, \ldots, v_n$ linearno neodvisni vektorji v $\mathbb{R}^n$. Množico

$$L(v_1, \ldots, v_n) = \{a_1 v_1 + \cdots + a_n v_n \mid \ a_i \in \mathbb{Z} \text{ za } 1 \leq i \leq n\}$$

imenujemo *rešetka*.

Spomnimo se, da je 2-norma vektorja x definirana kot $||x|| = \sqrt{x_1^2 + \cdots + x_n^2}$, kjer so $x_1, \ldots, x_n$ koordinate x. Recimo, da imamo podane vektorje $v_1, \ldots, v_n$, ki imajo vsi 2-normo večjo od nekega $a \in \mathbb{R}$. S sestavljanjem linearnih kombinacij $a_1 v_1 + \cdots + a_n v_n$, z $a_i \in \mathbb{Z}$ za vsak $1 \leq i \leq n$, je v določenih primerih možno sestaviti neničelen vektor, ki ima normo manjšo od a. Kot preprost primer navedimo $v_1 = (100, 99), v_2 = (100, 100)$, kjer ima $-v_1 + v_2 = (0, 1)$ manjšo normo od začetnih vektorjev.

Če za dane $v_1, \ldots, v_n$ lahko najdemo koeficiente $a_i \in \mathbb{Z}$, da je $a_1 v_1 + \cdots + a_n v_n$ neničeln vektor z majhno normo, potem velja, da v rešetki $L(v_1, \ldots, v_n)$ obstaja element z majhno normo. To, kako učinkovito najti take koeficiente oziroma se odločiti, ali sploh obstajajo, je pomemben algoritmičen problem.

Definicija 7. *Odločitveni problem GapSVP(n, s)*, kjer je $n \in \mathbb{N}$ in $s \geq 1$, je problem, katerega vhod so poljubni neodvisni vektorji $v_1, \ldots, v_n$, ki definirajo rešetko $L(v_1, \ldots, v_n)$, in pravilni izhod je vrednost 1, če obstaja $v \in L(v_1, \ldots, v_n) \backslash \{(0, \ldots, 0)\}$ z $||v|| \leq 1$, in 0, če za vsak $v \in L(v_1, \ldots, v_n) \backslash \{(0, \ldots, 0)\}$ velja $||v|| > s$. Če noben izmed pogojev ne velja, je izhod lahko poljuben.

Opomba: Ime GapSVP je bilo izbrano, saj v problemu odločamo o obstoju najkrajšega neničelnega vektorja (ang. *shortest vector problem*) z razmakom (ang. *gap*) s. Natančneje, treba je določiti, ali v rešetki obstaja kratek neničeln vektor z normo največ 1, ali pa so vsi neničelni vektorji daljši od s. Večji kot je s, lažji je problem.

Z naslednjim izrekom je Regev pokazal, da sta problema $\mathrm{LWE}_{n,m,p,\chi}$ in $\mathrm{GapSVP}(n,s)$ povezana.

Izrek 8 ([4]). *Naj bo $n \in \mathbb{N}$ in p, m, α vrednosti, ki so odvisne od n, da velja: p je praštevilo, $m \in \mathbb{N}$ ne več kot polinomsko večji od n in $\alpha \in (0,1)$ tak, da je $\sigma := \alpha p > 2\sqrt{n}$. Če obstaja algoritem, ki za vsak n reši odločitveni problem $LWE_{n,m,p,\bar{D}_\sigma}$ v polinomskem času (v parametru n), potem obstaja kvantni polinomski algoritem, ki reši problem GapSVP$(n, n/\alpha)$.*

Izrek pravi, da je problem $\mathrm{LWE}_{n,m,p,\bar{D}_\sigma}$ vsaj tako težek, kot je problem $\mathrm{GapSVP}(n, n/\alpha)$, če imamo dostop do kvantnega računalnika. Ker je problem $\mathrm{GapSVP}(n,s)$ že dlje časa preučevan in ne poznamo kvantnega algoritma, ki bi rešil $\mathrm{GapSVP}(n, n/\alpha)$ v polinomskem času, izrek vliva upanje, da polinomskega algoritma za reševanje $\mathrm{LWE}_{n,m,p,\bar{D}_\sigma}$ ni.

Zgornji rezultat nam torej zagotavlja, da vsi znani algoritmi za reševanje $\mathrm{LWE}_{n,m,p,\bar{D}_\sigma}$ s parametri, izbranimi tako, da zadoščajo pogojem iz izreka 8, potrebujejo eksponentno mnogo korakov (glede na n), da rešijo problem. Za praktično uporabo v kriptografiji bi želeli konkretne parametre: npr. na podlagi natančne analize znanih algoritmov za reševanje problemov na rešetkah v [1] ocenjujejo, da je za parametre $n = 256$, p 16-bitno praštevilo in $\sigma \approx 26$ časovna zahtevnost reševanja ustreznega problema LWE vsaj 2^{153}.

Kriptosistem z javnim ključem, osnovan na problemu LWE

Priljubljenost problema LWE izhaja iz dejstva, da omogoča konstrukcijo novih kriptografskih shem, katerih varnost temelji na težavnosti reševanja odločitvenega problema LWE. Prvo tako shemo je opisal že Regev v članku [4].

Naj bo $n > 1$ parameter, ki določa varnost, p praštevilo, da velja $n^2 \leq p \leq 2n^2$, $m = (1+\epsilon)(n+1)\log(p)$ za neko malo konstanto $\epsilon > 0$ (izbrano tako, da je $m \in \mathbb{N}$) in naj bo $\chi = \bar{D}_\sigma$, torej diskretna Gaussova porazdelitev nad $\mathbb{Z}_p$, kjer je $\sigma = p/(\sqrt{n}\log^2(n))$. Izbrani parametri ustrezajo pogojem izreka 8, tako da bi rešitev odločitvenega problema $\mathrm{LWE}_{n,m,p,\chi}$ pomenila velik preboj na področju reševanja problemov na rešetkah.

Opišimo kriptosistem z javnim ključem, ki temelji na problemu LWE. Vse aritmetične operacije v shemi opravimo po modulu p, torej v $\mathbb{Z}_p$:

- **Generiranje ključev:** Naj bo $s \in \mathbb{Z}_p^n$ enakomerno naključen vektor in $A \in \mathbb{Z}_p^{m \times n}$ enakomerno naključna matrika. Naj bo $e \in \mathbb{Z}^m$ vektor, katerega komponente so izbrane naključno iz porazdelitve $\bar{D}_\sigma$. Izračunajmo $b = As + e$. Potem je vektor s skrivni ključ in par (A, b) javni ključ kriptosistema.

- **Šifriranje:** Naj bo $M \in \{0, 1\}$ sporočilo, ki ga želimo šifrirati. Če poznamo javni ključ (A, b), lahko izberemo vektor $r \in \{0, 1\}^m$ enakomerno naključno in izračunamo

$$C = (c_0, c_1) = (r^T A, r^T b + M \cdot \lfloor p/2 \rfloor),$$

  ki ga obravnavamo kot šifriran M.

- **Dešifriranje:** S pomočjo skrivnega ključa s izračunamo $d = c_1 - c_0 s$, kar dešifriramo kot vrednost 0, če je d bližje 0, in 1, če je bližje $\lfloor p/2 \rfloor$.

Zgoraj opisani kriptosistem omogoča šifriranje sporočila $M \in \{0, 1\}$, torej enega bita. Če želimo poslati daljše sporočilo (256-bitno sporočilo je v praksi pogost primer), potem preprosto pošljemo več različnih sporočil, pri čemer za vsako izberemo nov naključen r. Slednje je računsko zahtevnejše kot šifriranje s pomočjo standardnih kriptosistemov z javnim ključem, vendar praktično izvedljivo s sodobnimi računalniki.

Vsak kriptosistem mora izpolnjevati dve zahtevi: po pravilnosti in varnosti. Za kriptosistem pravimo, da *deluje pravilno*, če je dešifrirano sporočilo enako prvotnemu sporočilu. Za določitev varnosti kriptosistema obstaja več matematičnih definicij. Najmanjša zahteva je, da napadalec samo iz kriptograma in javnih parametrov ne sme biti sposoben dešifrirati sporočila. Vendar to za sodobne standarde varnosti ne zadošča več: želimo, da napadalec iz kriptograma in javnih parametrov ne more izvedeti (skoraj) ničesar. Temu se približa naslednja definicija. Za kriptosistem pravimo, da je *IND-CPA* varen (ang. *indistinguishability of ciphertext*), če napadalec, ki ne pozna skrivnega ključa, na podlagi javnih parametrov in kriptograma C ne more razlikovati med dvema besediloma enake dolžine, ki sta bili šifrirani (v našem primeru, ali je bil šifriran bit $M = 0$ ali $M = 1$).

Skicirajmo, zakaj je kriptosistem, osnovan na problemu LWE, varen. Več podrobnosti o dokazu lahko bralec najde v [4].

Izrek 9. *Zgoraj opisan kriptosistem za dovolj velik n deluje pravilno – torej dešifrirana vrednost ustreza šifrirani – ter je IND-CPA varen pri predpostavki LWE s parametri n, m, p, χ.*

Skica dokaza. Dokažimo, da sistem pravilno dešifrira vrednosti:

$$d = c_1 - c_0 s = r^T b + M \cdot \lfloor p/2 \rfloor - r^T A s = r^T (As + e) + M \cdot \lfloor p/2 \rfloor - r^T A s$$
$$= M \cdot \lfloor p/2 \rfloor + r^T e.$$

Omejimo vrednost $r^T e$. Komponente e so izbrane iz porazdelitve $\bar{D}_\sigma$, kjer je $\sigma = p/(\sqrt{n}\log^2(n))$. Naj bodo $i_1, \ldots, i_k$, $k \leq m$ indeksi komponent vektorja r, ki so neničelni. Potem je $r^T e = \sum_{j=1}^{k} e_{i_j}$. Slednje je vsota neodvisnih diskretnih Gaussovih porazdelitev, kar ima porazdelitev računsko neločljivo diskretni Gaussovi porazdelitvi s standardno deviacijo $\sqrt{k}\sigma \leq \sqrt{m}\sigma \leq \sqrt{2n\log(2n^2)}p/(\sqrt{n}\log^2(n)) = \alpha p$, kjer je α v $O(1/\log(n))$. Za dovolj velik n je verjetnost, da je vrednost iz porazdelitve $\bar{D}_{p/\log(n)}$ večja od $p/4$, zanemarljivo majhna. Torej je $d = M \cdot \lfloor p/2 \rfloor + r^T e$ bližje $\lfloor p/2 \rfloor$ kot 0, če je $M = 1$, in bližje 0, če je $M = 0$. Sledi, da je dešifriranje pravilno.

Skicirajmo še, zakaj je kriptosistem varen. Pokazati moramo, da napadalec, ki ne pozna skrivnega ključa, na podlagi javnih parametrov in kriptograma ne more razlikovati, ali je bil šifriran bit $M = 0$ ali $M = 1$. Oglejmo si kriptogram $C = (r^T A, r^T b + M \cdot \lfloor p/2 \rfloor)$. Če velja predpostavka LWE, je za napadalca vrednost b neločljiva od enakomerno naključnega vektorja iz $\mathbb{Z}_p^m$. Tako imenovana »leftover hash lemma« [4] pravi, da je potem porazdelitev $r^T b$ za enakomerno naključen $r \in \{0,1\}^m$ statistično zelo blizu enakomerne porazdelitve. Enako velja za $r^T A$; napadalec torej ne more razločiti vrednosti $(r^T A, r^T b)$ od enakomerno naključno izbranih vrednosti. Potem je tudi porazdelitev $(r^T A, r^T b + M \cdot \lfloor p/2 \rfloor)$ za napadalca neločljiva od enakomerno naključne in ne more razločiti, ali je šifriran bit $M = 0$ ali $M = 1$. ∎

Homomorfno šifriranje

V prejšnjem razdelku smo spoznali, kako sestaviti kvantno varen kriptosistem z javnim ključem s pomočjo problema LWE. V tem razdelku pa bomo pokazali, da se tak kriptosistem z nekaj truda da nadgraditi v t. i. sistem homomorfnega šifriranja. Osnovna naloga klasičnih kriptosistemov je, da omogočajo varen prenos oziroma hrambo podatkov. Homomorfno šifriranje poleg slednjega omogoča še varno računanje na šifriranih podatkih.

V naslednjih podrazdelkih bomo natančneje spoznali homomorfno šifriranje in njegove uporabe. V podrazdelku Aditivno šifriranje bomo dokazali, da že kriptosistem, opisan v razdelku Kriptosistem z javnim ključem, osnovan na problemu LWE, vsebuje nekatere lastnosti homomorfnega šifriranja. Podrazdelka Generator psevdonaključnih vektorjev s stranskimi vrati in Dvojiško kodiranje sta tehnične narave, saj predstavita vse potrebno za nadgradnjo v kriptosistem za homomorfno šifriranje, ki je opisan v podrazdelku Homomorfno šifriranje.

Aditivno šifriranje

Kriptosistem, opisan v prejšnjem razdelku, ima zanimivo lastnost. Recimo, da z istim javnim ključem (A, b) šifriramo dve vrednosti: $m_1, m_2 \in \{0, 1\}$, tj.

$$(c_0^1, c_1^1) = (r_1^T A, r_1^T b + m_1 \cdot \lfloor p/2 \rfloor), \quad (c_0^2, c_1^2) = (r_2^T A, r_2^T b + m_2 \cdot \lfloor p/2 \rfloor).$$

Potem lahko brez poznavanja skrivnega ključa izračunamo:

$$(c_0, c_1) = (c_0^1, c_1^1) + (c_0^2, c_1^2) = ((r_1 + r_2)^T A,\ (r_1 + r_2)^T b + (m_1 + m_2) \cdot \lfloor p/2 \rfloor).$$

Opazimo, da lahko (c_0, c_1) obravnavamo kot šifro in jo poskusimo dešifrirati s pomočjo skrivnega ključa s. Dobimo:

$$\begin{aligned} d = c_0 s - c_1 &= (r_1 + r_2)^T (As + e) + (m_1 + m_2) \cdot \lfloor p/2 \rfloor) - (r_1 + r_2)^T As \\ &= (r_1 + r_2)^T e + (m_1 + m_2) \cdot \lfloor p/2 \rfloor). \end{aligned}$$

Če so vrednosti e dovolj majhne v primerjavi s p (kar pri kriptosistemu zahtevamo), potem je vrednost d bližje 0 kot $\lfloor p/2 \rfloor$, natanko tedaj, ko je $m_1 + m_2 = 0$ ali pa $m_1 + m_2 = 2$. Torej, par (c_0, c_1) ustreza kodiranemu sporočilu $m_1 + m_2 \mod 2$. Ali z drugimi besedami, dobimo šifrirano XOR-operacijo bitov m_1 in m_2.

Recimo, da imamo podatke, podane z biti $m_1, \ldots, m_k$, in bi želeli izračunati neko funkcijo $f(m_1, \ldots, m_k)$. Omejimo se na funkcije, ki se jih da opisati z zaporedno uporabo operacije XOR. Potem lahko podatke šifriramo in jih pošljemo ponudniku računanja v oblaku, ki nam pretvori šifrirane podatke v šifrirano vrednost $f(m_1, \ldots, m_k)$, ne da bi kakorkoli poznal podatke. Tako lahko računanje funkcij prenesemo na ponudnika takih storitev, brez ogrožanja osebnih podatkov.

Seveda so funkcije, ki jih lahko opišemo samo z uporabo vrat XOR, zelo omejene, pravzaprav neuporabne. Želeli bi kriptosistem, ki omogoča računanje poljubnih funkcij na šifriranih podatkih. Osnovna teorija računanja nam zagotavlja, da lahko poljubno funkcijo izrazimo z zaporedno uporabo NAND-vrat (znana tudi kot Shefferjev veznik). V naslednjih razdelkih bomo predstavili kriptosistem, ki omogoča seštevanje in množenje šifriranih podatkov in s tem uporabo NAND-vrat.

Generator psevdonaključnih vektorjev s stranskimi vrati

Problem LWE nam omogoča sestaviti nepričakovano orodje, ki ga bomo uporabili v shemi za homomorfno šifriranje. Tako kot prej naj bo $m \geq n \geq 1$, $A \in \mathbb{Z}_p^{m \times n}$ enakomerno naključno izbrana matrika, $x \in \mathbb{Z}_p^n$ enakomerno naključno izbran vektor in $e \in \mathbb{Z}^n$ vektor z majhnimi vrednostimi, naključno

izbran iz porazdelitve χ. Naj bo $b = Ax + e$ in naj bo $\beta = \lfloor p/2 \rfloor^{-1}$, torej inverz $\lfloor p/2 \rfloor$ v $\mathbb{Z}_p$. definirajmo matriko $B \in \mathbb{Z}_p^{m \times (n+1)}$, katere prvi stolpec je $-\beta b$, ostali stolpci pa ustrezajo A. Prav tako definirajmo $s \in \mathbb{Z}_p^{n+1}$, katerega prva komponenta je $\lfloor p/2 \rfloor$, ostale komponente pa ustrezajo x.

Predpostavimo, da je odločitveni problem $\mathrm{LWE}_{n,m,p,\chi}$ težek; npr. izberimo vrednosti $n, m, p\chi$ tako, da je problem vsaj tako težek kot problem na rešetkah, opisan v izreku 8. Potem nihče, ki ne pozna s, ne more razlikovati matrike B od enakomerno naključno generirane matrike, saj je b (in zato tudi $-\beta b$) neločljiv od enakomerno naključnega vektorja. Po drugi strani, če poznamo s, lahko izračunamo

$$Bs = -\lfloor p/2 \rfloor \beta b + Ax = -(Ax + e) + Ax = -e.$$

Po izreku 8 lahko parametre izberemo tako, da je $|e_i| < \sqrt{p}$ za vsako koordinato e_i vektorja e, saj lahko izberemo porazdelitev $\chi = D_\sigma$ z dovolj majhno standardno deviacijo. Torej je $-e$ vektor z majhnimi vrednostmi. Če poznamo s, lahko določimo, ali je B resnično enakomerna naključna matrika ali pa je bila generirana, kot je opisano zgoraj, saj lahko preprosto preverimo, če je vsaka komponenta Bs od 0 oddaljena za največ $\sqrt{p}$.

Zgornji postopek nam ob pravilni izbiri parametrov n, m, p, χ omogoča naslednje. Če naključno izberemo s, potem lahko generiramo $n+1$-dimenzionalne vektorje b_i (vrstice matrike B), ki jih nihče, ki ne pozna s, ne more razlikovati od enakomerno naključnih. Vendar porazdelitev teh vektorjev ni enakomerno naključna (je samo psevdonaključna), saj za njih velja, da je skalarni produkt b_i in s manjši od $\sqrt{p}$. Psevdonaključni vektorji imajo torej t. i. stranska vrata: čeprav se zdijo naključno izbrani, imajo posebne lastnosti, ki jih lahko izkoristimo.

Definicija 10. *LWE-generator psevdonaključnih vektorjev s stranskimi vrati* je par (G_s, s), kjer je G_s algoritem, ki generira naključne vektorje $b_i \in \mathbb{Z}_p^n$, katerih porazdelitev je brez poznavanja s računsko neločljiva od enakomerno naključnih vrednosti, ter $s \in \mathbb{Z}_p^n$ s prvo komponento $s_1 = \lfloor p/2 \rfloor$ tak, da je $|b_i^T s| < \sqrt{p}$ za vsak b_i generiran z G_s.

Zgoraj smo opisali, kako sestaviti LWE-generator psevdonaključnih vektorjev s stranskimi vrati, ki lahko generira vsaj m psevdonaključnih vektorjev pri predpostavki $\mathrm{LWE}_{n,m,p,\chi}$. Rekli bomo, da tak generator izberemo naključno, če naključno izberemo s, e in A iz ustreznih porazdelitev.

Dvojiško kodiranje

Preden spoznamo kriptosistem, ki omogoča homomorfno šifriranje, potrebujemo še zadnje orodje. Kodiranje je injektivna funkcija, ki vhodne podatke

pretvori v vektorje izbrane oblike. Za razliko od šifriranja kodiranje ne skrije podatkov, ampak jih samo preoblikuje. Da sestavimo kriptosistem s homomorfnim šifriranjem, potrebujemo orodje, ki nam bo vektorje nad $\mathbb{Z}_p$ pretvorilo v (daljše) vektorje z majhnimi vrednostmi.

Dvojiško kodiranje je funkcija, ki naravna števila pretvori v vektorje ničel in enk, t. i dvojiški zapis. Omejimo se na naravna števila, manjša od nekega $p \in \mathbb{N}$, torej števila iz $\mathbb{Z}_p$. Za vsak $x \in Z_p$ lahko enolično določimo vrednosti $y_i \in \{0,1\}$ za $0 \leq i < \lceil \log_2(p) \rceil$, da velja

$$x = \sum_{i=0}^{\lceil \log_2(p) \rceil - 1} 2^i y_i.$$

Preslikavo $x \mapsto \widehat{x}$, kjer je $\widehat{x} = (y_0, y_1, \ldots, y_{\lceil \log_2(p) \rceil - 1}) \in \{0,1\}^{\lceil \log_2(p) \rceil}$ tak, da velja zgornja enačba, imenujemo *dvojiško kodiranje* z $\lceil \log_2(p) \rceil$ biti. Inverzno preslikavo imenujemo dekodiranje in je po zgornji enačbi linearna preslikava, tj. x dobimo iz $\widehat{x}$ kot skalarni produkt $x = q \cdot \widehat{x}$, kjer je $q = (1, 2, 4, \ldots, 2^{\lceil \log_2(p) \rceil - 1})$.

Poleg elementov $\mathbb{Z}_p$ bi želeli dvojiško kodirati tudi vektorje in matrike nad $\mathbb{Z}_p$. Za vektorje nad $\mathbb{Z}_p^n$ dvojiško kodiranje definiramo kot preslikavo iz $\mathbb{Z}_p^n$ v $\{0,1\}^{n\lceil \log_2(p) \rceil}$. Dvojiško kodiranje vektorja $x \in \mathbb{Z}_p^n$ označimo z $\widehat{x}$ in ga definiramo kot vektor dolžine $n\lceil \log_2(p) \rceil$ s komponentami iz množice $\{0,1\}$, katerega bloki dolžine $\lceil \log_2(p) \rceil$ predstavljajo dvojiški zapis komponent x:

$$x = (x_1, x_2, \ldots, x_n) \mapsto (\widehat{x_1}, \widehat{x_2}, \ldots, \widehat{x_n}) = \widehat{x}.$$

Za tako definirano dvojiško kodiranje vektorjev je operacija dekodiranja linearna. Zato lahko s Q označimo matriko dimenzij $n \times n\lceil \log_2(p) \rceil$, da velja $Q\widehat{x} = x$ za vsak $x \in \mathbb{Z}_p^n$. Iz zgoraj opisanega je razvidno, da lahko matriko Q zapišemo kot

$$Q = \begin{bmatrix} 1 & 2 & 4 & \ldots & 2^{\lceil \log_2(p) \rceil - 1} & 0 & 0 & 0 & \ldots & 0 & \ldots & 0 & 0 & 0 & \ldots & 0 \\ 0 & 0 & 0 & \ldots & 0 & 1 & 2 & 4 & \ldots & 2^{\lceil \log_2(p) \rceil - 1} & \ldots & 0 & 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 0 & 0 & 0 & 0 & \ldots & 0 & \ldots & 1 & 2 & 4 & \ldots & 2^{\lceil \log_2(p) \rceil - 1} \end{bmatrix}.$$

Podobno lahko dvojiško kodiramo tudi matrike. Za matriko $C \in \mathbb{Z}_p^{m \times n}$ označimo s $\widehat{C}$ matriko dimenzij $m \times n\lceil \log_2(p) \rceil$, ki predstavlja dvojiško kodiranje vrstic c_i, za $1 \leq i \leq m$, v C:

$$C = \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_m \end{bmatrix} \mapsto \begin{bmatrix} \widehat{c_1} \\ \widehat{c_2} \\ \vdots \\ \widehat{c_m} \end{bmatrix} = \widehat{C}.$$

Po definiciji velja $\widehat{C}Q^T = C$ za vsako matriko $C \in \mathbb{Z}_p^{k\times n}$, kjer je $k > 0$ poljuben.

Homomorfno šifriranje

V tem razdelku bomo opisali kriptosistem za homomorfno šifriranje. Ta omogoča, da lastnik skrivnega ključa šifrira podatke, ki jih lahko nato (v šifrirani obliki) ne samo seštevamo, temveč tudi množimo. Za dešifriranje se uporabi isti ključ, tako da je tak sistem simetrične narave. Dokazali bomo, da sistem omogoča varno računanje v oblaku.

Varnost kriptosistema bo temeljila na težavnosti problema LWE, torej bo tak kriptosistem tudi kvantno varen ob pravilni izbiri parametrov:

- **Generiranje ključev:** Ključe, ki nam bodo omogočili šifriranje do k bitov, izberemo na naslednji način. Določimo $n, p, m = kn\lceil\log_2(p)\rceil$ in χ tako, da je odločitveni problem $\mathrm{LWE}_{n,m,p,\chi}$ težek – po izreku 8 to lahko storimo. Naključno izberemo LWE-generator psevdonaključnih vektorjev s stranskimi vrati (G_s, s) (torej izberemo A, e, s, kot opisano v podrazdelku Generirator psevdo-naključnih vektorjev s stranskimi vrati), ki temelji na težavnosti problema $\mathrm{LWE}_{n,m,p,\chi}$. Par (G_s, s) je skrivni ključ.

- **Šifriranje:** Da šifriramo bit $b \in \{0, 1\}$, uporabimo skrivni ključ (G_s, s), tako da s pomočjo G_s generiramo vektorje $d_1, \ldots, d_{n\lceil\log_2(p)\rceil} \in \mathbb{Z}_p^n$ in sestavimo matriko $D \in \mathbb{Z}^{n\lceil\log_2(p)\rceil\times n}$, katere vrstice so vektorji d_i. Izračunamo matriko $bQ^T + D$ in jo podamo v dvojiškem kodiranju:

$$C = b\widehat{Q^T + D}.$$

- **Dešifriranje:** S skrivnim ključem s in danim kriptogramom C izračunamo vektor $x = CQ^Ts$. Če je prva komponenta x bližje 0 kot $\lfloor p/2\rfloor$, potem vrnemo 0, sicer vrnemo 1.

Kriptosistem šifrira vsak bit b v dvojiško matriko C dimenzij $n\lceil\log_2(p)\rceil \times m\lceil\log_2(p)\rceil$. Kot bomo videli, lahko tako šifrirane podatke (matrike) seštevamo in množimo ter tako varno računamo funkcije brez poznavanja podatkov. Seveda je tako računanje časovno in prostorsko veliko zahtevnejše kot računanje na nešifriranih podatkih. Presenetljivo je, da je tak kriptosistem sploh teoretično mogoč. Še več; za ne preveč zahtevne funkcije je s sodobnimi računalniki računanje tudi praktično izvedljivo.

Analizirajmo varnost in pravilnost sheme:

Lema 11. *Če je C kriptogram, ki šifrira b, potem velja:*

$$CQ^T s = bQ^T s + e,$$

kjer je vsaka komponenta vektorja e manjša od $\sqrt{p}$.

Dokaz. Ker velja $\widehat{M}Q^T = M$ za vsako matriko M, lahko izračunamo:

$$CQ^T s = (b\widehat{Q^T + D})Q^T s = (bQ^T + D)s = bQ^T s + Ds.$$

Vrstice D so generirane z LWE-generatorjem psevdonaključnih vektorjev s stranskimi vrati (G_s, s), tako da za vsako vrstico $d_i \in \mathbb{Z}_p^{1\times n}$ velja $|d_i s| < \sqrt{p}$. ∎

Izrek 12. *Zgoraj opisan kriptosistem deluje pravilno in je IND-CPA varen.*

Dokaz. Pokažimo, da kriptosistem deluje pravilno. Ko v postopku dešifriranja izračunamo $x = CQ^T s$, dobimo vektor x, katerega prva komponenta ustreza prvi komponenti $bQ^T s + e$ po lemi 11. Spomnimo se, da je prva komponenta vektorja s enaka $\lfloor p/2 \rfloor$, medtem ko je prva vrstica Q^T enaka $[1, 0, \ldots, 0]$. Torej je prva komponenta $m_1 = b\lfloor p/2 \rfloor + e_1$, kjer je $|e_1| < \sqrt{p}$. Sledi, da če je $b = 1$, je m_1 bližje $\lfloor p/2 \rfloor$ kot 0, in obratno, če je $b = 0$.

Varnost kriptosistema se dokaže tako, da se argumentira, da nihče, ki ne pozna skrivnosti s, ne more računsko razlikovati šifrirane vrednosti $b = 0$ od šifrirane vrednosti $b = 1$. Ker je matrika D generirana z LWE-generatorjem psevdonaključnih vektorjev, je za vsakega, ki ne pozna s, računsko neločljiva od enakomerno naključne matrike. Torej je tudi vrednost $bQ^T + D$ neločljiva od enakomerno naključne matrike. Sledi, da nihče, ki ne pozna s, ne more ločiti, katera vrednost je bila šifrirana. ∎

Pripravljeni smo, da predstavimo, kako opisan kriptosistem omogoča homomorfno šifriranje. Naj bosta C_1 in C_2 kriptograma, ki šifrirata bita b_1 in b_2:

- **Seštevanje:** definirajmo $C_1 \oplus C_2 = C_1 + C_2$ in obravnavajmo slednje kot nov kriptogram. Za dešifriranje izračunamo

  $$(C_1 \oplus C_2)Q^T s = (C_1 + C_2)Q^T s = (b_1 + b_2)Q^T s + (e_1 + e_2),$$

  kjer je $||e_i||_\infty < \sqrt{p}$, po lemi 11. Vidimo, da se $C_1 \oplus C_2$ dešifrira v vrednost $b_1 + b_2 \mod 2$, torej v XOR-operacijo bitov b_1 in b_2, le da je šum $e_1 + e_2$, ki pri tem nastane, povečan.

- **Množenje:** definirajmo $C_1 \otimes C_2 = \widehat{C_1 Q^T} C_2$. Prav tako lahko izračunamo

$$\begin{aligned}(C_1 \otimes C_2) Q^T s &= \widehat{C_1 Q^T} C_2 Q^T s = \widehat{C_1 Q^T}(b_2 Q^T s + e_2) \\ &= b_2 C_1 Q^T s + \widehat{C_1 Q^T} e_2 = b_1 b_2 Q^T s + b_2 e_1 + \widehat{C_1 Q^T} e_2,\end{aligned}$$

  kjer prva enakost velja po definiciji $C_1 \otimes C_2$, druga in četrta po lemi 11 in tretja velja, saj je $\widehat{X} Q^T = X$ za vsako matriko X po lastnostih dvojiškega kodiranja. Po lemi 11 je $||e_i||_\infty < \sqrt{p}$. Tudi tokrat lahko na zgoraj navedeno gledamo kot na dešifriranje vrednosti $b_1 b_2 \mod 2$ s šumom $b_2 e_1 + \widehat{C_1 Q^T} e_2$. Prepričajmo se, da je slednja vrednost res majhna, torej da jo res lahko obravnavamo kot šum in ne pokvari dešifriranja. Ker velja $||e_1||_\infty < \sqrt{p}$ in $b_2 \in \{0, 1\}$, je prvi člen res majhen. Po drugi strani je $\widehat{C_1 Q^T}$ dvojiško kodiranje matrike $C_1 Q^T$, torej so njene komponente iz $\{0, 1\}$. Ker ima $n\lceil \log_2(p) \rceil$ stolpcev in je $||e_2||_\infty < \sqrt{p}$, vidimo, da je vsaka komponenta drugega člena omejena z $n\lceil \log_2(p) \rceil \sqrt{p}$. Za primerno izbrane parametre je taka vrednost še vedno manjša od $p/4$, torej dešifriranje $C_1 \otimes C_2$ uspe in vrne $b_1 b_2 \mod 2$, torej AND-operacijo bitov b_1 in b_2.

Kot vidimo, nam kriptosistem omogoča operaciji seštevanja in množenja kriptogramov in s tem operaciji XOR in AND na šifriranih podatkih. Želeli bi kriptosistem, ki bi lahko izračunal vsako funkcijo. Kot smo omenili v razdelku Aditivno šifriranje, zadošča, da sistem omogoča zaporedno izvajanje NAND-vrat (Shefferjevega veznika) na šifriranih podatkih, saj lahko s tem veznikom predstavimo vsako funkcijo. Uporabimo množenje za definicijo nove operacije na šifriranih podatkih:

- **NAND:** definirajmo $C_1 \barwedge C_2 = I - C_1 \otimes C_2$. Če slednje obravnavamo kot nov kriptogram in dešifriramo, dobimo

$$(C_1 \barwedge C_2) Q^T s = (I - C_1 \otimes C_2) Q^T s = (1 - b_1 b_2) Q^T s - b_2 e_1 - \widehat{C_1 Q^T} e_2.$$

  V izračunu smo uporabili enakost, ki smo jo dobili pri operaciji množenja. Vidimo, da se $C_1 \barwedge C_2$ dešifrira v vrednost $1 - b_1 b_2 \mod 2$, torej NAND-vrednost bitov b_1 in b_2.

S takim kriptosistemom lahko torej (teoretično) izračunamo poljubno funkcijo na šifriranih podatkih, vendar pri tem šum narašča in z večkratnim ponavljanjem operacije lahko naraste do takih vrednosti, da dešifriranje ni več uspešno. Zato je treba vnaprej omejiti število zaporednih operacij, ki

jih sistem še omogoča, oziroma v primeru kompleksnejših funkcij parametre povečati tako, da še sprejmejo izbrano funkcijo.

Takemu kriptosistemu pravimo tudi *delno homomorfno šifriranje*. Gentry je v [3] dokazal, da se v nekaterih primerih da delno homomorfno šifriranje spremeniti v *polno homomorfnega* s tehniko, ki jo je imenoval *bootstraping*. Tehnika deluje na vsakem delno homomorfnem sistemu, ki zadošča tako imenovani *ciklični varnosti*. Vendar je prehod na polno homomorfen sistem računsko zelo zahteven in zato počasnejši, tako da se večina praktičnih uporab omeji na delno homomorfno šifriranje. Zainteresiranega bralca, ki bi želel izvedeti več o uporabi problema LWE v kriptografiji, usmerimo k branju [2].

V času pisanja tega članka že obstaja več implementacij delno in polno homomorfnih kriptosistemov. Veliko truda je bilo vloženega v razvoj učinkovitejšega homomorfnega šifriranja, kot je bil opisan v tem razdelku. Glavni steber trenutnega razvoja predstavljajo problem LWE in njegove izpeljanke.

LITERATURA

[1] M. R. Albrecht, R. Player in S. Scott, *On the concrete hardness of learning with errors*, Journal of Mathematical Cryptology **9**(3) (2015), 169–203.

[2] B. Barak, *An intensive introduction to cryptography*, dostopno na `intensecrypto.org/public/index.html`, ogled 3. 11. 2020.

[3] C. Gentry, *Fully homomorphic encryption using ideal lattices*, v Proceedings of the forty-first annual ACM symposium on Theory of computing, 2009, 169–178.

[4] O. Regev, *On lattices, learning with errors, random linear codes, and cryptography*, Journal of the ACM **56**(6) (2009), 1–40.

[5] R. L. Rivest, L. Adleman in M. L. Dertouzos, *On data banks and privacy homomorphisms*, Foundations of secure computation **4**(11) (1978), 169–180.

[6] P. Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM review **41**(2) (1999), 303–332.

[7] *Post-Quantum Cryptography*, dostopno na `csrc.nist.gov/Projects/Post-Quantum-Cryptography`, ogled 3. 11. 2020.

VRTENJE ZRCAL

NADA RAZPET

Pedagoška fakulteta
Univerza v Ljubljani

Ključne besede: ravno zrcalo, konkavno cilindrično zrcalo, konstrukcije slik, lege slik

Najprej bomo vrteli dve med seboj pravokotni zrcali, ki z vodoravno ravnino oklepata kot 45°, okrog navpične osi, nato pa bomo vrteli konkavno cilindrično zrcalo. Pokazali bomo, da se pri zasuku zrcal za kot α slika v obeh primerih zavrti za kot 2α.

ROTATION OF MIRRORS

We first consider rotation about a vertical axis of two mutually perpendicular mirrors making an angle of 45° with the horizontal plane, then we consider rotation of a concave cylindrical mirror. We show that, in both cases, rotating mirrors by an angle α produces rotation of the image by an angle 2α.

Geometrijska optika je v vseh izobraževalnih programih na koncu študijskega leta. V osnovni šoli pokažemo nekaj poskusov z ravnimi in krogelnimi zrcali ter konstruiramo nekaj slik, ki nastanejo pri preslikavah s temi zrcali. Za konstrukcijo slik uporabljamo le karakteristične žarke. Večinoma preslikujemo pokončne predmete, najraje na optično os pravokotne daljice, pravzaprav le krajišča daljic z dvema žarkoma: z žarkom, ki je vzporeden z optično osjo, in žarkom, ki gre skozi teme zrcal.

V srednji šoli geometrijsko optiko »na hitro« ponovimo. Da pojmi niso razčiščeni, se hitro pokaže pri preverjanjih znanja, pa tudi naše izkušnje s tekmovanj v znanju fizike kažejo, da se tematiki ne posveča posebne pozornosti. Še več, opuščajo se tudi osnovni poskusi, ki pa so lahko še kako zanimivi.

Ravna in krogelna zrcala so lahko dostopna in so na voljo v različnih velikostih. S cilindričnimi se v šoli ne ukvarjamo, brez težav pa jih izdelamo sami iz zrcalne folije, ki jo dobimo tudi pri nas.

Ravno zrcalo

Navadno je ravno zrcalo obešeno na navpični steni. Pri poskusih pa ga postavimo pravokotno na mizo, kjer med poskusom miruje. Kaj pa se zgodi, če ravno zrcalo zasučemo? Ali je vseeno, okoli katere osi sučemo zrcalo? Kako naj bo postavljeno? Če sučemo le eno ravno zrcalo okrog osi, ki je pravokotna na ravnino zrcala, ne opazimo nič posebnega. Drugače pa je, če sučemo dve ravni zrcali, ki se stikata po eni stranici in sta med seboj

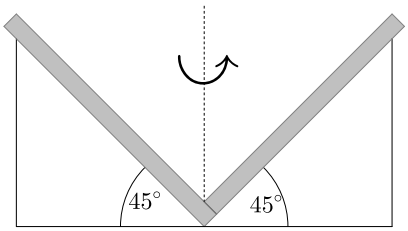
pravokotni. Lahko bi bili tudi pod drugačnim kotom, recimo 30°, 45° ali 60°. To so koti, ki so delitelji polnega kota. Medsebojni kot vpliva na število slik, ki jih vidimo.

Dve med seboj pravokotni ravni zrcali

Obravnavo poskusov z dvema, med seboj pravokotnima zrcaloma, najdemo v številnih učbenikih fizike, recimo v [1]. Pogosto avtorji predstavijo tudi konstrukcije slik v poševni projekciji ali pa v tlorisu. Pri tem sta zrcali postavljeni pravokotno na podlago in pri poskusih mirujeta. Izjemoma so predstavljeni kalejdoskopi, kjer pa se hkrati z vrtenjem zrcal spreminja tudi lega predmetov.

V članku [3] je opisan poskus z dvema pravokotnima zrcaloma v škatli, ki jo vrtimo okrog vodoravne osi. Naš poskus je enostavnejši, saj ne potrebujemo škatle in lepljenja zrcal.

Dve ravni zrcali postavimo na nosilec tako, da sta med seboj pravokotni in z vodoravno ravnino – mizo – oklepata kot 45°, kot kaže slika 1.



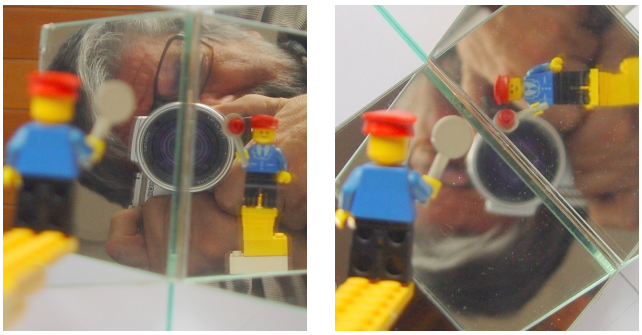
Slika 1. Dve, med seboj pravokotni ravni zrcali postavimo na vodoravno podlago, ki je vrtljiva okoli navpične osi.

Nad zrcali obesimo figuro prometnika. Na začetku poskusa je telo prometnika vzporedno z mizo in stično stranico zrcal. Zrcali vrtimo v vodoravni ravnini (x, y) okrog navpične osi z. Najprej ju zavrtimo za kot $\alpha = 45°$ (slika 2), nato pa za $\alpha = 90°$. Opazujemo sliko, ki nastane po odboju od obeh zrcal.

Kaj smo opazili? Ko zrcali zasučemo za kot α, se slika zavrti za kot 2α.

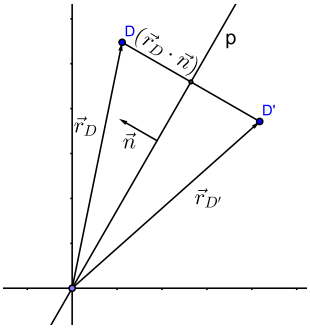
Račun za dve med seboj pravokotni zrcali

Zdaj pa izide poskusov utemeljimo še z računom. Najprej ponovimo, kako točko zrcalimo preko premice. Izberemo premico p, ki gre skozi koordinatno izhodišče. Točko D s krajevnim vektorjem $\overrightarrow{r_D}$ preslikamo preko premice p



Slika 2. Prometnik je obešen nad zrcaloma tako, da leži vodoravno in se med poskusom ne premika. Ko zrcalo zavrtimo za 45°, se slika zavrti za 90°. Tudi slika fotografove glave se je zavrtela, čeprav fotografira vedno z istega mesta. Opazujemo le sliko, ki nastane po odboju od obeh zrcal.

v točko D' s krajevnim vektorjem $\overrightarrow{r_{D'}}$. Enotski normalni vektor na premici p je vektor $\overrightarrow{n}$ (slika 3). Veljata zvezi:

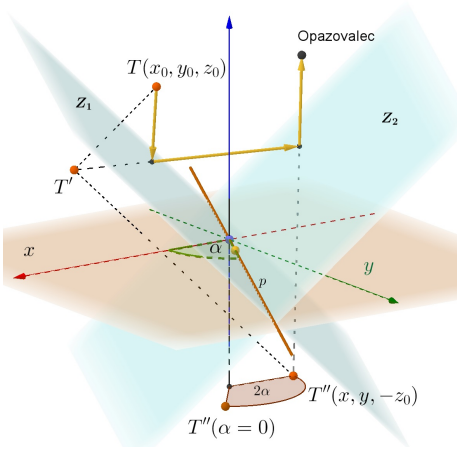


Slika 3. Preslikava točke preko premice.

$$d(DD') = 2\,\overrightarrow{r_D} \cdot \overrightarrow{n}, \qquad \overrightarrow{r_{D'}} = \overrightarrow{r_D} - 2(\overrightarrow{r_D} \cdot \overrightarrow{n})\,\overrightarrow{n}. \tag{1}$$

Pri zrcaljenju točke preko ravnine velja enaka povezava kot za preslikavo preko premice (enačba (1)), kjer je vektor $\overrightarrow{n}$ zdaj enotski normalni vektor na ravnino.

Narišimo še ustrezno skico (slika 4). Namesto celega predmeta bomo prezrcalili le eno točko in pogledali, kako se spreminja lega slike točke po odboju od obeh zrcal v odvisnosti od zasuka zrcal.



Slika 4. Če zrcali zavrtimo za kot α okrog navpične osi, se slika točke, po odboju od obeh zrcal, zavrti za kot 2α.

Normalna vektorja na ravninah Z_1 in Z_2 sta:

$$\overrightarrow{n_1}(\alpha) = \frac{\sqrt{2}}{2}(-\sin\alpha, \cos\alpha, 1), \qquad \overrightarrow{n_2}(\alpha) = \frac{\sqrt{2}}{2}(\sin\alpha, -\cos\alpha, 1),$$
$$\overrightarrow{n_2}(\alpha) = \overrightarrow{n_1}(\pi + \alpha).$$

Najprej točko T prezrcalimo preko ravnine Z_1 :

$$\begin{aligned} \overrightarrow{r_{'}} &= \overrightarrow{r} - 2(\overrightarrow{r} \cdot \overrightarrow{n_1})\overrightarrow{n_1}, \\ \overrightarrow{r_{'}} &= (x_0, y_0, z_0) - (-x_0 \sin\alpha + y_0 \cos\alpha + z_0) \cdot (-\sin\alpha, \cos\alpha, 1). \end{aligned}$$

Krajevni vektor točke T' je

$$\overrightarrow{r_{'}} = \begin{bmatrix} x_0 \cos^2\alpha + y_0 \sin\alpha\cos\alpha + z_0 \sin\alpha \\ x_0 \sin\alpha\cos\alpha + y_0 \sin^2\alpha - z_0 \cos\alpha \\ x_0 \sin\alpha - y_0 \cos\alpha \end{bmatrix}.$$

Točko T' potem prezrcalimo še preko Z_2, da dobimo točko T''. Krajevni vektor točke T'' je:

$$\overrightarrow{r_{''}} = \overrightarrow{r_{'}} - 2(\overrightarrow{r_{'}} \cdot \overrightarrow{n_2})\overrightarrow{n_2}. \tag{2}$$

Izračunamo vektor, ki kaže iz točke T' do točke T'', pri čemer upoštevamo povezavo

$$-2(\overrightarrow{r_{'}} \cdot \overrightarrow{n_2})\overrightarrow{n_2} = -\begin{bmatrix} x_0 \sin^2\alpha - y_0 \sin\alpha\cos\alpha + z_0 \sin\alpha \\ -x_0 \sin\alpha\cos\alpha + y_0 \cos^2\alpha - z_0 \cos\alpha \\ x_0 \sin\alpha - y_0 \cos\alpha + z_0 \end{bmatrix}.$$

Vstavimo v enačbo (2) in upoštevamo, da velja

$$\sin^2\alpha+\cos^2\alpha=1,\quad 2\sin\alpha\cos\alpha=\sin(2\alpha),\quad \cos^2\alpha-\sin^2\alpha=\cos(2\alpha). \tag{3}$$

Nazadnje dobimo:

$$\overrightarrow{r''}=\begin{bmatrix} x_0\cos(2\alpha)+y_0\sin(2\alpha)\\ x_0\sin(2\alpha)-y_0\cos(2\alpha)\\ -z_0\end{bmatrix}=$$

$$=\begin{bmatrix}\cos(2\alpha) & -\sin(2\alpha) & 0\\ \sin(2\alpha) & \cos(2\alpha) & 0\\ 0 & 0 & 1\end{bmatrix}\begin{bmatrix}1 & 0 & 0\\ 0 & -1 & 0\\ 0 & 0 & -1\end{bmatrix}\begin{bmatrix}x_0\\ y_0\\ z_0\end{bmatrix}.$$

Kaj smo ugotovili?

V začetni legi zrcal, ko je kot $\alpha=0$, dobimo sliko T'' točke T tako, da jo prezrcalimo preko osi x. Ko pa zrcali zasukamo za kot α, se prezrcaljena točka še zavrti okrog osi z za kot 2α.

Ker je predmet na začetku poskusa ležal vzporedno z mizo, tudi izbrana slika predmeta – slika po odboju od obeh zrcal – leži v ravnini, ki je vzporedna z mizo in od nje enako oddaljena kot predmet.

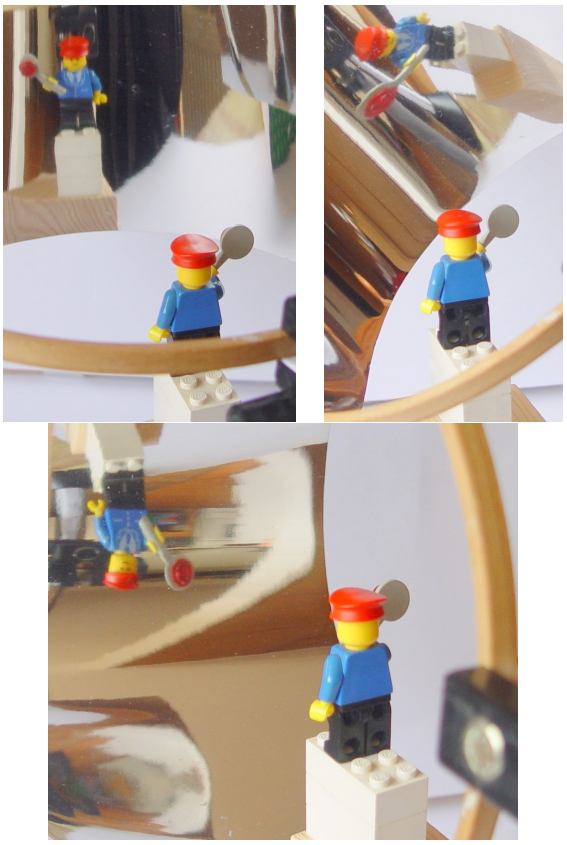
Poudarimo še to, da na sliki leva in desna roka prometnika nista zamenjani – lopar še vedno drži v desni roki, kot je to pri preslikavi z enim ravnim zrcalom.

Konkavno cilindrično zrcalo

Naredimo še poskus s konkavnim cilindričnim zrcalom. O tem lahko beremo v [2].

Konkavno cilindrično zrcalo izdelamo iz pravokotnega kosa zrcalne folije, ki ga pritrdimo na obroč. Mi smo vzeli pravokotnik z osnovnico, ki meri približno polovico obsega obroča. Obroč poteka po polovici višine pravokotnika. Zrcalna folija je torej del plašča valja, katerega os je pravokotna na ravnino obroča. Obroč vrtljivo pritrdimo na nosilec tako, da se vrti okrog vodoravne osi, ki gre skozi središče obroča. Os valja se potem vrti v navpični ravnini. Razdalja d prometnika do zrcala naj bo med r in $2r$, pri čemer je r polmer obroča, na katerem je pritrjena folija. Na začetku je obroč vodoravno, prometnik pa stoji navpično. Ravnino obroča zavrtimo najprej za 45°, nato pa za 90° (slika 5).

Kaj opazimo? Opazimo, da se slika predmeta tudi zavrti. V prvem primeru leži slika prometnika vodoravno, v drugem pa je obrnjen na glavo. Opazimo še, da leva in desna stran nista zamenjani. Na sliki prometnik še vedno drži lopar v desni roki. Da je slika res realna, bomo pokazali kasneje.

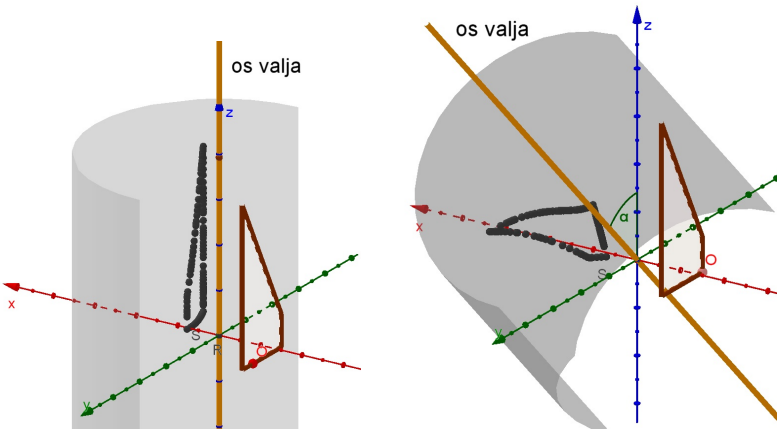


Slika 5. Predmet je pred konkavnim cilindričnim zrcalom in se med poskusom ne premika. Ko zrcalo zavrtimo za kot 45°, se slika zavrti za kot 90°, ko pa zrcalo zasukamo za kot 90°, se slika zasuka za 180°.

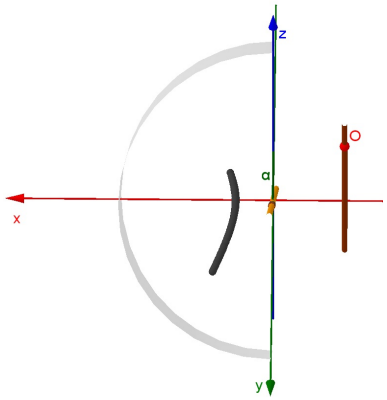
Ponazorimo si to še s skicama (slika 6 in 7), ki smo jih naredili s programom GeoGebra. Predmet je štirikotnik, ki leži v ravnini vzporedni z ravnino (y, z). Slika štirikotnika pa ni ravninski lik. Preslikani štirikotnik je »ukrivljen«, kar kaže slika 7.

Pokažimo še, da je slika realna. Poiščimo sliko točke T, katere oddaljenost od zrcala je med r in $2r$. Opazujemo žarke, ki ležijo v ravnini, ki je pravokotna na os valja. Na sliki 8 sta vpadni pravokotnici označeni črtkano. Slika točke T je točka T'. Sekata se odbita žarka, torej je slika realna. Za ozek trak konkavnega cilindričnega zrcala lahko privzamemo, da je del konkavnega krogelnega zrcala, za katerega velja:

$$\frac{1}{a} + \frac{1}{b} = \frac{1}{f}$$

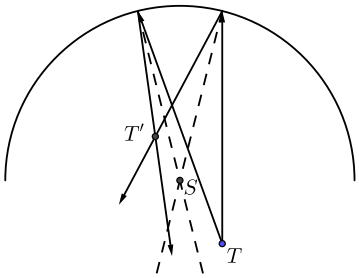


Slika 6. Leva slika kaže začetno lego predmeta – štirikotnika – in njegovo sliko. Desno: Ko zrcalo zavrtimo za kot 45°, se slika štirikotnika zavrti za kot 90°. Slika je realna.



Slika 7. Projekcija štirikotnika – daljica – in njegove slike – ukrivljena črta – na vodoravno ravnino (x, y) pri zasuku osi zrcala za 45°. Stranice slike štirikotnika so zakrivljene in ne ležijo v isti ravnini. Slika je realna.

Goriščna razdalja takega zrcala je $r/2$. Točke, ki so od temena oddaljene za $r \leq a < 2r$, se preslikajo v točke, za katere je oddaljenost od temena $2r/3 \leq b < r$. Pri računanju bomo tudi privzeli, da je oddaljenost y_0 vpadnega žarka od osi valja majhna v primerjavi s polmerom valja. Posledično to pomeni, da so vpadni koti žarkov majhni. Pri večjih vpadnih kotih bi morali upoštevati, da slika točke pri vrtenju zrcala opisuje krivuljo, ki ni ravninska (slika 7).



Slika 8. Sliko točke T dobimo s presečiščem odbitih žarkov. Vpadni pravokotnici sta označeni črtkano.

Račun za konkavno cilindrično zrcalo

Ugotovitve podkrepimo še z računom. Vrtilna os naj bo kar os x, kot vrtenja bomo označili z α, os valja, katerega del je zrcalo, pa naj leži v ravnini (y, z). Zapišimo enačbo zrcala v parametrični obliki, kjer sta u in v parametra, kot α pa kot nagiba osi valja;

$$\overrightarrow{r}(u, v) = (a\cos u, a\sin u\cos\alpha + v\sin\alpha, -a\sin u\sin\alpha + v\cos\alpha). \qquad (4)$$

Pri tem je a polmer valja, parametra pa zavzemata naslednje vrednosti: $u \in [-\pi/2, \pi/2]$ in $v \in [-h, h]$. S h smo označili polovično višino valja. Brez škode za splošnost lahko privzamemo, da je polmer valja $a = 1$.

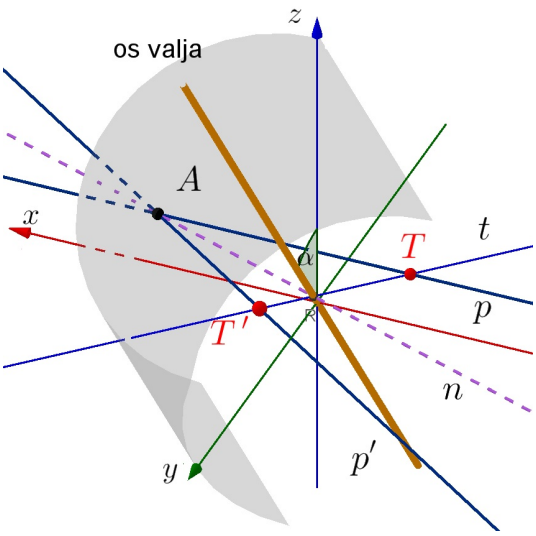
Smerni vektor na osi valja je $\overrightarrow{n} = (0, \sin\alpha, \cos\alpha)$. Preslikujemo točko $T(0, y_0, 0)$. Vpadni žarek naj bo vzporeden z osjo x in naj leži na premici p:

$$\overrightarrow{p} = (0, y_0, 0) + \lambda(1, 0, 0). \qquad (5)$$

Pri tem je λ parameter. Točka $A(x_1, y_0, 0)$ je prebodišče vpadnega žarka s plaščem valja, torej leži tako na premici p, ki je vzporedna z osjo x, kot na ploskvi $\overrightarrow{r}(u, v)$, zato mora veljati:

$$\begin{aligned} \lambda &= \cos u_0, \\ y_0 &= \sin u_0\cos\alpha + v_0\sin\alpha, \qquad (6) \\ 0 &= -\sin u_0\sin\alpha + v_0\cos\alpha. \qquad (7) \end{aligned}$$

Vpadni žarek prebada plašč valja v točki A. Lega vpadnega žarka se pri nagibanju osi ne spreminja. Spremeni pa se lega vpadne pravokotnice, to je premice, ki gre skozi prebodišče A in je pravokotna na os valja. Vpadni žarek p, prebodišče A, vpadna pravokotnica n in odbiti žarek p' ležijo v ravnini, ki je pravokotna na os valja. Slika točke T, točka T', leži na odbitem žarku p'.



Slika 9. Uporabljene oznake v računih.

Lega odbitega žarka pa je odvisna od lege vpadne pravokotnice n, ki pa jo lahko hitro zapišemo. Omenimo še, da sliko točke T dobimo s presečiščem odbitih žarkov, v našem primeru premic p' in t, torej je slika realna [6].

Prebodišče A se pri zasuku osi za kot α *premika* po premici p. Iz enačb (6) in (7) izrazimo v_0 in $\sin u_0$. Dobimo:

$$v_0 = y_0 \sin\alpha, \tag{8}$$
$$\sin u_0 = y_0 \cos\alpha. \tag{9}$$

Potrebujemo še ploskovno normalo, ki je vpadna pravokotnica za žarek, ki leži na premici p. Najprej izračunamo iz enačbe (4) parcialna odvoda:

$$\frac{\partial \overrightarrow{r}}{\partial u} = (-\sin u, \cos u\cos\alpha, -\cos u\sin\alpha), \qquad \frac{\partial \overrightarrow{r}}{\partial v} = (0, \sin\alpha, \cos\alpha),$$

nato pa normalni vektor $\overrightarrow{n}$ dobimo z vektorskim produktom parcialnih odvodov:

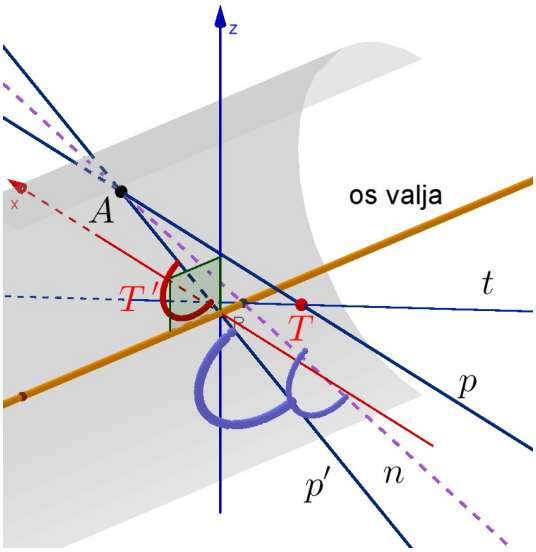
$$\overrightarrow{n} = \frac{\partial \overrightarrow{r}}{\partial u} \times \frac{\partial \overrightarrow{r}}{\partial v} = (\cos u, \sin u\cos\alpha, -\sin u\sin\alpha).$$

Za normalni vektor tangentne ravnine v točki A torej velja:

$$\overrightarrow{n_1} = (\cos u_0, \sin u_0\cos\alpha, -\sin u_0\sin\alpha). \tag{10}$$

Vstavimo za $\sin u_0$ izraz (9) in upoštevamo, da veljajo povezave (3);

$$\overrightarrow{n_1} = \begin{bmatrix} \sqrt{1 - y_0^2 \cos^2 \alpha} \\ y_0 \cos^2 \alpha \\ -y_0 \cos \alpha \sin \alpha \end{bmatrix}. \tag{11}$$



Slika 10. Slika točke T je točka T'. Poljubna točka na premici p' in poljubna točka na normali se zavrtijo za 180° (zaporedno od zgoraj navzdol), ko os valja zasukamo za 90°.

Zdaj pa poglejmo, kam se preslikajo nekatere točke. Ker gledamo žarke v ravninah, ki so pravokotne na os valja, izračunajmo središče krožnice, ki jo ta ravnina odreže od valja. Središče S leži na osi valja, ta pa je v ravnini (y, z). Poiskati moramo torej presečišče med osjo valja in premico, ki gre skozi točko T in je pravokotna na os valja. Teh dveh premic ni težko zapisati, saj obe ležita v isti ravnini.

$$z = y \cot \alpha, \qquad z = -(y - y_0) \tan \alpha$$

$$z = \frac{y_0 \tan \alpha}{1 + \tan^2 \alpha}, \qquad y = \frac{y_0 \tan^2 \alpha}{1 + \tan^2 \alpha}.$$

Presečišče teh dveh premic je točka

$$S(0, y_0 \sin^2 \alpha, y_0 \sin \alpha \cos \alpha).$$

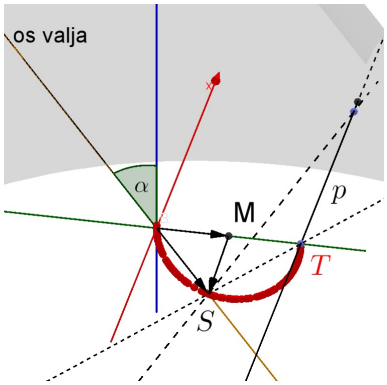
Ko je os valja navpično, je središče kroga v izhodišču ($S = O = (0, 0, 0)$) (slika 11). Ko os zasukamo za kot 90°, preide točka S v točko $S_1 =$

$(0, y_0, 0) = T$. Vzemimo, da potuje točka S po krožnici. Središče je točka $M = (0, y_0/2, 0)$. Da zares potuje po krožnici, mora biti $\left|\overrightarrow{OS} - \overrightarrow{OM}\right| = y_0/2$. Pa poglejmo:

$$\overrightarrow{OS} - \overrightarrow{OM} = \left(0, y_0 \sin^2\alpha - \frac{y_0}{2}, y_0 \sin\alpha\cos\alpha\right) = \left(0, -\frac{\cos 2\alpha}{2}\, y_0, \frac{\sin 2\alpha}{2}\, y_0\right),$$

$$\left|\overrightarrow{OS} - \overrightarrow{OM}\right| = \frac{|y_0|}{2}.$$

Absolutna vrednost razlike teh dveh vektorjev je konstantna, torej se točka S giblje po krožnici. Ko se os valja zavrti za kot $90°$, točka S opiše polkrožnico.



Slika 11. Točka S opisuje polkrožnico, ko os valja zavrtimo za $90°$.

To lahko zapišemo še drugače:

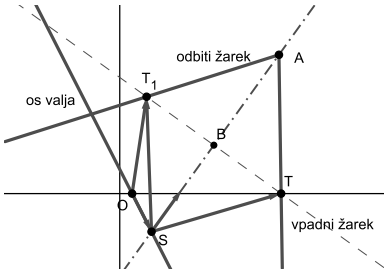
$$\overrightarrow{OS} - \overrightarrow{OM} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos 2\alpha & \sin 2\alpha \\ 0 & -\sin 2\alpha & \cos 2\alpha \end{bmatrix} \begin{bmatrix} 0 \\ -1 \\ 0 \end{bmatrix} \frac{y_0}{2}.$$

Točka S se torej pri zasuku valja – zrcala – za kot α zavrti za kot 2α.

Poiščimo še enačbo premice p', na kateri leži odbiti žarek. V ta namen najprej eno točko prezrcalimo preko vpadne pravokotnice. Vzemimo kar točko $T(0, y_0, 0)$. Pomagamo si s skico 12.

Naj bo točka B pravokotna projekcija točke T na vpadno pravokotnico. Iz skice razberemo, da velja:

$$\overrightarrow{ST} = (0, y_0\cos^2\alpha, -y_0\sin\alpha\cos\alpha), \qquad \overrightarrow{SB} = (\overrightarrow{ST}\cdot\overrightarrow{n_1})\overrightarrow{n_1}.$$



Slika 12. Točko T prezrcalimo preko vpadne pravokotnice. Dobimo točko T_1.

Pri tem je vektor $\overrightarrow{n_1}$ enotski vektor na vpadni pravokotnici. Dobimo:

$$\overrightarrow{SB} = y_0^2 \cos^2\alpha \left(\sqrt{1 - y_0^2 \cos^2\alpha},\, y_0 \cos^2\alpha,\, -y_0 \sin\alpha \cos\alpha \right).$$

In končno

$$\overrightarrow{ST_1} = \overrightarrow{ST} + 2\overrightarrow{TB} = 2\overrightarrow{SB} - \overrightarrow{ST}, \qquad \overrightarrow{OT_1} = \overrightarrow{OS} + \overrightarrow{ST_1},$$

$$\overrightarrow{OT_1} = \begin{bmatrix} 2y_0^2\sqrt{1 - y_0^2\cos^2\alpha} \cdot \cos^2\alpha \\ y_0\cos^2\alpha(2y_0^2\cos^2\alpha - 1) + y_0\sin^2\alpha \\ -2y_0\sin\alpha\cos\alpha(y_0^2\cos^2\alpha - 1) \end{bmatrix}.$$

Zapišimo še krajevna vektorja točke T_1 pri kotih $\alpha = 0°$ in $\alpha = 90°$:

$$\overrightarrow{r_1} = (2y_0^2\sqrt{1 - y_0^2},\, y_0(2y_0^2 - 1),\, 0), \qquad \overrightarrow{r_2} = (0, y_0, 0).$$

Točka T_1 leži na premici p', to je na odbitem žarku. Enačbe te premice ne bomo računali, je pa ni težko najti, saj sta na njej točka A, to je prebodišče, in točka T_1. Poglejmo, kakšno krivuljo opiše, ko se os valja zavrti za kot $90°$. Privzemimo, da potuje po krožnici, ki ima središče v točki B. Potem mora biti

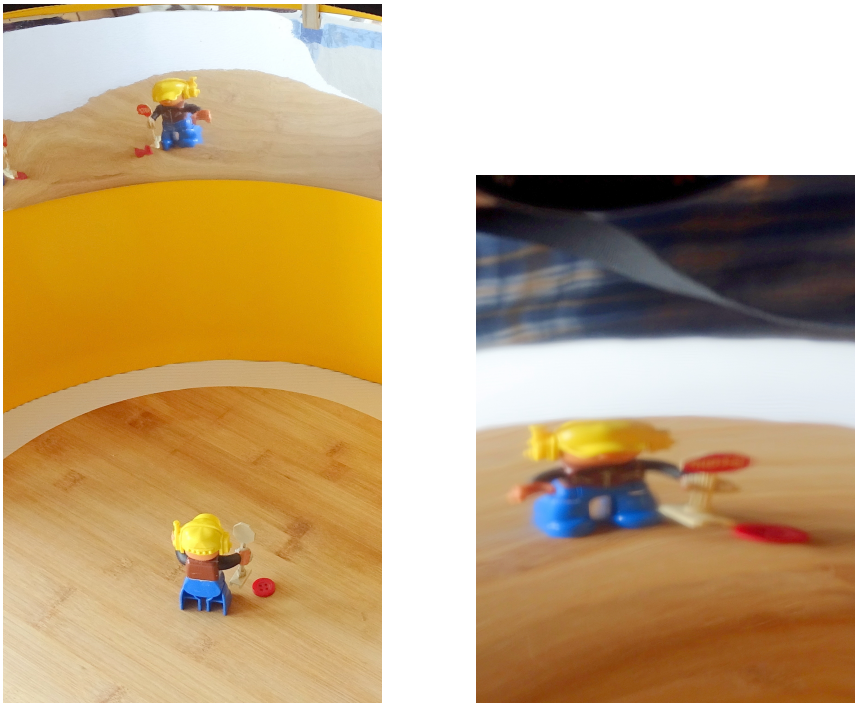
$$\left| \overrightarrow{OT_1} - \overrightarrow{OB} \right| = \left| \overrightarrow{BT} \right|.$$

Po daljšem računu pokažemo, da leva stran ni enaka desni. Lahko pa z uporabo enega od grafičnih programov hitro ugotovimo, da se krivulja pri majhnih vpadnih kotih kar dobro prilega krožnici.

Še ena zanimivost cilindričnega konkavnega zrcala

V članku [6] je napisan komentar na članek [2], kjer je opisano vrtenje opazovalčeve glave pri vrtenju konkavnega cilindričnega zrcala in narisana konstrukcija slike, ko je os valja horizontalna.

V komentarju avtor opozarja, da je treba opazovati ne le žarke, ki ležijo v ravninah, ki so pravokotne na os valja, ampak tudi tiste vpadne žarke, ki ležijo v ravninah, ki so vzporedne z osjo valja. Ti žarki namreč določajo navidezno sliko predmeta.



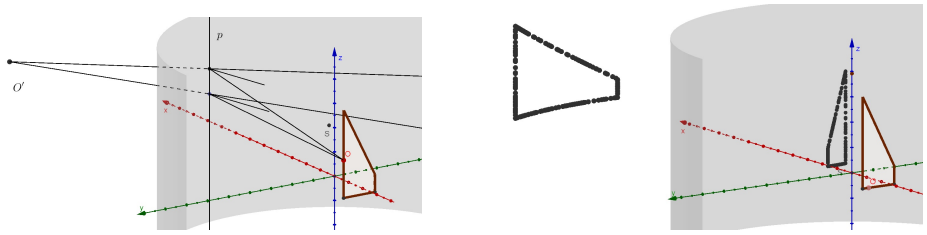
Slika 13. Levo: realna slika figure. Desno: navidezna slika figure. Figura je bila ves čas na istem mestu.

Ali res lahko vidimo obe sliki? Kažeta ju fotografiji na sliki 13. Poskus smo naredili z zrcalom, ki leži na valju s polmerom $r \approx 20$ cm. Figuro smo postavili pred središče osnovne ploskve valja. Leva fotografija kaže realno sliko – prometnik na sliki drži znak v desni roki, desna fotografija pa kaže navidezno sliko figure – prometnik na sliki drži znak v levi roki. Ta slika ni ostra in je nekoliko »raztegnjena«. Da vidimo navidezno sliko, se moramo zelo približati zrcalu. Oči morajo biti na razdalji, ki je manjša $r/2$. Med poskusoma figure nismo premikali.

Naredimo še konstrukcijo te slike. Kaže jo slika 14. Štirikotnik leži v ravnini, ki je pravokotna na os x. Njegova oddaljenost od plašča valja je med r in $2r$. Premica p je presečišče ravnine, ki je pravokotna na os y in ravnino štirikotnika ter gre skozi točko O, s plaščem valja. Na premici izberemo dve točki, narišemo vpadna žarka, poiščemo vpadni pravokotnici in odbita

žarka. Presečišče podaljškov odbitih žarkov je točka O'. Ko točka O potuje po štirikotniku, točka O' riše navidezno sliko štirikotnika. Poudarimo še, da vpadni žarek, vpadna pravokotnica in odbiti žarek ležijo v isti ravnini, ki pa ni vzporedna s premico p in z osjo valja.

Pri velikem r bi lahko privzeli, da je del plašča valja raven. Tedaj bi vsi trije žarki ležali v ravnini, vzporedni z osjo valja.



Slika 14. Levo: Konstrukcija navidezne slike. Desno: Lega realne in navidezne slike štirikotnika. Navidezna slika leži za zrcalom, realna pa pred njim in za predmetom.

Poskus s konkavnim cilindričnim zrcalom, ko je slika obrnjena na glavo, kažejo predavatelji na začetku predavanj iz optike [7]. Primer narobe obrnjene glave s konkavnim cilindričnim zrcalom je opisan tudi v knjigi [4] angleškega pisatelja detektivskih zgodb R. Austina Freemana.

Take poskuse kažejo tudi v *hišah eksperimentov*, kjer obiskovalci, ki stojijo pred zrcalom, vidijo svojo obrnjeno glavo. Nismo pa našli zapisov, da bi zrcalo vrteli. Ker sta poskusa primerna za ustvarjanje optičnih iluzij, bo morda naš prispevek vzpodbudil koga, da ju bo postavil v katero od slovenskih hiš eksperimentov ali pa v hišo iluzij.

LITERATURA

[1] P. Chagnon, *Animated displays II: Multiple reflections*, *Phys. Teach.* **30** (1992), 488–492.

[2] S. Derman, *An optical puzzle that will make your head spin*, *Phys. Teach.* **19** (1981), str. 395.

[3] A. J. DeWeerd, S. E. Hill, *Reflections on Handedness*, *Phys. Teach.* **42** (2004), 275–279.

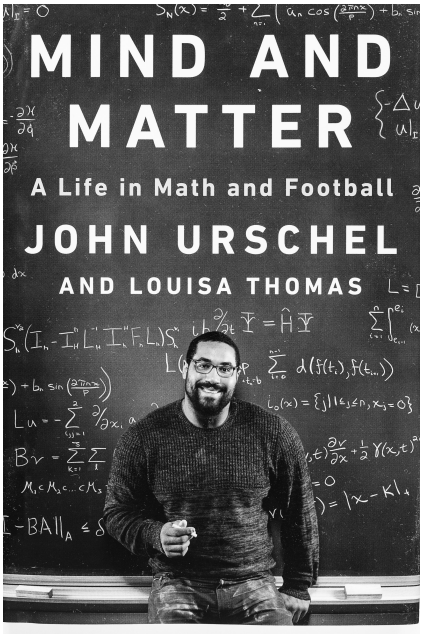
[4] R. A. Freeman, *The Apparition of Burling Court, in The Famous Cases of Dr. Thorndyke*, Hodder & Stoughton, London, 1929, 818–852.

[5] T. B. Greenslade Jr., *A Scientific Mystery*, *Phys. Teach.* **67** (2019), str. 221.

[6] T. M. Holzberlein, *How to become dizzy with Derman's optical puzzle*, *Phys. Teach.* **20** (1982), 401–402.

[7] *Real image from a concave mirror*, dostopno na `www.berkeleyphysicsdemos.net/node/723`, ogled 22. 9. 2020.

John Urschel in Louisa Thomas, Mind and Matter, A Life in Math and Football, Penguin Press, New York, 2019, 238 str.



Pred nami je nova, res zanimiva knjiga. John Urschel je več let presenetljivo združeval kariero igralca ameriškega nogometa in študenta matematike, tako na dodiplomski kot podiplomski ravni. Zelo kmalu je postal tudi soavtor in edini avtor znanstvenih člankov, ki sodijo na področja teorije grafov, linearne algebre in numerične analize. Trenutno je doktorski študent uporabne matematike na prestižni univerzi MIT v Bostonu. Soavtorica knjige je njegova žena Louisa Thomas, pisateljica in novinarka.

Urschelov oče je kanadski kirurg. Mati je sprva delala kot bolniška sestra, nato pa je končala pravo in postala odvetnica. Sina je stimulirala z matematičnimi ugankami, računanjem na pamet in poljudnoznanstvenimi knjigami. Urschel se v družbi sošolcev ni preveč znašel. Tudi šola se mu je zdela dolgočasna in ni sodeloval pri pouku, zato je bil razrednik mnenja, da je navadna šola zanj prezahtevna. Mati je posredovala s predlogom, da testirajo njegove sposobnosti, čemur je sledil nasprotni predlog, naj sin preskoči razred – a se mati s tem ni strinjala.

John Urschel je veselje do matematike začutil že v višjih razredih osnovne šole, vendar se je pri pouku dolgočasil. Poleti, v času počitnic pred osmim razredom ga je oče, ki se je po ločitvi v Johnovem zgodnjem otroštvu spet preselil bliže, poslal poslušat predavanja iz, kot bi temu rekli mi, Matematike 1 (z odvodom in integralom) za ekonomiste na Univerzi v Buffalu, kjer je oče takrat na tej univerzi vpisal magisterij iz ekonomije. Sinu, ki je že takrat imel 180 cm, je dal kar svojo študentsko izkaznico. Za mladega Johna so bila predavanja zahtevna, a je snov kmalu obvladal bolje od večine in celo pomagal drugim pri domačih nalogah.

Ameriški nogomet je za gledalce zelo privlačna športna panoga, ki ima bolj malo skupnega z našim nogometom. Ekipa ima na razpolago štiri poskuse, da prenese žogo vsaj deset jardov na nasprotno stran. Na igrišču

so zato črte v oddaljenosti deset jardov. Igralec teče z žogo, stisnjeno ob sebi, ali pa jo poda soigralcu. Nasprotniki mu poskušajo izbiti žogo ali prestreči podajo. Če ekipa ne napreduje deset jardov, dobi žogo druga ekipa. Če je videti, da ne bo šlo do naslednje črte, v četrtem poskusu streljajo z nogo skozi dvignjen okvir na nasprotni strani, kar prinese nekaj točk. Največ točk prinese prenos žoge do konca polja nasprotne ekipe (to imenujemo *touchdown*).

Občasno se kakšnemu izmed bolj atletskih igralcev posreči, da z žogo teče in se kot po čudežu izogiba nasprotnikom, dokler ne doseže konca igrišča. To seveda dvigne stadion na noge.

Šport igra pomembno vlogo na ameriških univerzah in moštvo ameriškega nogometa je običajno najpomembnejša ekipa. Diplomanti tudi desetletja kasneje obiskujejo tekme in navijajo za svojo univerzo. Šport je torej pomemben člen pri povezavi univerze z alumni, ki zbirajo denar za svojo univerzo in jo podpirajo tudi na druge načine. *Alma mater* (blagorodna mati) je izraz, ki ga diplomanti uporabljajo za univerzo, na kateri so študirali. (Morda bo čez nekaj desetletij kdo ta izraz uporabil tudi v Sloveniji.)

Univerze rekrutirajo igralce iz srednješolskih moštev, jim dajejo štipendije in nudijo pomoč pri študiju, denimo inštrukcije iz matematike. Odlični športniki obidejo običajno selekcijo glede na intelektualne sposobnosti, kar včasih povzroča slabo voljo pri drugih študentih. Pred desetletji je bil pisec teh vrstic na univerzi Tulane priča odmevni aferi. Na izpitu je nekaj igralcev ameriškega nogometa goljufalo, a asistent prekrška ni opazil. Dogodek so nekaj mesecev kasneje prijavili drugi študenti in kljub privilegijem je krivcem takrat grozil izpis z univerze.

Igralci ameriškega nogometa so skoraj brez izjeme veliki, močni, eksplozivni in, kot pravi sam Urschel, med igro praktično nimajo časa za razmišljanje: delujejo bolj ali manj instinktivno. Pogosto skušajo izvesti vnaprej natrenirane strategije podaj in premikov. Igra je že v osnovi groba in vzrok mnogih poškodb. V zadnjih letih pa je, podobno kot boks, prišla na slab glas zaradi številnih pretresov možganov in hudih dolgotrajnih posledic, kot je demenca. Več študij pravi, da so še posebej destruktivni udarci, pri katerih pride do naglega sukanja glave in posledičnega zvijanja možganov okrog dela, ki se nadaljuje v hrbtenjačo. Urschel ima verjetno srečo, da je čokat in ima izredno močan vrat, kar zmanjšuje možnost takega vrtenja. Tudi pri našem tipu nogometa so iz tega razloga fantje precej manj ogroženi kot dekleta.

Knjiga ameriški nogomet obravnava s stališča poznavalca igre in v določenih delih vsebuje precej tehničnega žargona, ki ga je pisec teh vrstic bolj

ali manj preskočil. (Kot pravi Urschel, je s temi pojmi imela težave tudi njegova mama.) Za Neameričane je bolje uživati v preostali pripovedi, ki je zelo lepo napisana, kar sam Urschel pripisuje soavtorici. (Dodaja pa, da je za morebitne napake v matematičnih delih odgovoren sam.)

John je začel ameriški nogomet igrati v gimnaziji. Kot izrazito tekmovalna oseba je zagrizeno treniral in uspelo mu je dobiti športno štipendijo na univerzi Penn State (Pennsylvania State University). Tu je njegovo nadarjenost za matematiko opazil profesor Vadim Kaloshin, ki mu je zastavil nalogo iz problema treh teles, torej nebesne mehanike. Tudi tu je Urschel zagrizel in skupaj s profesorjem sta napisala znanstveni članek.

Ob tem je tudi vneto treniral, se zelo dobro počutil v tesno povezanem nogometnem moštvu in užival v agresivni igri ter odzivu stotisočglave množice na stadionu (Penn State ima ogromen stadion). A kot trdi v knjigi, je bil pri 191 centimetrih in 135 kilogramih med manjšimi in je moral zato trenirati še toliko bolj kot ostali.

Za magisterij ga je pod svoje okrilje vzel profesor matematike Ludmil Zikatanov, po rodu iz Bolgarije. Spet je za magistrsko nalogo dobil originalen rezultat iz teorije grafov, a je kasneje v dokazu našel napako. Vendar je to po več mesecih dela odpravil in skupaj z mentorjem objavil članek.

Leta 2014 je začel igrati kot profesionalec v znanem moštvu Ravens (Krokarji) iz Baltimora. Mnogi, vključno z mamo, so ga opozarjali, naj raje izbere znanstveno kariero. Za podpis pogodbe je dobil 144 tisoč dolarjev. Glede na to, koliko bi igral, pa bi lahko v treh letih zaslužil še 2,3 milijona dolarjev. Dejansko je igral tri sezone in po [3] zaslužil 1,6 milijona dolarjev. Večino denarja je prihranil. A kot pravi, je bil v tem položaju bolj ali manj plačanec. Solidarnosti v moštvu je bilo bolj malo: če nisi bil izbran za igro, je bil zaslužek precej manjši. Kljub treningom je obdržal matematične stike in celo položaj mladega raziskovalca na Penn Statu.

Dejstvo, da nadarjen matematik igra v profesionalni ligi, je zbudilo veliko pozornosti v medijih. Opravil je veliko intervjujev, ki jih je izkoristil za reklamo za matematiko. Tudi Ameriško matematično društvo (American Mathematical Society) je izdalo plakat [4] z njegovo podobo in zgodbo, leta 2016 pa v reviji Notices objavilo intervju [2] z njim.

Leta 2015 se je potegoval za vpis v doktorski program na univerzi MIT – Massachusetts Institute of Technology. Pri tem sploh ni nameraval prenehati igrati, kar je spravilo v zadrego predstojnike oddelkov, ki so se prvič srečali s takim primerom. Vendar je imel za podiplomskega študenta zelo dobro bibliografijo in na koncu so ga vendarle sprejeli v program uporabne matematike, z začetkom študija spomladi 2016.

Med treningom v letu 2015 se je obrnil in nasprotni igralec ga je z glavo od strani zadel v sence. Izgubil je zavest in se zbudil z vsemi simptomi resnega pretresa možganov. Tri tedne ni mogel trenirati, še precej dlje pa se ni mogel ukvarjati z matematiko. Sposobnosti vizualizacije so ga zapustile, reševati ni mogel niti lažjih problemov. (Tudi naš boksar Dejan Zavec je po prejetem direktu v svojem zadnjem dvoboju izjavil, da ima težave z orientacijo in lahko do doma pride le s pomočjo navigacije.)

Urschel je eno leto nekako vzporedno vodil šport in študij, tako da je vpisal predmete, ki jih je že deloma obvladal in so imeli predpisan učbenik. Na predavanja ni hodil, domače naloge pa je pošiljal po elektronski pošti. V februarju 2017 je opravil zahteven doktorski izpit. Univerzitetna administracija mu je sporočila, da se bo jeseni moral posvetiti le študiju. Obenem je zaročenka pričakovala otroka. Opazil je, da so se mu začeli kriviti prsti, nabral pa si je tudi nekaj drugih poškodb.

Spomladi 2017 je izšla odmevna študija 111 možganov umrlih igralcev ameriškega nogometa, od katerih je 110 imelo nevrodegenerativne spremembe, značilne za ljudi, ki pogosto prejmejo udarce v glavo. (Kot pravi Urschel, so to bili skoraj zagotovo predvsem možgani ljudi, ki so tako in tako imeli težave.) Vse to je privedlo do nepričakovane odločitve maja 2017, da preneha igrati. Čeprav se je skušal izogniti publiciteti, je njegova poteza doživela velik odmev v medijih [3], ki so stvar takoj povezali z omenjeno zdravstveno študijo.

Zdaj Urschel dela na področju kombinatorične optimizacije. Njegov mentor je Michel Goemans. Očitno pa ima John preveč energije in se zdaj poskuša izkazati tudi v šahu. Svojo športno preteklost in impozantno postavo še naprej uporablja v prizadevanjih za popularizacijo matematike. V prostem času za matematiko in naravoslovne znanosti navdušuje otroke iz revnih okolij. V prispevku [5] za New York Times je izrazil mnenje, da bi učitelji matematike lahko bili bolj podobni trenerjem. Dijakom bi lahko razložili, da nadarjene matematike in druge znanstvenike čaka privlačna kariera, če so se seveda pripravljeni potruditi. Seznam njegovih objav in intervjujev v medijih je impresiven in si ga lahko ogledate na [4].

Knjiga vsebuje tudi precej matematične snovi, in sicer tako zgodovino matematike kot tudi opis nekaterih sodobnih študij ter celo raziskave. Ta del je zelo dobro in jasno napisan. Poskuša prikazati uporabo matematike, pa tudi njene omejitve. Nogometna moštva pri izbiranju igralcev uporabljajo statistiko. Ta mašinerija je odločala o njegovi usodi, a v njeno učinkovitost John Urschel ni bil preveč prepričan. O pasteh statistike piše na straneh 172–174:

Srečal sem slavno študijo [1], objavljeno leta 1975, o vpisu na podiplomski študij na kalifornijski univerzi (Berkeley). Avtorji študije so iskali dokaz o pristranskosti na podlagi spola prosilcev v postopku odobritve vpisa. Našli so ga – ali pa se je tako vsaj zdelo. Od 12.763 prijav za jesen 1973 je bilo sprejetih približno 44 odstotkov moških in le 35 odstotkov žensk. Tako je bilo sprejetih 277 žensk manj in 277 moških več, kot če bi bil vpisni postopek »spolno slep«, ob upoštevanju podobnih kvalifikacij za moške in ženske ... (Opomba prevajalca: skoraj vsi študenti so v tem času morali opraviti identični test: Graduate Record Examination.) Na tej univerzi o vpisu odloča profesorski zbor oddelka, na katerega se študent/študentka prijavi ... Avtorji so se odločili, da pogledajo, kateri oddelki so najbolj odgovorni za diskriminacijo, in potem individualno skušajo najti dokaze zanjo. Rezultat jih je šokiral. Univerza je imela 101 oddelek. Šestnajst oddelkov ni imelo prijav s strani žensk ali pa so sprejeli vse, ne glede na spol ... Med preostalimi 85 oddelki so našli štiri, pri katerih so bila vidna pomembna znamenja pristranskosti proti ženskam. Vsi ti oddelki so skupaj dali deficit 26 žensk. Našli pa so tudi šest oddelkov s pristranskostjo v *nasprotni* smeri, kar je dalo deficit 64 moških. Zmeda je bila zdaj popolna. Kaj se je zgodilo s pribitkom moških? In kje so bile manjkajoče ženske?

Avtorji so spoznali, da so zadeli ob nekaj, kar se v statistiki imenuje *Simpsonov paradoks* ali *zavajajoča korelacija* ... Izkazalo se je, da se je na nekatere oddelke prijavilo mnogo več ljudi kot na druge. Skoraj dve tretjini prijavljenih za anglistiko je bilo žensk, medtem ko je bilo med prijavljenimi za strojništvo le dva odstotka žensk. Več žensk se je prijavljalo na oddelke, kjer je bil naval prošenj velik, in manj na oddelke, ki so odobrili velik delež prošenj. Ko so avtorji to upoštevali, se je izkazalo, da je bila pristranskost proti ženskam zelo majhna.

Kako je v Sloveniji? Zahteven študij matematike (ali fizike) in naporni športni treningi ter potovanja na tekme niso ravno kompatibilni. Spomnim se kolega, ki je bil velik up v lahki atletiki. Po treningih pa je bil tako utrujen, da je lahko šel le spat, zato je športno kariero obesil na klin. Moj drugi kolega, fizik in odličen študent, je kot vrhunski plezalec dobil povabilo na himalajsko odpravo, a se mu je tveganje ozeblin in nesreč vseeno zdelo preveliko, zato se je raje posvetil zelo uspešni znanstveni in univerzitetni karieri.

Tudi pri nas pa najdemo izjeme. Prijetno sem bil presenečen nad vrhunskima športnico in športnikom, ki sta bila pri meni na obeh delih izpita med najboljšimi. **Maja Pohar** je imela množico naslovov državne prvakinje v badmintonu. Redno se je uvrščala med najboljših 25 na svetu, kar je ob silni priljubljenosti badmintona v Aziji velik dosežek. Tekmovala je tudi na olimpijskih igrah leta 2000. Nima vsak, tako kot ona, volje in sposobnosti za študiranje med vožnjami na tekme. (Vendarle se je tudi njej študij matematike zaradi športa nekoliko zavlekel.) Zdaj je profesorica statistike na Medicinski fakulteti.

Fizik **Aleš Česen** je vrhunski alpinist, ki je ob plezanju doktoriral na Fakulteti za gradbeništvo in geodezijo.

Med »našimi« mlajšimi športniki omenimo poklicno boksarko **Emo Kozin**, rojeno leta 1998 in trenutno študentko tretjega letnika finančne matematike. Je svetovna prvakinja kar v dveh kategorijah. V 21 dvobojih v poklicni karieri (od leta 2016) je bil izid enkrat neodločen (leta 2018), sicer pa je dvajsetkrat zmagala, dvakrat tudi v letu 2020.

Živa Dvoršak je diplomirala iz finančne matematike na Fakulteti za matematiko in fiziko. Na olimpijskih igrah 2012 je v streljanju z zračno puško na 10 metrov zasedla enajsto mesto. Naslednje leto je osvojila bronasto kolajno na evropskem prvenstvu. Na olimpijskih igrah leta 2016 je zasedla sedemnajsto mesto.

LITERATURA

[1] P. J. Bickel, E. A. Hammel in J. W. O'Connel, *Sex Bias in Graduate Admissions Data from Berkeley*, Science **187** (1975), 398–404.

[2] S. D. Miller, *»I plan to be a great mathematician«: An NFL Offensive Lineman Shows He's One of Us*, Notices AMS 63(2) 2016, 148–151, dostopno na `www.ams.org/publications/journals/notices/201602/rnoti-p148.pdf`, ogled 3. 11. 2020.

[3] T. Rohan, *A Calculated Decision: Why John Urschel Chose Math Over Football*, Sports Illustrated, dostopno na `www.si.com/nfl/2017/11/21/john-urschel-nfl-ravens-mit-mathematics`, ogled 3. 11. 2020.

[4] *John Urschel – Mathematician and Former Pro Football Player*, plakat, delo American Mathematical Society, 2017, dostopno na `www.ams.org/publicoutreach/posters/urschel`, ogled 3. 11. 2020.

[5] J. Urschel, *Math Teachers Should Be More Like Football Coaches*, podnaslov: *That style of motivation could help in the classroom, too*, The New York Times, 2019, dostopno na `www.nytimes.com/2019/05/11/opinion/sunday/math-teaching-football.html`, ogled 3. 11. 2020.

Peter Legiša

Aktualna vabila za mednarodne nominacije v matematiki

Odbor za matematiko pri DMFA Slovenije lahko v mednarodnih združenjih bodisi samostojno bodisi v sodelovanju z drugimi sorodnimi slovenskimi ali tujimi ustanovami sodeluje pri različnih nominacijah za nagrade ali predlogih za funkcije v mednarodnih telesih. V trenutnem obdobju so aktualni spodnji razpisi oziroma povabila k vložitvi nominacij. Člani DMFA Slovenije ali predstavniki slovenskih znanstvenih ustanov, ki bi želeli vložiti predlog nominacije preko DMFA Slovenije, lahko pošljejo ustrezno pobudo na naslov `tajnik@dmfa.si` in `mathematics@dmfa.si`.

Nagrade Mednarodne matematične unije (IMU prizes) se podelijo vsaka štiri leta na Mednarodnem matematičnem kongresu (ICM). Naslednji kongres bo predvidoma poleti 2022 v Sankt Petersburgu, rok za nominacije prejemnikov nagrad je 31. december 2020. Gre za naslednje nagrade:

- **Fieldsova medalja** se podeli 2 do 4 matematikom do 40. leta z namenom prepoznavanja izjemnih matematičnih dosežkov in podpore nadaljnjemu delu. Predsednik komisije je Carlos E. Kenig, predsednik IMU, več podrobnosti na `www.mathunion.org/imu-awards/fields-medal`.

- **Medalja IMU Abacus** se podeli za izjemne prispevke posameznika v matematičnih vidikih informacijskih znanosti. Predsednik komisije je James Demmel, več podrobnosti na `www.mathunion.org/imu-awards/imu-abacus-medal`.

- **Nagrada Carla Friedricha Gaussa** se podeli z namenom počastitve znanstvenika, katerega matematične raziskave so imele izjemen vpliv na drugih področjih, bodisi v tehnologiji, poslovnem svetu ali preprosto v vsakdanjem življenju. Predsednica komisije je Eva Tardos, več podrobnosti na `www.mathunion.org/imu-awards/carl-friedrich-gauss-prize`.

- **Chernova medalja** se podeli posamezniku za izjemne življenjske dosežke na področju matematike. Predsednik komisije je Yakov Eliashberg, več podrobnosti na `www.mathunion.org/imu-awards/chern-medal-award`.

- **Nagrada Leelavati** je nagrada za izjemne prispevke k povišanju družbenega zavedanja matematike kot intelektualne discipline in ključne vloge, ki jo igra v raznovrstnih človeških podvigih. Predsednik komisije je Pavel Etingof, več podrobnosti na `www.mathunion.org/imu-awards/leelavati-prize`.

- **ICM predavanje Emmy Noether** je posebno predavanje v okviru kongresa IMU, namenjeno počastitvi žensk, ki so ustvarile temeljne in trajne prispevke k matematičnim znanostim. Predsednica komisije je Sylvia Serfaty, več podrobnosti na `www.mathunion.org/imu-awards/icm-emmy-noether-lecture`.

Nominacije za člane Nominacijskega odbora IMU, rok za vložitev je **1. december 2020**. Nominacijski odbor je mednarodno telo, ki pripravi seznam nominacij in skrbi za izvedbo volitev Izvršnega odbora IMU na kongresu ICM 2022. Nominacijski odbor sestavljajo predsednik IMU, predsednik NO (ki ga izbere predsednik IMU), dve osebi s preteklimi izkušnjami pri IMU (ki ju izbereta predsednika IMU in NO) ter še tri naključno izbrane nominirane osebe po regionalnem ključu, več podrobnosti na `www.mathunion.org/fileadmin/IMU/EC/Procedures_for_Election_2020-08-19.pdf`.

Nagrada Shaw Prize 2021 za matematične znanosti, rok za nominacije 30. november 2020. Nagrade Shaw Prize za področja matematike, astronomije ter znanosti o življenju in medicini veljajo za ekvivalent Nobelove nagrade Daljnega vzhoda. Predsednik komisije za matematiko v letu 2021 je Sir Timothy Gowers. Več podrobnosti o nagradah na `www.shawprize.org`.

Boštjan Kuzman

Vabilo na 73. občni zbor DMFA Slovenije

Vse člane DMFA Slovenije vabim k udeležbi na rednem letnem občnem zboru Društva matematikov, fizikov in astronomov Slovenije. Občni zbor bo organiziran na daljavo prek spletne aplikacije ZOOM dne 3. decembra 2020 z začetkom ob 17. uri.

Povezava za udeležbo na občnem zboru bo tri dni pred sestankom poslana po elektronski pošti vsem članom društva. Hkrati pozivam vse člane,

ki smo jih zaprosili za dopolnitev osebnih podatkov, pa tega še niste storili, da na naslov `tajnik@dmfa.si` čimprej posredujete svoj elektronski naslov.

Dnevni red občnega zbora

1. Otvoritev
2. Izvolitev delovnega predsedstva
3. Društvena priznanja
4. Poročila o delu društva
5. Razprava o poročilih
6. Vprašanja in pobude
7. Računovodsko in poslovno poročilo DMFA
8. Razrešitve in volitve
9. Razno

V okviru občnega zbora nam bosta dva prejemnika Zoisove nagrade 2019 v kratkem 20-minutnem predavanju predstavila svoje delo: prof. dr. Denis Arčon o raziskavah kvantnega magnetizma in prof. dr. Enes Pasalic o kriptografiji in informacijski varnosti.

Letošnji Občni zbor je tudi volilni. Predlagana kandidatna lista za voljene organe DMFA Slovenije za obdobje 2020–2022 je naslednja.

UPRAVNI ODBOR

Predsednica DMFA Slovenije: **Nežka Mramor Kosta**
Podpredsednica DMFA Slovenije: **Marjeta Kramar Fijavž**
Tajnik DMFA Slovenije: **Janez Krušič**
Tajniki oz. tajnici stalnih komisij DMFA Slovenije za:

- popularizacijo matematike v osnovni šoli: **Aljoša Brlogar**
- popularizacijo matematike v srednji šoli: **Sandra Cigula**

- popularizacijo fizike v osnovni šoli: **Barbara Rovšek**
- popularizacijo fizike v srednji šoli: **Jurij Bajc**
- popularizacijo astronomije: **Andrej Guštin**
- »Mednarodni matematični kenguru«: **Gregor Dolinar**
- pedagoško dejavnost: **Aleš Mohorič**
- informacijsko tehnologijo: **Matjaž Željko**
- upravne in administrativne zadeve: **Ciril Dominko**

Predsedniki stalnih strokovnih odborov

- Slovenskega odbora za matematiko: **Boštjan Kuzman**
- Slovenskega odbora za fiziko: **Martin Klanjšek**
- Slovenskega odbora za astronomijo: **Andreja Gomboc**

Predstavnik Študentske sekcije DMFA Slovenije: **Nejc Zajc**
Predstavnica Odbora za ženske: **Marjetka Conradi**

NADZORNI ODBOR
Andrej Likar
Matej Brešar
Dragan Mihailović

ČASTNO RAZSODIŠČE
Maja Klavžar
Anton Suhadolc
Zvonko Trontelj

Člani DMFA Slovenije lahko predlagate dodatne kandidate. Predloge hkrati s pisno privolitvijo predlaganega kandidata pošljite na društveni naslov najkasneje do 26. novembra 2020.

Dragan Mihailović
predsednik DMFA Slovenije

OBZORNIK ZA MATEMATIKO IN FIZIKO
LJUBLJANA, MAJ 2020
Letnik 67, številka 3
ISSN 0473-7466, UDK 51 + 52 + 53

VSEBINA

CONTENTS

Na naslovnici: Zrcala odpirajo pogled v nov, navidezni svet. Foto: Aleš Mohorič