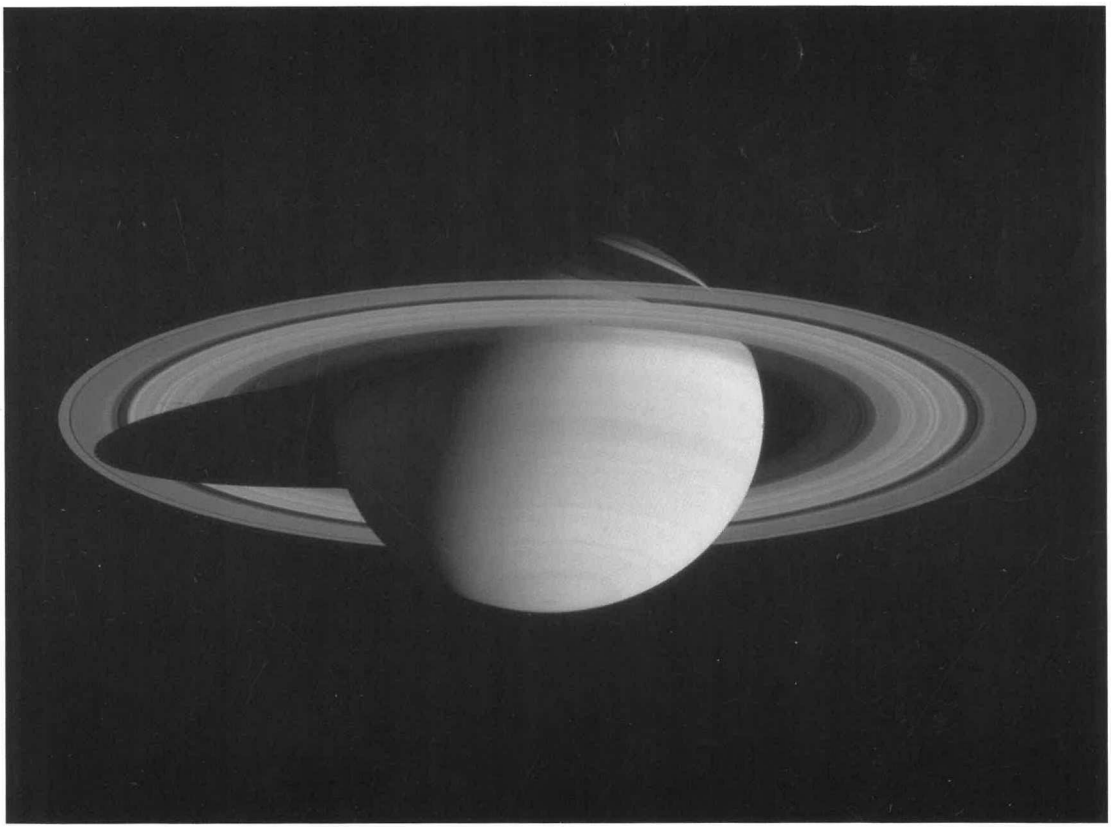
IZDAJA DRUŠTVO MATEMATIKOV, FIZIKOV IN ASTRONOMOV SLOVENIJE

ISSN 0473–7466

2004
Letnik 51
5

OBZORNIK ZA MATEMATIKO IN FIZIKO



OBZORNIK MAT. FIZ. • LJUBLJANA • LETNIK 51 • ŠT. 5 • STR. 129–160 • SEPTEMBER 2004

OBZORNIK ZA MATEMATIKO IN FIZIKO

Glasilo Društva matematikov, fizikov in astronomov Slovenije
Ljubljana, SEPTEMBER 2004, letnik 51, številka 5, strani 129–160

Naslov uredništva: DMFA–založništvo, Jadranska ulica 19, p. p. 2964, 1001 Ljubljana. **Telefon:** (01) 4766 553, 4232 460, 2512 005. **Telefaks:** (01) 2517 281. **Elektronska pošta:** Zaloznistvo@dmfa.si **Internet:** http://zaloznistvo.dmfa.si/omf/ **Transakcijski račun:** 03100–1000018787. **Devizna nakazila:** SKB banka d.d., Ajdovščina 4, 1513 Ljubljana. **SWIFT:** SKBASI2X. **IBAN:** SI56 0310 0100 0018 787.

Uredniški odbor: Mirko Dobovišek (glavni urednik), Roman Drnovšek (urednik za matematiko in odgovorni urednik), Irena Drevenšek Olenik (urednica za fiziko), Marko Zgonik, Nada Razpet (vesti), Pavle Saksida (nove knjige), Vladimir Bensa (tehnični urednik).

Jezikovno pregledal Janez Juvan, računalniško stavila Monika Testen.
Natisnila Tiskarna RAZVEDRILO v nakladi 1450 izvodov.

Člani društva prejemajo Obzornik brezplačno. Celoletna članarina znaša 5.000 SIT, za študente 2.500 SIT. Naročnina za ustanove je 8.000 SIT, za tujino 30 EUR. Posamezna številka za člane stane 1.000 SIT, stare številke 520 SIT.

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 Ministrstvo za šolstvo, znanost in šport.

© 2004 DMFA Slovenije – 1583

Poštnina plačana pri pošti 1102 Ljubljana

NAVODILA SODELAVCEM OBZORNIKA ZA ODDAJO PRISPEVKOV

Obzornik za matematiko in fiziko objavlja 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 ločeno od besedila. Avtorji člankov, ki želijo objaviti slike iz drugih virov, si morajo za to sami priskrbeti dovoljenje (copyright). Prispevki morajo biti poslani v dvojniku, 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 vsaj enemu anonimnemu recenzentu, ki mora 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 in če je besedilo napisano z računalnikom, potem urednik prosi avtorja za izvorno datoteko. Le-te naj bodo praviloma napisane v eni od standardnih različic urejevalnikov TEX oziroma LATEX, kar bo olajšalo uredniški postopek.

REED-SOLOMONOVE KODE

ALEKSANDAR JURIŠIĆ

Politehnika Nova Gorica

in

ARJANA ŽITNIK

Fakulteta za matematiko in fiziko
Univerza v Ljubljani

Math. Subj. Class. (2000): 94B{05,15,20}, 11T71, 51E22

Reed-Solomonove kode so izjemno uspešne na področju hranjenja podatkov (CD, DVD) ter prenašanja podatkov v našem osončju (sonda Cassini je po sedmih letih vstopila v Saturnovo orbito in bo naslednja štiri leta od tam pošiljala slike na Zemljo). V sestavku obravnavamo Reed-Solomonove kode. Opišemo originalen pristop Reeda in Solomona ter pristop z linearnimi cikličnimi kodami. Povezava med njima je izpeljana s končno Fourierovo transformacijo. Predstavimo tudi polinomski algoritem za njihovo odkodiranje.

REED-SOLOMON CODES

Reed-Solomon codes are thriving with its applications in the field of data storage (CD, DVD) and data transmition in our solar system (after seven years Cassini space probe has reached Saturn's orbit and will be sending images back to Earth for the next four years). Reed-Solomon codes are described via two different approaches: the original approach of Reed and Solomon using interpolation polynomials and the classical approach with linear cyclic codes. The connection between these two approaches is established through the finite Fourier transform. We also present a polynomial decoding algorithm.

1. Uvod

Namen transformiranja sporočila pred pošiljanjem (ali hranjenjem) informacije je lahko različen:

- dodajanje kontrolnih bitov, ki nam omogočajo odkrivanje in odpravljanje morebitnih napak po prejetju ali ponovnem branju;
- zakritje teksta pred nepooblaščeno osebo;
- kompresija teksta, da se izognemo nepotrebni informaciji.

Teorija kodiranja se ukvarja s prvo možnostjo, z drugo **kriptografija**, medtem ko ostaja zadnja običajno v domeni inženirjev. Prenosni mediji, na primer telefonske linije, omrežja in satelitske povezave, ter mediji za

shranjevanje, na primer optični in magnetni diski, trakovi, običajno še zdaleč niso popolni. Če želimo zanesljive prenose in hranjenje v podatkovnih bazah, potem so kode za odpravljanje napak nepogrešljive. Eden izmed zgodnjih uspehov teorije kodiranja je kvaliteta slik, ki jih pošiljajo sateliti. Če ne bi uporabljali kod za odpravljanje napak, pošiljke ne bi vsebovale slik, na Zemljo bi prišel le naključen šum!

Vesoljska sonda Cassini je na svoji poti k Saturnu posnela Jupiter. Saturn je dosegla julija 2004 (glej `http://www.ssd.rl.ac.uk/news/cassini/mission/cas.html`) in od tam pošilja slike na Zemljo. Sonda je prepotovala že milijardo kilometrov, v prihodnjih štirih letih pa bo 76-krat obkrožila Saturn in izvedla 52 preletov v bližino sedmih izmed 31 znanih Saturnovih lun. Je največja medplanetarna sonda doslej, uporablja pa tudi Reed-Solomonove kode (na kratko RS-kode) za prenos podatkov na Zemljo. Cassini je skupen projekt NASA ter evropske in italijanske vesoljske agencije, ki vključuje 4 300 ljudi in je vreden 3.3 milijarde dolarjev. Na dan lahko pošlje na Zemljo do 4 GB podatkov.

Drugi zelo pomemben uspeh RS-kod pa so zgoščenke (CD in DVD). Njihovo matematično plat smo opisali že v Preseku [7].

V tem sestavku bomo torej spoznali kode, ki sta jih v 60. letih prejšnjega stoletja vpeljala Irving Reed in Gustave Solomon [9]. Takrat sta bila zaposlena v enem izmed Lincolnovih laboratorijev na slovitem MIT. Za svoje kode sta uporabila več kot 100 let staro teorijo končnih obsegov francoskega matematika Evarista Galoisa. Reed-Solomonov članek je predlagal zelo eleganten način procesiranja podatkov, vendar pa se nihče ni zavedal pravega pomena, npr. ali je tak način res praktičen (in tedaj verjetno sploh ni bil). Kar nekaj časa je bilo treba, da je tehnologija ujela korak s teorijo in omogočila učinkovite implementacije teh kod (v 60. letih prejšnjega stoletja ni bilo hitre digitalne elektronike, vsaj glede na današnje standarde). Prvi korak v to smer pa je bila ugotovitev, da so Reed-Solomonove kode samo poseben primer širšega razreda cikličnih BCH-kod. Danes so RS-kode primer učinkovitih in popularnih kod na številnih področjih, kot so:

- naprave za skladiščenje/hranjenje podatkov (trdi diski, CD, DVD ...) in njihovo branje (predvajalniki, digitalna televizija ...);
- brezžične komunikacije (mobilni telefoni, mikrovalovne povezave ...);
- satelitske komunikacije (Voyager, Mariner, Mars Lander, Cassini ...);
- modemi za širokopasovne povezave (ADSL, xDSL ...).

Prednost RS-kod je v tem, da znajo z enako lahkoto popraviti simbol z eno samo bitno napako kakor tudi simbol, pri katerem so napačni vsi biti. Zato so RS-kode posebej primerne za odpravljanje *grozdnih napak* (tj. napak, kjer

se napačni biti držijo skupaj). To pa pomeni, da so RS-kode občutljive za enakomerno porazdeljene napake. Druge kode, kot npr. konvolucijske kode, so boljše za odpravljanje naključnih napak, zato pogosto bloke RS-kod še prej zakodiramo s konvolucijskimi kodami in tako omogočimo odpornost tako na grozdne kakor tudi na naključne napake.

Ta članek je kratek uvod v Reed-Solomonove kode, ki dosežejo Singletonovo mejo (glej naslednji razdelek). Po razdelku, v katerem na kratko opišemo najosnovnejše o kodah, je v tretjem razdelku opisan originalen pristop Reeda in Solomona. Prepričamo se, da gre za linearne kode. Po krajšem razdelku o končnih obsegih pokažemo v naslednjem razdelku s končno Fourierovo transformacijo, da so RS-kode ekvivalentne posebnemu razredu linearnih cikličnih kod. V 5. razdelku predstavimo še polinomski algoritem za odkodiranje RS-kod.

2. Osnove kodiranja

Koda je podmnožica nekega prostora, v katerem je definirana razdalja. Elementom kode bomo rekli tudi **kodne besede**. **Kodiranje** je prirejanje kodnih besed posameznim informacijam. Če pri prenosu/hranjenju kodne besede ni prišlo do napak, je **odkodiranje** obratno prirejanju. V nasprotnem primeru pa pri odkodiranju običajno prejeto besedo „popravimo“ tako, da izberemo kodno besedo, ki je prejeti besedi najbližja. Temu rečemo princip **najbližjega soseda**. Precej raziskav na področju teorije kodiranja je usmerjeno v izboljšavo razmerja med verjetnostjo, da je ugibanje odkodirnega postopka pravilno, in kompleksnostjo kodiranja in odkodiranja.

Intuitivno si lahko predstavljamo prostor kot večnadstropno stanovanjsko hišo (blok), kodne besede pa so središča izbranih sob. Informacijo predstavimo (zakodiramo) tako, da v središča nekaterih izbranih sob postavimo žoge. Prenos informacij je potem podoben potresu, ki žoge prestavlja. Odkodirni proces pa poskuša žoge vrniti nazaj v središča. Če je potres zelo močan in žoga konča v drugi sobi, potem pride do napačnega popravka, kadar pa žoga ne zapusti sobe, vsaj na prvi pogled ni problema.

Najpogosteje si za prostor izberemo množico vseh n-teric s simboli iz neke končne množice F, imenovane tudi **abeceda**:

$$F^n = \{(a_0, a_1, \ldots, a_{n-1}) \mid a_i \in F,\ i = 0, 1, \ldots, n-1\}.$$

Razdalja kode je najmanjša razdalja med različnimi kodnimi besedami. V tem primeru je razdalja med dvema n-tericama število mest, na katerih se razlikujeta. Pravimo ji tudi **Hammingova razdalja**, po enem izmed pionirjev teorije kodiranja. Kadar je koda podmnožica takega prostora, rečemo,

da gre za **bločne kode dolžine n**. Običajno razbijemo dano sporočilo na bloke fiksne dolžine (oznaka k, kjer je $0 < k \leq n$), ki jih nato povežemo s kodnimi besedami z neko bijektivno korespondenco. Taka korespondenca je posebno naravna, kadar kodo predstavlja k-razsežen linearen podprostor n-razsežnega vektorskega prostora. Tedaj rečemo, da gre za **linearno (n, k)-kodo**.

Lahko pa bi si za prostor izbrali tudi kaj drugega, na primer graf, kjer je razdalja med dvema vozliščema dolžina najkrajše poti med njima. Za uvod v teorijo kodiranja glej Jurišić [7], Klavžar [8] ter Vanstone in Van Oorschot [11], za referenčno knjigo pa Pless idr. [5].

Če privzamemo odkodirni princip najbližjega soseda, ima koda, ki odpravi (do) t napak, razdaljo $d \geq 2t + 1$, saj morajo biti krogle s središčem v kodnih besedah in radijem t disjunktne. Pri kodi nas najbolj zanima, koliko napak lahko odpravimo glede na to, koliko kontrolnih bitov smo dodali osnovni informaciji. V tej smeri nam pomaga naslednji rezultat:

Lema 1 (Singletonova meja [10]). *Naj bo C bločna koda dolžine n nad abecedo s q elementi in d njena razdalja. Potem je število elementov kode C kvečjemu q^{n-d+1}.*

Dokaz. Naj bo C' koda, ki jo konstruiramo iz kode C tako, da izberemo $d-1$ koordinat in jih zbrišemo v vseh kodnih besedah. Ker je razdalja kode C enaka d, imata obe kodi enako število elementov (iz različnih elementov kode C nismo mogli dobiti istega elementa kode C'). Koda C' ima dolžino $n - d + 1$, zato ima (in s tem tudi koda C) največ q^{n-d+1} elementov. ∎

Če izberemo za sporočila vse možne k-terice nad abecedo s q elementi ter obstaja bijekcija med sporočili in kodnimi besedami iz $C \subseteq F^n$, ima koda C q^k elementov in pravimo, da gre za **(n, k)-kodo**. V tem primeru se Singletonova meja prevede v zgornjo mejo za razdaljo kode:

$$d \leq n - k + 1\,. \tag{1}$$

Od tod in iz neenakosti $2t + 1 \leq d$ sledi, da ima koda vsaj $2t$ kontrolnih bitov, tj.

$$t \leq \left\lfloor \frac{n-k}{2} \right\rfloor. \tag{2}$$

Torej lahko (n, k)-koda odpravi kvečjemu $\lfloor (n-k)/2 \rfloor$ napak.

Vpeljimo še nekaj oznak, ki jih bomo uporabljali skozi celoten članek. Za abecedo si izberimo elemente končnega obsega s q elementi, kjer je q potenca nekega praštevila, oznaka $\mathbb{F} = \mathrm{GF}(q)$ (angl. Galois Field). Če je q praštevilo,

je GF(q) kar obseg $\mathbb{Z}_q$, v katerem računamo z ostanki po modulu q. Za razumevanje članka si lahko bralec, ki mu pojem končnega obsega ni domač, pod končnim obsegom predstavlja kar le-tega. Množica $\mathbb{F}^n$ z običajnim seštevanjem in množenjem po komponentah je vektorski prostor nad $\mathbb{F}$. Čeprav ne bi bilo nujno, bomo obravnavo poenostavili in v nadaljevanju privzeli, da je dolžina kodnih besed enaka kar $n = q - 1$. Dobro je znano, da je multiplikativna grupa končnega obsega $\mathbb{F}$ ciklična. To pomeni, da obstaja v $\mathbb{F}$ **primitiven** element α, tj. tak element $\alpha \in \mathbb{F}$, da je $\alpha^n = 1$ in $\alpha^i \neq 1$ za vsak $i \in \{1, \ldots, n-1\}$.

3. Polinomi

Reed in Solomon sta vpeljala RS(n, k)-kode s pomočjo polinomov. Za **sporočilo**

$$m = (m_0, m_1, \ldots, m_{k-1}) \in \mathbb{F}^k$$

s prirejenim polinomom $m(x) = m_0 + m_1 x + \cdots + m_{k-1}x^{k-1}$ izračunamo vrednosti $c_i = m(\alpha^i)$, $i \in \{0, \ldots, n-1\}$ in iz njih sestavimo **kodno besedo**

$$c = (c_0, c_1, \ldots, c_{n-1}).$$

Da bo odkodiranje možno, mora seveda veljati $k < n$. V tem primeru nas Lagrangeeva formula za polinomsko interpolacijo prepriča, da ni preveč pričakovati obstoj odkodirnega algoritema za RS-kode, ki bi opazil morebitne nepravilnosti in jih odpravil. Bistveno vprašanje pa je, ali je tak algoritem učinkovit. Prvi postopek za odkodiranje sta predlagala Reed in Solomon. Le-ta temelji na reševanju velikega števila sistemov enačb. Ko sprejmemo kodno besedo $c = (c_0, c_1, \ldots, c_{n-1})$, lahko sporočilo $m = (m_0, m_1, \ldots, m_{k-1})$ izračunamo iz naslednjega (predoločenega) sistema enačb:

$$\begin{array}{rcllllll}
c_0 & = & m_0 & + & m_1 & + & m_2 & + \cdots + \; m_{k-1}\,, \\
c_1 & = & m_0 & + & m_1\alpha & + & m_2\alpha^2 & + \cdots + \; m_{k-1}\alpha^{k-1}\,, \\
c_2 & = & m_0 & + & m_1\alpha^2 & + & m_2\alpha^4 & + \cdots + \; m_{k-1}\alpha^{2(k-1)}\,, \\
 & \vdots & & & & & & \vdots \\
c_{n-1} & = & m_0 & + & m_1\alpha^{n-1} & + & m_2\alpha^{(n-1)\cdot 2} & + \cdots + \; m_{k-1}\alpha^{(n-1)(k-1)}\,.
\end{array} \tag{3}$$

Poglejmo množico poljubnih k enačb, ki ustrezajo k-elementni podmnožici

$$\{a_1, a_2, \ldots, a_k\} \subseteq \{1, \alpha, \ldots, \alpha^{n-1}\}.$$

Njihovi koeficienti tvorijo Vandermondovo matriko z determinanto

$$\begin{vmatrix} 1 & a_1 & a_1^2 & \dots & a_1^{k-1} \\ 1 & a_2 & a_2^2 & \dots & a_2^{k-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & a_k & a_k^2 & \dots & a_k^{k-1} \end{vmatrix} = \prod_{1 \le i < j \le k} (a_j - a_i) . \tag{4}$$

Le-ta je v obsegu $\mathbb{F}$ različna od 0, saj je $a_i \neq a_j$ za vse $i, j \in \{1, \dots, k\}$, za katere velja $i \neq j$. Zato ima sistem enolično rešitev v $\mathbb{F}$.

Če se pri prenosu ne bi pojavila napaka, bi lahko z izbiro poljubne k-elementne podmnožice obrnljivih elementov v $\mathbb{F}$ dobili sistem enačb, iz katerega bi lahko določili celotno sporočilo $(m_0, \dots, m_{k-1})$. Tako k-elementno podmnožico lahko izberemo na $\binom{n}{k}$ načinov. Če pa pri prenosu nastanejo napake, nam lahko različni sistemi enačb dajo različne rešitve. Naslednja lema nam zagotovlja, da se prava rešitev pojavi največkrat, če le število napak ni preveliko.

Lema 2. *Če pride pri prenosu ali pri branju kodne besede $(c_0, \dots, c_{n-1})$ RS(n, k)-kode do s napak, se pri reševanju podsistema k-tih enačb iz* (3) *pojavi napačna rešitev (k-terica) največ*

$$\binom{s+k-1}{k} \text{-krat.}$$

Dokaz. Enačbe sistema (3) ustrezajo hiperravninam v k-razsežnem prostoru. Zaradi linearne neodvisnosti poljubnih k vektorjev, ki določajo te hiperravnine, se poljubnih k hiperravnin seka v eni točki (4). V napačni točki pa se lahko seka največ $s + k - 1$ hiperravnin, saj je med njimi lahko največ $k - 1$ takih, ki se pri prenosu niso spremenile (k nespremenjenih enačb nam namreč že da pravo rešitev) in največ s takih, ki so se spremenile. Napačno točko (tj. k-terico) lahko dobimo torej na največ toliko načinov, kot smo želeli dokazati. ∎

Izrek 3. *RS(n, k)-koda je linearna (n, k)-koda.*

Dokaz. Naj bosta c in c' poljubni kodni besedi RS-kode ter $m(x)$ in $m'(x)$ polinoma sporočila, katerima ustrezata ti dve kodni besedi. Potem za λ, $\lambda' \in \mathbb{F}$ in $i \in \{0, 1, \dots, n-1\}$ velja

$$\left(\lambda c + \lambda' c'\right)_i = \lambda m\left(\alpha^i\right) + \lambda' m'\left(\alpha^i\right) = p\left(\alpha^i\right),$$

kjer je $p(x) = \lambda m(x) + \lambda' m'(x)$. Od tod sledi, da je $\lambda c + \lambda' c'$ kodna beseda, ki ustreza sporočilu $\lambda m + \lambda' m'$ in je RS-koda linearna. Kodne besede $a_i := (1, \alpha^i, \alpha^{2i}, \ldots, \alpha^{(n-1)i})$ s prirejenimi polinomi x^i, $i \in \{0, 1, \ldots, k-1\}$ so linearno neodvisne, saj jih lahko zložimo v Vandermondovo matriko, katere determinanta je različna od nič, ker so števila $1, \alpha, \alpha^2, \ldots, \alpha^{k-1}$ paroma različna.

Potrebno je le še preveriti, da je poljubna kodna beseda c, ki ustreza nekemu polinomu sporočila $m(x) = \sum_{i=0}^{k-1} m_i x^i$, linearna kombinacija leteh:

$$c = \left(\sum_{i=0}^{k-1} m_i \left(\alpha^0\right)^i, \sum_{i=0}^{k-1} m_i \left(\alpha^1\right)^i, \ldots, \sum_{i=0}^{k-1} m_i \left(\alpha^{n-1}\right)^i \right) =$$
$$= \sum_{i=0}^{k-1} m_i \left(\left(\alpha^0\right)^i, \left(\alpha^1\right)^i, \ldots, \left(\alpha^{n-1}\right)^i \right) = \sum_{i=0}^{k-1} m_i a_i \,.$$

Torej je RS-koda res k-razsežna. ■

Sedaj pa se prepričajmo, da za RS(n, k)-kode v Singletonovi oceni velja enakost, tj. za dani naravni števili n in k odpravijo RS(n, k)-kode največje možno število napak.

Izrek 4. *RS(n, k)-koda odpravi $\lfloor (n-k)/2q \rfloor$ napak, njena razdalja pa je $n-k+1$.*

Dokaz. Privzemimo, da je pri prenosu RS-kodne besede prišlo do s napak. Potem dobimo po lemi 2 pri reševanju vseh možnih podsistemov k-tih enačb vsako napačno rešitev največ $\binom{s+k-1}{k}$-krat, pravo pa $\binom{n-s}{k}$-krat. Slednje število je večje natanko tedaj, ko je $n-s > s+k-1$ oziroma $s < (n-k+1)/2$. Ker je s celo število, lahko RS-koda na ta način odpravi poljubnih $\lfloor (n-k)/2 \rfloor$ napak. Torej je njena razdalja vsaj $n-k+1$. Iz izreka 3 sledi, da ima RS-koda q^k elementov. Zaradi Singletonove meje (1) pa je razdalja enaka $n-k+1$. ■

Seveda je ta način za odkodiranje prepočasen, saj zahteva reševanje $\binom{n}{k}$ sistemov enačb velikosti $k \times k$, kar je eksponentna časovna zahtevnost glede na k. V nadaljevanju bomo spoznali tudi polinomske algoritme.

4. Računanje v končnih obsegih

Končne obsege je vpeljal Galois v tridesetih letih 19. stoletja. V slovenski literaturi so predstavljeni že v učbeniku *Algebra* Ivana Vidava [12], pred

kratkim pa smo v *Preseku* [7] lahko brali tudi o računanju v (manjših) končnih obsegih. Zato si le na konkretnem primeru, ki ga bomo uporabljali v naslednjih razdelkih, oglejmo, kako v praksi seštevamo in množimo.

Obseg $\mathrm{GF}(2^4)$ lahko skonstruiramo z razširitvijo obsega $\mathbb{Z}_2$ z ničlo α nerazcepnega polinoma $p(x) = x^4 + x + 1$, glej npr. Vidav [12, VII.5]. Obseg $\mathrm{GF}(2^4)$ je vektorski prostor nad $\mathbb{Z}_2$ z bazo $\{1, \alpha, \alpha^2, \alpha^3\}$. Seštevanje v tem obsegu je čisto običajno seštevanje vektorjev (aritmetika koeficientov se izvaja v $\mathbb{Z}_2$). Za množenje je množica neničelnih elementov $\mathrm{GF}(2^4)$ ciklična grupa. Neničelne elemente tega obsega predstavimo kar kot potence elementa α. Ker je α ničla polinoma $p(x)$ in je karakteristika obsega enaka 2, velja $\alpha^4 = \alpha + 1$ in lahko potenco α^4 predstavimo s četverico (1100). Podobno iz $\alpha^5 = \alpha^2 + \alpha$ sledi, da lahko α^5 predstavimo z (0110), α^6 z (0011) in iz $\alpha^7 = \alpha^4 + \alpha^3 = \alpha^3 + \alpha + 1$ še α^7 z (1101). Če ta postopek nadaljujemo ter dodamo še element 0, ki ga predstavimo z α^∞, dobimo zvezo med eksponentno in vektorsko predstavitvijo elementov obsega $\mathrm{GF}(2^4)$, glej tabelo 1. Množenje je pri t. i. eksponentni predstavitvi obsega seveda enostavnejše, npr.

$$\alpha^8 \cdot \alpha^{10} = \alpha^{18} = \alpha^3\,,$$

(pri zadnjem enačaju smo upoštevali $\alpha^{15} = 1$, saj je α generator multiplikativne grupe $\mathrm{GF}(2^4)$ in ima zato red 15), pri seštevanju v eksponentni predstavitvi pa uporabimo ZechLog tabelo (tabela 1), s katero prevedemo seštevanje na množenje, npr. elementa α^3 in α^5 seštejemo na naslednji način:

$$\alpha^3 + \alpha^5 = \alpha^3(1 + \alpha^2) = \alpha^3\alpha^{z(2)} = \alpha^3\alpha^8 = \alpha^{11}\,.$$

Naj opomnimo, da je pri zelo velikih končnih obsegih (ki jih uporabljamo npr. v kriptografiji) sestavljanje ZechLog tabele, pa tudi njeno hranjenje, absolutno prezahtevna naloga.

5. Reed-Solomonove kode kot linearne ciklične kode

Linearna koda $C \subseteq \mathbb{F}^n$ je **ciklična**, če je za vsako kodno besedo $c = (c_0, c_1, \ldots, c_{n-1})$ tudi njen ciklični pomik, tj. beseda $c' = (c_{n-1}, c_0, c_1, \ldots, c_{n-2})$, kodna beseda. Zelo uporabno reprezentacijo ciklične kode dobimo, če kodne besede predstavimo s polinomi. Kodni besedi c podobno kot pri sporočilu priredimo polinom $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$. Cikličnemu pomiku potem ustreza polinom

$$c'(x) = c_{n-1} + c_0x + c_1x^2 + \cdots + c_{n-2}x^{n-1} = x \cdot c(x) - c_{n-1}(x^n - 1)\,.$$

α^i	0000	1000	0100	0010	0001	1100	0110	0011
i	∞	0	1	2	3	4	5	6
$z(i)$	0	∞	4	8	14	1	10	13
α^i	1101	1010	0101	1110	0111	1111	1011	1001
i	7	8	9	10	11	12	13	14
$z(i)$	9	2	7	5	12	11	6	3

Tabela 1. ZechLog tabela vektorske in eksponentne predstavitve obsega $\mathrm{GF}(2^4)$, ki je generiran z ničlo α nerazcepnega polinoma $p(x) = 1 + x + x^4$. Z njo lahko prevedemo seštevanje na množenje, saj iz enakosti $\alpha^k + \alpha^h = \alpha^{\min(k,h)}\left(1 + \alpha^{\max(k,h)-\min(k,h)}\right)$ sledi, da je dovolj za vsak i najti tako število $z(i)$, da bo veljalo $1 + \alpha^i = \alpha^{z(i)}$.

V kolobarju polinomov $R_n = \mathbb{F}[x]/(x^n - 1)$, kjer gledamo polinome po modulu polinoma $x^n - 1$, dobimo ciklični pomik kar z množenjem s polinomom x. Zato bomo pogosto enačili kodne besede s polinomi po modulu polinoma $x^n - 1$, tj. delali v kolobarju R_n.

Za obravnavo cikličnih kod je izdelana lepa in zanimiva teorija, katere osnove lahko najdemo v večini učbenikov iz teorije kodiranja, glej npr. Vanstone idr. [11], mi pa se omejimo le na najnujnejše.

Izrek 5. *Naj bosta n in k naravni števili, $n > k$, $g(x)$ moničen polinom (tj. polinom z vodilnim koeficientom 1) stopnje $n - k$, ki deli polinom $x^n - 1$. Potem je $S = \{a(x)g(x); \deg(a) < k\}$ cikličen podprostor vektorskega prostora R_n in $B = \{g(x), x\,g(x), \ldots, x^{k-1}g(x)\}$ baza podprostora S.*

Dokaz. Očitno je S podprostor v R_n. Pokažimo, da je S cikličen, tj. za polinom $p(x) := a(x)g(x) \in S$ moramo pokazati, da je tudi polinom $p_1(x) := x\,p(x) \mod (x^n - 1)$ v S. To je očitno, saj je razlika $p_1(x) - x\,p(x)$ deljiva z $x^n - 1$, ki je deljiv z $g(x)$, polinom $p(x)$ pa je tudi deljiv z $g(x)$. Zato je z $g(x)$ deljiv tudi polinom $p_1(x)$.

Sedaj pa pokažimo, da je množica B baza podprostora S. Predpostavimo, da je poljubna linearna kombinacija $\sum_{i=0}^{k-1} \lambda_i x^i g(x)$ enaka 0. Če obstaja največji indeks j, za katerega je $\lambda_j \neq 0$, potem je koeficient ob x^{n-k+j} enak λ_j, kar pomeni, da mora biti $\lambda_j = 0$. Torej je B res množica linearno neodvisnih vektorjev.

Enostavno preverimo še, da vektorji iz B napenjajo ves podprostor S. Vzamemo poljuben $p(x) \in S$, potem je $p(x) = a(x)g(x)$ za neki $a(x) = a_0 + a_1x + \cdots + a_{k-1}x^{k-1}$. Torej je $p(x) = a_0g(x) + a_1xg(x) + \cdots + a_{k-1}x^{k-1}g(x)$ res linearna kombinacija polinomov iz $\{g(x), xg(x), \ldots, x^{k-1}g(x)\}$. ∎

Podmnožica S je **ideal** komutativnega kolobarja R, če je zaprta za seštevanje in je za vsak $r \in R$ in za vsak $s \in S$ tudi $rs \in S$. Izrek nam torej pove, da je vsak k-razsežni podprostor S, ki ustreza idealu/kodi v R_n, generiranemu s polinomom $g(x)$ stopnje $n-k$, ki deli $x^n - 1$, cikličen. Polinom $g(x)$ imenujemo **generatorski polinom** linearne ciklične kode S.

Kolobar R_n je **glavni kolobar**, tj. vsak njegov ideal je generiran z enim samim polinomom. Ni se težko prepričati, da ideali v R_n ustrezajo natanko cikličnim kodam v $\mathbb{F}^n$. Ustrezen polinom ciklične kode deli modul $x^n - 1$. **Kodiranje** pri cikličnih kodah je potem kar množenje polinoma sporočila z generatorskim polinomom $g(x)$.

RS-kode lahko opišemo tudi kot posebne vrste linearne ciklične kode.

Izrek 6. *Naj bo $\mathbb{F}$ končen obseg s q elementi in $n := q-1$. Naj bo k tako število, da velja $1 \leq k < n$ in $d := n-k+1$ ter α primitiven element v $\mathbb{F}$. Koda C_1 naj bo linearna ciklična koda z generatorskim polinomom $g(x) = (x-\alpha)(x-\alpha^2)\dots(x-\alpha^{d-1})$, koda C_2 pa naj bo RS-koda, pri kateri sporočilu $m \in \mathbb{F}^k$ s prirejenim polinomom $m(x) = m_0 + m_1 x + \dots + m_{k-1}x^{k-1}$ priredimo kodno besedo $(m(\alpha), m(\alpha^2), \dots, m(\alpha^n))$. Potem kodi C_1 in C_2 sestavljajo iste kodne besede.*

Naj opozorimo, da zgornji izrek ne trdi, da istemu sporočilu v obeh primerih priredimo isto kodno besedo in da izrek velja tudi, če pogoj $n = q-1$ zamenjamo s $(q-1) \mid n$.

Dokaz. Naj bo $c = (c_0, c_1, \dots, c_{n-1})$ beseda iz kode C_1, ki pripada sporočilu m. Prirejeni polinom $c(x) = c_0 + c_1 x + \dots + c_{n-1}x^{n-1}$ potem lahko zapišemo v obliki $c(x) = m(x)g(x)$. Prepričajmo se, da je beseda c tudi v kodi C_2. Torej je treba poiskati tak polinom $f(x)$ stopnje največ $k-1$, da bo $c_i = f(\alpha^i)$ za $i \in \{0, \dots, n-1\}$. Naj bo $p(x) = p_0 + p_1 x + \dots + p_{n-1}x^{n-1}$, tako da velja

$$p_j = \frac{c(\alpha^{-j})}{n}, \quad j = 0, \dots, n-1. \tag{5}$$

Izračunajmo najprej vrednosti $p(\alpha^i)$, $i \in \{0, \dots, n-1\}$. Iz (5) sledi

$$p(\alpha^i) = \sum_{j=0}^{n-1} \frac{c\left(\alpha^{-j}\right)}{n} \cdot \left(\alpha^i\right)^j = \frac{1}{n} \sum_{j=0}^{n-1} \left(\sum_{h=0}^{n-1} c_h \alpha^{-jh} \right) \alpha^{ij} =$$

$$= \frac{1}{n} \sum_{h=0}^{n-1} c_h \cdot \left(\sum_{j=0}^{n-1} \alpha^{(i-h)j} \right) = c_i \,.$$

Pri zadnjem enačaju smo upoštevali, da je izraz v zadnjem oklepaju enak n za $h = i$, sicer pa 0. To vidimo takole: α je primitiven element, zato je $\alpha^n = 1$ in $\alpha \neq 1$, se pravi, da je α ničla polinoma $(x^n - 1)/(x - 1) = 1 + x + x^2 + \cdots + x^{n-1}$; enako velja tudi za vse potence α, ki so različne od ena.

Polinom $c(x)$ je deljiv s polinomom $g(x)$, zato so $\alpha, \alpha^2, \ldots, \alpha^{d-1}$ tudi njegove ničle. Ker je $d-1 = n-k$, to pomeni, da za $j \in \{n-1, n-2, \ldots, k\}$ velja $c(\alpha^{-j}) = c(\alpha^{n-j}) = 0$ in zato tudi $p_j = 0$. Torej ima polinom $p(x)$ stopnjo največ $k-1$ in si ga lahko izberemo za iskani polinom $f(x)$. Ker je bilo m poljubno sporočilo iz $\mathbb{F}^k$, sklepamo, da velja $C_1 \subseteq C_2$.

Končno iz izrekov 3 in 5 sledi, da sta kodi C_1 in C_2 linearni in k-razsežni, torej mora veljati enakost $C_1 = C_2$. ∎

Pravkar dokazani izrek nam da alternativno definicijo RS-kod. Le-ta omogoča enostavno in hitro odkodiranje, ki ga bomo predstavili v naslednjem razdelku. Zgoraj opisana transformacija, ki preslika $c(x)$ v $f(x)$, je znana kot **(inverzna) Fourierova transformacija** v končnih obsegih in je diskreten analog Fourierove transformacije v analizi [3, Ch. 6].

6. Polinomski algoritem za odkodiranje

Naj bo $\mathbb{F}$ končen obseg s q elementi in $n := q - 1$. Naj bo k tako število, da velja $1 \leq k < n$ in $d := n - k + 1$. Naj bo α primitiven element v $\mathbb{F}$ in

$$g(x) = (x - \alpha)(x - \alpha^2) \ldots (x - \alpha^{d-1}) .$$

Obravnavamo odkodiranje pri RS(n, k)-kodi, generirani s polinomom $g(x)$. Naj bo $c(x) = a(x)g(x)$ poslana kodna beseda, $r(x)$ pa prejeta beseda. Lahko jo zapišemo v obliki

$$r(x) = c(x) + e(x) , \tag{6}$$

kjer je $e(x)$ **polinom napake**. Če pri prenosu ni prišlo do napake, je $e(x)$ enak nič in je polinom $r(x)$ deljiv z $g(x)$. Polinom sporočila $a(x)$ dobimo iz $r(x)$ kar z deljenjem s polinomom $g(x)$. Če je prišlo do napake, pa bo odkodiranje težje. Opisali bomo metodo, ki odkodiranje prevede na reševanje posebnega sistema enačb.

Vemo, da obstajata taka polinoma $h(x)$ in $s(x)$, da je

$$r(x) = h(x) \cdot g(x) + s(x) \quad \text{in} \quad \deg(s(x)) < \deg(g(x)) . \tag{7}$$

Polinom $s(x)$ imenujemo **sindrom** prejete besede $r(x)$. Ker so α, α^2, ..., α^{d-1} ničle polinoma $g(x)$ in zato tudi polinoma $c(x)$, velja zaradi (6) in (7) naslednja zveza:

$$r\left(\alpha^i\right) = e\left(\alpha^i\right) = s\left(\alpha^i\right) \quad \text{za } i = 1, \ldots, d-1. \tag{8}$$

Predpostavimo, da pri prenosu ni prišlo do več kot $\ell \leq \lfloor (d-1)/2 \rfloor$ napak, kolikor jih koda največ lahko odpravi. Naj bodo $a_0, a_1, \ldots, a_{\ell-1} \in \{0, \ldots, n-1\}$ mesta v kodni besedi, na katerih je prišlo do napake. Potem lahko polinom $e(x)$ zapišemo v obliki

$$e(x) = \sum_{j=0}^{\ell-1} \lambda_j x^{a_j}.$$

Količino $s(\alpha^i)$ označimo s S_i. Eksponenti a_j v potenci α^{a_j} nam povedo položaje napak, zato števila α^{a_j} imenujemo **lokatorji napak**. Vrednosti λ_j pa so **velikosti napak**. Iz (8) dobimo sistem enačb

$$S_i = \sum_{j=0}^{\ell-1} \lambda_j (\alpha^i)^{a_j} = \sum_{j=0}^{\ell-1} \lambda_j (\alpha^{a_j})^i \quad \text{za } i = 1, \ldots, d-1 \tag{9}$$

z neznankami λ_j in α^{a_j}, $j = 0, \ldots, \ell-1$. Z uvedbo oznak $X_j = \alpha^{a_j}$, $j = 0, \ldots, \ell-1$, sistem (9) zapišemo v obliki

$$\begin{array}{lllll} S_1 & = \lambda_0 X_0 & + \lambda_1 X_1 & + \cdots + & \lambda_{\ell-1} X_{\ell-1}, \\ S_2 & = \lambda_0 X_0^2 & + \lambda_1 X_1^2 & + \cdots + & \lambda_{\ell-1} X_{\ell-1}^2, \\ & \vdots & & \vdots & \\ S_{d-1} & = \lambda_0 X_0^{d-1} & + \lambda_1 X_1^{d-1} & + \cdots + & \lambda_{\ell-1} X_{\ell-1}^{d-1}. \end{array} \tag{10}$$

Ta sistem $d-1$ enačb z 2ℓ neznankami (λ_j in X_j) se je v preteklosti pojavil pri reševanju različnih problemov, glej Barg [1]. Prvi se je verjetno z njim ukvarjal baron de Prony že okrog leta 1795 pri reševanju nekega interpolacijskega problema. Zanimivo je, da so različni avtorji predlagali precej podoben način za reševanje sistema (10), ki ga bomo opisali spodaj. Najprej poiščemo vrednosti X_j, nato pa lahko iz sistema (10) poiščemo še velikosti napak, saj je sistem enačb za λ_i, $i = 0, \ldots, \ell-1$, linearen.

Naj bo $\sigma(x) = 1 + \sigma_1 x + \sigma_2 x^2 + \cdots + \sigma_\ell x^\ell$ **polinom lokatorjev napake** oziroma bolj precizno polinom, ki ima za ničle ravno inverzne vrednosti lokatorjev napak, tj. $\prod_{i=0}^{\ell-1}(1 - X_j x)$. Zato velja:

$$\lambda_j X_j^{\ell+u} \sigma(X_j^{-1}) = 0 \quad \text{za } j = 0, \ldots, \ell-1, \tag{11}$$

kjer je u naravno število manjše ali enako ℓ. Seštejmo enačbe (11), upoštevajmo še sistem (10) in dobimo

$$0 = \sum_{j=0}^{\ell-1} \lambda_j X_j^{\ell+u} \left(1 + \sum_{i=1}^{\ell} \sigma_i X_j^{-i}\right) = S_{u+\ell} + \sum_{i=1}^{\ell} \sigma_i \sum_{j=0}^{\ell-1} \lambda_j X_j^{\ell+u-i} =$$
$$= S_{u+\ell} + \sum_{i=1}^{\ell} \sigma_i S_{\ell+u-i}\,,$$

kar je rekurzivna enačba za zaporedje $\{S_i\}$:

$$\sigma_1 S_{u+\ell-1} + \sigma_2 S_{u+\ell-2} + \cdots + \sigma_\ell S_u = -S_{u+\ell}\,. \tag{12}$$

Ko u teče od $1, \ldots, \ell$, dobimo sistem linearnih enačb za σ_i, $i = 1, \ldots \ell$, ki ga lahko zapišemo v matrični obliki

$$\begin{bmatrix} S_1 & S_2 & \ldots & S_\ell \\ S_2 & S_3 & \ldots & S_{\ell+1} \\ \vdots & \vdots & \ddots & \vdots \\ S_\ell & S_{\ell+1} & \ldots & S_{2\ell-1} \end{bmatrix} \begin{bmatrix} \sigma_\ell \\ \sigma_{\ell-1} \\ \vdots \\ \sigma_1 \end{bmatrix} = - \begin{bmatrix} S_{\ell+1} \\ S_{\ell+2} \\ \vdots \\ S_{2\ell} \end{bmatrix}. \tag{13}$$

Vnaprej ne poznamo ℓ, zato namesto z ℓ računamo z $\lfloor (d-1)/2 \rfloor$. Izkaže se, glej npr. [4, str. 149], da je rang matrike sistema v tem primeru enak številu napak. Ko poznamo število napak, lahko iz sistema (13) izračunamo koeficiente polinoma $\sigma(x)$. Da dobimo lokatorje napak, moramo poiskati ničle $\sigma(x)$ in njihove inverze. Ker smo v končnem obsegu, ničle lahko poiščemo tudi tako, da kar po vrsti preizkušamo elemente obsega (v praksi namreč obseg nima več kot 32 elementov).

Algoritem za odkodiranje Reed-Solomonovih kod, ki smo ga predstavili zgoraj, je bistveno hitrejši od tistega iz drugega razdelka, saj je polinomski. Rešimo le dva sistema enačb (13) in (10) velikosti $\mathcal{O}(d \times d)$, iščemo inverze ℓ elementov, ki so lahko shranjeni tudi v tabeli, ter vrednosti polinoma $\sigma(x)$ v največ n točkah. Skupna zahtevnost algoritma je v najslabšem primeru enaka $\mathcal{O}(n^3)$.

Z iskanjem algoritmov za dekodiranje RS-kod so se ukvarjali številni raziskovalci. Med njimi je bil tudi Elwyn Berlekamp, profesor elektrotehnike na kalifornijski univerzi v Berkeleyu, ki je konec 60. let prejšnjega stoletja odkril učinkovit algoritem za odkodiranje RS-kod [2]. Danes ga poznamo pod imenom Berlekamp-Masseyev algoritem in je izrednega pomena tudi v kriptografiji. Njegova predstavitev žal presega okvire tega članka. Odkodiranje porabi tipično do 10-krat več strojne opreme (npr. logike, pomnilnika,

procesorjevih ciklov) kot kodiranje. Običajno se uporabljajo strojne implementacije RS-kod, vendar pa so danes zaradi občutno povečane hitrosti mikroprocesorjev možne tudi programske implementacije (npr. Texas Instruments daje na voljo brezplačen program za odkodiranje).

Primer 1. Oglejmo si kodiranje z RS(15, 9)-kodo nad obsegom $\mathrm{GF}(2^4)$, ki smo ga opisali v četrtem razdelku. Za primitivni element obsega pa si zopet izberemo ničlo α modulskega polinoma. Razdalja kode je enaka $d = 15 - 9 + 1 = 7$, tako da koda popravi do tri napake. Stopnja generatorskega polinoma $g(x)$ je $n - k = 15 - 9 = 6$. Z uporabo tabele 3.1 izračunamo

$$\begin{aligned} g(x) &= (x-\alpha)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4)(x-\alpha^5)(x-\alpha^6) = \\ &= \alpha^6 + \alpha^9 x + \alpha^6 x^2 + \alpha^4 x^3 + \alpha^{14} x^4 + \alpha^{10} x^5 + x^6 . \end{aligned}$$

Kodiranje je množenje s polinomom $g(x)$. Besedo $m = (0, 0, 1, 0, \alpha^{10}, 0, \alpha^2, 0, 0)$ zakodiramo torej kot $c(x) = m(x) \cdot g(x) = \alpha^6 x^2 + \alpha^9 x^3 + \alpha^{11} x^4 + \alpha^{11} x^6 + \alpha^{11} x^8 + \alpha^9 x^9 + \alpha^8 x^{10} + \alpha^{12} x^{11} + \alpha^2 x^{12}$ oziroma $c = (0, 0, \alpha^6, \alpha^9, \alpha^{11}, 0, \alpha^{11}, 0, \alpha^{11}, \alpha^9, \alpha^8, \alpha^{12}, \alpha^2, 0, 0)$.

Poglejmo sedaj še, kako poteka odkodiranje. Če je prirejeni polinom $c(x)$ kodne besede c deljiv s polinomom $g(x)$, potem je polinom sporočila $m(x)$ enak $c(x)/g(x)$. Poskusimo odkodirati še prejeto besedo r s prirejenim polinomom $r(x) = \alpha^6 x^2 + \alpha^9 x^3 + x^4 + x^5 + x^6 + \alpha^{10} x^7 + \alpha^3 x^8 + \alpha^3 x^9 + \alpha^2 x^{12}$. Polinom $r(x)$ ni deljiv z $g(x)$, saj je ostanek enak $s(x) = \alpha^5 + \alpha^{10} x + \alpha x^2 + \alpha^{10} x^3 + \alpha^3 x^4 + \alpha^9 x^5$. Izračunamo $S_i = s(\alpha^i)$ za $i = 1, \ldots, 6$ in dobimo naslednje vrednosti:

S_1	S_2	S_3	S_4	S_5	S_6
α^{12}	0	α^3	α^2	α^3	1

Sestavimo matriko iz sistema (13):

$$\begin{bmatrix} \alpha^{12} & 0 & \alpha^3 \\ 0 & \alpha^3 & \alpha^2 \\ \alpha^3 & \alpha^2 & \alpha^3 \end{bmatrix} . \tag{14}$$

Matriko (14) enostavno prevedemo na zgornjetrikotno obliko. Od tretje vrstice odštejemo prvo, pomnoženo z α^6, in nato še drugo, pomnoženo z α^{14} (ker ima obseg karakteristiko 2, je odštevanje kar enako seštevanju). Dobimo matriko ranga 2, kar pomeni, da je pri prenosu kodne besede najverjetneje prišlo do dveh napak. Zato je treba rešiti sistem dveh enačb z dvema neznankama

$$\begin{bmatrix} \alpha^{12} & 0 \\ 0 & \alpha^3 \end{bmatrix} \begin{bmatrix} \sigma_2 \\ \sigma_1 \end{bmatrix} = - \begin{bmatrix} \alpha^3 \\ \alpha^2 \end{bmatrix} , \tag{15}$$

ki nam da rešitev $\sigma_1 = \alpha^{14}$ in $\sigma_2 = \alpha^6$. Sedaj poznamo polinom $\sigma(x) = 1 + \alpha^{14}x + \alpha^6 x^2$. Z računanjem njegovih vrednosti v vseh elementih obsega $\mathrm{GF}(2^4)$ preverimo, da sta njegovi ničli α^4 in α^5. Njuna inverza α^{11} in α^{10} nam povesta, da sta napaki pri prejeti besedi na desetem in enajstem mestu. Preostane nam le še, da izračunamo velikosti teh napak. V našem primeru bo to najenostavneje kar z reševanjem sistema (10). Le-ta je predoločen; če nima rešitve, je bila predpostavka, da je prišlo do največ treh napak, napačna. Velikosti napak izračunamo iz prvih dveh enačb

$$\begin{aligned} \alpha^{12} &= \lambda_0 \alpha^{11} + \lambda_1 \alpha^{10} \\ 0 &= \lambda_0 \left(\alpha^{11}\right)^2 + \lambda_1 \left(\alpha^{10}\right)^2 \end{aligned} \tag{16}$$

in z deljenjem s polinomom $g(x)$ preverimo, da smo res dobili kodno besedo. Velikosti napak sta $\lambda_0 = \alpha^{12}$ in $\lambda_1 = \alpha^{14}$. Polinom poslane kodne besede je potem $c_1(x) = \alpha^6 x^2 + \alpha^9 x^3 + x^4 + x^5 + x^6 + \alpha^{10} x^7 + \alpha^3 x^8 + \alpha^3 x^9 + \alpha^{14} x^{10} + \alpha^{12} x^{11} + \alpha^2 x^{12}$. Ker velja $c_1(x) = g(x) \cdot (x^2 + \alpha^7 x^4 + \alpha^2 x^6)$, je polinom sporočila enak $x^2 + \alpha^7 x^4 + \alpha^2 x^6$, samo sporočilo pa je enako $(0, 0, 1, 0, \alpha^7, 0, \alpha^2, 0, 0)$.

LITERATURA

[1] A. Barg, *At the dawn of the theory of codes*, Math. Intelligencer **15** (1993), str. 20–26.

[2] E. R. Berlekamp, *Algebraic Coding Theory*, Aegean Park Press, 1968 (dopolnjena izdaja, 1984).

[3] Richard E. Blahut, *Algebraic Codes for Data Transmission*, Cambridge University Press, 2003.

[4] D. G. Hoffman, D. A. Leonard, C. C. Lindner, K. T. Phelps, C. A. Rodger in J. R. Wall, *Coding Theory: The Essentials*, Marcel Dekker, Inc., 1991.

[5] W. C. Huffman, V. S. Pless in R. A. Brualdi (uredniki), *Handbook of Coding Theory*, Vol. 1 & 2, North-Holland, 1998.

[6] A. Jurišić, *Računala nove dobe, 1. in 2. del*, Presek **30** (2002–03), str. 226–231 in 291–296.

[7] A. Jurišić, *Napake niso za vedno*, Presek **30** (2002–03), str. 361–366.

[8] S. Klavžar, *O teoriji kodiranja, linearnih kodah in slikah z Marsa*, Obzornik mat. fiz. **45** (1998), str. 97–106.

[9] I. S. Reed in G. Solomon, *Polynomial codes over certain finite fields*, J. Soc. Indust. Appl. Math. **8** (1960), str. 300–304.

[10] R. C. Singleton, *Maximum distance q-nary codes*, IEEE Trans. Inform. Theory IT-10(2) (1964), str. 116–118.

[11] S. A. Vanstone in P. C. van Oorschot, *An Introduction to Error Correcting Codes with Applications*, Kluwer Academic Publishers, 1989.

[12] I. Vidav, *Algebra*, Mladinska knjiga, Ljubljana 1972.

NUMERIČNA ANALIZA PERKOLACIJSKEGA PRAGA PREVODNOSTI V KERMETIH

MILAN AMBROŽIČ

Institut Jožef Stefan

PACS: 64.60.Ak

Prispevek opisuje teoretično študijo vpliva kotne porazdelitve paličastih prevodnih delcev v neprevodni keramični matriki na perkolacijski prag električne prevodnosti materiala. Perkolacijski prag v tem primeru pomeni najmanjši prostorninski delež prevodne snovi v kermetu, da postane zmes električno prevodna.

NUMERICAL ANALYSIS OF PERCOLATION THRESHOLD IN CERMETS

I have theoretically investigated the influence of the angular distribution of elongated conductive particles in a nonconductive host matrix on the conductivity threshold of the material, i.e., the minimum volume fraction of conductive phase for the whole sample to become conductive.

1. Uvod

V zmesi keramične snovi in kovine ali kermetu (kermet = keramika + metal) se kovinska faza pojavlja v delcih, ki so med seboj nepovezani, če je kovine premalo. Kovinski delci so lahko različnih oblik, odvisno od kemijske sestave kermeta in pogojev nastanka. Pri nepovezanih kovinskih delcih je električna prevodnost zmesi zelo majhna in določena s prevodnostjo keramike, ki je navadno zelo dober izolator. Pri večjem prostorninskem deležu kovine v keramiki pa nastanejo gruče kovinskih delcev, ki se med seboj stikajo, dokler pri dovolj veliki vrednosti prostorninskega deleža kovine ne nastane prevodna pot za električni tok v neki smeri. Temu deležu rečemo na kratko perkolacijski prag in ga navadno izražamo v odstotkih. Značilne vrednosti perkolacijskega praga so nekaj deset odstotkov.

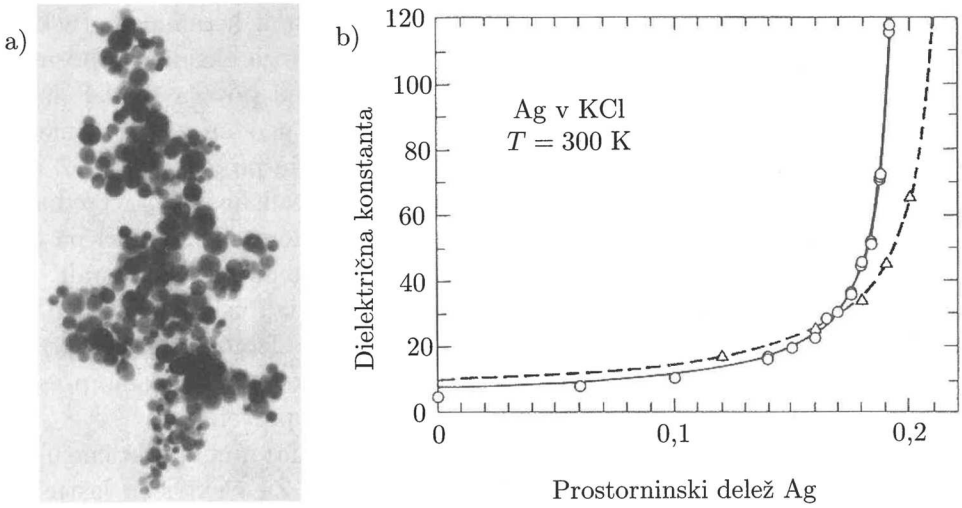
Kermete veliko uporabljajo v tankoplastni tehnologiji: v mikroelektronskih vezjih so uporniki narejeni iz naparjenih tankih kermetnih plasti. Uporabni keramični materiali za kermete so razni oksidi, kovina pa je navadno krom, zlitina nikelj-krom itd. Pri kermetnih upornikih skušajo doseči dvoje: veliko specifično upornost in čim manjše spreminjanje upornosti s temperaturo. Čisti keramični materiali imajo sicer veliko specifično upornost, vendar imajo neustrezno velik koeficient temperaturnega spreminjanja upornosti, in sicer največkrat negativnega (v nasprotju s kovinami se upornost z višanjem

temperature zmanjšuje). Za primerjavo: pri značilnih keramičnih (nekermetnih) upornikih na osnovi manganovega in nikljevega oksida se upornost zmanjša za 4 % na kelvin, medtem ko se pri platini poveča za 0,4 % na kelvin. Velik temperaturni koeficient upornosti je ugoden za termometre na osnovi keramičnih upornikov, za elektronska vezja pa je neželen. Z dodatkom kovine v keramiko naj bi čim bolj zmanjšali absolutno vrednost negativnega temperaturnega koeficienta upornosti keramike, hkrati pa obdržali veliko upornost. Zato preskušajo različne kombinacije keramike in kovin. Seveda morajo biti kovine in keramični materiali usklajeni tudi glede raznih kemičnih in mehanskih lastnosti, kar omejuje izbiro. Neželen pojav je npr. oksidacija kermetnih plasti. Z dodajanjem kovine ne smemo preseči perkolacijskega praga, zato delež kovine ne sme biti prevelik.

Vedenje kermeta blizu perkolacijskega praga za zdaj nima praktične uporabe, zanimivo pa je s stališča osnovnih raziskav. Za električne lastnosti snovi blizu perkolacijskega praga je značilno nelinearno ali kritično vedenje. Že majhne spremembe fizikalnih parametrov, kot so sestava, napetost in temperatura, lahko povzročijo velike spremembe električnih lastnosti [1, 2, 3, 4, 5, 6, 7]. Med drugim sta pri perkolacijskem pragu značilna nenaden porast prevodnosti in divergenca dielektričnosti. Na primer, Grannan in sodelavci [6] so pripravili kompozit, kjer so bili srebrni delci neurejeno porazdeljeni v neprevodnem mediju KCl. Najprej so pripravili okrogle srebrne delce povprečnega premera 20 nm (slika 1a), potem pa so primešali določeno količino teh delcev v praškasti KCl, stisnili pod velikim tlakom v tablete, vse skupaj zmleli, še večkrat stisnili in zmleli, nazadnje pa toplotno obdelali. Izmerili so odvisnost dielektrične konstante od prostorninskega deleža srebra v KCl (slika 1b), medtem ko so mešanici dodajali vedno več srebra. Naredili so dve seriji meritev in dobili rahlo različne rezultate (krožci in trikotniki na sliki), kar kaže na to, kako so fizikalne količine močno odvisne od natančnih pogojev nastanka kompozitov in je zelo težko doseči ponovljivost. Teoretični potenčni odvisnosti (polna in črtkana črta) so dobili z najboljšo prilagoditvijo prostih parametrov meritvam.

Za raziskovanje teh pojavov je pomembno čim natančneje ugotoviti in nadzorovati perkolacijski prag. V praksi je to zelo zahtevno, saj je pri znani kemijski sestavi zmesi in drugih makroskopskih fizikalnih parametrov natančna vrednost perkolacijskega praga odvisna od mikrostrukturnih lastnosti sistema, kot sta fazna porazdelitev in morfologija.

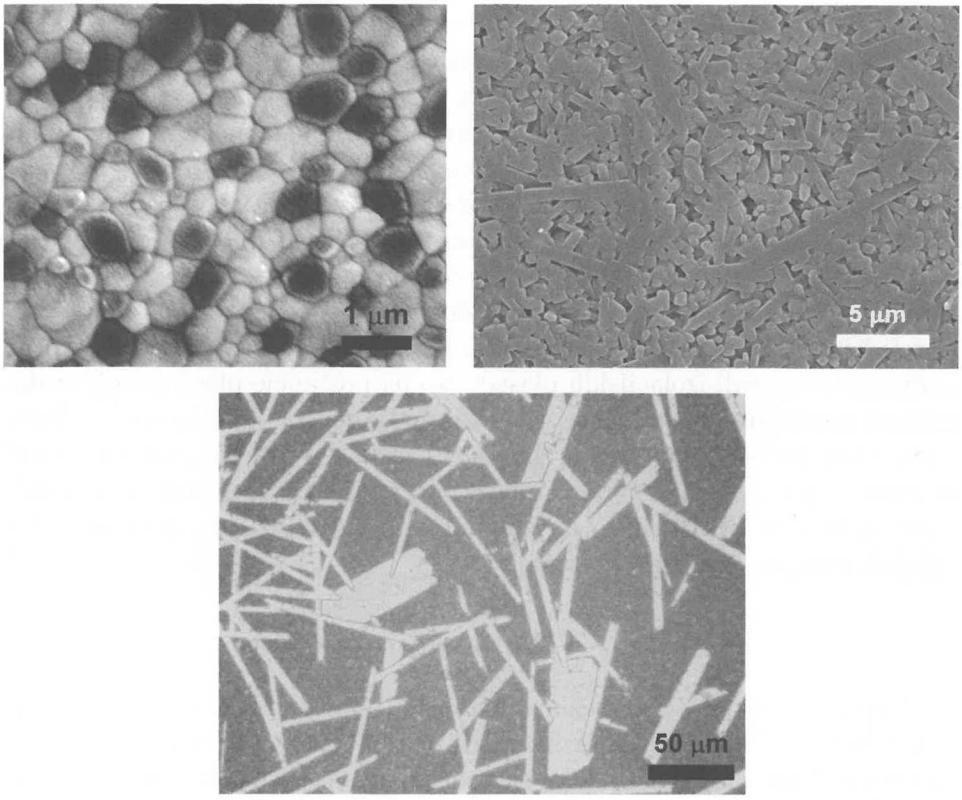
Veliko objavljenih raziskav perkolacijskega praga uporablja modele z okroglimi prevodnimi delci, zato je njihova uporabnost omejena. Quintanilla in drugi [8] so s posebno prirejeno numerično metodo celo na 6 veljavnih decimalnih mest izračunali perkolacijski prag krogov v ravnini (ali vzporednih



Slika 1. Elektronska slika okroglih srebrnih delcev s povprečnim premerom 20 nm in odvisnost dielektrične konstante od prostorninskega deleža srebra v kompozitu Ag-KCl (vir [6]). Z dovoljenjem American Physical Society.

valjev v prostoru, 2D problem), ki se lahko brez omejitev prekrivajo med sabo; dobili so vrednost 0,676339. Podobno sta Lorenz in Ziff [9] s posebno metodo izračunala perkolacijski prag „švicarskega sira" (tj. enakih okroglih por v trdni snovi) zelo natančno: 0,289572. Takšne raziskave so pomembne v kemiji pri preučevanju vpliva poroznosti na difuzijo plinov v snovi. Prve perkolacijske numerične simulacije sta že leta 1974 opravila Pike in Seager [10], in sicer ne le za kroglice, temveč tudi za druga geometrijska telesa, npr. za izotropno usmerjene paličke z zanemarljivo debelino v ravnini. Bliže realnim sistemom so bile numerične raziskave Balberga in sodelavcev [11, 12, 13], ki so obravnavali delce v obliki valjev s krogelnima kapicama (v tem prispevku jih imenujem paličke) v dveh ali treh dimenzijah. De Bondt in sodelavci [14] so doslej najbolj sistematično opisali vpliv izotropije in anizotropije smeri simetrijskih osi paličk na perkolacijski prag.

Huseby in sodelavci [15] so sistematično numerično preučevali povezave med dvorazsežnimi nepravilnimi in pravilnimi mnogokotniki z naključnimi orientacijami (smermi normal) v prostoru, kar naj bi koristilo pri preučevanju vpliva mreže geoloških razpok na pretakanje snovi v zemeljskem površju. Te raziskave so uporabne tudi splošneje, ker lahko vsako geometrijsko telo aproksimiramo z nepravilnim poliedrom, ki ima za stranske ploskve mnogokotnike. Čeprav je problem sekanja takšnih poliedrov v prostoru analitično rešljiv, pa je postopek dolg in zato numerična metoda časovno potratna.



Slika 2. Morfologija kompozitnih struktur z delci različnih oblik. Prvi dve sliki sta bili narejeni s SEM (Scanning Electronic Microscope = vrstični elektronski mikroskop), tretja pa z optičnim mikroskopom. Slike so bile narejene na različnih odsekih za keramiko na IJS (avtorji slik D. Kolar, T. Kosmač, A. Dakskobler idr.).

Pregled eksperimentalnih, analitičnih in numeričnih raziskav perkolacijskega praga je med drugim podan v viru [16]. Numerično so raziskovali perkolacijski prag tudi za druge delce, npr. kocke. Z različnimi postopki [17] dobijo zelo raznolike prevodne delce, od skoraj kroglastih do paličastih ali ploščatih. Nekaj jih je prikazanih na sliki 2. Namen tega prispevka je obravnavati vpliv usmerjenosti podolgovatih prevodnih delcev na perkolacijski prag in primerjava rezultatov predvsem z virom [14]. V omenjenem viru so avtorji preučevali odvisnost perkolacijskega praga od kotne porazdelitve smeri delcev, njihove povprečne smeri, razmerja dimenzij in dovoljene penetracijske globine enega delca v drugega. Sam sem ponovil račune pri enakih parametrih zaradi neposredne primerjave izidov in s tem posredne preverbe njihovih zanesljivosti. Bolj sistematično sem raziskal vpliv kotne porazdelitve smeri delcev na perkolacijski prag.

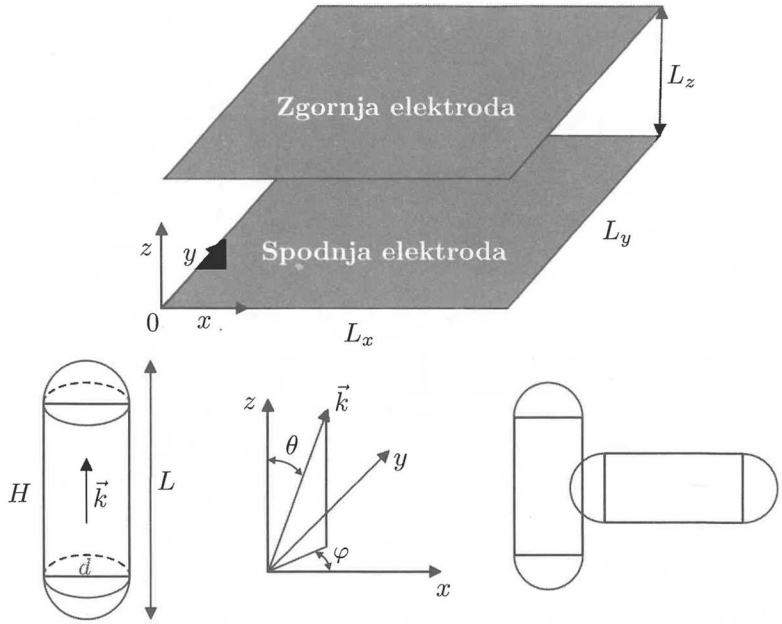
Spodbuda za moje izračune so bile nekatere nejasnosti pri doseženem perkolacijskem pragu za nekatere keramične kompozite, narejene med drugim na Odseku za inženirsko keramiko na Institutu Jožef Stefan [18, 19]. V [19] je opisan način, kako s ponavljajočim pregibanjem in valjanjem keramičnih plastičnih suspenzij dobijo plastovite kompozite, kjer si izmenično sledijo prevodne kermetne plasti (Al_2O_3 + Cr) in neprevodne keramične plasti (Al_2O_3). S pregibanjem in valjanjem dobijo vedno tanjše posamezne plasti. Seveda sledi valjanju suspenzij običajna toplotna obdelava, da dobijo keramični kompozit. Dokler so plasti dovolj debele, so izidi merjenj prevodnosti kompozita običajni: kompozit je prevoden v smeri plasti, pravokotno nanje pa ne (zaradi izolacijskih plasti). Ko pa postanejo plasti dovolj tanke, nastopi prevodnost tudi v smeri pravokotno na plasti. To si razložimo tako, da se plasti začnejo zvijati in prelamljati, tako da se bližnje prevodne plasti staknejo s prekinitvijo vmesnih neprevodnih plasti. To je bilo vidno tudi z mikroskopom. Medtem ko so izidi merjenj v delu [19] kvalitativo dobro opisani, manjka kvantitativna analiza.

2. Model

Ukvarjal sem se s trirazsežnim perkolacijskim problemom. Obravnaval sem celico v obliki kvadra z razsežnostmi L_x, L_y in L_z, za elektrodi pa sem vzel ploskvi pri $z = 0$ in $z = L_z$, kot prikazuje slika 3. Tako sem preučeval prevodnost v smeri osi z. Vzel sem prevodne delce v obliki cilindričnih paličic s polkroglama na obeh koncih (na kratko paličke, slika 3). Takšna telesa imenujemo tudi sferocilindri.

Zamisel za model sem vzel iz vira [14]. Programski postopek za izračun perkolacijskega praga je takle. Računalniški program je naključno vstavljal delce v celico, enega za drugim. Po vstavitvi vsakega delca je program preveril, ali je že nastala prevodna pot med elektrodama s stikanjem nekaterih delcev. Slika 4 shematsko prikazuje doseženi perkolacijski prag za paličke v dvorazsežni celici. Ko je nastala prevodna pot, je program seštel prostornine vseh delcev v celici in iz tega perkolacijski prag: $v_p = V_p/V$, kjer je V_p prostornina prevodne faze, V pa celotna prostornina kermeta. Za določitev naključnih vrednosti parametrov, kot so lege posameznih kovinskih delcev, sem uporabil generator naključnih števil.

Zaradi statistične napake se pri omejenem številu delcev izračunani perkolacijski prag ne ujema natančno s pravo teoretično vrednostjo. Zato sem pri istem naboru fizikalnih parametrov (konfiguraciji) postopek iskanja perkolacijskega praga ponovil večkrat, večinoma 18- do 30-krat. S temi izidi sem za izbrano konfiguracijo izračunal povprečno vrednost perkolacijskega



Slika 3. Koordinatni sistem za celico in oblika prevodnih delcev. Opredelitev smernega vektorja delcev. Penetracija delcev v primeru polkrogla-valj.

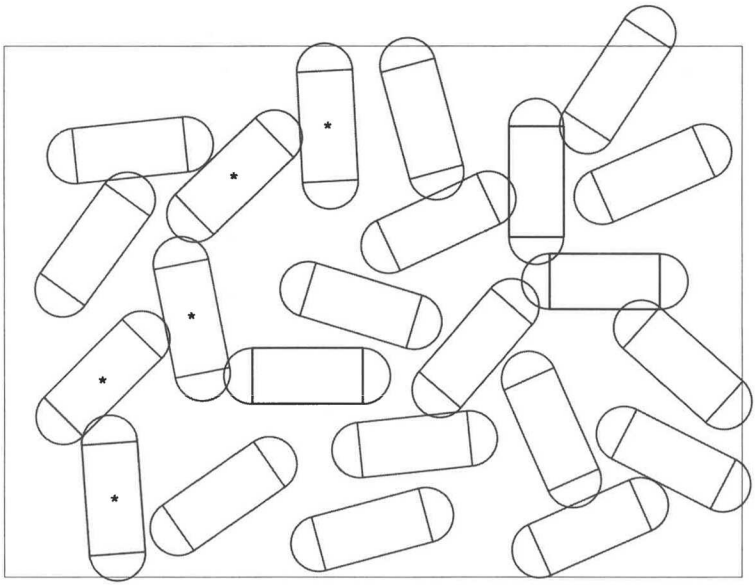
praga v_p in njegovo statistično napako. Statistična napaka je močno odvisna od približnega števila delcev v celici, pri katerem ravno pride do praga prevodnosti. Pri izbranih parametrih sem dobil nekako med 2 000 in 10 000 delcev v celici pri doseženem perkolacijskem pragu, kar je dalo absolutno statistično napako okrog enega ali dveh odstotkov. To je bil nekako optimum glede na potrebni čas računanja in zanesljivost izidov. Za 30 ponovitev in pri približnem številu delcev 5 000 je potrebnih več ur računanja za eno samo konfiguracijo. Število delcev je odvisno predvsem od tega, kako veliko celico vzamemo pri dani velikosti delcev (ali, kar je isto, kako velike delce vzamemo pri dani velikosti celice).

Za nabor naključnih vrednosti parametrov sem vzel dve vrsti porazdelitev:

a) enakomerno (npr. enako verjetne vse vrednosti koordinate x delcev med vrednostma $x = 0$ in $x = L_x$),

b) neenakomerno porazdelitev „klobuček“.

Razložimo porazdelitev klobuček na zgledu formalne spremenljivke s, ki ima povprečno vrednost s_{pov}, dovolimo pa njeno variacijo σ_s okrog povprečne vrednosti: $s_{pov} - \sigma_s < s < s_{pov} + \sigma_s$. Za verjetnostno porazdelitveno funkcijo za

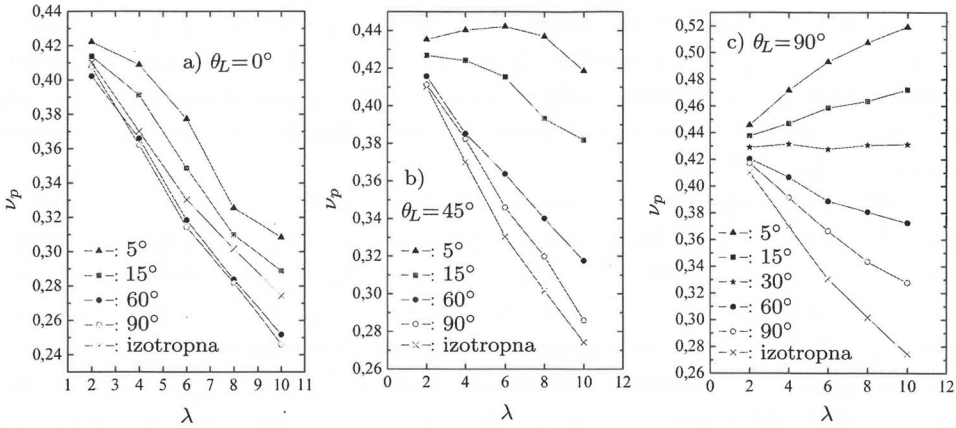


Slika 4. Shematski dvorazsežni prikaz doseženega perkolacijskega praga za paličaste delce. Skupina delcev s prevodno potjo je označena z zvezdicami.

klobuček sem uporabil kar kosinusno funkcijo z vrhom pri $s = s_{pov}$ in ničlama pri $s = s_{pov} - \sigma_s$ in $s = s_{pov} + \sigma_s$ (seveda pa je zunaj dovoljenega intervala funkcija identično enaka nič). Kosinusna porazdelitvena funkcija je opisana v matematičnem dodatku. Porazdelitvena funkcija $w(s)$ spremenljivke s ima običajen pomen: $w(s)ds$ pomeni verjetnost, da ima spremenljivka s vrednost na intervalu $(s, s + ds)$. Porazdelitev klobuček sem normaliziral, tako da je verjetnost, da ima delec vrednost spremenljivke s na opisanem intervalu, res enaka 1. Program je poskrbel za pretvorbo med enakomerno porazdelitvijo generatorja naključnih števil med 0 in 1 ter katerokoli enakomerno porazdelitvijo ali pa porazdelitvijo klobuček. Razloga za izbiro kosinusne porazdelitvene funkcije sta dva:

1) predhodne raziskave [14] so pokazale, da vrsta porazdelitve, če so si vse kvalitativno podobne, ne vpliva znatno na kvalitativne rezultate za perkolacijski prag,
2) s kosinusno porazdelitvijo je dovolj preprosto računati, kar je za našo časovno zahtevno numerično metodo pomembno.

Za razsežnosti celice sem izbral $L_x = L_y = L_z = 1$ in meril vse dolžinske razsežnosti v enotah L_z. Izbral sem povprečni premer valjev d_{pov} in dovolil tudi variacijo premerov σ_d okrog povprečne vrednosti; tako se premer d



Slika 5. Odvisnost perkolacijskega praga paličk od razmerja $\lambda = L/d$ (L je dolžina paličk, d pa premer); v vseh primerih je povprečni premer paličk = 0,025 z 10 % možnim relativnim odmikom od povprečja, maksimalna relativna penetracijska globina pa je 0,2. Azimutalni kot je popolnoma neurejen. Laboratorijski polarni kot ima vrednosti: a) $\theta_L = 0°$; b) $\theta_L = 45°$; c) $\theta_L = 90°$. Zgledi z različnimi odstopanji relativnega kota σ_{θ_R} so označeni z različnimi grafičnimi simboli. Izidi za izotropno porazdelitev delcev so označeni s križci.

različnih delcev naključno spreminja v mejah $d_{pov} - \sigma_d < d < d_{pov} + \sigma_d$. Vzel sem porazdelitev klobuček z vrhom pri d_{pov}. Kovinski delci v neprevodni keramiki nikoli niso popolnoma enaki med seboj.

Vendar pa se je izkazalo, da neenakost velikosti delcev (če so vsaj primerljivi po velikosti) ni bistvena za perkolacijski prag. Če je delcev v celici dovolj (vsaj nekaj tisoč), tudi ni pomembno, kako veliki so v primerjavi z velikostjo celice. Značilni premeri valjev so bili okrog 0,01 do 0,05 (v enotah L_z), kar je bilo navadno dovolj, da zanemarimo površinske pojave in je izračunani perkolacijski prag neodvisen od povprečne velikosti delcev.

Razsežnosti paličke so podane z dvema parametroma: premerom d valja oz. krogelnih kapic in celotno dolžino L (slika 3). Označimo njuno razmerje na kratko $\lambda = L/d$. Za paličke moramo vzeti $\lambda > 1$. Program omogoča variacijo obeh parametrov, d in λ, za posamezne delce: $d_{pov} - \sigma_d < d < d_{pov} + \sigma_d$ in $\lambda_{pov} - \sigma_\lambda < \lambda < \lambda_{pov} + \sigma_\lambda$. Vendar sem vedno obravnaval paličke s skoraj homogenim razmerjem dolžin λ in dovolil variacijo 10 % okrog povprečja. Zato je na slikah 5 z oznako λ označena kar povprečna vrednost za paličke.

Paličke imajo še dve prostostni stopnji: polarni kot θ in azimutalni kot φ, ki podajata smer geometrijske osi delca v prostoru (slika 3). Glede prostorske urejenosti obeh kotov sem obravnaval dve možnosti: popoln nered in delni red. Popolni nered pomeni izotropno porazdelitev dolgih osi paličk

v prostoru. To dobim s kosinusno porazdelitveno funkcijo za polarni kot z maksimumom pri 90° in vrednostjo nič pri 0° in 180° ter homogeno porazdelitvijo azimutalnega kota med 0° in 360° (glej matematično prilogo). Tu poudarim, da sem za argument porazdelitvenih funkcij vedno vzel kot in ne katere od kotnih funkcij.

Delni red je opisan s povprečno orientacijo delcev, ki jo podaja laboratorijski polarni kot θ_L, tako da je povprečna orientacija opisana z enotskim vektorjem: $\vec{e}_{pov} = (\sin\theta_L, 0, \cos\theta_L)$. Ravnino (x, z) sem izbral zaradi nazornosti. Dejanska orientacija posamezne paličke je dana z njeno relativno orientacijo: le-to opisujeta naključno izbrana relativna kota θ_R in φ_R (relativna glede na povprečno orientacijo, priloga 5.2). Iz parametrov θ_L, θ_R in φ_R lahko izračunamo orientacijska kota θ in φ glede na laboratorijski sistem. Smer dolge osi delca (tj. valjne osi) podamo s smernim vektorjem $\vec{k} = (\sin\theta\cos\varphi, \sin\theta\sin\varphi, \cos\theta)$.

V opisani numerični proceduri je dovoljeno delno prekrivanje (vdiranje, penetracija) enega delca v drugega. Za vse delce je predpisana maksimalna relativna penetracijska globina (MRPG), ki pove, kolikšna je lahko največja penetracija enega delca v drugega glede na njuna polmera. Dejanska penetracijska globina g_{pen} dveh delcev v stiku ne sme preseči največje vrednosti $g_{pen,max}$, kjer opredelimo $g_{pen,max} = \mathrm{MRPG} \cdot R_{min}$, pri tem pa je R_{min} manjši od obeh radijev sekajočih se kroglic. Na sliki 3 je zgled penetracije valjnega oz. krogelnega dela dveh paličk.

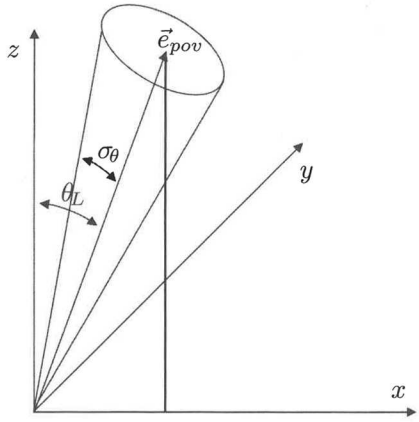
Vzemimo, da smo že postavili $N-1$ delcev v celico, sedaj pa dodamo N-ti delec. Če se po naključni postavitvi zgodi, da zadnji delec vdira v enega od prejšnjih do večje globine kot $g_{pen,max}$, ga preprosto zavrnemo in se postopek za njegovo vstavitev v celico ponovi. Opisani postopek uporabljam zaradi naslednjega razloga. Če prekrivanje delcev ne bi bilo dovoljeno, bi bila verjetnost, da se samo dotikajo, enaka nič, če imajo naključne lege. Tako ne bi nikoli dosegli perkolacijskega praga. Še en razlog je za uporabo numeričnega preprostega postopka z največjo dovoljeno penetracijo: model naj približno opiše raznovrstne kompozitne strukture, kjer so interakcije med prevodnimi delci zelo različne in odvisne od neprevodne keramične matrike. Lahko se zgodi, da se bližnja delca pri kemijski obdelavi privlačita in stakneta: namesto da bi prodrla drug v drugega, se rahlo deformirata in nastane med njima povezovalni vrat, pri tem pa se središči primakneta. V tem primeru se navadno prostornini začetnih okroglih delcev ohranita. Zato sem upošteval celotno prostornino vseh delcev in nisem odšteval dela prostornine sekajočih se delcev. Značilna vrednost MRPG v računih je bila reda 10 %. Vpliv MRPG na perkolacijski prag sem namesto na paličkah preskusil kar na kroglicah in ugotovil močno odvisnost: npr. pri MRPG = 10 % je v_p enak 45 %,

pri MRPG = 50 % pa je v_p le 35 %. Pri paličkah sem izbral MRPG = 20 % in ga nisem spreminjal.

3. Ugotovitve

Za preskus zanesljivosti opisane numerične metode sem izračunal perkolacijski prag za okrogle delce z enakimi polmeri, pri tem pa dovolil neomejeno prekrivanje kroglic. To pomeni, da sem vzel MRPG = 200 %, saj je pri popolnem prekritju enakih krogel (središči sovpadata) penetracijska globina enaka (glej matematično prilogo): $g_{pen} = R + R - d$, $d = 0$, $g_{pen} = 2R$. Pri tem preskusu seveda nisem predpostavil ohranitve prostornine kroglic, temveč sem prostornino preseka dveh kroglic upošteval samo po enkrat, tako da bi lahko neposredno primerjal svoje izračune z virom [9]. Pri velikosti kroglic $d = 0{,}05$ sem pri perkolacijskem pragu dobil okrog 10 000 kroglic v celici; 24 ponovitev računa mi je dalo povprečni perkolacijski prag 0,2915. Pri $d = 0{,}03$, kar da okrog 25 000 kroglic za perkolacijski prag, ter 60 ponovitvah sem dobil perkolacijski prag 0,288, kar je res blizu vrednosti 0,289572 iz vira [9]. Kot zanimivost in dokaz težavnosti perkolacijskega problema celo pri tako preprosti geometriji, kot so enake kroglice, naj omenim, da bi bilo treba predvideti npr. tudi zglede sekanja treh krogel s skupnim presekom. Ugotavljanje takšnega preseka in izračun njegove prostornine za vse kroglice bi bilo zelo zapleteno, tako programsko kot matematično. Zato tega nisem delal, saj sem tudi ocenil, da lahko verjetnost sekanja treh krogel z nekim skupnim presekom zanemarim.

Perkolacijski prag za paličke je močno odvisen od razmerja $\lambda = L/d$ in od porazdelitve dolgih osi delcev v prostoru. Pomembna je tudi povprečna orientacija delcev, ki je podana s polarnim kotom θ_L. Če so paličke pretežno usmerjene v smeri osi z ($\theta_L = 0°$), dobimo z večjim razmerjem λ nižji perkolacijski prag (slika 5a). Nasprotno velja, če so paličke pretežno usmerjene pravokotno na os z ($\theta_L = 90°$, slika 5c). Na sliki 5b je prikazan vmesni primer s $\theta_L = 45°$. Z delnim neredom dosežemo nižji perkolacijski prag kot pri popolnem redu (popolni red pomeni, da so vse paličke poravnane natančno v povprečni smeri $\vec{e}_{pov}$). V vseh treh zgledih sem izbral popolnoma neurejen relativni azimutalni kot φ_R, tj. enakomerno porazdeljen med 0° in 360°. Najprej si oglejmo rezultate, prikazane na sliki 5a. Za porazdelitev relativnega polarnega kota θ_R sem vzel kosinusno porazdelitev s povprečjem nič in največjim odstopanjem σ_{θ_R}. Večje odstopanje, ki pomeni večji nered, povzroči nižji perkolacijski prag; na sliki 5a je primerjava perkolacijskih pragov za odstopanja 5°, 15°, 60° in 90°. Vseeno pa lahko z delnim redom dosežemo nižji perkolacijski prag kot pri popolnem neredu (izotropna poraz-



Slika 6. Stožec porazdelitve smeri paličk pri neurejenem azimutalnem kotu

delitev smeri delcev). Na sliki 5 je za primerjavo dodana še odvisnost $v_p(\lambda)$ pri popolnem neredu (križci).

Še bolj dramatično odvisnost perkolacijskega praga od urejenosti relativnega polarnega kota vidimo na sliki 5c, kjer je $\theta_L = 90°$. Za $\sigma_{\theta_R} = 30°$ je perkolacijski prag v okviru numerične napake neodvisen od razmerja razsežnosti λ. Za manjše vrednosti σ_{θ_R} se perkolacijski prag viša z λ, kot sem že omenil, vendar pa za večje vrednosti σ_{θ_R} pada z λ, kakor v primeru $\theta_L = 0°$ na sliki 5a.

Po napovedih Balberga in drugih [13] naj bi bil za zelo velika razmerja λ perkolacijski prag obratno sorazmeren z λ, če so paličke usmerjene pretežno v smeri osi z. S slike 5a je razvidno, da se moji izidi kvalitativno ujemajo s to ugotovitvijo, čeprav razmerja λ niso zelo velika.

Doslej smo si ogledali le primere popolnoma enakomerne porazdelitve relativnega azimutalnega kota med 0° in 360°. To pomeni, da so smeri dolgih osi paličk znotraj stožca, katerega geometrijska os se ujema s povprečno smerjo $\vec{e}_{pov}$, kot ob njegovem vrhu pa je enak dvojnemu kotu σ_{θ_R} (slika 6). Takšna verjetnostna porazdelitev je osno simetrična, ni pa enakomerna (največja je na osi stožca in pade na nič na plašču, izjema je le skrajni primer z izotropno porazdelitvijo smeri). Preskusil sem tudi drugačne porazdelitve relativnega azimutalnega kota, vendar te v okviru statistične napake zanemarljivo vplivajo na perkolacijski prag.

Podobnosti in razlike med mojo raziskavo in tisto v viru [14] so naslednje. V obeh delih smo proučevali sferocilindre podobnih oblik in dimenzij, obravnavali smo podobne relativne penetracijske globine in vzeli kosinusno porazdelitveno funkcijo za parametre z neenakomerno porazdelitvijo vredno-

sti. V viru [14] so se posvetili skoraj izključno primeru s povprečno usmeritvijo delcev v smeri osi z. V tem primeru se ugotovitve v obeh raziskavah ujemajo, tj. perkolacijski prag pada z večanjem vrednosti naslednjih parametrov: relativne penetracijske globine, razmerja dimenzij paličk in kota odstopanja smeri posameznih delcev od povprečne smeri. Absolutna razlika v izidih za perkolacijski prag v obeh delih je 1 % ali 2 %, kar je v okviru statistične napake. Sam sem dodal še primerjavo z izotropno porazdelitvijo, obravnaval sem tudi različne povprečne smeri delcev.

4. Sklep

V prispevku v glavnem obravnavam delce v obliki valjev s krogelnima kapicama, ker:

a) je postopek za ugotavljanje sekanja sosednjih delcev dovolj preprost,
b) imajo paličke dovolj fizikalno zanimivih parametrov,
c) so že bili narejeni podobni računi [12, 13, 14], kar omogoča primerjavo rezultatov in preverbo,
č) je v resnici mogoče izdelati podobne prevodne delce v keramični matriki.

Moji rezultati se v glavnih točkah ujemajo z virom [14], po drugi strani pa sem bolj poudaril nekaj točk problema, npr. razliko med urejenimi in neurejenimi sistemi.

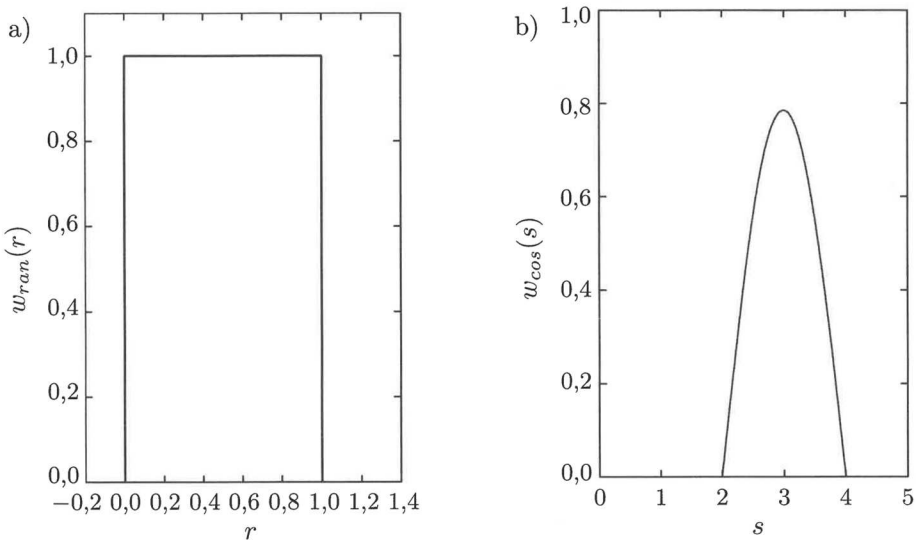
Poleg paličk (sferocilindrov) sem obravnaval tudi okrogle in ploščate prevodne delce. Opisano delo je šele prvi korak k razumevanju zapletenih struktur v keramičnih plastovitih kompozitih [18, 19].

5. Matematična priloga

5.1 Porazdelitev naključnih spremenljivk

Za naključna števila r (angl. r = random number) med 0 in 1 sem uporabljal generator naključnih števil z enakomerno porazdelitveno funkcijo $w_{ran}(r) = 1$ na intervalu (0,1) (slika 7a). Preveril sem kvaliteto generatorja, npr. z nekaj parametri, kot je povprečje, povprečje kvadratov itd. Enakomerno porazdeljene naključne spremenljivke dobimo iz števil r preprosto. Na primer, naključno koordinato delca x, ki naj leži v intervalu $0 < x < L_x$, izračunamo kot $x = L_x \cdot r$. Podobno izračunamo npr. relativni azimutalni kot: $\varphi_R = 2\pi \cdot r$ (v radianih), če je popolnoma neurejen, itd.

Za delno urejene naključne spremenljivke (npr. kote in velikosti delcev) z dovoljenimi vrednostmi na izbranem intervalu sem vedno uporabljal kosinusno porazdelitev, s katero je računanje dovolj preprosto (slika 7b). Na



Slika 7. Enakomerna naključna porazdelitev in zgled kosinusne verjetnostne porazdelitve. Obe porazdelitvi sta normirani, tako da je ploščina med grafom in vodoravno osjo enaka 1.

primer, porazdelitev premera d valjev, ki naj ima vrednosti na intervalu $d_{pov} - \sigma_d < d < d_{pov} + \sigma_d$, je opisana s funkcijo

$$w_{cos}(d) = \frac{\pi}{4\sigma_d} \cos\left(\frac{\pi}{2\sigma_d}(d - d_{pov})\right).$$

To porazdelitev dobimo iz porazdelitve w_{ran} z enačbo, ki povezuje spremenljivki r in d:

$$d = d_{pov} + \frac{2\sigma_d}{\pi} \arcsin(2r - 1).$$

Kot sem že omenil, dobimo izotropno porazdelitev smeri paličk v prostoru z naslednjima porazdelitvenima funkcijama za kota: $w_{cos}(\theta) = \frac{\pi}{4\sigma_\theta} \cdot \cos\left(\frac{\pi}{2\sigma_\theta}(\theta - \theta_{pov})\right)$ in $w(\varphi) = \frac{1}{2\pi}$, kjer je $\theta_{pov} = \sigma_\theta = \frac{\pi}{2}$. Kot vidi bralec, lahko porazdelitveno funkcijo za polarni kot zapišemo enostavneje kot sinusno funkcijo. Napačno bi bilo vzeti enakomerno porazdelitev za polarni kot, saj bi bile s tem gosteje zastopane smeri okrog osi z.

Namesto kosinusne porazdelitvene funkcije bi bila primerna tudi uporaba Gaussove porazdelitvene funkcije, za katero obstajajo učinkovite numerične metode, saj nimamo neposredne analitične zveze med enakomerno in Gaussovo porazdelitvijo.

5.2 Povprečna in naključna usmeritev paličastih delcev

V primeru paličk si lahko mislimo vektor povprečne usmerjenosti delcev $\vec{e}_{pov}$ kot smerni vektor osi z novega koordinatnega sistema, zavrtenega za kot θ_L okrog osi y laboratorijskega sistema. Glede na zavrteni sistem opredelimo relativna orientacijska kota θ_R in φ_R za posamezen delec. Tako lahko zapišemo komponente vektorja $\vec{k}$ v obeh koordinatnih sistemih (bazne vektorje v laboratorijskem sistemu označimo z $\vec{e}_x$, $\vec{e}_y$ in $\vec{e}_z$, tiste v zavrtenem sistemu pa s $\vec{f}_x$, $\vec{f}_y$ in $\vec{f}_z$):

$$\begin{aligned}\vec{k} &= \sin\theta\cos\varphi\vec{e}_x + \sin\theta\sin\varphi\vec{e}_y + \cos\theta\vec{e}_z = \\ &= \sin\theta_R\cos\varphi_R\vec{f}_x + \sin\theta_R\sin\varphi_R\vec{f}_y + \cos\theta_R\vec{f}_z\,.\end{aligned}$$

Če upoštevamo še smeri novih baznih vektorjev: $\vec{f}_x = \cos\theta_L\vec{e}_x - \sin\theta_L\vec{e}_z$, $\vec{f}_y = \vec{e}_y$, $\vec{f}_z = \sin\theta_L\vec{e}_x + \cos\theta_L\vec{e}_z$, lahko direktno izračunamo komponente vektorja $\vec{k}$ v laboratorijskem sistemu za posamezen delec:

$$\begin{aligned}\vec{k} = (&\cos\theta_L\sin\theta_R\cos\varphi_R + \sin\theta_L\cos\theta_R, \sin\theta_R\sin\varphi_R, \\ &\sin\theta_L\sin\theta_R\cos\varphi_R + \cos\theta_L\cos\theta_R)\,.\end{aligned}$$

5.3 Sekanje preprostih geometrijskih teles

Delci v tem prispevku so sestavljeni iz preprostih geometrijskih teles: polkrogel in valjev, tako da se da analitično ugotoviti, ali se med seboj sekajo. Na primer, za preverbo sekanja dveh valjev najprej ugotovimo najbližjo razdaljo med njunima geometrijskima osema, ki sta med seboj mimobežni itd. Maksimalno relativno penetracijsko globino (MRPG) vzamemo glede na polmer R valjev. Penetracijsko globino izračunamo kot $g_{pen} = R_1 + R_2 - d$, pa naj gre za sekanje dveh polkrogel, polkrogle in valja ali dveh valjev. Pri tem sta R_1 in R_2 radija polkrogel ali valjev, d pa v vseh treh primerih izračunamo drugače:

1) za dve polkrogli je to razdalja med njunima središčema,
2) za kroglo in valj vzamemo za d najbližjo razdaljo med središčem krogle in osjo valja,
3) za dva valja vzamemo za d najbližjo razdaljo med osema valjev – mimobežnicama.

Morda bo bralec pomislil, da nam morebitno sekanje končnih valjev na njunih robovih (sekanje osnovnih ploskev) povzroča težave; vendar pa tega ni treba računati, saj gre v tem primeru tako in tako za sekanje krogelnih kapic na konceh paličk. S tako izračunano udorno globino g_{pen} preverjamo, ali ni penetracija dveh delcev pregloboka.

LITERATURA

[1] A. L. Efros in B. Shklovskii, *Critical Behaviour of Conductivity and Dielectric Constant near the Metal/Non-Metal Transition Threshold*, Phys. Stat. Sol. **76**, 475 (1976).

[2] D. Lisjak, I. Zajc, M. Drofenik in J. Jamnik, *Investigation of the PTCR Effect in ZnO-NiO Two-Phase Ceramics*, Solid State Ionics **99**, 125 (1997).

[3] D. Lisjak, M. Drofenik in D. Kolar, *Composite Ceramics with a Positive Temperature Coefficient of Electrical Resistivity Effect*, J. Mater. Res. **15**, 417 (2000).

[4] A. A. Gusev in O. A. Guseva, *Voltage Breakdown in Random Composites*, Adv. Eng. Mater. **5**, 713 (2003).

[5] D. J. Bergman in Y. Imry, *Critical Behavior of the Complex Dielectric Constant near the Percolation Threshold of Heterogeneous Materials*, Phys. Rev. Lett. **39**, 1222 (1977).

[6] D. M. Grannan, J. C. Garland in D. B. Tanner, *Critical Behavior of the Dielectric Constant of a Random Composite near the Percolation Threshold*, Phys. Rev. Lett. **46**, 375 (1981).

[7] F. Lux, *Review: Models Proposed to Explain the Electrical Conductivity of Mixtures Made of Conductive and Insulating Materials*, J. Mater. Sci. **28**, 285 (1993).

[8] J. Quintanilla, S. Torquato, R. M. Ziff, *Efficient Measurement of the Pecolation Threshold for Fully Penetrable Discs*, J. Phys. A **33**, L339 (2000).

[9] C. D. Lorenz in R. M. Ziff, *Precise Determination of the Critical Percolation Threshold for the Three-dimensional "Swiss Cheese" Model Using a Growth Algorithm*, J. Chem. Phys. **114**, 3659 (2001).

[10] G. E. Pike in C. H. Seager, *Percolation and Conductivity: A Computer Study*, Phys. Rev. B **10**, 1421 (1974).

[11] I. Balberg in N. Binenbaum, *Computer Study of the Percolation Threshold in a Two-dimensional Anisotropic System of Conducting Sticks*, Phys. Rev. B **28**, 3799 (1983).

[12] I. Balberg, N. Binenbaum in N. Wagner, *Percolation Thresholds in the Three-Dimensional Sticks System*, Phys. Rev. Lett. **52**, 1465 (1984).

[13] I. Balberg, C. H. Anderson, S. Alexander in N. Wagner, *Excluded Volume and its Relation to the Onset of Percolation*, Phys. Rev. B **30**, 3933 (1984).

[14] S. De Bondt, L. Froyen in A. Deruyttere, *Electrical Conductivity of Composites: A Percolation Approach*, J. Mater. Sci. **27**, 1983–1988 (1992).

[15] O. Husby, J. F. Thovert in P. M. Adler, *Geometry and Topology of Fracture Systems*, J. Phys. A **30**, 1415 (1997).

[16] M. Sahimi, *Heterogeneous Materials*, Vol. 1, Springer (1984).

[17] D. Kolar, *Tehnična keramika*, ZRSŠŠ (1993).

[18] A. Dakskobler, *Keramični kompoziti s trakasto mikrostrukturo*, Doktorska disertacija, Univerza v Ljubljani (2002).

[19] M. Leverkoehne, A. Dakskobler, M. Valant, R. Jansen, T. Kosmač, *Cr-Al_2O_3 Layered Composites with a High Electrical Anisotropy Prepared by Repeated Deformation Processing*, J. European Ceramic Soc., v tisku (2004).

VABILO NA STROKOVNO SREČANJE, 4. KONFERENCO FIZIKOV V OSNOVNIH RAZISKAVAH IN 56. OBČNI ZBOR

Društvo matematikov, fizikov in astronomov Slovenije vabi svoje članice in člane na 56. občni zbor Društva matematikov, fizikov in astronomov Slovenije, na *4. konferenco fizikov v osnovnih raziskavah* in na izobraževalni seminar *Delo z nadarjenimi otroki in mladostniki.*

Izobraževalni seminar Delo z nadarjenimi otroki in mladostniki

Seminar se bo pričel v petek, 12. 11., ob 9. uri (registracija ob 8.30) in končal v soboto, 13. 11. 2004, v popoldanskih urah, potekal pa bo v Cerknem v *Hotelu Cerkno.* Natančnejši urnik je objavljen na spletni strani DMFA Slovenije (`http://www.dmfa.si/`), na programu pa so naslednji prispevki:

Stane Arh,	Dodatne aktivnosti nadarjenih učencev pri matematiki in fiziki
Jožko Battestin,	Zbirka poskusov iz optike
Claudio Battelli,	Projekt DUO–DUM: pot za spodbujanje in razvoj nadarjenih
Maja Rakun Beber,	Matematika drugače
Jana Draksler,	Delo z nadarjenimi učenci
Darjo Felda,	Pravokoten trikotnik ter včrtana in pričrtane krožnice
Stanislav Južnič,	Ivo Lah, pionir slovenske uporabne matematike
Marija Kavkler,	Nadarjeni učenci s specifičnimi učnimi težavami pri matematiki
Boris Kham,	Astronomski tabor in pouk
Jan Makarovič,	Spodbude in možnosti: paradoks ustvarjalnega okolja
Zlatan Magajna,	Računalniško generirani odprti geometrijski problemi
Marija Pavčnik,	Fizika potapljanja
Gorazd Planinšič,	Primeri aktivnega učenja ob poskusih
Marijan Prosén,	Slovenska astronomija skozi stoletja, Keplerjeva enačba in Jurij Vega (poster)
Marko Razpet,	Nekaj primerov kombinatoričnega preštevanja Grb Franca Močnika (poster)
Nada Razpet,	Prekrivanja Razvedrilna fizika
Barbara Rovšek,	Primeri napačnega dojemanja fizikalnih pojmov in konceptov
Janez Strnad,	Poročilo o drami Carla Djerassija *Calculus*
Milena Strnad,	Učiteljeva popotnica v devetletno osnovno šolo
Nataša Vaupotič,	Poskusi iz toplote

Lucija Željko,	Reševanje matematičnih problemov in branje
Matjaž Željko,	Kaj imata skupnega Steiner in Soddy?
Jurij Bajc, Gorazd Planinšič ter študentje FMF in PeF,	Verižni eksperiment

V okviru strokovnega srečanja boste lahko poslušali vabljeni predavanji prejemnikov Zoisovega priznanja za znastvenoraziskovalno delo za leto 2003:

Janez Bonča,	Termodinamske lastnosti frustriranih spinskih sistemov
Tomaž Košir,	Problemi lastnih vrednosti v več parametrih

Nekateri prispevki bodo predstavljeni hkrati vsem udeležencem, drugi pa bodo izvajani vzporedno (ločitev matematičnih in fizikalnih prispevkov).

Hotelske storitve si morajo udeleženci seminarja rezervirati sami najkasneje do 30. oktobra (Hotel Cerkno, Sedejev trg 8, 5282 Cerkno; telefon: (05) 3743 400 ali (031) 858 876 (Majda Rojc), telefaks: (05) 3743 433, elektronska pošta: Hotel.Cerkno@siol.net). Pri prijavi navedite, da se prijavljate na seminar DMFA. Več o hotelu si lahko preberete na njihovi strani http://www.hotel-cerkno.si/.

4. konferenca fizikov v osnovnih raziskavah

Predstavitve in predavanja v okviru konference bodo v petek, 12. novembra 2004, v *Hotelu Cerkno* v Cerknem. Srečanje organizira Nacionalni komite za fiziko pri Društvu matematikov, fizikov in astronomov Slovenije s podporo Fakultete za matematiko in fiziko, Ministrstva za šolstvo, znanost in šport ter Instituta „Jožef Stefan“.

Namen 4. konference fizikov v osnovnih raziskavah je nadaljevati redna srečanja slovenskih fizikov, ki delujejo na različnih področjih osnovnih raziskav. V okviru srečanja želimo predstaviti predvsem raziskovalno delo uspešnih raziskovalcev mlajše generacije, ki so doktorirali v zadnjem obdobju ali so tik pred doktoratom.

Letos bodo prvič na srečanju sodelovali tudi študenti 3. in 4. letnika študija fizike na FMF. Na konferenci bodo predstavljeni prispevki v naslednjih oblikah:
- 30-minutna vabljena predavanja
- 20- in 15-minutna predavanja
- plakati

Raziskovalna področja, ki bodo predstavljena na 4. konferenci fizikov v osnovnih raziskavah:
- teorija in eksperimentalna fizika trdne snovi
- statistična fizika
- molekularna fizika
- fizika površin in nanostruktur

- fizika tekočih kristalov, mehke kondenzirane materije in biofizika
- astronomija
- teorija osnovnih delcev
- eksperimentalna fizika osnovnih delcev
- fizika nizkih in srednjih energij
- reaktorska fizika

Konferenčni razpored:

7.30	odhod avtobusa izpred stavbe FMF, Jadranska 19, registracija na avtobusu
10.00–13.00	predavanja, vmes odmor s kavo in čajem
13.00–15.00	kosilo, proste aktivnosti (bazen)
15.00–17.00	predavanja, odmor s kavo in čajem
17.00–20.30	ogled plakatov, postrežba s čajem in kavo
20.30–23.30	večerja, družabni večer
23.30	odhod avtobusa v Ljubljano

Peter Petek in Igor Muševič

VABILO

Društvo matematikov, fizikov in astronomov Slovenije vabi na januarski (2005) seminar

Stoletje fizike – najpomembnejša odkritja.

Seminar bo na Fakulteti za matematiko in fiziko v Ljubljani, Jadranska ulica 19. Teme:

dr. Jurij Bajc,	Svetovno leto fizike (1 ura)
dr. Anže Slosar,	Od klasične do relativistične mehanike (2 uri)
prof. dr. Igor Poberaj,	Laserji (2 uri)
doc. dr. Gorazd Planinšič,	Moderna fizika v poskusih (3 ure)
doc. dr. Tomaž Podobnik,	Osnovni delci (2 uri)
prof. dr. Anton Ramšak,	Od polprevodnikov do superprevodnikov (2 uri)
doc. dr. Denis Arčon,	Nanomateriali (2 uri)
doc. dr. Primož Ziherl,	Biološke strukture pod rentgenskim žarometom (2 uri)

Predvidena kotizacija je 12.000 SIT na udeleženca. Člani DMFA Slovenije imajo 50 % popusta. Podrobnejše obvestilo bo objavljeno na domači strani DMFA (`http://www.dmfa.si/`).

Koordinatorja seminarja:
Žiga Šmit in Denis Arčon

OBZORNIK ZA MATEMATIKO IN FIZIKO
Letnik 51, številka 5
ISSN 0473–7466, UDK 51 + 52 + 53

VSEBINA

Članki **Strani**

Reed-Solomonove kode, Aleksandar Jurišić in Arjana Žitnik 129–143

Numerična analiza perkolacijskega praga prevodnosti v kermetih, Milan Ambrožič 144–158

Vesti

Vabilo na strokovno srečanje, 4. konferenco fizikov v osnovnih raziskavah in 56. občni zbor, Peter Petek in Igor Muševič 159–XIX

Vabilo, Žiga Šmit in Denis Arčon XIX

CONTENTS

Articles **Pages**

Reed-Solomon Codes, Aleksandar Jurišić and Arjana Žitnik 129–143

Numerical Analysis of Percolation Threshold in Cermets, Milan Ambrožič 144–158

News 159–XIX

Na naslovnici je planet Saturn, kot ga je 7. maja 2004 z oddaljenosti 28,2 milijonov km posnela vesoljska sonda Cassini. Podrobnejše slike planeta in njegovih lun si lahko ogledate na spletnem naslovu `http://ciclops.lpl.arizona.edu/`.