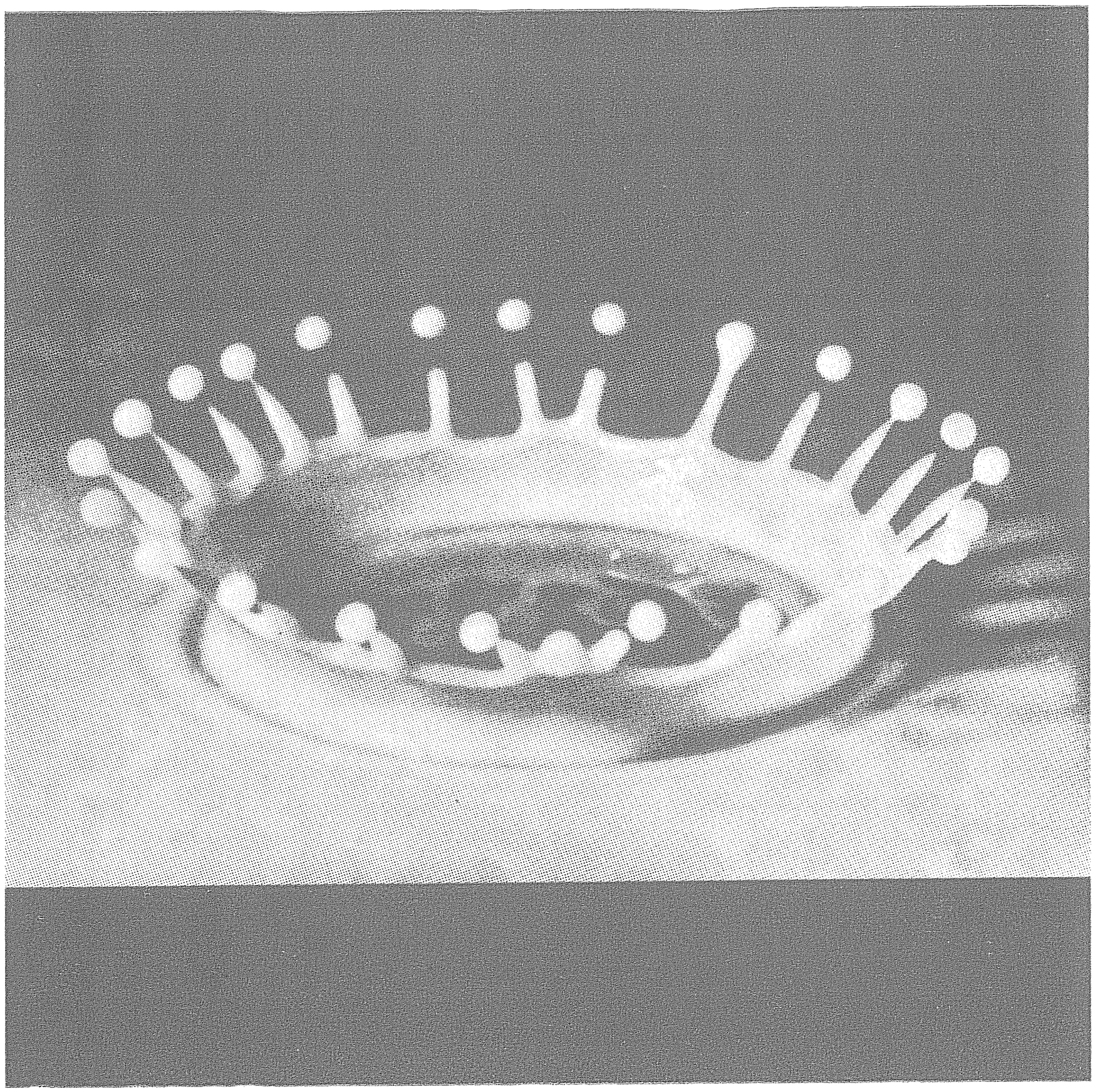
IZDAJA DRUŠTVO MATEMATIKOV, FIZIKOV IN ASTRONOMOV SR SLOVENIJE

OBZORNIK ZA MATEMATIKO IN FIZIKO



1978
Letnik 25
4

LETNIK 25. — ŠTEVILKA 4

OBZORNIK ZA MATEMATIKO IN FIZIKO

LJUBLJANA, JULIJ 1978

Glavni in odgovorni urednik: Janez Strnad.

Uredniški odbor: France Avsec, gimnazija Kranj; Robert Blinc, FNT; Alojz Kodre, FNT; France Kvaternik, tehniška šola za lesarstvo, Ljubljana; Peter Legiša, FNT; Jože Lep, VTŠ, Maribor; Anton Moljk, FNT; Mitja Rosina, FNT; Tomaž Skulj, gimnazija Moste, Ljubljana; Janez Strnad (urednik za fiziko), FNT; Anton Suhadolc (urednik za matematiko), FNT; Ciril Velkovrh (urednik), FNT; Ivan Vidav, FNT; jezikovni pregled Marija Janežič, inštitut za slovenski jezik SAZU. Slike je narisal Marjan Turk.

Naročnina: za posameznike 170.— din (za člane društva je že vračunana članarina), za dijake in študente 80.— din, za ustanove in podjetja 215.— din, za tujino 15 $ = 270.— din, posamezna številka 30.— din, dvojna številka 60.— din.

Dopise pošiljajte in list naročajte na naslov: **Komisija za tisk DMFA SRS**, 61001 Ljubljana, Jadranska c. 19, p. p. 227, tel. št. 265-061/53, žiro račun 50101-678-48363, devizni račun pri Ljubljanski banki 32009-007-900.

Tiska tiskarna Ljudske pravice v Ljubljani, Kopitarjeva ul. 2. Naklada 1500 izvodov.

Izdajo revije sofinancirata Izobraževalna skupnost Slovenije in Raziskovalna skupnost Slovenije.

YU ISSN 0473-7466

VSEBINA

Članki

Nekaj o kriptografskih metodah (Jure Zupan) 129

Mikroskopična slika površinske napetosti (Marjan Hribar) 137

Šola

Posvetovanje o matematiki in fiziki v reformirani šoli (Martina Koman, Anton Moljk, Stanko Uršič, Aleksander Kregar, Marija Munda, France Perne, Franc Galič, Anton Moljk) 144

Vprašanja (112 — Dušan Repovš) 151

Domače vesti

Poročilo o seminarju Matematična logika (Martina Koman) 152

Obvestilo (Martina Koman) 153

Deseto zvezno tekmovanje študentov matematike (Mirko Dobovišek) 154

Razmišljanje o tekmovanju iz matematike (Ciril Velkovrh) 157

Prejeli smo v oceno (Jože Vrabec, Peter Legiša, Tomaž Pisanski, Gabrijel Tomšič, Zvonimir Bohte, Janez Strnad, Tomaž Slivnik, Jože Grasselli) 158

Nove knjige (Zvonimir Bohte) 136

CONTENTS

Articles

On cryptography methods (Jure Zupan) 129

Microscopic theory of surface tension (Marjan Hribar) 137

School 144

Questions 151

Home news 152

Reviews 158

New books 136

Na ovitku: Fotografija kapljice mleka, ki je padla na trdno podlago in se na njej razbila. Pojav je v podrobnostih prav zapleten, pri nastanku drobnih kapljic pa ima odločilno vlogo površinska napetost. Edgertonova fotografija je posneta po knjigi F. W. Sears, M. W. Zemansky, *College Physics*, Reading, Mass., Addison-Wesley 1960, str. 259.

Obzornik mat. fiz. 25 (1978) 4

NEKAJ O KRIPTOGRAFSKIH METODAH

JURE ZUPAN

AMS Subj. Class. (1970) 10A25, 20A30, 68A20

Opisanih in razloženih je nekaj metod, ki se uporabljajo za šifriranje podatkov in sporočil. Navedena in obravnavana so merila za kvaliteto šifrirnih algoritmov ter smernice za razvoj modernih kriptografskih metod z računalniki.

ON CRYPTOGRAPHY METHODS

Some simple cryptography methods and algorithms, together with the directions of the recent development in the field of modern computer cryptography are explained and discussed.

Uvod

Z nedavnim prodorom računalniške tehnologije na skoro vsa področja gospodarstva, sociologije, politike, vojske ter še marsikam, se je predvsem povečal pretok podatkov med posameznimi avtomatiziranimi enotami. Varovanje zaupnosti, točnosti in avtentičnosti poslanih ali sprejetih podatkov je postala osnovna zahteva vseh uporabnikov. Varnost vsebine podatkov ni samo stvar vojaškega ali političnega pomena, prav tako se tiče bank, industrijskih obratov in laboratorijev, trgovskih mrež, patentnih pisarn, zasebnih telefonskih pogovorov ter še mnogo drugih uporabnikov, sodobnih komunikacijskih sistemov [1].

Poleg zaščite vsebine, ki je nedvomno najpomembnejši dejavnik vsakega šifrirnega sistema, obstaja še problem, ki je navadno odrinjen, a ni zaradi tega nič manj važen, to je avtentičnost podatkov. Avtentično je sporočilo s posebnim »pečatom« odpošiljatelja, ki prejemniku nedvomno dokazuje, da je bilo poslano s pravega naslova. Lahko se zgodi, da je vsebina manj pomembna kot izvor. Avtentičnost podatkov je problem pri letaliških radarjih zelo obremenjenih letališč, kjer je natančno določanje izvora informacij bistveno — da o vojaških potrebah niti ne govorimo.

Seveda so na voljo tudi bolj preprosti in vsakdanji primeri, pri katerih je zaščita podatkov nujna. Vzemimo samo srednje velik računalnik, ki ga skupno uporablja nekaj ljudi. Vse njihove datoteke morajo biti načelno zaščitene pred nedovoljenim kopiranjem, spreminjanjem ali kaki drugačni zlorabi. Še bolj morajo biti zaščiteni statistični podatki, npr. o bolnikih in njihovih boleznih v bolnicah, življenjepisi in podobno.

Pri vsesplošnem naraščanju zmogljivosti računalniške tehnologije seveda ne smemo pozabiti, da postaja tudi odkrivanje šifer vedno lažje. Postavlja se vprašanje, kdo bo zmagal v tej tekmi? Če predpostavljamo, da pri ogromni množici šifriranih podatkov nikakor ne moremo zahtevati, da ostanejo vsa šifrirana sporočila večno tajna, moramo istočasno postaviti zahtevo, da mora biti šifrirni algoritem sestavljen tako, da se ga ne da razkriti, tudi če je na voljo poljubno dolg šifriran tekst z znano vsebino.

Če sedaj na hitro strnemo, kar smo povedali, dobimo naslednje zahteve, ki jim mora ustrezati sodoben kriptografski sistem oz. postopek:

— šifrirni algoritem mora biti tak, da ga z najhitrejšimi znanimi algoritmi in z najsodobnejšo računalniško opremo ne moremo »zlomiti« v doglednem času (npr. v 1000 letih);
— algoritem mora biti nerešljiv tudi pri predpostavki, da poznamo poljubno dolg šifrirani tekst in
— šifrirano sporočilo mora biti avtorizirano, vsebovati mora avtorjev »pečat«.

Vsem tem zahtevam nikakor ni lahko ustreči in šele v zadnjih letih (1976/77) se je z deli Diffieja in Hellmana [2] ter Rivesta [3] pokazala realna možnost, da bi v tem uspeli.

Substitucijske šifre

Sem sodijo vsi šifrirni sistemi, ki zamenjujejo posamezne črke znanega teksta z drugimi znaki v skladu z naprej določenimi pravili ali ključem. Če so ti drugi znaki zopet črke abecede (to pot seveda z drugim pomenom) ni tajnost šifre nič manjša, znatno pa se olajša prenos šifriranega teksta z računalniki ali teleprinterji.

Med najbolj preproste substitucijske metode sodi nedvomno monoalfabetska substitucija s cikličnim premikom črk, znana pod imenom Cezarjeva šifra [1], [4]. Ključ **K** je v tem primeru ciklični premik vrste števil:

$$0, 1, 2, 3, 4, \ldots\ldots 23, 24, 25,$$

ki ustrezajo 26 znakom naše abecede:

presledek, A, B, C, Č, ... V, Z, Ž.

Če *i-ti* znak teksta označimo s $t(i)$, ustrezni šifrirani znak pa z $x(i)$, lahko šifrirni in dešifrirni postopek s Cezarjevo šifro napišemo v obliki:

$$\text{šifriranje:} \quad x(i) = (t(i) + \mathbf{K}) \bmod 26 \qquad (1\,a)$$

$$\text{dešifriranje:} \quad t(i) = (x(i) - \mathbf{K}) \bmod 26 \qquad (1\,b)$$

Pri tem smo funkcijo x mod y definirali kot:

$$x \bmod y = x - y \,.\, \lfloor x/y \rfloor$$

Znak $\lfloor a \rfloor$ pomeni največje celo število, ki je še manjše od a.

Čeprav je Cezarjeva šifra izredno preprosta in lahko zlomljiva, saj ne izpremeni frekvenčne porazdelitve znakov znanega teksta, ampak jo samo ciklično premakne, je zanimiva zaradi osnovnega pristopa, ki se v izboljšani obliki uporablja tudi pri teže rešljivih polialfabetskih substitucijah.

Osnovni način šifriranja s polialfabetsko substitucijo je podan v tabeli I za primer ključa s tremi črkami. To je 3-črkovna substitucija, kjer je ključ beseda »TRI«.

Ključ **K** v tem primeru ni konstanta, ampak končna množica $\{\mathbf{K}\}$ p elementov $k(i)$, $i = 0, 1, 2, \ldots p-1$. Izraza (1 a) in (1 b) se ustrezno spremenita:

$$x(i) = (t(i) + k(i \bmod p)) \bmod 26 \qquad (2\,a)$$

$$t(i) = (x(i) - k(i \bmod p)) \bmod 26 \qquad (2\,b)$$

Polialfabetska substitucija ali z drugim imenom Vigenerova šifra je tem teže rešljiva, čim večji je p, oz. čim daljši je ključ $\{\mathbf{K}\}$. Tuckerman [5] je pokazal, da je Vigenerova šifra vedno rešljiva, če imamo na voljo najmanj $20\,p$ znakov šifriranega teksta. Če je:

TABELA I

Šifriranje s 3-črkovno substitucijo. Ključ je beseda »TRI«.

Sporočilo	Ključ	Šifriranje	Šifra
O 16	T 21	(16 + 21) mod 26 = 37 mod 26 = 11	11 J
B 2	R 18	(2 + 18) mod 26 = 20 mod 26 = 20	20 Š
Z 24	I 10	(24 + 10) mod 26 = 34 mod 26 = 8	8 G
O 16	T 21	(16 + 21) mod 26 = 37 mod 26 = 11	11 J
R 18	R 18	(18 + 18) mod 26 = 36 mod 26 = 10	10 I
N 15	I 10	(15 + 10) mod 26 = 25 mod 26 = 25	25 Ž
I 10	T 21	(10 + 21) mod 25 = 31 mod 26 = 5	5 D
K 12	R 18	(12 + 18) mod 26 = 30 mod 26 = 4	4 Č

a) perioda p daljša od teksta

b) ključ $\{\mathbf{K}\}$ uporabljen samo enkrat in

c) znani tekst ne pride v roke dešifrantu,

je Vigenerova šifra teoretično nerešljiva [6] in se imenuje Vermanov sistem. Vernamov sistem se veliko uporablja za prenos izjemno važnih informacij. Ker morata potovati šifrirani tekst in ključ do prejemnika po dveh ločenih poteh, je šifra za široko uporabo zelo neprikladna.

Ideja, ki se ponuja sama od sebe, je konstrukcija neskončno dolgega ključa $\{\mathbf{K}(i)\}$, $i \to \infty$. Za to je navadno potreben generator slučajnostnih števil (GSS). Dobri algoritmi za izračun slučajnostnih števil ne dajo samo števil, ki so »slučajnostno« porazdeljene med 1 in neko maksimalno vrednostjo m, ampak poleg tega generirajo vsa ta števila, preden se ponove, na tak način, da je videti izbor slučajnosten. Algoritma, ki generira dovolj dolgo vrsto slučajnostnih števil — v praksi jo lahko imenujemo »neskončna« — nikakor ni lahko konstruirati [7]. Knuth [7] je pokazal, da generira linearni GSS v obliki:

$$\mathbf{T}(i + 1) = (\mathrm{a}\mathbf{T}(a) + c) \bmod m \tag{3}$$

vrsto s periodo $m = 2^k$ takrat in le takrat, ko je c lih in $a \bmod 4 = 1$. Vrednost $\mathbf{T}(0)$ imenujemo kal generatorja. Ker je k navadno izbran tako, da je malo manjši od števila bitov v računalniški besedi, je vrsta $\mathbf{T}(i)$, preden se začne ponavljati, zelo dolga. S 60-bitno besedo naredimo lahko 10^{19} elementov dolgo »slučajnostno« vrsto, preden se začne ponavljati.

V tabeli II so podane frekvenčne porazdelitve nekaj manj kot 2600 znakov dolge Prešernove Turjaške Rozamunde, kodirane s Cezarjevo ($\mathbf{K} = 2$), 3-črkovno (ključ »TRI«) in »neskončno« dolgo [6, 8, 9] substitucijo. V zadnjem stolpcu je za primerjavo podana še frekvenčna porazdelitev 100 000 enakih znakov (presledkov), šifriranih z algoritmom [6, 8, 9]. Teoretično enakomerno porazdelitev 26 znakov je 3,85 % na znak in se, kot je razvidno iz tabele II, precej dobro ujema s porazdelitvijo črk kriptograma. Za primerjavo so v tabeli III navedeni še prvi 4 verzi omenjene pesmi, kodirane na vse tri načine.

Še namig za dešifriranje 3-črkovne substitucije: vsota frekvenc črk T, R in I (tabela II, stolpec 4) je natanko enaka frekvenci presledka pri znanem tekstu (stolpec 2, 3,56 + 7,19 + 6,57 = 17,32).

TABELA II.

Frekvenčne porazdelitve črk Prešernove Turjaške Rozamunde, šifrirane na tri različne načine. Število vseh znakov (s presledki, a brez ločil) je 2565.

Znak	Znani tekst	Cezarjeva šifra	3-črkovna substitucija	Algoritem [6, 8, 9] Rozamunda	100 000 presledkov
presl.	17,32	1,52	4,81	4,03	3,76
A	8,01	0,86	1,92	4,81	3,77
B	1,92	17,32	3,83	4,15	3,91
C	0,63	8,01	2,78	3,09	3,96
Č	1,29	1,92	3,87	4,07	3,83
D	2,97	0,63	3,40	3,25	3,91
E	11,02	1,29	2,89	3,87	3,88
F	0,00	2,97	3,21	3,87	3,69
G	1,41	11,02	3,36	4,11	3,79
H	1,06	0,00	7,74	3,91	3,81
I	5,00	1,41	6,57	3,68	3,82
J	4,50	1,06	3,82	3,95	3,84
K	2,93	5,00	3,05	3,40	3,72
L	3,56	4,50	2,81	3,56	3,86
M	2,03	2,93	2,27	3,76	3,85
N	4,65	3,56	5,55	3,83	3,96
O	7,23	2,03	1,65	3,64	3,93
P	2,46	4,65	2,19	4,34	3,79
R	5,08	7,23	7,19	3,99	3,90
S	4,30	2,46	4,65	4,34	3,93
Š	1,60	5,08	7,35	3,91	3,79
T	3,52	4,30	3,56	3,87	3,86
U	1,95	1,60	2,19	3,72	3,80
V	3,17	3,52	1,64	3,99	3,86
Z	1,52	1,95	5,43	3,17	3,88
Ž	0,86	3,17	3,21	3,68	3,88

Šifra DES (Data Encription Standard)

Leta 1973 je NBS (National Bureau of Standards) pripravil smernice [6] za izdelavo standardnega šifrirnega algoritma katerega tajnost naj ne bi bila odvisna od tajnosti algoritma, pač pa od ključa, ki bi dajal toliko možnosti, da ga ne bi bilo mogoče odkriti, če bi hotel preizkusiti vse možnosti. Smernice so vsebovale tudi stališče, da mora biti algoritem dostopen vsem zainteresiranim uporabnikom. Po dveh letih je bil v *Federal Register* [10], [11] objavljen ustrezni algoritem, za katerega avtorji trdijo, da ustreza vsem sodobnim zahtevam uporabnikov in tudi zahtevam NBS.

Algoritem DES deluje na 64-bitnem (2 32-bitni besedi) bloku teksta (8 ASCII-1968 8-bitnih znakov) in ga v skladu s 56-bitnim ključem predela v 64-bitni blok kodiranega teksta.

Morda bolj zanimive kot sam algoritem DES so bile reakcije in kritike, ki jih je sprožila njegova objava v *Federal Register*. Najbolj očitno je bilo

TABELA III.

Prvi štirje verzi Turjaške Rozamunde (*a*), kodirani s tremi šiframi: (*b*) Cezarjeva šifra, (*c*) 3-črkovna substitucija in (*d*) algoritem (6, 8, 9).

a	HRAST STOJI V TURJAŠKEM DVORU
b	JŠCTVBTRLVKBŽBVZŠLCUMGOBFŽRŠZB
c	CIILLHLLŽDBHPRČOIŠTKT EHŽNŽKMH
d	CTJUATL OČGLJŽPŽ IAFUŽ CJOGSRA
a	VRH VZDIGUJE SVOJ V OBLAKE
b	ŽŠJBŽ FKIZLGBTŽRLBŽBRČCNMGB
c	PIRŠNFŽBPOCNŠJEICHPRŽUDIEZH
d	AJACTCATŠSDFŠOTASPFNŠSC EDO
a	V SENCI PRI KAMNITNI MIZI
b	ŽBTGPDKBSŽKBMCOPKVPKBOK KB
c	PRB FKČR KBHESVHBČHBHGBRBA
d	MOŠBRVFIKIHRFJVHŽCBKCBTOFM
a	ZBOR SEDI GOSPODE ŽLAHTNE
b	ČRŠBTGFKBIRTSRFGBANCJVPGB
c	RŠŽKRB VSŠ ŽLHŽŽZHSDICZL R
d	LČN AJALPOSEKŽVVSŠIABTČDNK

predvsem, da stoji za algoritmom IBM, ki je s tem zopet dosegel eno od prednosti pri boju za tržišče.

Firme v ZDA, ki bodo vgrajevale šifrirni software v svojo opremo, bodo »vezane« na 32-bitni blok, kar je seveda v prid IBM. Drugi, bolj resni ugovor pa zadeva zlomljivost šifre. Marca 1976 sta Diffie in Hellman [12] kritično vzela v pretres izbiro 56-bitnega ključa in postavila vprašanje, zakaj je prišlo do te odločitve, ko bi 94 ali 128-bitni ključ z gotovostjo pokopal vse upe dešifrantov. Sestavila sta predračun hipotetičnega računalnika, ki bi imel vgrajenih 10^6 chipov za paralelno preizkušanje vseh $2^{56} \cong 10^{17}$ mogočih ključev. S tehnologijo iz leta 1976 se da izdelati specialni chip, ki bi preizkusil 10^6 ključev v sekundi, kar bi pomenilo, da bi celotno vezje lahko pregledalo vseh 10^{17} možnosti v 10^5 sekundah, tj. v približno enem dnevu. Pri ceni 10 $ na chip in pri 5-letni amortizaciji celotnega sistema, ki je obremenjen še s 100 % stroški za energijo in kontrolo, bi to pomenilo ceno 10 000 $ za eno rešitev; če pa upoštevamo, da je mogoče priti do rešitve v pol dneva, je cena še nižja.

Julija 1977 je G.B. Kolata v Science [13] objavila zanimivo informacijo, da je nad razvojem DES ves čas bedela NSA (National Security Agency), ki jo je predvsem zanimal tisti del smernic NBS, ki so zagotavljale dobavo šifrirnega sistema vsem potencialnim uporabnikom. Članek citira kritike DES, ki trdijo, da NSA gotovo ni zainteresirana za to, da bi ZDA izvažale šifrirni algoritem, ki ga ni mogoče razkriti. Cena dešifrirnega računalnika, ki sta jo navedla Diffie in Hellman, je ravno tako visoka, da si jo lahko privošči vlada, ne pa privatna firma. Zanimiv je še podatek, da je predstavnik Bell Telephon Company izjavil, da je DES preveč nezanesljiv, da bi ga firma uporabljala.

Delno na pritisk Diffiea in Hellmana, delno pa na rastoče zanimanje drugih računalniških strokovnjakov sta NBS in IBM organizirali avgusta in septembra 1976 dva seminarja, na katerih so diskutirali o varnosti algoritma DES. Na prvem sestanku so vztrajali, da dešifrirnega računalnika, kot ga opisujeta Diffie in Hellman, ne bo mogoče izdelati do leta 1990. Na drugem simpoziju so strokovnjaki IBM izjavili, da tudi IBM raziskuje možnost izdelave takega sistema do leta 1981; stal pa bi 10-krat toliko, kot predvidevata Diffie in Hellman, tj. 200 milijonov dolarjev. Dodatni zaključek obeh sestankov je bil še, da je algoritem DES kljub nekaterim pomanjkljivostim trenutno (1976) najboljši komercialno dobavljivi šifrirni sistem.

Šifrirni sistem za javno uporabo

Komaj slabo leto po tej ugotovitvi je Rivest s sodelavci [3] objavil izpopolnjeno inačico šifrirnega sistema, kot sta ga zasnovala Diffie in Hellman [2], [4]. To in pa napoved, da bo MIT (Massachusetts Institute of Technology) pričel izdelovati integrirano vezje za šifriranje podatkov, ki bo delovalo na omenjenem postopku, dokazuje, da si je sistem, ki mu vsi priznavajo visoko kvaliteto, vredno ogledati.

Po zamisli Diffieja in Hellmana lahko tak sistem primerjamo z javnim telefonskim omrežjem. Vsakdo, ki bi želel sprejemati in oddajati šifrirana sporočila, bi dobil »številko« in »telefon«. »Številka« vsakega uporabnika bi bila skupaj z njegovim imenom in naslovom natisnjena in objavljena v javnem »telefonskem« imeniku. »Številka« so vsi parametri šifrirne funkcije, s katero lahko šifriramo poljubno sporočilo. Kdor želi poslati šifrirano sporočilo komu, ki je naveden v »imeniku«, pogleda njegovo »številko« (šifro) in kodira ter pošlje sporočilo. Če sam nima »telefona«, lahko uporabi »javno govorilnico«, ker je tudi funkcija ali algoritem za šifriranje javen. Še več: vsakdo, ki ima »številko« oz. »telefonski priključek«, lahko sporočilu doda avtoriziran »pečat«, ki dokazuje, da je pošiljatelj res on. Tak, na prvi pogled skoraj nemogoči šifrirni sistem, je osnovan na tipu algoritma, ki ga Diffie in Hellman imenujeta »one-way trap function« (OWT) ali po naše enosmerna past. Funkcija OWT ima naslednje lastnosti:

— je enolična nad prostorom ključev $\{\mathbf{K}\}$: $y = f_k(x)$, $k \in \{\mathbf{K}\}$;
— ima inverzno funkcijo g, tako da je: $g_k(f_k(x)) = f_k(g_k(x)) = x$;
— eksistira algoritem Z, s katerim lahko za vsak k iz $\{\mathbf{K}\}$ izračunamo f_k in g_k;
— računalniško nemogoče (v doglednem času) je najti ali določiti funkcijo g_k ali njej ekvivalentni algoritem, če poznamo samo f_k in algoritem Z.

Pri predpostavki, da poznamo algoritem Z za določitev parov f_k in g_k, ki skoraj za vsak k iz $\{\mathbf{K}\}$ ustrezajo zgornjim pogojem, bi javni šifrirni sistem deloval takole:

Vsak uporabnik i ima dva algoritma f_i in g_i. Vsi f_i so objavljeni v »imeniku«, svoj g_i pa obdrži uporabnik i v tajnosti. Z uporabo f_i lahko vsak — tudi tisti, ki nima lastne šifre — spremeni sporočilo t v šifro x in jo pošlje uporabniku i:

$$x = f_i(t)$$

Ker je zadnji pogoj izpolnjen se ni bati, da bi kdor koli razen lastnika funkcije g_i lahko dešifriral sporočilo:

$$t = g_i(x) = g_i(f_i(t)) = t$$

Z dvojnim šifriranjem lahko dodatno pošiljatelj j (lastnik »številke j«) pošlje uporabniku i tudi avtorizirano sporočilo t:

$$z = g_j(t); \qquad x = f_i(z) = f_i(g_j(t))$$

Ko prejemnik i dobi sporočilo x in ga prvič dešifrira z uporabo lastne funkcije g_i, dobi nerazumljivo sporočilo z, ki postane smiselno šele, ko uporabi pošiljateljevo javno »številko« f_j. Dejstvo, da dobi smiselno sporočilo po uporabi prave f_j, mu nedvomno dokazuje, da je sporočilo lahko poslal le uporabnik j, ki je prvič šifriral poročilo z lastnim g_j:

$$z = g_i(x) = g_i(f_i(z)); \qquad t = f_j(z) = f_j(g_j(t))$$

Vse bi bilo lepo in prav, če bi bilo funkcijo OWT lahko določiti in najti algoritem Z. Diffie in Hellman ugotavljata, da kljub nekaterim sugestijam [2] nista našla primerne rešitve zastavljene naloge.

Kot sem že prej omenil, so Rivest in sodelavci iz MIT lani prišli do originalne rešitve, temelječe na teoriji praštevil, ki omogoča izvedbo omenjenega sistema v vseh podrobnostih. Še več, avgusta je bilo v reviji Scientific American objavljeno [4], da je Rivestovo poročilo [3] brezplačno na voljo vsem zainteresiranim. Istočasno je navedeno tudi, da bo integrirano vezje, ki ga namerava izdelovati MIT, slonelo na 128-bitnem ključu. Ta bo zanesljivo jamčil varnost šifre. Prav tako je bilo objavljeno, da bo tekla na simpoziju o kriptologiji oktobra 1977 na Cornell University pod pokroviteljstvom IEEE (Institute of Electrical and Electronics Engineers) diskusija o Rivestovem algoritmu. S tem se je stvar zapletla. NSA je posvarila IEEE, da je javna objava takih raziskav v nasprotju z zakonom o zaščiti zaupnih tehničnih podatkov ... atomskega orožja in kriptografije [15]. IEEE je predal obvestilo MIT in Stanfordu, kjer so se odvetniki takoj spravili na delo in izjavili, da je po njihovem mnenju objava še v mejah zakona. Kljub temu je bilo razpošiljanje Rivestovega poročila ustavljeno. Reakcija na vmešavanje NSA v raziskovalno dejavnost je bila zelo hitra: Science [16] se je vprašala, dokod segajo meje svobodnih raziskav in celo *The New York Times* [17] je na prvi strani postavil isto vprašanje.

Za konec lahko navedem samo grobi obris Rivestove metode, kolikor je bila objavljena [4], [14], saj sem tudi sam med tistimi, ki niso dobili njegovega poročila. [18]

Vsak uporabnik objavi dve številki s in r, ki rabita za šifriranje do 20 znakov dolgega bloka teksta t:

$$x = t^s \bmod r$$

Dešifriranje poteka na isti način:

$$t = x^w \bmod r$$

pri čemer igra potenca w vlogo tajne inverzne funkcije g; r je produkt dveh praštevil p in q, ki pa morata biti večji od 2^{63}. Obe števili s in w sta tudi funkciji p in q. Da bi zlomili šifro, moramo najti potenco w oz. obe števili p in q, ki določata vse tri parametre šifre: s, r in w. Rivest ocenjuje, da je čas, potreben za določitev dveh 63-bitnih praštevil, ki tvorita določen 126-bitni produkt, z najboljšim znanim algoritmom in z najzmogljivejšim računalnikom 4.10^{25} let.

Vsekakor dovolj.

LITERATURA

[1] D. Kahn, *The Codebreakers,* Macmillan, New York 1967.
[2] W. Diffie, M. E. Hellman. IEEE Trans. Inform. Theory **22**, (1976), 644.
[3] R. L. Rivest, A. Shamir, L. Adleman, *On Digitam Signatures and Public-Key Cryptosystem,* Technical Memo 82, MIT, April 1977.
[4] M. Gardner, Scientific American (8), 120 (1977).
[5] B. Tuckerman, IBM Report RC 2879, May (1970).
[6] L. J. Hoffman, *Modern Methods for Computer Security and Privacy,* Prentice Hall, 1977, str. 49, 59, 80—86.
[7] D. E. Knuth, *The Art of Computer Programming,* Sec. Ed., Addison Wesley, Reading, 1973, Vol. II, s. 78, 155.
[8] J. M. Carroll, P. M. Lelland, *Security and Privacy in Computer Systems,* Ed. L. J. Hoffman, Melville Publ. Co., Los Angeles 1973.
[9] J. McCarthy, Comm. AMC **18**, 131 (1975).
[10] *Federal Register,* **40** (52), 12134 (1975).
[11] *Federal Register* **40** (149), 32395 (1975).
[12] W. Diffie, M. E. Hellman, Comm. ACM, **19**, 164 (1976).
[13] G. B. Kolata, Science, **197**, 438 (1977), July 29.
[14] G. B. Kolata, Science, **197**, 747 (1977), August 19.
[15] *International Traffic in Arms Regulations,* 22 CFR, 125.01 + ITAR, 125.01, Category XIII (b).
[16] G. B. Kolata, Science **197**, 1345 (1977), September 30.
[17] N. W. Brown, The New York Times, 19. oktober 1977, s. 1.
[18] Decembra 1977 je bila objava Rivestovega poročila [3] legalizirana in poročilo so odposlali vsem zainteresiranim. Bralec, ki ga zanimajo podrobnosti, lahko dobi omenjeni odtis na vpogled pri avtorju tega sestavka.

NOVE KNJIGE

Dirk J. Struik, Kratka zgodovina matematike, Državna založba Slovenije 1978. Cena 125.— din (Knjižnica Sigma; 27).

Zgodovina matematike je zelo zanimiv in obširen predmet. Matematika je stara toliko kot civilizacija, to je več tisoč let. Zato ni čudno, da je večina učbenikov, ki obsegajo celotno zgodovino matematike, zelo obsežnih in zaradi tega neprivlačnih za prvo branje. Drugi učbeniki so posvečeni le posameznim obdobjem in ne dajejo dovolj vpogleda v razvoj matematike. Struikova knjiga A Concise History of Mathematics je morda posrečen kompromis med popolno obdelavo celotne zgodovine matematike in primernim obsegom. Prvič je izšla v založbi Dover Publications leta 1948. Doživela je več izdaj in je prevedena v mnoge evropske jezike. Na 300 straneh daje avtor zgoščen pregled zgodovine matematike od prvih začetkov do konca devetnajstega stoletja. Poudarek je na razvoju idej, povezanem s splošnimi kulturnimi in družbenimi značilnostmi posameznih obdobij. Avtor se je posebej potrudil, da bi jasno razlikoval med ugotovljenimi dejstvi, plavzibilnimi teorijami, tradicionalnimi zgodbicami in čistim ugibanjem. V knjigi je malo matematičnih razlag, zato je primerna tudi za laičnega bralca. Matematik pa prav gotovo pogreša več podrobnosti o metodah reševanja posameznih problemov. S takšnimi podatki, ki jih lahko prispeva učitelj, je knjiga primerna za učbenik zgodovine matematike. Knjiga je bogato ilustrirana in navaja mnogo literature. Poglavja so: Uvod. Začetki. Stari Orient. Grčija. Orient po propadu grške civilizacije. Začetki v Zahodni Evropi. Sedemnajsto stoletje. Osemnajsto stoletje. Devetnajsto stoletje. V slovenski jezik je knjigo prevedla T. Bohte.

Zvonimir Bohte

Obzornik mat. fiz. **25** (1978) 4

MIKROSKOPIČNA SLIKA POVRŠINSKE NAPETOSTI

MARJAN HRIBAR

UDK 532.61

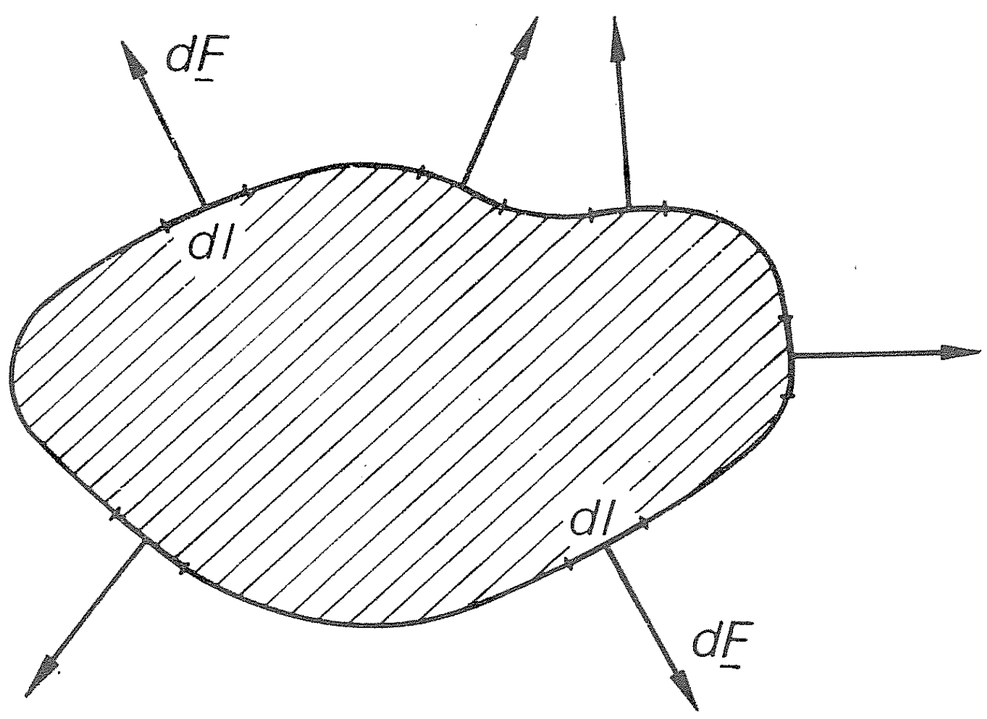
Članek vsebuje pregled kinetične teorije površinske napetosti in podaja zvezo med makroskopičnimi in mikroskopičnimi količinami.

MICROSCOPIC THEORY OF SURFACE TENSION

The kinetic theory of surface tension is reviewed.

Uvod

Površje kapljevin spominja na izotropno napeto prožno opno. Okolni deli delujejo na opazovalni del površja (sl. 1) s silami, ki so vzporedne s površjem in pravokotne na mejo. Stanje površja pri dani temperaturi opredelimo s silo dF, ki deluje na del meje z dolžino dl. Koeficient $\gamma = dF/dl$ imenujemo *koeficient površinske napetosti* ali kratko *površinsko napetost*. Do istega koeficienta pridemo, če določimo delo, ki je potrebno, da izotermno povečamo površje pri nespremenjeni prostornini kapljevine. Če pri taki izotermni spremembi opravimo delo dA, ko povečamo površje za dq, je površinska napetost $\gamma = (dA/dq)_{T,V}$. V termodinamiki opredelimo koeficient γ s prosto energijo kot $\gamma = (\partial F/\partial q)_{T,V}$. Zadnji dve definiciji sta ekvivalentni.



Sl. 1. Sile na izbrani del površja kapljevine

Ukvarjali se bomo s sliko površinske napetosti preprostih kapljevin z nepolarnimi, približno kroglastimi molekulami. Pri takih kapljevinah je koeficient γ odvisen le od temperature. V enačbi stanja za površje

$$\gamma = \gamma_0(1 - T/T_c)^\alpha$$

je T temperatura, T_c kritična temperatura, γ_0 je parameter, ki je značilen za kapljevino, eksponent α pa je za vse kapljevine enak — približno 11/9 [1]. Koeficient γ_0 se da izraziti s kritično temperaturo in s kritično prostornino

Preglednica 1. Reducirani koeficient površinske napetosti γ^* pri temperaturi $T = 0{,}56\, T_c$ za nekaj izbranih kapljevin

Kapljevina	Površinska napetost (N/m)	Reducirani koeficient γ^* ($J\, K^{-1}\, kmol^{-2/3}$)
Ne	$5{,}55.10^{-3}$	$1{,}500.10^{-5}$
CH_4	13,79	1,548
Kr	16,081	1,568
Ar	13,28	1,570
Xe	18,98	1,583
O_2	14,04	1,605
CO	11,05	1,704

izbrane kapljevine. *Reducirani koeficient* $\gamma^* = \gamma T_c^{-1} V_c^{2/3}$ je namreč univerzalna funkcija reducirane temperature $T^* = T/T_c$:

$$\gamma^* = \gamma_0^* (1 - T^*)^\alpha$$

Koeficient $\gamma_0^* = \gamma_0\, T_c^{-1} V_c^{2/3}$ ima pri tem vrednost $4{,}4.10^{-5}\, JK^{-1}\, kmol.^{-2/3}$ Preglednica 1 potrjuje zgornjo enačbo za nekaj izbranih kapljevin [2].

Mikroskopične slike

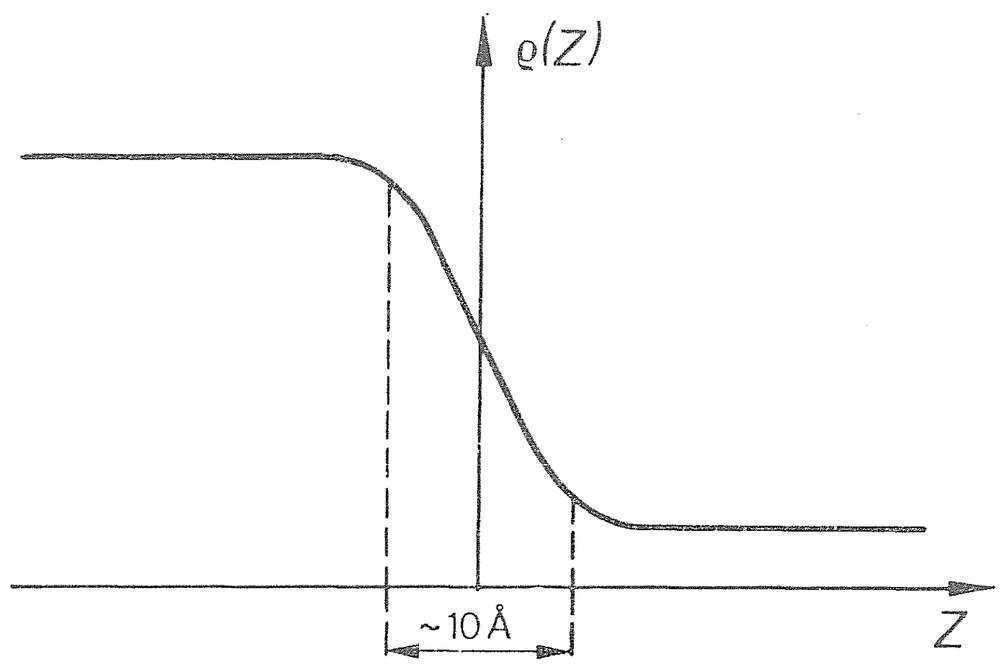
Univerzalno temperaturno odvisnost koeficienta γ pri izbranih preprostih kapljevinah lahko pojasnimo že z zelo grobo sliko. Mislimo si, da pri konstantni temperaturi pretrgamo stolpec kapljevine s prečnim presekom q. S tem ustvarimo novo površje s ploščino $2q$ in po definiciji opravimo delo $A = 2\gamma q$. To delo je enako spremembi vezavne energije molekul, ki so iz notranjosti prešle na površje. Molekula v notranjosti je namreč popolnoma obkrožena s sosedami in ima zasedene vse razpoložljive vezi, molekula na površju pa ima v povprečju zasedenih le polovico vezi. Naj ima molekula v notranjosti kapljevine v povprečju po z vezi z vezavno energijo ε. Če je na površju N molekul, je sprememba njihove vezavne energije $\frac{1}{2} z \varepsilon N$. Ko izrazimo N z gostoto n molekul v kapljevini: $N = q\, n^{2/3}$, dobimo za površinsko napetost izraz $\gamma = \frac{1}{4} \varepsilon\, z\, n^{2/3}$.

Izrazimo gostoto molekul s kilomolskimi podatki pri izbrani temperaturi $n = N_A/V$ in izračunajmo še reducirani koeficient površinske napetosti. Dobljeni izraz $\gamma^* = 2\, k\, N_A^{2/3}\, (V_c/V)^{2/3}$ se sklada s semiempirično formulo. Tudi za kapljevine namreč velja van der Waalsova enačba, po kateri je razmerje V_c/V univerzalna funkcija reducirane temperature [2].

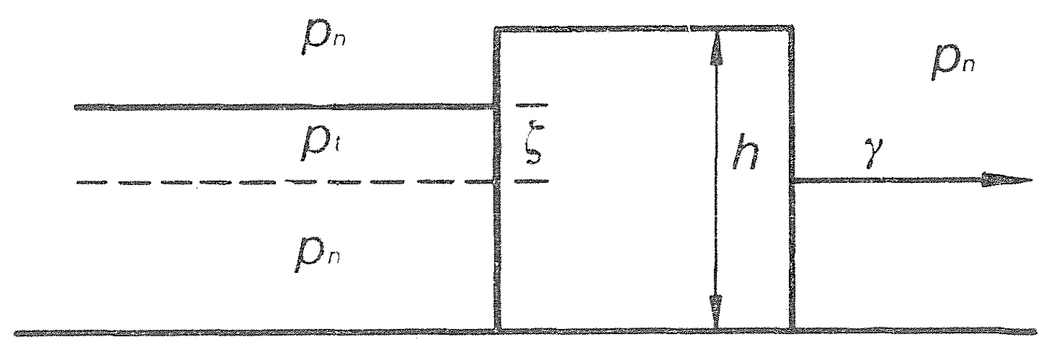
Groba slika nam ne pojasni sil, ki so vzporedne s površjem. Zaradi podobnih težav z drugimi približnimi slikami je za daljši čas obveljalo mnenje, da so površinske sile le koristno slepilo in da je smiselna le termodinamična definicija koeficienta γ. To stališče je obveljalo kljub temu, da pri določanju površinske napetosti merimo prav sile, ki so vzporedne s površjem [5], [6].

Poglejmo mikroskopično sliko površja kapljevine. Molekule na površju neprestano uhajajo iz tekoče faze in vanjo ponovno ponikajo. V povprečju deluje kapljevina na te molekule s privlačnimi silami. Molekule se gibljejo pojema-

joče, ko se odmikajo od kapljevine, in pospešeno, ko se ji spet približujejo. Ko se zarijejo v goste plasti, se zaradi odbojnih sil odbijejo nazaj. Posledica termičnega gibanja molekul je, da je prehod iz kapljevine v plin zvezen. Ker so sile med molekulo in kapljevino kratkega dosega, je prehod med kapljevino in paro zelo oster in ne meri več kot nekaj povprečnih razdalj med molekulami v kapljevini. Ko se temperatura približuje kritični temperaturi, se prehodna plast širi in se nazadnje popolnoma razblini [3]. Sl. 2 kaže tipični potek gostote molekul v smeri, ki je pravokotna na površje kapljevine. V izbranem koordinatnem sistemu ima os z smer pravokotnice na površje. Gostoto molekul v našem primeru definiramo kot povprečno število molekul v enoti prostornine na izbranem mestu, če je čas opazovanja velik v primeri s časom med zaporednima trkoma molekule.*



Sl. 2. Tipični potek gostote molekul pri prehodu iz kapljevine v paro



Sl. 3. Ravnovesje premične prečke na površju kapljevine

Poglejmo ravnovesje izbranega dela snovi v prehodni plasti v primeri z ravnovesjem v homogenih fazah. Pri tem zanemarimo prostorninske sile, ki so majhne v primerjavi s silami okolne kapljevine. Stanje opišemo tedaj s tenzorjem tlaka $\mathbf{p}$, ki mora zadoščati enačbi div $\mathbf{p} = \emptyset$. V homogenih fazah je tenzor tlaka izotropen $\mathbf{p} = -p_0.\mathbf{1}$. V površinski plasti mora tenzor izražati anizotropijo površja. Iz simetrijskih razlogov so komponente tenzorja odvisne le od koordinate z; zahtevamo pa še, da vse komponente zvezno preidejo v komponente, ki jih ima tenzor v homogenih fazah.

Iz pogoja za ravnovesje dobimo za komponente tenzorja enačbe:

$$\partial p_{xz}/\partial z = \partial p_{zy}/\partial z = \partial p_{zz}/\partial z = \emptyset$$

iz katerih sledi ob upoštevanju robnih pogojev $p_{zx} = p_{xz} = \emptyset$ in $p_{zz} = -p_n = konst. = -p_0$. Ker na površju ni strižnih napetosti, morata biti komponenti $p_{xy} = p_{yx} = \emptyset$. Preostali diagonalni komponenti p_{xx} in p_{yy} morata biti enaki, postavimo $p_{xx} = p_{yy} = -p_t$. V nadaljnjem bomo p_t imenovali *tangentni tlak*, $p_n = p_o$ pa *normalni tlak*. V homogenih fazah morata biti tlaka enaka, v prehodni plasti pa pričakujemo, da je tangentni tlak negativen. Zvezo med tlakom in površinsko napetostjo dobimo, ko opazujemo ravnovesje sil, ki delujejo na prečko okvira, ki napenja kapljevinsko opno (sl. 3). Da je površje v ravnovesju,

* Navajeni smo definirati makroskopične količine le tedaj, ko se na razdalji, ki je velika v primeri z medmolekulsko razdaljo, bistveno ne spreminjajo. V našem primeru preide gostota od vrednosti v tekoči fazi do vrednosti v pari v nekaj medmolekulskih razdaljah. V prehodni plasti moramo zato gostoto definirati posebej. Enak premislek je potreben tudi pri drugih makroskopičnih količinah.

moramo vleči v pravokotni smeri s silo γ na dolžinsko enoto prečke. Z vseh strani deluje na prečko okolna tekočina s tlakom $p_n = p_0$, ob površju v plasti z debelino ζ pa je povprečni tlak $\bar{p}_t$ [4].

V ravnovesju je tedaj:

$$\gamma + \bar{p}_t\zeta + p_n(h - \zeta) = p_n h$$

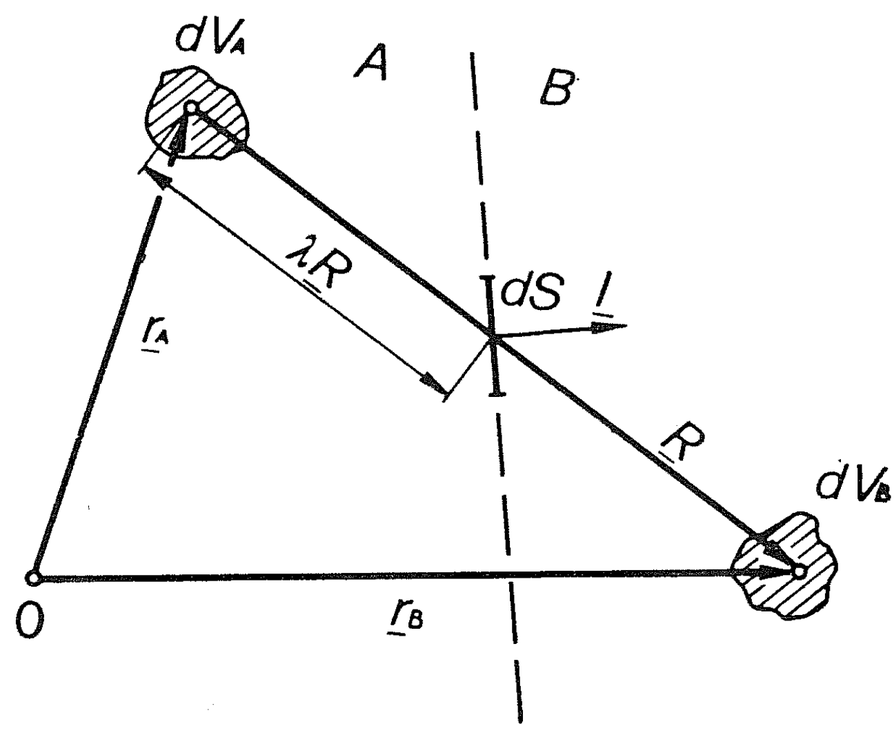
Iz tega izračunamo $\gamma = (p_n - \bar{p}_t)\zeta$. V resnici je tlak po površinski plasti odvisen od lege in je

$$\gamma = \int_{-\infty}^{\infty} (p_n - p_t(z))dz \tag{1}$$

Ocenimo povprečni tagentni tlak pri vodi. Površinska napetost je okoli 70.10^{-3} N/m, debelina prehodne plasti pa okoli 7.10^{-10} m. Povprečni tangentni tlak je tedaj $\bar{p}_t = -\gamma/\zeta = -1000$ atm.

Negativni tlak in njegov potek po višini naj razloži mikroskopična teorija. Tlak si mislimo sestavljen iz dveh delov. Prvi del predstavlja kinetični tlak $p' = nkT$ kot posledico pretoka gibalne količine skozi zamišljeno ploskvico. Drugi del p'' — statični tlak — je posledica sil med molekulami, katerih zveznice potekajo skozi ploskvico. V plinu, v katerem so molekule v povprečju daleč druga od druge, je $p'' = 0$ in je kinetični tlak $p' = p_0$ V kapljevini je p'' negativen in izravna povečani kinetični tlak tako, da je skupni tlak enak tlaku v plinu: $p' + p'' = p_0$. Oba prispevka in skupni tlak so izotropni. V prehodni plasti se oba dela tlaka spreminjata z višino in sta lahko odvisna od smeri opazovanja.

Zamislimo si ravnino, ki razdeli sistem v podsistema A in B. Opazujmo interakcijo med podsistemoma, ki poteka preko izbrane ploskvice s ploščino dS (sl. 4). Lego ravnine in s tem ploskvice naj določa enotni vektor $\mathbf{l}$. Naj bo $\mathbf{dF}$ komponenta sile, s katero podsistem B deluje na podsistem A v smeri pravokotnice $\mathbf{l}$. Tedaj definiramo ustrezni tlak z enačbo $\mathbf{dF} = p(\mathbf{r}, \mathbf{l})\mathbf{l}\, dS$.



Sl. 4. K računanju sile med molekulami v kapljevini

Kinetični tlak $p'(\mathbf{r}, \mathbf{l}) = n(\mathbf{r})kT$ je izotropen. Statični tlak dobimo, ko seštejemo sile med molekulami, katerih zveznice gredo skozi dS. Privzamemo, da lahko izrazimo silo med molekulama kot odvod potenciala, ki je odvisen le od razdalje. Silo med molekulama v A in B tedaj izrazimo takole:

$$\mathbf{F}(\mathbf{r}_A, \mathbf{r}_B) = -\operatorname{grad} \Phi\,(|\mathbf{r}_B - \mathbf{r}_A|) = -(\mathbf{R}/R)\Phi'(R); \qquad \mathbf{R} = \mathbf{r}_B - \mathbf{r}_A$$

Ko poiščemo komponento sile v smeri **l** in seštejemo po vseh parih, dobimo za statični tlak enačbo

$$p''(\mathbf{r}, \mathbf{l}) = -(dS)^{-1} \iiint \Phi'(R)\, (\mathbf{R}\,\mathbf{l}/R) n_2\, (\mathbf{r}_A, \mathbf{r}_B)\, dV_A\, dV_B \tag{2}$$

$n_2\, (\mathbf{r}_A, \mathbf{r}_B)$ je dvodelčna porazdelitvena funkcija, ki jo izrazimo z ustrezno korelacijsko funkcijo $g\, (\mathbf{r}_A, \mathbf{r}_B)$ in z gostoto molekul:

$$n_2(\mathbf{r}_A, \mathbf{r}_B) = n(\mathbf{r}_A)\, n(\mathbf{r}_B)\, g\, (\mathbf{r}_A, \mathbf{r}_B) \tag{3}$$

Z uvedbo novih spremenljivk λ in $\mathbf{R}$ postavimo

$$\mathbf{r}_A = \mathbf{r} - \lambda \mathbf{R}, \mathbf{r}_B = \mathbf{r} + (\lambda - 1)\, \mathbf{R}, dV_A = \mathbf{l}\,\mathbf{R}\, d\lambda dS, dV_B = d^3R$$

in dobimo:

$$p''(\mathbf{l}, \mathbf{r}) = -\tfrac{1}{2} \iiint d^3R\, R^{-1}\, (\mathbf{R}\,\mathbf{l})^2\, \Phi'(R) \int_0^1 d\lambda\, n_2\, (\mathbf{r} - \lambda \mathbf{R}, \mathbf{r} + (\lambda - 1)\mathbf{R}) \tag{4}$$

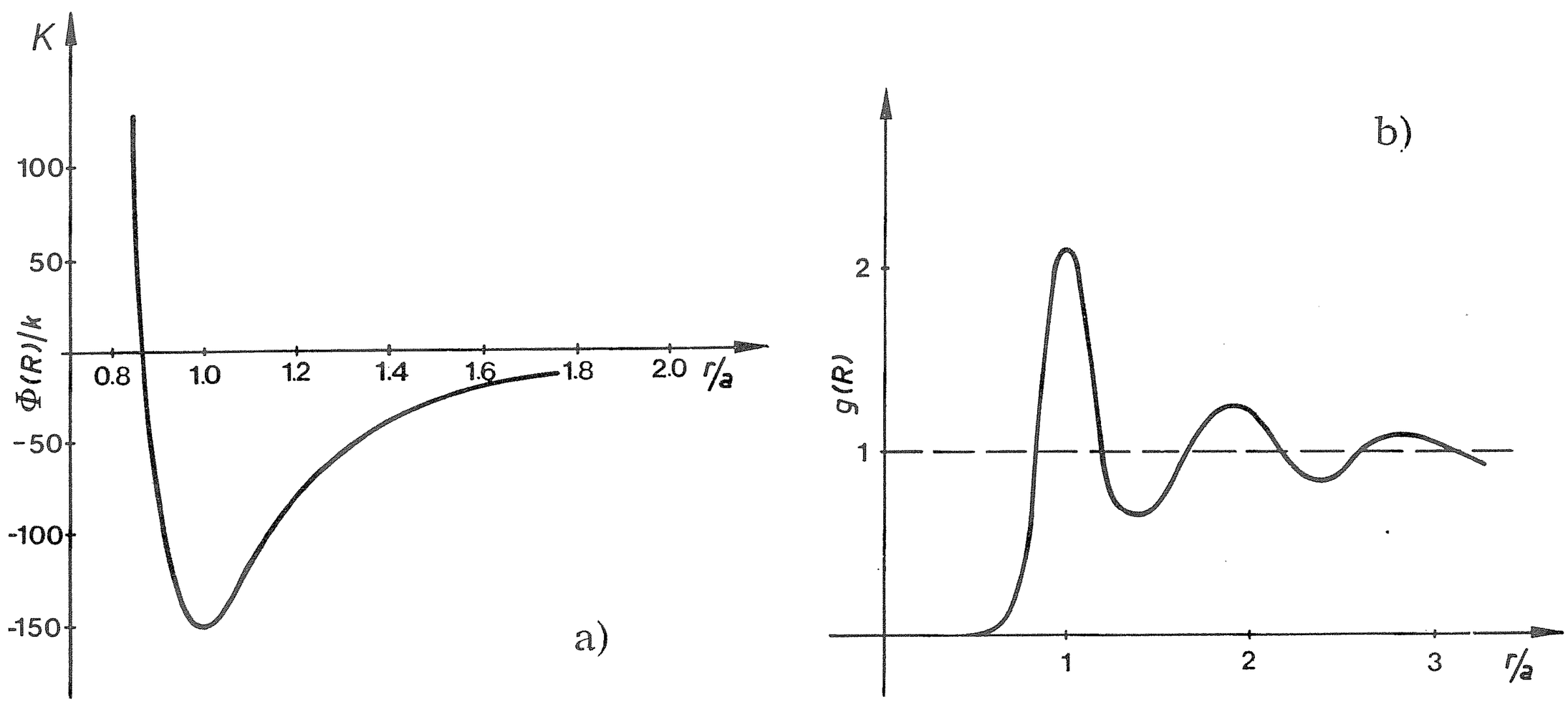
Skupni tlak je tedaj

$$p\, (\mathbf{r}, \mathbf{l}) = n(\mathbf{r}) kT - p''(\mathbf{r}, \mathbf{l})$$

V obeh homogenih fazah je gostota molekul konstantna in je korelacijska funkcija odvisna le od razdalje. Lahko zapišemo $n_2(\mathbf{r}_A, \mathbf{r}_B) = n^2\, g(R)$. Ko integriramo po sferičnih koordinatah, dobimo za tlak enačbo:

$$p(\mathbf{r}, \mathbf{l}) = p = nkT - \frac{2\,\pi n^2}{3} \int d\,R\, R^3\, \Phi'\, (R)\, g\, (R) \tag{5}$$

Sl. 5 kaže potek potenciala $\Phi\, (R)$ in korelacijske funkcije $g(R)$ za kapljevinski argon. Analitično zapišemo potencial z Lennard-Jonesovo enačbo $\Phi = \varepsilon[(a/R)^{12} - 2(a/R)^6]$. Funkcija pod integralom je znatna le na območju privlačnih sil, kjer je $\Phi' > 0$, zato je integral za kapljevinsko fazo po pričakovanju pozitiven. V plinski fazi je integral 0, ker so medmolekulske razdalje velike v primeri s premerom molekule.



Sl. 5. Medatomski potencial za tekoči argon (a) in tipična dvodelčna korelacijska funkcija (b)

V prehodni plasti sta n_2 in g anizotropna. Tudi $p''(\mathbf{r}, \mathbf{l})$ je anizotropen. Izračunajmo najprej komponento, ki je pravokotna na površje. Enotni vektor $\mathbf{l}$ je tedaj usmerjen v smeri osi z. Upoštevamo, da je gostota molekul odvisna le od koordinate z in da je $\mathbf{l}\mathbf{R} = Z$. Tako dobimo za normalno komponento tlaka izraz:

$$p_n(z) = n(z)kT - \tfrac{1}{2}\iiint d^3 R\, Z^2 R^{-1} \Phi'(R) \int_0^1 d\lambda\, n_2(z - \lambda Z, \mathbf{R}) \tag{6}$$

Podobno dobimo za tangentno komponento izraz:

$$p_t(z) = n(z)kT - \tfrac{1}{2}\iiint d^3 R\, X^2 R^{-1} \Phi'(R) \int_0^1 d\lambda\, n_2(z - \lambda Z, \mathbf{R}) \tag{7}$$

Enotni vektor smo usmerili v smeri osi x in upoštevali, da je $\mathbf{l}\mathbf{R} = X$. Z enačbami (1), (6), (7) in enačbo:

$$\int_{-\infty}^{\infty} dz \int_0^1 d\lambda n_2(z - \lambda Z, \mathbf{R}) = \int_{-\infty}^{\infty} dz\, n_2(z, \mathbf{R})$$

dobimo za koeficient γ enačbo

$$\gamma = \tfrac{1}{2}\int_{-\infty}^{\infty} dz \iiint d^3 R\, R^{-1} (X^2 - Z^2) \Phi'(R)\, n_2\, z, \mathbf{R}) \tag{8}$$

Dvodelčna porazdelitvena funkcija $n_2(z, \mathbf{R})$ je v prehodni plasti anizotropna in odraža gostoto molekul. Iz zahteve, da mora biti normalna komponenta tlaka p_n po vsej kapljevini konstantna, sledi tudi v prehodni plasti $dp_n/dz = 0$. Po odvajanju enačbe (6) dobimo iz tega pogoja enačbo, ki povezuje dvodelčno porazdelitveno funkcijo z gostoto molekul:

$$kT\, dn(z)/dz = \iiint d^3R\, (Z/R)\, \Phi'(R)\, n_2(z, \mathbf{R}) \tag{9}$$

Enačba da gostotni profil $n(z)$ kot funkcijo dvodelčne porazdelitvene funkcije. V računu običajno izrazimo to funkcijo s korelacijsko funkcijo za homogeno in izotropno kapljevino, upoštevajoč, da je gostota molekul odvisna od lege:

$$n_2(z, \mathbf{R}) = n(z)n(z + Z)g_0(R)$$

S tem dobimo iz enačbe (9) gostotni profil

$$n(z) = n_0 \exp\{-(4\pi n_0/3kT) \int_0^{\infty} d\,R\, R^3 \Phi'(R)\, g_0(R) +$$

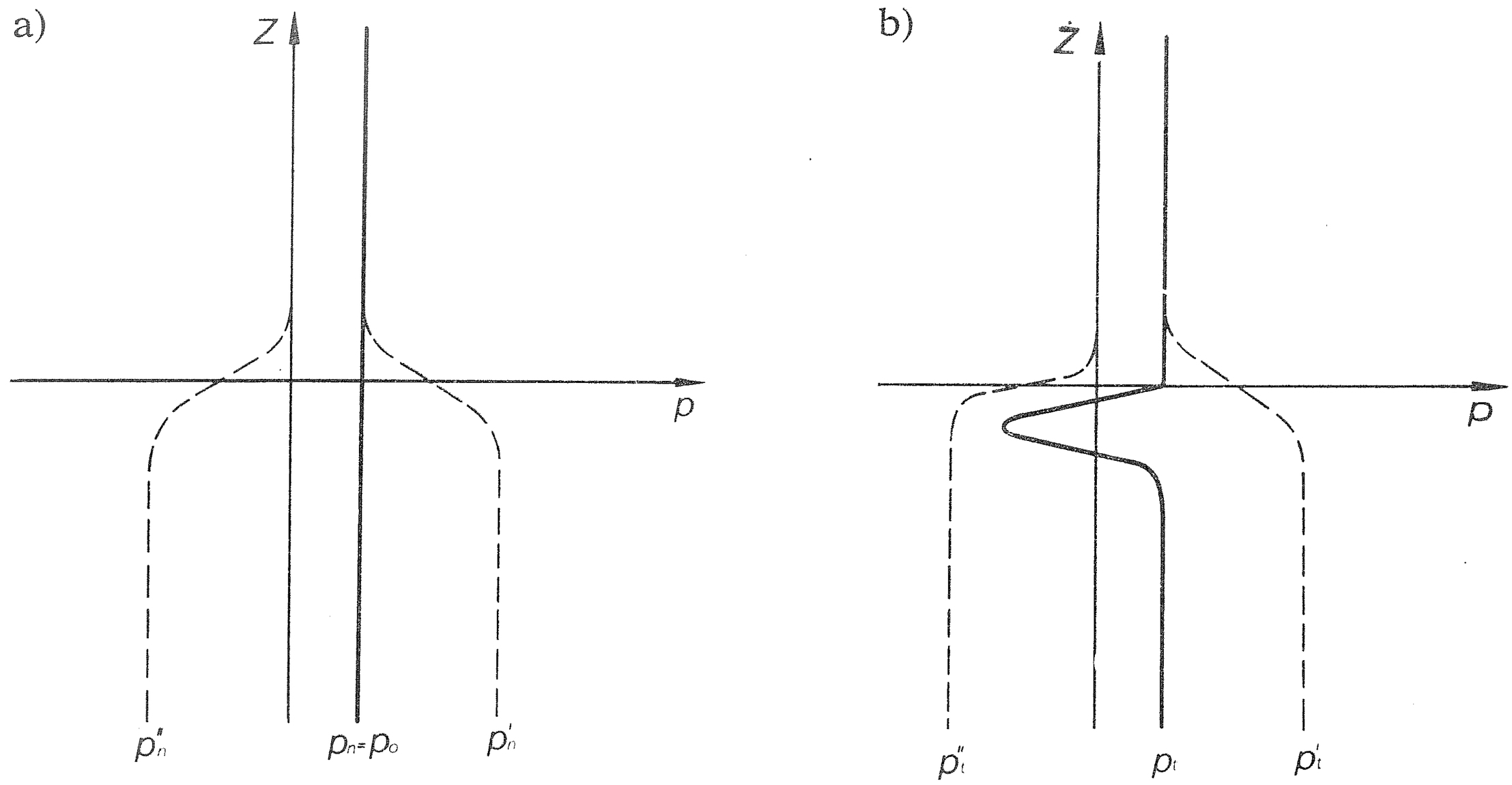
$$+ (\pi/kT) \int_{-\infty}^{\infty} d\,Z\, n(z + Z) \int_{|Z|}^{\infty} d\,R\, (R^2 - Z^2) \Phi'(R)\, g_0(R)\} \tag{10}$$

če je n_0 gostota molekul v homogeni kapljevini. Iz enačbe (8) izračunamo s tem koeficient γ na nekaj procentov natančno.

Oglejmo si kvalitativno potek kinetičnega in statičnega dela pri obeh komponentah tlaka. Kinetični del tlaka je pri obeh komponentah enak, je pozitiven in sorazmeren z gostoto delcev. Statični del je pri obeh komponentah negativen. Pri normalni komponenti je sorazmeren z gostoto molekul $n(z)$. To uvidimo takole. Ploskvica, ki nam rabi za definicijo tlaka, je tedaj vzporedna s površjem, opazujemo pa komponente sil v smeri, pravokotni na površje. Te komponente izvirajo predvsem od molekul v globljih plasteh,

kjer je gostota že konstantna. Sila na ploskvico je tedaj sorazmerna z lokalno gostoto molekul.

Pri tangentni komponenti je statični del odvisen od gostote molekul s potenco, ki je večja od 1. Ploskvico si mislimo v tem primeru pravokotno na površje, opazujemo pa komponento sil v vodoravni smeri. Ta je približno sorazmerna z lokalno gostoto molekul, sila na našo ploskvico pa zato približno sorazmerna s kvadratom lokalne gostote molekul. Posledica tega je, da postane v prehodni plasti skupni tlak negativen. Potek tlaka kaže sl. 6.



Sl. 6. Potek normalnega (a) in tangentnega (b) tlaka na meji med kapljevino in paro

Pojav negativnega tlaka lahko razumemo tudi takole. V prehodni plasti so molekule v povprečju dalj druga od druge kot v kapljevini. V kapljevini odbojne sile med bližnjimi sosedami uravnovešajo privlačne sile med bolj oddaljenimi sosedami. V prehodni plasti na površju kapljevin pa so molekule v povprečju v območju medsebojnih privlačnih sil. Zaradi teh sil se površje skrči, če jih ne uravnovešajo druge sile; sicer pa je enakomerno napeto.

LITERATURA

[1] S. Ono in S. Kondo, *Molecular Theory of Surface Tension in Liquids*, Handbuch der Physik, Band X, Springer Verlag, Berlin, 1960.

[2] M. V. Berry, *Liquid Surfaces*, Surface Science, Vol. I, IAEA, Dunaj, 1975.

[3] M. V. Berry, *The Molecular Mechanism of Surface Tension*, Physics Education, **6** (1971) 79—84.

[4] R. C. Brown, *The Surface Tension of Liquids*, Contemp. Phys. **15** (1974) 301—327.

[5] R. C. Broln, *The Fundamental Concepts Cocerning Surface Tension and Capillarity*, Proc. Roy. Soc. **A 159** (1947) 429—448.

[6] G. D. Yarnold, *Understanding Surface Tension*, Contemp. Phys. **1** (1959/60) 267—275.

POSVETOVANJE O MATEMATIKI IN FIZIKI V REFORMIRANI ŠOLI

Na posvetovanju v dvorani hotela Kanin v Bovcu 27. 10. 1977 je sodelovalo 120 učiteljev in profesorjev matematike in fizike iz vse Slovenije. Objavljamo skrajšano pregledno poročilo, uvodna sporočila in razprave v upanju, da bo uspešno posvetovanje pustilo sled in vzpodbujalo naslednja.

POGLED NA POSVETOVANJE

Posvetovanje je zajelo spremembe pouka, ki jih terja usmerjeno izobraževanje, oblike obšolske dejavnosti, krožke in tekmovanja. Težko bi bilo vse to obdelati v treh urah, če ne bi bilo gradivo naprej pripravljeno. Tako so poročevalci v uvodnih besedah nakazali le glavne misli. Prvi del posvetovanja je bil posvečen učnima načrtoma za matematiko in fiziko v programski zasnovi usmerjenega izobraževanja, drugi pa dejavnosti društva za večanje zanimanja za matematiko in fiziko.

Predloge učnih načrtov za matematiko in za fiziko sta predstavila Stanko Uršič in Aleksander Kregar. Število ur matematike je v prvem letniku za vse enako, v naslednjih letih pa se menja glede na usmeritev. Imamo program A in zahtevnejši program AB z večjim številom ur. Fizika je v prvem letniku splošnoizobraževalni predmet. V nekaterih programskih usmeritvah se javlja v 2. letniku kot fundamentalni predmet, v nekaterih finalnih programskih usmeritvah kot strokovni predmet. Skupna programska osnova obsega nihanje, valovanje in atomiko. Usmerjene šole zahtevajo seveda specializirano učno vsebino. Tako na primer bodo pri fiziki za družboslovno smer pedagoške usmeritve obravnavali poglavja: razvoj fizike, fizika in tehnika, fizika in družba. To so nova poglavja — dozdaj se v srednjih šolah niso obravnavala. Razprava je bila usmerjena pretežno k smotrom in izbiri učne vsebine matematike in fizike v prvem letu usmerjenega izobraževanja. V učnih programih je ponavadi snovi preveč. (Anton Moljk) Treba je paziti, da se ta napaka v načrtih usmerjenega izobraževanja ne bo ponovila. Člani društva matematikov, fizikov in astronomov naj po svojih izkušnjah presodijo in povedo svoje mnenje. Po smotrih, ki morajo biti navedeni za vsak predmet, bi se moralo videti, kolikšen je splošni in kolikšen usmerjeni delež pri pouku predmeta. Tudi fizika ima splošno in usmerjeno izobraževalno vlogo. Snov bo treba prav izbirati, zato bo pri usmerjenem izobraževanju ta učiteljeva vloga še bolj pomembna.

Fran Dominko je bil mnenja, da reforma srednjega šolstva na univerzah in pedagoških akademijah premalo odmeva. Premalo je bilo prepričevanja, da bi se za reformo navdušili. Ali mislimo dovolj na to, da moramo spremeniti miselnost človeka, da bo učinkovit na delovnem mestu in v samoupravljavski družbeni vlogi? Kakšna bo vloga univerze; ali je to samo mesto, kjer se izvaja finalna programska usmeritev, ali ima še druge naloge? Ali ima nalogo spremljati razvoj duha po vsem svetu, ga soustvarjati in prenašati v naše okolje? Ko se spreminja srednja šola, se mora menjati tudi univerza. Izbranih poglavij iz naravoslovnih ved na univerzi ne poučujemo. O okvirnih spremembah in programih bi bilo treba več razpravljati v tisku, radiu in na televiziji.

Udeleženci so obravnavali tudi usmerjeno izobraževanje v pedagoških gimnazijah. Na koncu leta naj bi se učitelji posameznih predmetov pogovorili o rezultatih in izkušnjah ter predlagali izboljšave.

O oblikah obšolske dejavnosti so poročali: Marija Munda in France Perne o krožkih, France Galič in Anton Moljk o tekmovanjih. Pri krožkih moramo upoštevati želje učencev in njihovo zanimanje. Pri fiziki so to gotovo eksperimenti in meritve. Toda manjka učil, instrumentov in literature, iz katere bi se učenec seznanil z novostmi. Naloge in primerno čtivo bi lahko objavljala *Obzornik* in *Presek*. Dobrodošle bi bile tudi knjige. Ker pa je učenec preobremenjen s 30 šolskimi urami na teden in še z domačim delom, za obšolsko dejavnost ne ostane mnogo časa. Poskušati moramo učence razbremeniti. V osnovnih šolah se število matematičnih krožkov manjša. Za dodatni pouk sta predvideni samo dve uri na teden. Pozna se pomanjkanje učiteljev matematike in fizike, raste pa število učiteljev, ki odhajajo iz prosvetne službe.

Tekmovanja za Vegova priznanja na osnovni šoli potekajo že sedem let. Občinskih tekmovanj se udeleži okrog 3000 učencev, republiških tekmovanj za učence 8. razreda od 200 do 300. Organizacije tekmovanja, ki je že utečena, ni treba spreminjati. Pri tekmovanjih za srednje šole ne smemo povečevati težavnosti. Dobro pa bo spremeniti zlasti pri fiziki vsebino in način tekmovanja. Naloge pri fiziki naj ne bodo samo računske, treba je upoštevati tudi druge cilje pouka fizike. Pri tekmovanjih naj se navedejo tudi področja, ne le razredi.

Mladega človeka je treba navdušiti. Idej ni malo: poletna šola za matematike, za fizike, konference mladih fizikov. Poskrbeti bi morali za več oddaj iz fizike in o fiziki na radiu in televiziji. Pri širjenju znanja bi se morali poslužev ati tudi uspešnih reklamnih metod. Izkušnje nekaterih članov kažejo, da so naša podjetja pripravljena prispevati nagrade za učence. Tako sodelovanje z združenim delom bi bilo treba utrditi.

Martina Koman

VNAPREJŠNJE OBVESTILO O POSVETOVANJU*

Društvo že deset let seli občne zbore v razne kraje po Sloveniji, da se člani seznanjajo z razvojem krajev in z napredkom šolstva. Ti zbori dajejo tudi priznanje in pobudo kolegom, ki delajo na tamkajšnjih šolah. Zadnja tri leta je dan pred zborom strokovno posvetovanje, na katerem se obravnavajo aktualni problemi stroke in pouka.

Vsebine letošnjega posvetovanja v Bovcu ni težko uganiti. Saj je ob velikih spremembah v šolstvu koristno v širokem krogu matematikov in fizikov pregledati naloge društva v novih okoliščinah.

Z družbenim usklajevanjem je bila sprejeta zasnova usmerjenega izobraževanja, po kateri je treba oblikovati učno vsebino. Saj bo usmerjeno izobraževanje opredeljeno šele z usmerjeno učno vsebino.

Matematika in fizika sta splošno izobraževalna predmeta; poleg splošnega deleža pa imata tudi usmerjeni delež pri posameznih učnih usmeritvah. Deleže določajo učni smotri, ki omogočajo izbiro in dimenzioniranje učne snovi. Znanje za predvideno delo dobiva prednost pred znanjem na zalogo. Prvi del razprave je namenjen učni snovi iz matematike in fizike v 1. letu usmerjenega

* Obvestilo je oddajal Radio Ljubljana 19. 10. 1977.

izobraževanja. Uvodna pojasnila bosta dala tov. S. Uršič in tov. A. Kregar z Zavoda za šolstvo SRS.

Spreminja se tudi način pouka v šoli in podajanja snovi v učbenikih. Učencem bo treba bolj kot doslej pojasnjevati, kakšen je pomen posameznih poglavij učne snovi, zakaj je dobro, da jih poznajo in koliko bi bili na slabšem, če jih ne bi. Ker bodo učenci lahko delno izbirali ustrezne skupine predmetov, bo treba skrbeti za reklamo za matematiko in fiziko. O tem bo govor v drugem delu razprave. Saj je poleg šole tudi društvo že od nekdaj navduševalo za matematiko in fiziko in skrbelo za večanje znanja. Društvo izdaja Presek in Obzornik in poljudnoznanstvena dela iz svojih strok, prireja predavanja, krožke ter šolska, republiška in zvezna tekmovanja iz matematike in fizike.

Posodabljanje pouka in uka matematike in fizike je skrb in interes vseh učiteljev. Zato bo na posvetovanju gotovo podanih mnogo dragocenih misli in pobud, ki bodo izvirale iz bogatih izkušenj in iz domiselnih predvidevanj.

Posvetovanje naj bi pokazalo, da z uvajanjem novih možnosti sledimo razvoju in da ga lahko tu in tam tudi soustvarjamo.

Anton Moljk

MATEMATIKA V USMERJENEM IZOBRAŽEVANJU

V 1. letu usmerjenega izobraževanja je predvidenih 114 ur pouka matematike ali 3 ure na teden za vse smeri z enotnim učnim načrtom. Učenci, ki uspešno končajo osnovno šolo, bodo delali po enotnem programu, imeli bodo enako učno-vzgojno vsebino pri vseh predmetih. Ta program je sedaj v javni razpravi, ki se bo predvidoma končala konec marca 1978.

Pri matematiki so posamezna poglavja učnega načrta naslednja:

Osnovni pojmi matematične logike ter operacije z množicami.

S to snovjo so se učenci že delno seznanili v osnovni šoli. Zdaj poglobimo znanje in obdelamo tista poglavja, ki so potrebna za nadaljnje razumevanje snovi.

Kolobar in obseg.

Osvežimo predznanje učencev ter v nadaljevanju razširimo in poglobimo to snov. Poudarimo tudi, da so posploševanje pojma števila, od naravnega do realnega, določale zahteve praktičnih aplikacij matematike in zahteve razvoja matematike kot znanosti.

Linearna funkcija in linearna enačba.

Najprej analitično prikažemo funkcijo, nato preidemo na algebrajski aparat in formalizem. Predvidena je tudi obravnava nekaterih delov analitične geometrije. Poudarek pa je na grafičnih metodah pri reševanju enačb in neenačb.

Vektorji.

Obravnavamo osnovne pojme ter operacije z vektorji, in sicer vsoto in razliko ter produkt vektorja z realnim številom. S tem skušamo zadovoljiti potrebe pouka fizike.

Geometrija.

Dopolnimo znanje iz osnovne šole. Pri planimetriji obravnavamo uporabo podobnosti, pri stereometriji obdelamo nekatere nove pojme, pri telesih pa še prisekano piramido, stožec ter dele krogle.

V skupnem 1. letu usmerjenega izobraževanja ima pouk matematike splošnoizobraževalni značaj. Učni načrt si prizadeva, da bi bil pouk enak po obsegu in vsebini na vseh šolah.

V 2. letu usmerjenega izobraževanja pa imajo nekatere smeri samo 76 ur matematike letno, druge pa 114 ali tudi več. Učni načrt je sestavljen tako, da so nekatera poglavja enotna za vse usmeritve. Navedeno je tudi število ur, potrebnih za obdelavo posameznih poglavij; to število pa ni obvezno, temveč je le napotilo za določanje obsega v posameznih smereh.

Naslovi poglavij so:

1. Odvod
2. Eksponentna funkcija in enačba
3. Kompleksna števila
4. Kvadratna funkcija in enačba
5. Kotne funkcije
6. Vektorji
7. Uporabno računstvo

Učenci, ki imajo v 2. letu usmerjenega izobraževanja le 76 ur matematike, bodo predelali drugo, peto in sedmo poglavje, drugi pa prvih šest poglavij. Ta učno-vzgojna vsebina bo prav tako deležna javne razprave in jo bodo dobile v obravnavo vse zainteresirane ustanove.

Stanko Uršič

FIZIKA V USMERJENEM IZOBRAŽEVANJU

Spremembe učnega načrta in pouka fizike so potrebne zaradi nove programske zasnove usmerjenega izobraževanja pa tudi zaradi posodobitve vsebine in načina pouka.

Fiziko najdemo v vseh treh programskih sestavinah. V skupnih programskih osnovah je namenjena vsem učencem, v primarnih programskih usmeritvah je prilagojena potrebam poklicev, v finalnih programskih usmeritvah pa se pojavlja kot samostojen strokovni predmet.

Fizika v skupnih programskih osnovah je splošnoizobraževalni predmet, ki se začenja v osnovni šoli in se zaključuje v 1. razredu usmerjenega izobraževanja s 76 urami letno. V vseh treh razredih obsega tako začetni pouk fizike skupaj 228 ur. V primarnih programskih usmeritvah nastopa fizika kot predmet, ki je osnova tehničnim predmetom in omogoča uspešno napredovanje učencev v raznih tehničnih strokah, podobno kot fizika v tehničnih šolah danes. Tej fiziki je namenjeno 76 ur, oz. 114 ur, pač glede na zahtevnost usmeritve. V finalnih programskih usmeritvah je fizika glavni predmet. Pojavlja se v naravoslovno-matematičnih smereh.

V načrtu srednjega usmerjenega izobraževanja je novost, da je fizika namenjena vsem učencem kot splošnoizobraževalni predmet. Osnovnošolsko fiziko v 7. in 8. razredu smo pred nekaj leti obnovili. Spremljava pa je pokazala, da je učnega gradiva v 8. razredu nekoliko preveč. Zato smo nekaj te snovi, ki sodi med temeljno učno gradivo, prenesli iz 8. razreda v 1. razred usmerjenega izobraževanja. Obsežneje pa smo zajeli poglavja iz atomike.

Učni načrt prvega razreda obsega: nihanje in valovanje, ki je bilo v manjšem obsegu v 8. razredu osnovne šole, elektromagnetno valovanje in (valovno) optiko ter poglavja iz atomike. Ta zajemajo foton, elektron, atome, jedra in osnovne delce. Zaključni učni program začetnega pouka fizike je temeljna učna snov, ki naj jo po zaključku 1. skupnega razreda srednje šole

pozna vsakdo. Za ta razred pripravljamo didaktični komplet, ki je sestavni del celote za potrebe začetnega pouka fizike.

Fizika kot osnovni predmet v primarnih programskih usmeritvah nastopa kot program A in kot program AB. Oba programa sta aplikativno in tehnično zasnovana in zajemata zlasti poglavja mehanike, elektrotehnike in termodinamike. S tem se s fiziko približamo zahtevam proizvodnje.

Program A je namenjen predvsem tehničnim usmeritvam, ki trajajo približno tri leta. Program AB je zahtevnejši in zajema program A v celoti. Predviden je za štiriletne srednje šole. Učenci, ki obvladajo program A, lahko z dopolnitvijo dobijo celotni program AB. V primeri z učnimi načrti v sedanjih tehničnih šolah obravnavamo v novem drugem letniku učno snov, ki je nismo v 1. letniku. Učno snov, ki smo jo prej obravnavali v drugem razredu, obdelamo po novem v prvem letniku, seveda v spremenjeni obliki. V drugem razredu pa poglobimo in razširimo osnovnošolsko učno vsebino; pri tem se naslanjamo na primere uporabe.

O fiziki, ki je strokovni predmet, še ne razpravljamo, ker je treba prej izdelati nove profile poklicev, ki jih zahtevajo nekatere gospodarske panoge.

Aleksander Kregar

OBŠOLSKA DEJAVNOST IZ MATEMATIKE V USMERJENI ŠOLI

Kot mentorica krožka mladih matematikov na gimnaziji Miloš Zidanšek v Mariboru imam že petnajst let izkušenj. Vsako leto vodim krožek za prvi razred; v njem se zbere okrog petnajst učencev iz vseh paralelk. Krožek dela po eno uro na teden, običajno pred poukom. Obravnavamo osnovni izrek iz kombinatorike, matematično indukcijo, linearno diofantsko enačbo in rešujemo veliko nalog iz tekmovalnih programov. Naloge morajo biti zanimive, da učence pritegnejo.

Učenci višjih razredov vodijo krožke sami. V teh krožkih je v poprečju samo še po pet učencev. Sestajajo se le občasno, kadar kdo pripravi kakšno zanimivo nalogo. Učencem izberem in razmnožim naloge, ki so večinoma v zvezi s tekočim učnim gradivom, včasih pa so vzete iz tujih virov. Svetujem jim literaturo in pomagam pri nalogah. V šolski knjižnici imamo dovolj gradiva za delo krožkov. Pri rednem pouku pogosto zastavim kako posebno nalogo. Vedno se najde kdo, ki se je loti in potem poroča o rešitvi.

Doslej so bili najuspešnejši tekmovalci tisti učenci, ki so sami veliko delali in znali študirati po domači in tuji literaturi.

Predlagam, da naj bo obšolska dejavnost v usmerjeni šoli programirana vzporedno z rednim delom. Na razpolago naj bo čas, mentor, gradivo in finančna stimulacija. Mentor bi moral dobiti program dela s seznamom dosegljive literature in imeti možnost za izmenjavo izkušenj pri delu s krožki. Šolska, republiška in zvezna tekmovanja pa naj ostanejo, kakršna so bila doslej.

Marija Munda

OBŠOLSKA DEJAVNOST IZ FIZIKE

Bil sem v zadregi, ko sem prejel vabilo, naj napišem nekaj o krožkih za fiziko, ker stalnih krožkov zaradi preobremenjenosti nisem imel. Imam pa izkušnje za delo z boljšimi fiziki pri praktičnih znanjih. V okviru rednih ur

smo obravnavali zahtevnejša poglavja in reševali težje naloge, predvsem pa opravljali praktične meritve.

V zadnji izdaji *Fizike* I. Kuščerja in A. Moljka lahko preberemo citat: »Ni široke ceste niti bližnjice do znanja.« Kot si znanost mukoma utira pot, tako si tudi mlad človek s trudom pridobiva znanje. Razni pripomočki lahko delno olajšajo umski napor, odpraviti pa ga ne morejo. Učitelj — mentor krožka naj bi vzbudil v mladih ljudeh zanimanje in veselje do predmeta, jih vodil in usmerjal pri njihovem razmišljanju in delu. Dobršen del celotnega dela naj opravijo dijaki sami v šoli pa tudi doma. Pri težavah naj jim pomaga učitelj.

Mlade ljudi veliko bolj zanima praktično delo kot teorija. Zato je primerneje, da jim damo konkretno nalogo, npr. merjenje določene količine. Dijaki pa si naj sami izberejo primeren način in ustrezne pripomočke in izvedejo meritve. Ob praktičnem delu se začno zanimati tudi za teoretično osnovo. Pri takem načinu dela nam manjka ustrezne literature. Mogoče pa se bo našel avtor, ki bi napisal izbrana poglavja iz fizike na srednješolski ravni. Knjiga bi lahko izšla v zbirki *Sigma*, posamezna poglavja pa morda v *Preseku* ali v *Obzorniku*.

France Perne

OBŠOLSKA DEJAVNOST IZ MATEMATIKE V OSNOVNI ŠOLI

Ena izmed nalog osnovne šole je skrbeti za nadarjene učence in za tiste, ki se še posebno zanimajo za kak učni predmet. Glede tega je pouk matematike v zadnjih letih nedvomno napredoval. Uveljavile so se individualne in skupinske oblike dela, pri katerih lahko obseg in zahtevnost nalog prilagodimo učencem.

Dodatni pouk, ki obsega tudi delo v matematičnih krožkih, je po zakonu o osnovni šoli sestavni del vzgojnoizobraževalnega programa. Zanj je treba zagotoviti potreben denar. Dodatni pouk pa je bolj zahtevno delo od rednega. Ker tega načela ne spoštujejo povsod, naj bi društvo opozorilo na pravilno vrednotenje dela.

Matematični krožki imajo tudi na osnovnih šolah lepo tradicijo. V celodnevni osnovni šoli jih bo treba še razširiti in izpopolniti, saj mora nova šola razvijati interesne dejavnosti učencev. Razprave na aktivih in rezultati tekmovanj pa kažejo, da je delo v krožkih v zadnjih letih manj uspešno. Vzrok niso le finančne težave, temveč zlasti pomanjkanje in preobremenjenost usposobljenih učiteljev matematike. Vedno več učiteljev zapušča osnovno šolo ali pa se takoj po končanem študiju zaposli drugje; to je že dalj časa pereč pojav.

Društvo je veliko pomagalo učiteljem pri delu z nadarjenimi učenci s prispevki v *Preseku* in z zbirkami tekmovalnih nalog. Žal še nimamo metodične literature za to področje.

Verjetno bi lahko posvetili krožkom več skrbi v aktivih, ki bi jih organizirali za manjša območja in povezali s hospitacijami pri izkušenih učiteljih. Metodiko dela z nadarjenimi učenci bo treba vključiti v program seminarjev za izpopolnjevanje učiteljev, že med študijem pa moramo prihodnje učitelje metodično pripraviti na dodatni pouk. Študenti drugega letnika pedagoških akademij naj bi sodelovali pri delu krožkov v osnovnih šolah.

Mogoče so še druge oblike dela z nadarjenimi učenci. Poletne matematične šole v Beogradu so se lani udeležili trije naši učenci, letos pa štirje. Ali ne bi mogli take šole organizirati tudi pri nas, npr. za 20 učencev, ki so bili uspešni na republiškem tekmovanju? Ker so šole prevzele stroške za svoje učence na zveznem tekmovanju, verjetno ne bi bilo težav s financiranjem poletne šole.

Tekmovanja za Vegova priznanja potekajo že sedmo leto. Pri organizaciji uspešno sodelujejo šole, društvo in zavod za šolstvo. Na občinskih tekmovanjih je vsako leto okrog 3000 učencev. Od teh si približno tretjina pridobi srebrno Vegovo priznanje. Na republiških tekmovanjih, ki so samo za učence 8. razreda, je od 200 do 300 udeležencev. Skupaj jih je bilo dozdaj 1593, osvojili pa so 469 zlatih Vegovih priznanj.

Tekmovanja naj bodo spodbuda in nagrada za sposobne in prizadevne učence. Ta cilj dosežemo, če so učenci na tekmovanje dobro pripravljeni in naloge primerno izbrane. Za oboje je treba v prihodnje še bolj skrbeti.

Franc Galič

TEKMOVANJE IN DRUGE PROPAGANDNE MOŽNOSTI ZA FIZIKO

Društvo že 12 let prireja tekmovanja iz fizike. Dijaki, ki so uspešni na šolskih tekmovanjih, se lahko udeleže republiškega. Tekmujejo v reševanju računskih nalog iz šolske učne snovi za fiziko, in sicer po letnikih.

Dobro bi bilo jasneje določiti, v čem se tekmuje, v katerem znanju in spretnostih. Za tekmovanje naj bi se pripravljali že med letom. Tekmovalna komisija naj bi občasno objavljala informativne vzorne naloge v ustreznem časopisu ali pa jih pošiljala interesentom. Na dan tekmovanja naj bi bil tudi strokovni program srečanja: razgovori s fiziki, pregledna predavanja, strokovni kvizi, poučni filmi itd.

V novih okoliščinah učna snov ni več določena samo z letniki. Zato je treba pri razpisu navesti vsako leto tudi področja fizike, ki se izberejo za tekmovanje.

Tekmuje naj se ne le v reševanju nalog, ampak tudi v načrtovanju poskusov in meritev, v znanju pojavov izbranega področja in pojasnjevanju fizikalnih osnov uporab, v zgodovinskem razvoju izbranega področja.

Med letom naj se objavi po nekaj primerov tekmovalnih nalog za vsako podskupino.

S širšim tekmovalnim programom bomo morda pritegnili več mladih, ki imajo veselje za fiziko, pa ne izključno za računske naloge.

Potrebno pa bi bilo, da bi več članov sodelovalo pri načrtovanju tekmovanj in pri obsežnejših pripravah.

Ker bo fizika učencem deloma na izbiro, bo treba izkoristiti razne možnosti za informiranje o pomenu znanja fizike in za pridobivanje zanimanja in naklonjenosti javnega mnenja, skratka za reklamo za fiziko. Take možnosti so na primer:

Obveščanje javnosti o *tekmovanjih,* da bi postala družbeno pomemben kulturni dogodek.

Dobri in navdušujoči članki v časopisih o novostih iz fizike in o fizikalnih osnovah novih strokovnih dosežkov; potrebne so tudi brošure o problem-

skih področjih fizike in čitanke s študijskim berilom, saj razen učbenikov nimamo skoraj nič.

Razpisi za esejsko obravnavo določene teme ali teme po izbiri v okviru razpisanega študijskega projekta. Najboljše izdelke bi lahko brali avtorji na tekmovalni dan v okviru strokovnega programa.

Konferenca mladih fizikov: društvo naj organizira konference po zgledu konferenc za starejše fizike. Na konferencah bodo mladi poročali o rezultatih manjših študijskih ali eksperimentalnih raziskovalnih nalog, ki si jih izberejo v okviru področja konference po dogovoru z učiteljem kot mentorjem. Konferenco je treba napovedati eno leto naprej.

Poletna šola za mlade fizike iz raznih področij fizike, iz fizikalnega eksperimentiranja ali računskega simuliranja eksperimentov. Večdnevno šolo naj bi izmenoma organizirali šolski centri v raznih krajih Slovenije v sodelovanju z društvom.

Fizika na RTV. Društvo naj skuša pridobiti vsaj 15 minut na mesec za fiziko na R in na TV z načrti aktualnih obravnav in mikavnih scenarijev. Seveda je priprava zahtevna in se ne uspe več brez priprave, samo z improvizacijo. Treba bo sestaviti skupino zainteresiranih sodelavcev.

Tekmovanje v naravoslovnem znanju v okviru družabne prireditve.

Uporaba reklamnih metod za širjenje znanja fizike. Lepaki z gesli in slikami na raznih mestih in predmetih bi lahko prinašali več fizike v vsakdanje življenjsko okolje, da ne bo ostala le v knjigah kot sedaj.

Z delno prosto izbiro predmetov bo šolsko življenje bolj razgibano. Novosti, ki se jim sedanji pouk fizike izogiba, bodo dobile večjo veljavo. Zato bo treba neprestano dopolnjevati možnosti za navduševanje za fiziko.

Seveda pa društvo ni edina interesna skupnost za fiziko. Marsikaka strokovna iniciativa se bo lahko izvedla z medšolskimi dogovori v okviru rednega dela učiteljev.

Anton Moljk

VPRAŠANJA

Vprašanje 112

Na nekem otoku živi n živalskih vrst. Vsaka si je prisvojila n-ti del otoka, tako da so njihovi življenjski prostori popolnoma *ločeni.* Na otok pripluje n ladij, na vsaki drugo pleme. Poselijo otok tako, da ga razdele vsakomur *enako* — kot so to storile že živali pred njihovim prihodom. Vsako pleme mora imeti svojo *sveto žival*, vendar mora ta izpolnjevati dve zahtevi:

1. ozemlje, na katerem živi, se mora vsaj deloma ujemati z ozemljem plemena, kateremu pripada;

2. ne sme biti hkrati sveta žival več plemen.

Vprašanje: *Ali je tak izbor vselej mogoč, ne glede na to, kako se plemena razselijo po otoku?*

Dušan Repovš

DOMAČE VESTI

POROČILO O SEMINARJU MATEMATIČNA LOGIKA

Seminar *Matematična logika* je — kot je že navada — pripravilo Društvo matematikov, fizikov in astronomov SRS ob sodelovanju odseka za matematiko fakultete za naravoslovje in tehnologijo, Inštituta za matematiko, fiziko in mehaniko ter Zavoda za šolstvo SRS. Za seminar smo porabili štiri dni zimskih počitnic od 1. do 4. februarja.

Na seminarju so se predstavili mladi člani odseka za matematiko. Samo vodja Niko Prijatelj je bil po letih izjema, pa še on je zaradi mladeniške vneme ob predavanjih leta čisto zatajil. Ob izbiri predavanj so predavatelji privzeli, da nam je uvod v matematično logiko znan vsaj v tolikšnem obsegu, kot ga vsebuje ustrezna knjižica zbirke Sigma.

Ker je matematična logika razmeroma mlada veda, ki se naglo razvija, je v njej še marsikaj nedodelanega. Vedno znova nam matematična logika razčiščuje in bolj natančno določa osnovne pojme. O teorijah je predaval Vladimir Batagelj. Čeprav obravnavajo teorije različna področja, imajo nekaj skupnega. Določene so z elementarnimi izjavami in izreki. V formalnih teorijah aksiomi implicitno določajo razred objektov in iščemo odgovor na vprašanje, ali sploh obstaja razred objektov, ki zadošča aksiomom. Razvoj nauka o teorijah je vplival tudi na logično utemeljitev analize in teorije množic. Znani so paradoksi, ki so posledica premalo točno formuliranih aksiomov.

V predavanju Nika Prijatelja smo se naučili še enega »tujega jezika«, in sicer jezika prvega reda. Jezik prvega reda je bolj skop kot materinščina, saj ima samo sedem različnih sort znakov, je pa dovolj bogat, da sestavimo sintakso jezika. Za primer smo v jeziku prvega reda izrazili elementarno teorijo naravnih števil in teorijo množic. Sintaksi jezika smo dodali še njegovo semantiko ali pomenoslovje. Simboli jezika zadobe pomen z interpretacijo. Če ima teorija še lastne aksiome, je vprašanje, ali obstaja takšna interpretacija teorije, pri kateri so vsi lastni aksiomi pravilni.

Izidor Hafner je izpeljal izrek o dedukciji. Svoje predavanje je popestril z izpeljavami izrekov iz elementarne matematike po formalno logični poti. Težava je že v tem, ker so aksiomi marsikdaj tako formulirani, da jih ne moremo napisati v jeziku prvega reda. Zato tudi dokazi niso mogoči v jeziku prvega reda. Že Evklid se je pri dokazovanju marsikdaj oprl na sliko.

Tomaž Pisanski se je lotil zahtevne naloge, ki je že zelo stara: ali je mogoče vsak matematični problem rešiti že po vnaprej znanem postopku, tako kot znamo zmnožiti dve števili? Ali je mogoče napraviti stroj, ki bi znal z univerzalnim algoritmom rešiti vsak matematični problem? Ukvarjali smo se z delovanjem Turingovega stroja in ugotovili, da stroji ne bodo nadomestili matematikov. So problemi, ki jih Turingov stroj ne more rešiti. Udeleženci seminarja so se ob tem predavanju razveselili domačih nalog, čeprav so jih nekateri pogumno »prešpricali«.

O logiki in množicah v srednji šoli je govoril Janez Rakovec. Logiko in teorijo množic vpeljemo že takoj v začetku srednje šole. V prvi letnik pridejo izjave in njihove povezave. Logične ekvivalence in implikacije obdelamo hkrati z analognimi ugotovitvami o množicah. Izjavni račun uporabljamo pri dokazovanju že v 1. letniku, z njim se srečamo ponovno v 4. letniku pri Boolovi

algebri. Ob vpeljavi spremenljivk se je treba ustaviti pri vlogi konstant in spremenljivk v sami logiki. Funkcijo kot preslikavo med množicama vpeljemo navadno šele v 3. letniku. Lahko pa to napravimo takoj v 1. letniku. Tudi pojme surjektivnosti, injektivnosti, bijektivnosti funkcije bi s pridom uporabili že v 2. letniku. Aksiomatično metodo najbolj dosledno izkoristimo pri poučevanju geometrije in algebre. Relacije, zlasti dvomestne in še posebej ekvivalenčne relacije vpeljemo že v 1. letniku. Primerov za te relacije v aritmetiki in geometriji ne manjka.

Še o rezultatih ankete. Nekateri udeleženci so mnenja, da je nivo predavanj previsok. Pogosto želijo, naj bi predavanja vsebovala več primerov, ki bi bili uporabni v srednji šoli. Anketa kaže še na neko hibo seminarja: na prenatrpanost. Sedem ur tako zahtevnih predavanj na dan je preveč, po drugi strani pa ne kaže podaljševati seminarja na več dni; večina meni, naj bi trajal le tri dni. Nekateri predlagajo, naj bi seminar organizirali zunaj Ljubljane, da bi udeleženci tudi preostali čas preživeli skupaj. Predlogi za naslednji matematični seminar so dokaj pestri: matematika v usmerjenem izobraževanju (obravnavanje morebitne nove snovi, nove učne metode), statistika, informatika, zgodovina matematike.

Na seminarju je bilo 110 udeležencev, ki so pogumno sledili zahtevnim predavanjem. Zvečine so bili učitelji s srednjih šol. Veseli smo, da smo spet imeli v svoji sredi kolege iz Trsta in Celovca. Tako dobro kot seminar pa ni uspel družabni večer društva v hotelu Bellevue. Očitno kolegi matematiki v domačem okolju niso znali logično utemeljiti potrebo po navzočnosti na družabnem večeru, saj je bilo število udeležencev nepričakovano majhno.

Naslov seminarja so izbrali udeleženci takratnega seminarja že pred dvema letoma. Upam si trditi, da nad tem seminarjem udeleženci niso bili razočarani, čeprav je bil del predavanj prezahteven zlasti za starejše kolege, ki jim je ta snov bolj tuja. Nekaj pa smo vsi odnesli s seminarja: spoznanje, da je matematika živa znanost, da pogumno odpravlja svoje zmote in pomanjkljivosti in da razvoj matematike odlično dokazuje resničnost Cantorjevega izreka: Bistvo matematike je v njeni svobodi.

Martina Koman

OBVESTILO

Na podlagi pravil o podeljevanju priznanja učiteljem matematike, fizike in astronomije za delo z mladimi (Obzornik mat. fiz. **21** *(1974) 5) vabimo podružnice Društva matematikov, fizikov in astronomov, aktive matematikov in fizikov na šolah, da do 1. oktobra 1978 predlagajo kandidate za priznanje za delo z mladimi.*

Predloge z utemeljitvami pošljite na naslov DMFA SRS, Komisija za pedagoško dejavnost, 61001 Ljubljana, Jadranska 19, poštni predal 227.

Martina Koman

DESETO ZVEZNO TEKMOVANJE ŠTUDENTOV MATEMATIKE

Lansko deseto zvezno in tretje mednarodno tekmovanje študentov matematike je bilo od 1. do 4. aprila 1977 v Beogradu. Organizator je bila osnovna organizacija Zveze socialistične mladine odseka za matematiko, mehaniko in astronomijo beograjske prirodoslovno matematične fakultete. Cilj tekmovanja naj bi bila demonstracija znanja, ustvarjanje vezi in izmenjava izkušenj med študenti jugoslovanskih in tudi tujih fakultet.

Na letošnjem tekmovanju je sodelovalo 18 ekip v konkurenci in 5 z nematematičnih fakultet (elektro, strojna...) izven konkurence. Med ekipami v konkurenci so bile tudi skupine z Dunaja, iz Prage, Szegeda in Budimpešte, kar je dalo tekmovanju mednarodni značaj.

Strokovni del tekmovanja, ki je v resnici najobčutljivejši, ni bil najbolje pripravljen, ker je — kot običajno — padel na ramena majhnega števila bolj zagnanih beograjskih asistentov. Tu naj predvsem omenimo neutrudna M. Božića in V. Jankovića. Zaradi različnih učnih načrtov je sestavljanje nalog, ki bi bile primerne za vse, skoraj nemogoče.

Prvi in drugi letniki niso mogli izbirati. Rešiti so morali štiri naloge iz analize in linearne algebre. Višji letniki pa so imeli na izbiro naslednja področja: funkcionalna analiza, geometrija, topologija, algebra, programiranje, verjetnostni račun, funkcije kompleksnih spremenljivk in diferencialne enačbe. Vsak je izbral po dve področji. Za reševanje štirih nalog so imeli tekmovalci štiri ure časa.

Popravljanje nalog je bilo organizirano neracionalno. Vsak je popravljal vse naloge tekmovalcev svoje ekipe in nato so jih popravili še enkrat. Vsak član žirije je tako izgubil okrog pet ur časa. Kot že mnogokrat prej, se je tudi letos primerilo, da ni naloga štela nič, če je študent uporabil znan izrek, ki ga je slišal pri predavanju ali vajah, ni ga pa v učnem programu beograjske fakultete. Predvsem na to past opozarjam bodoče tekmovalce.

Ljubljansko fakulteto sta zastopali dve ekipi (beograjsko štiri). Tekmovalci so bili Franci Forstnerič, Dušan Repovš, Andrej Vitek in Bojan Mohar, Meta Suhač in Barbara Šorli. Prva ekipa je zasedla šesto, druga pa dvanajsto mesto med skupno osemnajstimi ekipami. Najboljše tri ekipe so bile: 1. Budimpešta, 2. prva ekipa Beograda in 3. ekipa iz Szegeda. Pri posameznikih je bil v skupini prvih in drugih letnikov najboljši Kolar iz Budimpešte, ki je dosegel 100% točk. Med Jugoslovani je bil v tej skupini najboljši Franci Forstnerič in se je zato udeležil balkaniade matematikov, ki je bila poleti v Beogradu. Pri višjih letnikih je bil najboljši Facfi iz Budimpešte, od Slovencev pa Andrej Vitek.

Kar se tiče drugega cilja tega tekmovanja, mislim, da ni bil dosežen. Program je bil tako zelo natrpan, da študentje skorajda niso imeli časa za pogovor s komerkoli iz drugih ekip.

Naloge za prvi in drugi letnik

1. Ali obstaja zaporedje pozitivnih realnih števil $\{a_n\}$, za katero velja:

$$\sum_{n=1}^{\infty} (a_{n+1}\, a_{n+1} \dots a_{n+m})^{1/m} = \begin{cases} < \infty : m & \text{sod} \\ + \infty : m & \text{lih} \end{cases}$$

2. Naj bo A nesingularna realna matrika $n \times n$, za katero velja:

$a_{ij} \leqq 0$, če $i \neq j$ in

$$\sum_{j=1}^{n} \lambda_j a_{ij} \geqq 0 \qquad (i = 1, 2, \dots n) \quad \text{za neka pozitivna števila } \lambda_j$$

Naj bodo $b_1, b_2, \dots, b_n$ poljubna nenegativna realna števila. Dokaži, da ima sistem

$$AX = \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} \qquad \text{nenegativno rešitev.}$$

3. Naj bosta f, g: $[a, b] \to R$ zvezni funkciji, za kateri obstajata desna odvoda v vsaki točki $x \in [a, b]$. Dokaži: Če je $|f'_+(x)| \geqq g'_+(x)$ za vsak $x \in [a, b)$, potem je $|f(b) - f(a)| \leqq$ $\leqq g(b) - g(a)$.

4. Naj bo f: $[-1, 1] \to R$ petkrat odvedljiva funkcija.

a) Določi konstante A, B, C, D, E tako, da velja

$$Af(2h) + Bf(h) + Cf(0) + Df(-h) + Ef(-2h) = f''(0)h^2 + 0(h^5)$$

b) Ali je tak izbor vedno mogoč, če predpostavimo, da je f samo štirikrat odvedljiva?

Funkcionalna analiza

1. Naj bo $\geq$ taka relacija linearne urejenosti na $[0, 1]$, da je za vsak $y \in [0, 1]$ množica $\{x;\ x \leq y\}$ največ števna. Ali je množica

$$E = \{(x, y) \in [0, 1]^2;\ x \leq y\}$$

merljiva?

2. Naj bo X realen Banachov prostor in $x_1, x_2, \ldots x_n \in X$. Ali je množica

$$A = \{\lambda_1 x_1 + \lambda_2 x_2 + \ldots + \lambda_n x_n;\ \lambda_i \geqq 0\}$$

zaprta?

Geometrija

1. V ravnini π imamo dana dva skladna trikotnika nasprotne orientacije: ABC in $A'B'C'$. V absolutni geometriji dokaži, da središča P, Q, R daljic AA', BB', CC' ležijo na skupni premici.

2. V geometriji Lobačevskega dokaži, da imata dve nekomplanarni premici eno samo skupno normalo.

Topologija

1. Naj bo X kompakten in Y poljuben topološki prostor, F poljubna podmnožica produkta $X \times Y$ in $p_1: X \times Y \to X, p_2: X \times Y \to Y$ naravni projekciji. Dokaži, da za poljubno točko $y_0 \in p_2(F)$ in poljubno okolico U množice $p_1(F \cap p_2^{-1}(\{y_0\}))$ obstaja okolica V točke y_0 v Y, da je za vsak $y \in V$

$$p_1(F \subset p_2^{-1}(\{y\})) \subseteq U.$$

2. Naj bosta f: $I \to I$ in g: $I \to I$ takšni zvezni preslikavi intervala $I = [0, 1]$ vase, da komutirata ($f \circ g = g \circ f$). Pokaži, da obstaja $x \in I$, za katerega velja $f(x) = g(x)$.

Algebra

1. Naj bo $(G, +)$ Abelova grupa, v kateri ima vsak element red dva (to je: $x + x = 0$). Ali lahko v G tako definiramo operacijo $\cdot$, da bo $(G, +, \cdot)$ Boolov kolobar (to je: kolobar z enoto, v katerem je $x^2 = x$)?

2. Dokaži ali ovrzi naslednjo trditev:
V množici celih števil lahko definiramo množenje s pomočjo seštevanja, odštevanja in potenciranja s poljubnimi lihimi eksponenti (to je: obstaja tak izraz $t(x, y, +, -, {}^3, {}^5, \ldots)$, da je $x \cdot y = t(x, y, +, -, {}^3, {}^5, \ldots)$

Programiranje

1. Podanih je n mest in razdalje med njimi, če med njimi obstajajo poti. Pri danem paru števil med 1 in n je treba izračunati najmanjšo razdaljo med mestoma s tema številkama.

2. Podana je vrstica z naslednjo vsebino:

$$\langle a \rangle = \langle b \rangle$$

kjer je:

$\langle a \rangle$ ime celoštevilčne spremenljivke, sestavljeno iz ene črke (torej I, J, K, L, M, N), $\langle b \rangle$ pa je celoštevilčni izraz, v katerem nastopajo le konstante med 0 in 9, operacije +, —, * in poljubno število oklepajev.

Napišite algoritem in program, ki izpiše vrednost spremenljivke.

Verjetnostni račun

1. Naj bo $\lambda \in (0, 1)$. Razišči, ali obstaja verjetnostni prostor $(\Omega, \mathcal{F}, P)$ in zaporedje neodvisnih nekonstantnih slučajnih spremenljivk $\{X_n\}$, definiranih na $(\Omega, \mathcal{F}, P)$, tako da pri tem v $\mathcal{F}$ ni niti enega elementa, katerega verjetnost (P-mera) je λ.

2. a) Naj bo $0 \leqq a \leqq b$ in U, V slučajni spremenljivki, obe enakomerno porazdeljeni na $[a, b]$. Pokaži, da je

$$\frac{a^2 + 4ab + b^2}{6} \leqq E(UV) \leqq \frac{a^2 + ab + b^2}{3}$$

b) Naj bodo X_n in Y_n slučajne spremenljivke, enakomerno porazdeljene na $[0, n]$ in definirane na istem verjetnostnem prostoru. Naj bo $X_n^{-1}([m-1, m]) = Y_n^{-1}([m-1, m])$ $m = 1, 2, \ldots n$.

Dokaži, da za koeficiente korelacije ρ_n med X_n in Y_n velja neenakost $1 - \frac{2}{n^2} \leq \rho_n$.

Funkcije kompleksnih spremenljivk

1. Naj bo f: $K \to C$ $(K = \{z \in C : |z| < 1\})$ taka enolista analitična funkcija, da je $f(0) = 0$ in $f'(0) \neq 0$. Naj bo F: $K \to C$ analitična funkcija, za katero velja $(F(z))^n = f(z^n)$. Pokaži, da je tudi F enolista!

2. Naj bo f: $[a, b] \to C$ dvakrat zvezno odvedljiva funkcija, za katero velja:

$$|f'(t)| \geqq 1 \quad \text{in} \quad |f'(t)| \geqq |f(t)| \quad \text{za vsak } t \in [a, b]$$

Pokaži, da je

$$\int_a^b |f''(t)|\, dt \geqq b - a - 2$$

Diferencialne enačbe

1. Naj bo f zvezna funkcija, definirana na celi realni osi, in naj bo $\lim_{x \to +\infty} f(x) = +\infty$. Ali ima enačba

$$y'' + f(x)y = 0$$

rešitev, ki ni omejena, ko gre x proti ∞?

2. Ali ima enačba

$$y' = (y^2 - 1)(y - f(x))$$

nekonstantno periodično rešitev za vsako zvezno realno periodično funkcijo $f(x)$?

Mirko Dobovišek

RAZMIŠLJANJE O TEKMOVANJU IZ MATEMATIKE

Kakor tekmovanje iz fizike*, ima tudi tekmovanje srednješolcev iz matematike že lepo tradicijo. Letos so v Mariboru organizirali že 22. republiško tekmovanje. Prvih tekmovanj se je udeleževalo malo dijakov. Kasneje se je število povečalo, na nekaterih šolah pa so prirejali tudi šolska tekmovanja. Zdaj veljajo ta kot kvalifikacije za republiško tekmovanje. Tako popularna in koristna dejavnost društva in šol pa zahteva vse več priprav in organizatorji se pritožujejo nad obilico administrativnega dela. V letošnjem letu smo vabilo za republiško tekmovanje objavili prvič kar v *Preseku,* tako da so izvedeli zanj učitelji in učenci hkrati. Zato so lahko tudi učenci sami prevzeli iniciativo za udeležbo. Dijakov in učencev, ki se zanimajo za tekmovanja, na Presek pa niso naročeni, je pa zagotovo zelo malo.

Republiški komisiji za tekmovanja, ki pripravlja in pošilja naloge na vse srednje šole, je vseeno ostalo še veliko dela. Torej bi morda kazalo razmisliti o novem načinu tekmovanja. Pri tem bi lahko prinesla naloge za šolska tekmovanja vsakokratna tretja številka *Preseka* in bi dijaki naloge reševali doma brez »policijskega nadzorstva«. Imeli bi več časa za premišljevanje in bi lahko oddali tudi po obliki lep izdelek. Verjetno je tudi, da bi se jih več lotilo reševanja, naloge pa bi oddali le tisti, ki bi uspeli. Izdelkov ne bi pošiljali naravnost republiški komisiji, pač pa bi jih oddali učiteljem na šoli. Nevarnost, da bi tekmovalci naloge prepisovali, je po dosedanjih izkušnjah zares velika. Če pa bi dijakom pravilno razložili pomen in namen tekmovanj, se nam z leti tega ne bi bilo treba več bati. Poleg tega bi slabi dijaki le težko rešili vse naloge in ne bi na republiškem tekmovanju ponovili uspeha s predtekmovanja. Tudi dosedanja praksa pri reševanju nalog iz *Preseka* jih vzgaja v tem smislu.

O tem predlogu in o tekmovanju nasploh (težavnost in povezanost nalog z učnim programom, posebne naloge za tehniške šole, sodelovanje pri sestavljanju nalog, organizacija, nagrajevanje itd.) bi se bilo morda vredno pogovoriti na posebnem sestanku učiteljev matematike, ki so doslej organizirali tekmovanja. Ker po končanih republiških tekmovanjih vsi hitijo domov, bi bil tak sestanek smiseln ob občnem zboru društva. Tedaj je nekaj časa za take razgovore. Ker se vsi udeleženci ne ukvarjajo s tekmovanji, ker je v tako velikem krogu (150) le težko doseči živo debato (navadno se sprejmejo po hitrem postopku prav vsi predlogi ne glede na to, koliko so bili prediskutirani), bi bilo primerno morda tudi o nekaterih drugih vprašanjih (vsebina Preseka), ki ne zanimajo vseh članov društva, razpravljati po komisijah in seznaniti občni zbor z že izoblikovanimi predlogi.

Ciril Velkovrh

---

* Posvet o tekmovanju iz fizike, Obzornik mat. fiz. **24** (1977) 149.

PREJELI SMO V OCENO

Chow Yutze, Modern Abstract Algebra, vol. 1, 2. New York, Gordon and Breach, 1976, 742 str., cena 40 £.

Delo je zamišljeno kot učbenik algebre, in sicer predvsem za podiplomski študij; vendar je čisto ustrezno tudi za učbenik na dodiplomskem študiju, ker je lahko berljivo in ker avtor privzame za znane le osnovne pojme teorije množic (sem pa opazil nekaj spodrsljajev, ki bi utegnili začetnika zmesti). Vsekakor je *Modern Abstract Algebra* popolnoma enotno delo in je bilo razdeljeno na dve knjigi le zaradi obsega. Moram pa opozoriti, da ni tako zelo obsežno, kot bi bilo sklepati iz števila strani. Knjigi namreč nista tiskani z običajnim tiskom, ampak gre za kopijo tipkopisa. Pri običajnem tisku delo ne bi obsegalo več kot 400 strani.

Navedimo spisek poglavij: 1. Monoidi in polgrupe, 2. Grupe, 3. Kolobarji, 4. Moduli, 5. Homomorfizmi modulov, 6. Algebre. Ta spisek seveda ne pove vsega o vsebini. Mislim, da je v primeri z drugimi splošnimi učbeniki algebre zajeta snov dokaj široka, globokih izrekov pa zato seveda ne more biti prav dosti. Naj omenim zanimivost, da je avtor profesor fizike (prej pa je bil profesor elektrotehnike); vendar je *Modern Abstract Algebra* čisto matematično delo in nikjer niti ne omenja kake uporabe algebre v fiziki.

Jože Vrabec

Joram Lindenstrauss in Lior Tzafriri, Classical Banach spaces I, Sequence spaces, Ergebnisse der Mathematik und ihrer Grenzgebiete 92, Springer Verlag, Berlin Heidelberg New York 1977, 190 str.

Zaporedje $\{x_1, x_2, \ldots\}$ elementov Banachovega prostora X je *Schauderjeva baza* za X, če za vsak $x \varepsilon X$ obstaja natanko določeno zaporedje skalarjev $\{a_1, a_2, \ldots\}$, tako da je $x = \sum_{n=1}^{\infty} a_n x_n$. (Primer: ortonormirana baza separabilnega Hilbertovega prostora). Že Banach je vprašal, ali ima vsak separabilen Banachov prostor kako Schauderjevo bazo. Preden povemo odgovor, definirajmo: Banachov prostor X ima *aproksimacijsko lastnost,* če za vsak Banachov prostor Y in vsak kompakten operator $T : Y \to X$ in vsak $\varepsilon > 0$ obstaja izrojen operator $T_1 : Y \to X$, tako da je $\| T - T_1 \| < \varepsilon$. Leta 1973 je švedski matematik Per Enflo objavil primer Banachovega prostora, ki nima aproksimacijske lastnosti. Tak prostor pa tudi ne more imeti Schauderjeve baze. Primere takih »grdih« prostorov so pozneje našli celo med podprostori prostorov c_0 in l_p $(2 < p < \infty)$.

Vse to lahko med drugim zvemo v prvi knjigi dela Classical Banach spaces L. Lindenstraussa in L. Tzafririja. Snov spada v izomorfno teorijo Banachovih prostorov, ki je prav v zadnjem času doživela velik razmah. Značilnost tega področja je izredna, skoraj nepregledna množica rezultatov, med katerimi pa so nekateri zelo težki in tudi presenetljivi.

Naša knjiga obravnava samo prostore zaporedij. Poglavja so razvrščena takole: Schauderjeve baze. Prostori c_0 in l_p. Simetrične baze. Orliczevi prostori zaporedij. Slog je jasen in energičen, dokazi so kratki, mnoge pripombe in obširen seznam literature pa bodo pomagali tudi raziskovavcu. Kot trdita avtorja, je večina materiala tu prvič podana v knjižni obliki. Tudi brez tega ima knjiga vse možnosti, da postane standarden učbenik in referenca na tem področju.

Peter Legiša

Pál Quittner, Problems, Programs, Processing, Results. Software Techniques for Sci-Tech Programs, Akadémiai Kiadó, Budapest 1977, 381 str.

Knjiga je razdeljena na 12 razdelkov: Uvod — Problemi in rezultati — Od programa do rezultatov — Strojni jezik — Zbirni jeziki in zbirniki — Prevajalniki — Loaderji — Preverjanje programov in dokumentacija — Organizacija podatkov in podatkovne strukture — Operacijski sistemi — Nekaj praktičnih nasvetov — Slovarček pojmov.

Zastavljena je izredno široko, morda preširoko. Obravnava takorekoč vsa pomembna območja računalništva. Avtor jo je namenil inženirjem, kemikom, fizikom, ekonomistom in drugim, ki pišejo programe v problemsko usmerjenih jezikih.

Zaradi bogatosti področja, ki ga delo obravnava, so nekatere teme obdelane le povrhu, tako da ima knjiga enciklopedičen značaj. To pa ji štejemo v škodo, saj je ne moremo priporočiti tistim bralcem, za katere je pisana, vsaj začetnikom ne.

V naših razmerah lahko knjigo priporočimo za pomožni učbenik — priročnik tistim bralcem, ki že imajo trdne osnove računalništva, pa bi želeli svoje znanje na tem področju poglobiti. Knjiga jim bo z določeno rezervo vodnik po računalniški deželi.

Alain Bouvier, Théorie élémentaire des séries. Paris, Hermann, 1971, 227 str.

Pomemben del klasične analize je posvečen študiju vrst. Knjiga Alaina Bouviera obravnava vrste od navadnih številskih pa tja do Fourierovih vrst. Zanimiva bo za vse študente, ki poslušajo matematiko. Pogoj je seveda znanje francoščine. Avtor pa od bralca pričakuje hkrati z znanjem srednješolske matematike še poznavanje infinitezimalnega računa in linearne algebre.

Knjiga je zanimiva, saj kaže analizo iz posebnega zornega kota. Kopica nalog v njej (žal (?) brez rešitev) bo samoukom predvsem pa študentom pred kolokviji in izpitom v veliko pomoč pri preverjanju znanja.

Tomaž Pisanski

Arlen Brown, Carl Pearcy, Introduction to Operator Theory I, Elements of Functional Analysis, Springer-Verlag, New York, Heidelberg, Berlin, 1977, XIV + 474 str. (Graduate Texts in Mathematics; 55) Cena DM 54.—

Knjiga je učbenik funkcionalne analize in je nastala na osnovi predavanj te snovi. Za razumevanje funkcionalne analize in operatorske teorije je treba poznati nekaj linearne algebre, splošne topologije, kompleksne analize in teorije mere. Vendar avtorja nista kar predpostavljala takega znanja, ampak sta tej snovi posvetila kar 10 poglavij. — Drugi del knjige pa obravnava normirane linearne prostore, omejene linearne transformacije, Hahn-Banachov izrek, Banachove prostore s teorijo integracije, prostore $\psi(X)$ in baze.

Matematike se pač ne da naučiti le z branjem izrekov in dokazov, ampak je treba snov ilustrirati z zgledi, predvsem pa razumevanje snovi preskusiti z nalogami in problemi. In zato sta avtorja vsako poglavje bogato opremila z zgledi in seveda problemi, katerih namen je v glavnem utrjevanje snovi, včasih pa se z njimi vpeljejo tudi novi pojmi in rezultati. Morda je posebnost knjige, da so problemi na široko opisani in da so pri marsikaterem dana tudi navodila za reševanje.

Knjiga je pisana strogo, sistematično in ne v preveč strnjenem slogu in bo tudi glede na zbrano snov prav gotov dobrodošel učbenik funkcionalne analize našim študentom matematike in tudi tistim, ki bi kdaj pa kdaj hoteli poglobiti oziroma obnoviti znanje funkcionalne analize.

Gabrijel Tomšič

Sparse matrix techniques, Berlin, Springer-Verlag 1977.

V zbirki Lecture Notes in Mathematics (Springer-Verlag, Berlin • Heidelberg • New York, 1977), je pod uredništvom V. A. Barkerja izšla na 184 straneh knjiga Sparse Matrix Techniques. V njej so objavljena štiri predavanja, ki so jih imeli avtorji na tečaju z naslovom Course in Advance Sparse Techniques; organiziral ga je Inštitut za numerično matematiko Tehnične univerze v København leta 1976. Vsi štirje predavatelji so vodilni strokovnjaki v svetu na področju numeričnih metod za reševanje problemov linearne algebre v zvezi z razpršenimi matrikami, to je takimi, ki imajo pretežno število ničel, neničelni elementi pa so v bolj ali manj pravilnem vzorcu razmetani po celi matriki. Namen tečaja je bil posredovati znanstvenikom in inženirjem stanje znanosti na tem čedalje bolj pomembnem področju. Ta štiri predavanja podrobno obravnavajo nekatera poglavja, ki imajo osrednjo vlogo, ne pokrivajo pa celotnega področja.

Vsebina:

Owe Axelsson, Solution of linear systems of equations: iterative methods.

J. Alan George, Solution of linear systems of equations: direct methods for finite element problems.

John K. Reid, Solution of linear systems: direct methods (general).

Axel Ruhe, Computation of eigenvalues and eigenvectors.

Zvonimir Bohte

W. Bartl, W. Köchner, J. Mitterauer, R. Patzelt, G. Schiffner. Impulse in der Grenzphysik, R. Oldenbourg, Wien-München 1976, 172 strani. (Impulstechniker; 6)

H. Bertele izdaja pri založbi R. Oldenbourg zbirko knjižic z naslovom Tehnike sunkov. Pred nami je šesta knjižica te zbirke Sunki na mejnih področjih fizike. Prejšnje knjižice so obravnavale uvod v tehnike električnih sunkov, sunke v informacijski tehniki, uvod v stohastično-ergodijsko tehniko sunkov, krmiljenje in uravnavanje z električnimi sunki in tehniko močnih sunkov. Bralec se najprej vpraša, komu naj služijo knjižice in šele po podrobnejšemu pregledu kake izmed njih — denimo šeste — ugotovi, da so napisane za fizike ali študente fizike, ki si želijo dobiti pregled nad čimvečjim številom območij. Tako se začetno nerazpoloženje počasi umakne.

Prvo poglavje o obdelavi sunkov pri merjenju ionizirajočega sevanja je prispeval P. Patzelt. Prav prikupno in brez nepotrebnih podrobnosti uvede bralca v osnove števcev in merjenja z njimi. G. Schiffner in W. Köchner pišeta o laserjih, ki delujejo v sunkih. Tudi to poglavje ni nič zahtevnejše. Vsebuje pa nekaj več podatkov, ki utegnejo biti za marsikoga prav zanimivi. W. Bartl obravnava v poglavju o tehniki sunkov v fiziki visokih energij delovanje tiratronov, Marxovega generatorja in zakasnilnega voda ter izoblikovanje sunkov. Zadnje poglavje J. Mitterauerja je posvečeno generatorjem z veliko energijo za poskuse zlivanja lahkih jeder. Obdela osnove zlivanja, načrte za fuzijski reaktor, zahteve za te naprave, njihovo razvrstitev in dokaj podrobno generatorje in stikala. Vsako poglavje spremljajo navedbe najpomembnejše literature. Za bralca, ki mu pride po naključju v roke, je knjžica — zelo verjetno velja to tudi za druge iz te zbirke — kar zanimivo, poučno in neprezahtevno branje.

Janez Strnad

M. H. Protter, C. B. Morrey, A First Course in Real Analysis, Springer Verlag, New York, 1977, 507 strani.

Knjiga je izšla v zbirki učbenikov Undergraduate Texts in Mathematics. Zamišljena je kot učbenik za prvi tečaj realne analize, predpostavlja pa znanje elementarne analize. Vsebina knjige je precej bogata in je razdeljena na šestnajst poglavij. Prvih pet poglavij — realni številski sistemi, zveznost in limite, osnovne lastnosti funkcij v R_1, elementarna teorija odvajanja, elementarna teorija integracije — obravnava analizo v R_1. Ta del naj utrdi znanje elementarne analize, ki naj jo bralec pozna že od prej. Sledijo poglavja: metrični prostori in upodobitve, odvajanje v R_n, integracija v R_n, kjer avtor zgradi analizo funkcij več premenljivk. Nato sta na vrsti poglavji o vrstah: neskončna zaporedja in vrste, Fourierove vrste in poglavje o funkcijah definiranih z integralom. Zadnja poglavja pa so: funkcije omejene variacije in Riemann-Stieltjesov integral, upodobitve, ki krčijo slike in diferencialne enačbe, izrek o implicitnih funkcijah in diferenciabilne upodobitve, funkcije v metričnih prostorih, teorija vektorskih polj z Greenovim in Stokesovim izrekom.

Knjiga privede začetnika precej globoko v analizo. Pisana je zgoščeno, v stilu — definicija, izrek, dokaz, posledice. Obravnava je jasna, dokazi so izdelani podrobno. Poudarek je na obravnavi teorije, vendar precejšnje število nalog pomaga bralcu, da mu novi pojmi tudi zaživijo. Dobro bo rabila za dodatno branje študentom prvih letnikov matematike.

Tomaž Slivnik

N. Koblitz, p-adic Numbers, p-adic Analysis, and Zeta-Functions. Graduate Texts in Mathematics Vol. 58. Springer-Verlag. Berlin-Heidelberg-New York. 1977. X + 122 str.

Knjiga uvaja bralca v p-adično analizo in prikaže njeno uporabnost ob opisu rešitve dveh problemov. Kratka vsebina:

Prvo poglavje vpelje obseg p-adičnih števil Q_p in opisuje njegovo aritmetiko in topologijo. Izhodišče tretjega poglavja je dejstvo, da je obseg Q_p, ki je metričen prostor, poln, ni pa algebraično zaprt. Če je obseg Q'_p algebraično zaprtje obsega Q_p, se da sicer metrika iz Q_p raztegniti enolično na Q'_p, vendar v njej Q'_p ni poln. Napolnitev Q'_p pripelje do obsega Ω_p, ki je tudi algebraično zaprt. Četrto poglavje obravnava potenčne vrste nad obsegom Q_p in nekatere funkcije, ki se dajo na ta način opredeliti. Drugo in peto poglavje prinašata kot uporabo p-adičnih števil rešitev dveh problemov. V drugem poglavju gre za razširitev Riemannove funkcije zeta od celoštevilčnih racionalnih argumentov (kolikor so v def. območju) na celoštevilčne p-adične argumente. Sama zahteva zveznosti v Q_p zagotavlja enoličnost razširitve. V zadnjem, petem poglavju je podan dokaz Dworkovega izreka o racionalnosti funkcije zeta, prirejene sistemu polinomskih enačb s koeficienti iz končnega obsega. Med snovjo je posejanih še okrog 170 vaj in nalog.

Obsegi p-adičnih števil imajo pomembno vlog v raznih področjih matematike, zlasti še v teoriji števil in algebri. Ker dajejo primer za nearhimedsko analizo, so zanimivi tudi s te plati. Kogar ta vprašanja mikajo, bo knjigo s pridom vzel v roke.

Jože Grasselli

POSTDIPLOMSKI SEMINAR IZ MATEMATIKE

Komisija za tisk DMFA SRS
61001 Ljubljana, pp 227

5

I. Vidav

GRUPE K_0, K_1 in K_2

12.— din (10.— din)

6

F. Križanič

TOPOLOŠKE GRUPE

12.— din (10.— din)

7

A. Suhadolc

O KOLOKACIJI

10.— din (8.— din)

50.— din (40.— din)

8

F. Križanič

LIEJEVE GRUPE

20.— din (16.— din)

1

J. Strnad

FAZNA, SKUPINSKA, SIGNALNA HITROST

10.— din (8.— din)

2

S. Pahor

SLUČAJNI PROCESI

20.— din (16.— din)

4

J. Strnad

POSKUSI V POSEBNI IN SPLOŠNI TEORIJI RELATIVNOSTI

20.— din (16.— din)

5

A. Čadež

FIZIKA ZVEZD

V oklepaju so cene za študente in člane društva

POSTDIPLOMSKI SEMINAR IZ FIZIKE