Pokroky matematiky, fyziky a astronomie

Jan Vyšín

Co nového přináší Nico?

Pokroky matematiky, fyziky a astronomie, Vol. 19 (1974), No. 2, 99--102

Persistent URL: http://dml.cz/dmlcz/139237

kému postupu v oboru matematika. Samozřejmě lze také mít názor, že účinné aplikování matematiky v jakékoli situaci, v níž ještě aplikována nebyla, je věcí velmi obtížnou, vyžadující speciální, vzácný talent a že výsledek tohoto druhu by měl být vysoko oceněn.

Jsem úplně na straně přívrženců tohoto posledního hlediska. Jde však i o to, že obtížné je nejen aplikování matematiky v nových situacích, ale že je obtížné i hodnocení výsledků tohoto druhu. Je nutné, aby alespoň v první fázi rozvoje průmyslové matematiky byla zachována co největší opatrnost a aby hodnocení prací tohoto druhu prováděli především matematikové.

Vyslovené poznámky bych chtěl zakončit dost zásadním zdůrazněním svého stanoviska. Snažil jsem se je charakterizovat v úvodu. Jsem přesvědčen, že vlastně existuje pouze čistá matematika nebo prostě matematika. Myslím však, že v zájmech matematiky samé je zdůraznit tu část matematické činnosti, která dovoluje těsně spojovat matematiku se základními potřebami společnosti.

Přeložil Ilja Černý

---

vyučování

Co nového přináší Nico?

Jan Vyšín, Praha

Vracíme se k informaci o pěti číslech časopisu Nico, kterou jsme otiskli v 6. čísle minulého ročníku Pokroků a kde jsme čtenářům slíbili podrobnější výtah ze stati L. Buysta.

Článek L. Buysta o kódování ukazuje, že jde o tematiku matematicky ne příliš náročnou, která souvisí s různými úseky současné školské matematiky (poziční soustavy; algebraické struktury, zejména vektorový prostor, metrický prostor, maticová algebra aj.), která náleží plně do aplikací a může se probírat tak, že žáky zaujme. Menší část článku se dá uplatnit na úrovni I. cyklu, větší část na úrovni II. cyklu; celý článek je vhodná četba pro učitele.

Základní problém je přenos depeše způsobem, který je technicky snadno realizovatelný, umožňuje při příjmu odkrýt chyby a většinou je i opravit.

Depeše, kterou máme přepravit nebo uschovat do paměti počítače, je sestavena z výchozích symbolů (písmen, číslic nebo jiných znaků); tyto symboly převedeme v jiné symboly, vhodnější pro přepravu, nazývané kódová slova (mots-code). Kódové slovo se skládá z elementárních znaků (bits). Kódování je tvoření kódových slov (překlad depeše) podle určité instrukce, zvané kód. Po přenosu nebo vyzdvihnutí depeše z paměti počítače následuje tzv. dekódování, tj. překlad depeše do výchozích symbolů. Příkladem nedokonalého kódu je Morseova abeceda.

Článek se omezuje na kódy těchto vlastností:

a) všechna kódová slova zvaná bloky mají stejný počet n elementárních znaků;
b) jsou jen dva typy elementárních znaků, které se zapisují 0,1; každý blok je tedy uspořádání n-tice znaků 0,1.

Kódová slova lze tedy pokládat za objekty (vektory n-rozměrného binárního prostoru), jejichž souřadnice jsou vyjádřeny v dvojkové soustavě.

Volba dvou bitů je motivována technicky; signály 0,1 se velmi dobře přepravují, ať drátově nebo bez drátu, a také pro zjišťování a opravování chyb jsou výhodné.

Článek L. Buysta se pak zabývá podrobně otázkami detegování a korigování chyb, resp. konstrukcí kódů, které dovolují detegovat aspoň d chyb a korigovat aspoň t chyb. Pro řešení tohoto problému se zavádí pojem testového slova: je to taková uspořádaná n-tice znaků 0,1, která není kódovým slovem. Je-li n počet znaků každého bloku a b počet bloků, má kód $2^n - b$ testových slov. Na jednoduchém příkladě kódu se čtyřmi výchozími symboly vysvětluje pak autor detegování i korigování chyb a konstrukci detegujících a korigujících kódů.
Uvedeme příslušnou tabulku pro 4 výchozí symboly A, B, C, D:

by nedovolil ani detegovat ani korigovat chybu. Tabulka (T), kterou můžeme nazvat dekódovací, je upravena tak, že všechna „doručitelná slova", tj. všechny uspořádané n-tice bitů 0,1 jsou rozloženy na třídy podle počtu chyb vzhledem ke kódovým slovům (zajímavý příklad rozkladu množiny).

Dále se zavádí tzv. Hammingova vzdálenost dvou doručitelných slov $x = (x_1, x_2, \ldots, x_n)$, $y = (y_1, y_2, \ldots, y_n)$ (kde $x_i, y_i = 0$ nebo 1):

$$HD(x, y) = \sum_1^n |x_i - y_i| .$$

Dekódovací tabulky se pak užívá takto: je-li doručeno slovo y (kódové nebo testové), vyhledá se kódové slovo x tak, aby vzdálenost $HD(x, y)$ byla minimální. Tímto způsobem je zajištěno, že daný kód (o jehož konstrukci jsme zatím nehovořili) bude detegovat a korigovat co nejvíce chyb.

Výchozí symbol	*A*	*B*	*C*	*D*	
Kódové slovo	11 000	00 110	10 011	01 101	
Chyba v 1 bitu	110 01	00 111	10 010	01 100	
	110 10	00 100	10 001	01 111	
	111 00	00 010	10 111	01 001	(T)
	100 00	01 110	11 011	00 101	
	010 00	10 110	00 011	11 101	
Chyba ve 2 bitech	111 10	00 000	01 011	10 101	
	010 10	101 00	111 11	00 001	

Řady nazvané „chyba v 1 bitu" a „chyba ve 2 bitech" obsahují všech 28 testových slov. Pro kódování 4 symbolů A, B, C, D by stačily dvoučlenné bloky 00, 01, 10, 11, tj. kód bez testových slov, ale tento kód

O blokových kódech K*) platí tato věta:

*) Písmenem K značíme také množinu všech kódových i testových slov.

a) Kód K deteguje všecky chyby v nejvýše d bitech, právě když platí

$$\forall x, y \in K; \quad HD(x, y) \geqq d + 1 .$$

b) Kód K koriguje všecky chyby v nejvýše t bitech, právě když platí

$$\forall x, y \in K; \quad HD(x, y) \geqq 2t + 1 .$$

Je zřejmé, že struktura (K, HD) je metrický prostor; z této skutečnosti se mohou odvodit další důsledky.

Další část článku se zabývá studiem struktury $(K, +, .)$ jako n-rozměrného vektorového prostoru nad konečným tělesem $B = (\{0,1\}, +, .)$, kde sčítání a násobení je dáno známými tabulkami:

+	0	1
0	0	1
1	1	0

.	0	1
0	0	0
1	0	1

Vektory jsou tedy n-tice bitů, pro něž jsou zavedeny operace sčítání a násobení takto: Jsou-li $a_i, b_i, k \in \{0,1\}$, je

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) =$$
$$= (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n) ;$$
$$k \,.\, (a_1, a_2, \ldots, a_n) = (ka_1, ka_2, \ldots, ka_n) .$$

Tento vektorový prostor lze normovat zavedením tzv. Hammingovy normy: $HN(v)$ je počet jednotkových „souřadnic" vektoru v. Souvislost mezi Hammingovou normou a Hammingovou vzdáleností je dán vztahem $HN(a - b) = HD(a, b)$, přičemž $a - b = a + b$.

Zavádění tohoto poměrně složitého, ale zajímavého aparátu je motivováno tím, že kódy obsahují velký počet kódových slov (např. 10^{10}). Takovéto kódy nelze zavést výčtem; také dekódování, detegování a korigování chyb je třeba provádět rychle a ekonomicky.

Obsah další části článku jen stručně načrtneme: Dekódování záleží v tom – jak už jsme uvedli – že k doručenému (přijatému) slovu nebo vektoru y se vyhledá nejbližší (ve smyslu minimální HD) kódové slovo vektor x. Aby se tato otázka dala řešit vektorovým aparátem, specializuje se kód ještě dále: zavede se tzv. lineární kód. Je to takový kód, jehož množina všech kódových slov tvoří vektorový podprostor prostoru všech slov; jeho dimenze budiž k.

Vektorový prostor V, a tedy i C je normován pomocí HN, která umožňuje detegování chyby. Zavedeme-li však skalární součin vektorů $a = (a_1, a_2, \ldots, a_n)$, $b = (b_1, b_2, \ldots, b_n)$ formulí

$$a \,.\, b = a_1 b_1 + a_2 b_2 + \ldots + a_n b_n ,$$

je $a \,.\, a = 0$ nebo 1, tj. není to Hammingova norma. Nejbližší vektor $x \in C$ k doručovanému slovu (vektoru) y nedostaneme tedy jako ortogonální průmět vektoru y do prostoru C.

L. Buyst naznačuje pak jinou cestu, kterou lze tuto nesnáz obejít. Prakticky je nemožné zkoumat, zda přijatý vektor y je lineární kombinací vektorů báze prostoru C. Místo toho sestrojíme vektorový prostor C^* ortogonální k C. Podprostor $C^* \in V$ má dimenzi $n - k$; jeho báze je dána maticí

$$H = \begin{Vmatrix} h_{11} & h_{12} & \ldots & h_{1n} \\ h_{21} & h_{22} & \ldots & h_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ h_{n-k,1} & h_{n-k,2} & \ldots & h_{n-k,n} \end{Vmatrix}$$

která se nazývá kontrolní maticí. Pro detegování chyb postačí ověřit, zda doručený vektor y je ortogonální ke všem vektorům báze prostoru C^*, daným $n - k$ řádky kontrolní matice H.

Poslední část článku je věnována dešifrování a dalším jeho zjednodušením prostředky maticové algebry. Ačkoli se na první pohled zdají některé pojmy i použitý aparát příliš komplikované, není tomu tak; jestliže ilustrujeme postup numerickými příklady (kódy o malém počtu slov), lze jistě principy kódování a dekódování vyložit srozumitelně na úrovni I. cyklu, principy detegování a korigování na úrovni II. cyklu.

Závěrem můžeme slíbit, že se pokusíme publikovat volné zpracování nejzávažnějších statí, o nichž jsme se zmínili v přehledu pěti sešitů Nica; domníváme se, že to budou dobré studijní materiály pro učitele i pro modernizační pokusy.

K výkladu teorie elektromagnetického pole na střední škole

Oldřich Lepil, Olomouc

Jedním ze základních vzdělávacích úkolů vyučování elektřině na střední škole je postupné vytváření představ o elektromagnetickém poli od nejjednoduššího případu statického elektrického pole nábojů v klidu, až k obecnému případu nestacionárního elektromagnetického pole v prostředí bez elektrických nábojů. Didaktickým problémem je, jak včlenit do učiva středoškolské fyziky Maxwellovu teorii elektromagnetického pole s cílem dovršit tak soustavu poznatků z elektřiny. Úvahy obsažené v tomto článku předkládáme jako diskusní příspěvek k tomuto problému.

1. Teorie elektromagnetického pole ve středoškolských učebnicích fyziky

Rozbor osnov fyziky pro střední školu a jejich vývoje [1] ukazuje, že poznatky o elektromagnetickém poli se vesměs vytvářejí ve spojitosti s výkladem tématu *Elektromagnetické kmitání a vlnění.* Přitom se však jen málo uplatňují souvislosti s ostatními tématy učiva elektřiny, takže se pojem nestacionárního elektromagnetického pole buduje izolovaně, vcelku nezávisle na poznatcích o ostatních speciálních formách elektromagnetického pole. Přitom je nesporné, že jedině uplatněním těchto souvislostí lze na střední škole dospět k tak široce založenému pojmu elektromagnetického pole, aby žák pochopil, že dříve poznané jevy ve statickém, stacionárním, popř. kvazistacionárním elektrickém nebo magnetickém poli jsou jen zvláštními případy jevů v obecném poli elektromagnetickém.

Ve většině středoškolských učebnic se však tento problém uspokojivě neřeší, popř. se ani neklade, a pojetí tématu elektromagnetické kmity a vlnění je zaměřeno převážně na výklad principů radiotechniky. Tento stav ovlivňuje také skutečnost, že výklad teorie elektromagnetického pole je náročný a nejsou k dispozici jednoduché metodické postupy výkladu. Hluboce založený výklad o elektromagnetickém poli vyžaduje užití kvantitativních, matematicky formulovaných vztahů, které nelze snadno upravit do tvaru vhodného pro žáky střední školy. Proto se ve většině středoškolských učebnic výklad řeší jen na kvalitativním základě a pokusy o kvantitativní zvládnutí Maxwellovy teorie elektromagnetického pole na střední škole jsou z hlediska metodického málo uspokojivé.

Společným nedostatkem všech pokusů o zpracování teorie elektromagnetického