31 (1986) APLIKACE MATEMATIKY No. 6, 500—504

RECENZE

R. Thiele: MATEMATICKÉ DŮKAZY. Polytechnická knižnice řady Věda a technika populárně, SNTL Praha 1985, stran 160, cena 22,— Kčs.

Recensovaná kniha začíná citátem romantického básníka Novalise „Kdo k matematické knize nepřistupuje ve zbožném rozjímání ..., ten jí nerozumí." Autor jej staví do protikladu ke způsobu, jakým by se měly číst matematické důkazy, ale to, co následuje, dává za pravdu básníkovi.

První kapitola knihy ukazuje, proč jsou matematické důkazy nutné. Druhá kapitola s názvem Collegium logicum se zabývá výroky, logickými spojkami, pravdivostí výroků, zavádí proměnné, kvantifikátory a výrokové funkce. Axiomatická metoda je předvedena na příkladech klasických axiomatik (Eukleidova geometrie, Peanova aritmetika), které byly vytvořeny k popisu jediného univerza, a na příkladech moderních axiomatických systémů (teorie grup), které vznikly k popisu společných vlastností velmi různorodých modelů. Čtvrtá a pátá kapitola je autorovým pokusem a klasifikaci jednotlivých druhů důkazů. Matematické indukci je věnována celá šestá kapitola a závěrečná sedmá se zabývá psychologickými momenty práce matematika. Zamýšlí se nad tím, jak matematici nalézají důkazy, na čem spočívají nesprávné úsudky a dalšími problémy. Text je doplněn řadou cvičení, jejichž řešení jsou uvedena na konci knihy.

Překladatelé v předmluvě uvádějí: „Úvahy o tom, co je a co není matematický důkaz, související úzce s matematickou logikou a mají i výrazně filozofické rysy. A právě tyto „filozofující" partie mohou leckdy připouštět různý subjektivní výklad, leckterý matematik by asi to či ono řekl nebo vyložil jinak než autor (nebo překladatelé)". Tím předjímají kritiku, které se však nelze vyhnout. Nejde však jen o subjektivní výklad filozofujících partií, ale bohužel i o hrubé matematické nedostatky, které překlad věrně tlumočí (a ve dvou nebo třech případech rozmnožuje).

Na str. 25 čteme: „Pravdivostní hodnota výroku je objektivní fakt, je tedy nezávislá na osobě, která výrok vyslovuje, nezávisí na místě ani čase, na kterém byl výrok učiněn." Ale v poznámce pod čarou na téže straně čteme „Pravdivostní hodnota výroku „Dnes je pěkné počasí" je velmi subjektivní, protože nelze přesně vymezit pojem pěkný." (Hodnotu uvedeného „výroku" autor považuje za nezávislou na místě a čase, ledaže by nešlo o výrok nebo že by pravdivostní hodnota nebyla objektivním faktem.)

Někdy překvapí srovnání různých míst textu. Na str. 26 jsou matematické věty definovány jako „výroky s pravdivostní hodnotou pravdivý". Ponechme stranou, že takový postup je z hlediska logiky zcela nepřiměřený. Na str. 76 čteme „Geometrická teorie, v níž lze současně odvodit větu V... i větu non V..., je bez užitku". To už čtenář ví, že výroky V a non V nemohou být současně pravdivé, a tedy v autorově pojetí nemohou být současně větami. Snad proto na následující straně autor mluví o „všech pravdivých větách".

Na str. 77 se hovoří o Eukleidově systému axiomů geometrie prostoru a jako příklad je uveden tento axiom „Okolo každého bodu lze sestrojit kružnici (!) o libovolném poloměru". (V jaké rovině?) Přitom o dva řádky dále se uvádí slavný axiom o rovnoběžkách (v Eukleidově pojetí, jak autor zdůrazňuje), ve kterém slova „v rovině" nechybí.

Ve větě o matematické indukci (str. 121) je předpoklad o indukčním kroku vysloven takto: „Z platnosti výroku $A(n)$ pro každé n plyne též platnost výroku $A(n + 1)$". Čtenář má nejméně tři možnosti, aby určil, k čemu se vztahují slova „pro každé n", ale jenom jedna vyhovuje. (Tato chyba vznikla překladem.)

Na str. 45 se dočteme: „Nad množinou přirozených čísel dávají funkce non $A(x) : x$ není sudé číslo a $A_0(x) : x$ je liché číslo stejné (!) výroky ... ". Potom už nepřekvapí, když na str. 78 čteme: „A je otcem B a B je synem A jsou rovnocenné popisy jediné skutečnosti".

Vedle podobných útoků proti zdravému rozumu text obsahuje i jemnější věcné nedostatky. Popis Vennových diagramů na str. 46 se zásluhou překladu stává hádankou (kde je objekt M?). Na str. 48 se uvádí, že z výrokové funkce lze získat výroky přípustným dosazením za volné proměnné nebo kvantifikací volných proměnných. Autor však neuvedl, že výrok může vzniknout jen tehdy, pokud to provedeme se všemi volnými proměnnými.

Peanovy axiomy pro přirozená čísla (str. 66) jsou vysloveny v logice druhého řádu, jakkoli se to autor snaží zakrýt: k základním pojmům „přirozené číslo" a „bezprostřední následník" je nutno počítat i pojem „množina přirozených čísel", jinak poslední axiom ztrácí smysl. Ostatně žádná axiomatizace přirozených čísel v logice prvního řádu nemůže zajistit izomorfnost všech modelů, která je v textu zdůrazněna. Uspořádání přirozených čísel není určeno prvními třemi axiomy, jak se tvrdí na str. 67. Tyto axiomy připouštějí i modely, které nejsou uvažovány, na příklad lineární uspořádání podle typu $\omega + \omega$ nebo dvě disjunktní kopie množiny přirozených čísel položené vedle sebe.

Ve výčtu nedostatků textu by bylo možné ještě pokračovat. Za zmínku stojí i bibliografie. Překladatelé nahradili původní seznam třiceti odkazů sedmi odkazy na českou literaturu většinou staršího data. Přitom jen v knize Co víte o moderní logice od *V. Čecháka, K. Berky* a *I. Zapletala,* Horizont, Praha 1981, která není v překladu citována, najdeme stejný počet českých pramenů novějšího data. Je nepochopitelné, proč překladatelé vynechali jediný odkaz na českou literaturu, odkaz na knihu *J. Vyšína:* Metodika řešení matematických úloh, SPN Praha 1972 (německy Teubner, Lepzig 1975).

Hlavní problém je však jinde. Autor zvolil neformální výklad logiky. Výroky se vyjadřují v běžném jazyce stejně jako soudy o nich. Formální symbolický jazyk pro vyjadřování výroků a výrokových funkcí se nezavádí. Cena za takové pojetí je dobře známa: syntaktická struktura výroků, jejich věcný obsah a semantika jsou spleteny v jediném klubku. Autorovi se ho nepodařilo rozplést. Nepomohl Sokrates, Karel IV, francouzský král, měsíc jako zelený sýr, černý vraník ani další postavy, které známe z podobných textů, ani výklady na str. 25, 26, 42, 44 a jinde. Autor nakonec konstatuje (str. 51) „Nebudeme dále sledovat logické usuzování, protože rigoroznější výstavba logiky by nás oddálila od usuzování, které je obvyklé v matematice." Anachronismus zvoleného pojetí vynikne, uvědomíme-li si, že logické obvody dnes používají i domácí kutilové a formální jazyky jsou prostředkem dorozumívání s počítači, které se stávají běžnou součástí našeho života.

Korunu všemu nasazuje anotace uvedené v záhlaví knihy, která je mimochodem v rozporu s přemluvami autora i překladatelů. Vzhledem k uvedeným nedostatkům díla ji lze považovat jen za ironickou nadsázku. Recenzovaná kniha není úvodem do formální logiky a bojím se domyslet, kde bychom byli, kdyby nezdařenou knihu ze žákovské edice (Mathematische Schülerbücherei) u nás se zájmem četli fundovaní odborníci.

Čtenář může posbírat střípky anekdot a příkladů, ale doporučuji, aby pokusy navléknout jim logický kabát nebral vážně. Autorův postoj k logice snad nejlépe charakterizují jeho vlastní slova (str. 17): „Ačkoli se v řadě případů nepovažujeme za kompetentní, tvoří logika jistou výjimku ... ".

(Poznámka na závěr: druhé vydání recenzované knihy vyšlo dříve než tato recenze.)

Petr Štěpánek

Hans Riesel: PRIME NUMBERS AND COMPUTER METHODS FOR FACTORIZATION. Progress in Mathematics, Vol. 57. Birkhäuser, Boston—Basel—Stuttgart 1985, stran 464, obr. 13, cena sFr. 118,—.

Autor napsal tuto knihu nejen pro matematiky a inženýry, ale i pro laiky, kteří k matematice inklinují. Jak to často bývá v číselné teorii, její problematika je snadno srozumitelná, ale důkazy pochopí jen čtenář s hlubším vzděláním. Riesel zde shrnul mnoho látky, ale nesnaží se všechny výsledky dokazovat. Náhražkou jsou mu bohaté literární odkazy, kde si může náročnější zájemce důkaz najít.

Hlavní text se skládá ze šesti kapitol, jež jsou vzájemně nezávislé a čtenář je může v podstatě studovat v libovolném pořadí. Začíná se definicí prvočísla a Eratosthenovým sítem, pokračuje se sérií známých i méně známých výsledků o rozložení prvočísel a pak se autor dostává k problému rozpoznávání prvočísel. Ukazuje se, že se tento problém naštěstí nemusí řešit faktorizací, ale existují jednodušší algoritmy, jimiž se dá otázka rozhodnout. Zájemce tu najde i programy v jazyce PASCAL, což ostatně platí pro všechny algoritmy probírané v této knize. Rozkladu velkých celých čísel v součin prvočísel se věnuje předposlední kapitola hlavního textu, která popisuje pokroky dosažené v posledních asi patnácti letech (M. A. Morrison, J. Brillhart, C. Pomerance, J. M. Pollard aj.). V poslední, šesté kapitole se dočteme o aplikacích číselné teorie v kryptografii, což je nauka o posílání šifrovaných zpráv. Systém RSA (zkratka jmen Rivest, Shamir a Adleman), který je tu popsán, nevyžaduje už absolutní utajení při podávání informace, ale pracuje jen s utajením relativním. Zakládá se na tom, že násobení celých čísel je snadné, ale faktorizace velkých přirozených čísel je nesmírně pracná záležitost. Případný protivník může tedy mít k dispozici všechny informace nutné k přečtení poselství, ale zakódovanou zprávu nerozluští, nemá-li k dispozici počítač schopný provést onu složitou faktorizaci. [Na rok 1986 oznamuje nakladatelství John Wiley & Sons samostatnou publikaci s názvem Primality and cryptography (autor *E. Kranakis*).]

Prostřední část knihy tvoří devět dodatků, které obsahují základní pojmy z vyšší algebry a teorii kvadratických zbytků, seznamují s aritmetikou kvadratických těles, s řetězovými zlomky, se Stieltjesovým integrálem a dalšími pojmy klasické matematiky. Konečně na posledních zhruba devadesáti stránkách této monografie najdeme různé tabulky, které mohou být užitečné v číselné teorii (všechna prvočísla od 2 do 12 553, faktory Fermatových a Mersenneových čísel ap.).

Jiří Sedláček

G. Heinig, K. Rost: ALGEBRAIC METHODS FOR TOEPLITZ-LIKE MATRICES AND OPERATORS. Birkhäuser-Verlag, Basel—Boston—Stuttgart 1984, 212 stran.

Autoři knihy shrnují poměrně široký a ucelený okruh problémů, především praktických, které se týkají konečných Hankelových a Toeplitzových matic. V této oblasti je publikace tohoto druhu velmi cenná, neboť velký počet vycházejících článků vytváří značný chaos a novější přehledné jednotící práce neexistují. Přitom se jedná o oblast, která je stále středem živého zájmu. Kniha není omezena jen na Hankelovy a Toeplitzovy matice, ale autoři využívají původní metody pro studium mnoha příbuzných tříd matic a dále podávají stručný výklad Wienerovy-Hopfovy teorie, aby ukázali vzájemné souvislosti konečně a nekonečně dimenzionálních problémů.

První část je věnována konečným Toeplitzovým a Hankelovým maticím. Hlavním obsahem je odvození rychlých algoritmů (vyžadujících $O(n^2)$ operací) pro inverzi, řešení soustav, LU-rozklad a určení signatury. Je podán popis nulových množin matic libovolných rozměrů (obdélníkových) a je rozebrán i problém zobecněných inverzních matic. Dále jsou mj. uvedeny některé vlastnosti Bézoutových a rezultantních matic.

V druhé části zavádějí autoři tzv. metodu UV-redukce pro charakterizaci tříd matic příbuzných Toeplitzovým. Postup je aplikován na tři speciální typy matic: matice blízké Toeplitzovým

(Bézoutovy matice, součiny Toeplitzových matic, matice složené z více toeplitzovských bloků), matice blízké Vandermondovým a matice příbuzné maticím typu $(1/(b_i - c_j))$. Pro všechny tyto typy matic jsou podány algoritmy rychlé inverze. Tyto výsledky využívají autoři též pro výpočty s maticemi typu „Hankel plus Toeplitz". Poslední tři kapitoly se zaměřují na Wienerovu-Hopfovu teorii a podávají algoritmy pro inverzi operátorů příbuzných Toeplitzovým, popis nulových množin aj.

Kniha by měla být významnou pomůckou pro všechny, kdo se setkávají s aplikacemi Hankelových či Toeplitzových matic. Pro matematiky pracující v oblasti teorie těchto matic je seznámení s touto prací naprostou nezbytností.

Zdeněk Vavřín

P. Mandl: PRAVDĚPODOBNOSTNÍ DYNAMICKÉ MODELY. Academia, Praha 1985, 181 stran, cena Kčs 20.—.

Jedná se o vysokoškolskou učebnici, která se zabývá modely takových procesů, že přítomný stav systému plně určuje jeho budoucí vývoj, a to převážně ve stochastickém smyslu, tj. modely procesů majících Markovovou vlastnost. Existence náhodných vlivů působících na systém je popisována příslušnými (semi-)Markovovými procesy a řetězci a stochastickými diferenciálními rovnicemi. Určitá pozornost je věnována i deterministickým modelům a otázce vhodnosti jejich použití v některých situacích. Vedle výstavby pravděpodobnostních modelů se autor často věnuje i statistickým úlohám vyplývajícím z dané problematiky.

Kniha je členěna do čtyř kapitol. První je věnována modelům s konečným nebo spočetným počtem stavů. Po názorné konstrukci Poissonova procesu a jeho aplikacích v jednodušších modelech hromadné obsluhy následují klasické výsledky z teorie Markovových řetězců a procesů a posléze základy teorie semimarkovovských procesů. Ve druhé kapitole jsou uvedeny deterministické modely růstu a existenčního boje založené na diferenciálních rovnicích a dále pak tzv. atomistické modely (jejich název má kořeny v procesu radioaktivního rozpadu), které se zaměřují na studium vývoje jedince dané populace při působení náhodných vlivů. Velmi podnětné jsou autorovy poznámky o dvou základních nedostatcích atomistických modelů — studium vývoje edince je často nepoměrně obtížnější než studium zákonitostí růstu populace jako celku a navíc u rozsáhlejších populací se atomistický model blíží působením zákona velkých čísel k deterministickému. Třetí kapitola se zabývá stochastickou analýzou. Čtenář se postupně seznámí se způsobem výstavby a vlastnostmi Wienerova procesu a stochastického integrálu a s Itôovou formulí. Určitý prostor je věnován řešení lineárních stochastických diferenciálních rovnic a problematice difúzních procesů včetně difúzních aproximací Markovových řetězců. Poslední, co do rozsahu nejmenší kapitola pojednává o dynamickém programování v případech konečného i nekonečného plánovacího horizontu a speciálně o řízení lineárních soustav s kvadratickým kritériem.

Kniha je napsána velice přehledně a pečlivě. Zdůraznit je však třeba zejména promyšlený způsob výběru a uspořádání probírané látky. Základní linie výkladu je dobře sledovatelná a jeho snadnějšímu a hlubšímu pochopení napomáhá řada příkladů z nejrůznějších oblastí, např. telefonní sítě, dopravní nehody, přehradní nádrže, kolektivní teorie rizika v pojišťovnictví, Chandlerův pohyb zemského pólu, síťování polymerů. Některé ze studovaných příkladů (např. četnost tlupy paviánů v rezevaci Amboseli nebo hranice rozšíření potomků pěti ondater dovezezených roku 1905 do Dobříše) nejen plně zapadají do uvažované problematiky svým matematickým obsahem, ale vzbuzují u čtenáře i pocity jistého uvolnění a zážitku ze zajímavé četby.

Antonín Lešanovský

MATHEMATICS IN BIOLOGY AND MEDICINE, Proceedings, Bari 1983. V. Capasso, E. Grosso a S. L. Paveri-Fontana, eds. Springer-Verlag, Berlin—Heidelberg—New York—Tokyo, 1985, v edici Lecture Notes in Biomathematics (S. A. Levin, ed.), XVIII + 524 str., 87 obr., cena DM 79,—.

Do sborníku přispělo celkem 127 autorů nejrůznější provenience: čistá i aplikovaná matematika, biologie, medicína. Důraz byl kladen na formulaci, analýzu a numerická řešení matematických modelů v uvedených oborech. Pozornost byla věnována též simulačním metodám a problémům validace modelů pomocí empirických dat. Ze známějších autorů je možno uvést K. Cooke, P. DeMottoni, K. Dietz, K. P. Hadeler, L. M. Ricciardi, P. T. Saunders, Y. Takeuchi, aj. Kniha volně navazuje na svazek téže edice Mathematical Ecology (T. G. Hallam a S. A. Levin, eds.).

Pavel Kindelmann