Pokroky matematiky, fyziky a astronomie

Michal Křížek

Má ryze teoretická matematika uplatnění v technické praxi?

Pokroky matematiky, fyziky a astronomie, Vol. 44 (1999), No. 1, 14--24

Persistent URL: http://dml.cz/dmlcz/140977

Má ryze teoretická matematika uplatnění v technické praxi?

Michal Křížek, Praha

Hlavním cílem přednášky bude ukázat, že řadu abstraktních matematických výsledků týkajících se prvočísel, komplexních čísel, funkcí, mnohostěnů atd. lze bezprostředně uplatnit při řešení mnoha důležitých praktických problémů. Uvedeme 10 jednoduchých příkladů, na nichž budeme demonstrovat užitečnost teoretického výzkumu v rozmanitých matematických disciplínách. Každý učitel matematiky by totiž měl znát některé důležité a zajímavé aplikace matematických výsledků, aby nebyl od zvídavých žáků zaskočen otázkami typu: A k čemu jsou nám vůbec dobrá prvočísla? Kde mají uplatnění komplexní čísla? Proč se učíme funkce?

Uvidíme, že některé matematické věty a metody našly skutečné uplatnění až mnoho desítek (popř. stovek) let po svém vzniku.

1. Teorie čísel

Přirozená čísla hrají důležitou roli ve fyzice částic či astronomii (interference, rezonance, vázané rotace apod.). Výsledky teorie čísel se používají např. ke kódování televizního signálu. K dalším užitečným aplikacím teorie čísel patří generátory pseudonáhodných čísel, které jsou mj. součástí těch počítačových her, kde je zapotřebí nějaké nahodilosti (pro pohyb protivníků, figurek apod.). Také poselství mimozemským civilizacím, vyslané v roce 1974 z největšího radioteleskopu světa, bylo založeno na základní větě aritmetiky. O praktickém použití Čínské věty o zbytcích jsme se již zmínili v [14]. V této kapitole stručně popíšeme použití prvočísel v kryptografii.

Při přenosu tajných vojenských zpráv, finančních a obchodních údajů, různých strategických dat a dalších důvěrných informací je nutno dodržovat maximální obezřetnost. Kdysi se k šifrování používalo *tajného klíče*. Jeho nevýhodou bylo, že jej musely znát všechny komunikující strany, a tak mohlo snadno dojít k jeho prozrazení. Pro zcela bezpečné šifrování zpráv pomocí tzv. *veřejného klíče* byla vyvinuta *metoda RSA* (nazývaná podle počátečních písmen příjmení autorů článku [23]).

Nechť $n = pq$, kde p a q jsou velká prvočísla (zhruba o sto cifrách), která nejsou veřejně známa. Vysílanou zprávu nejprve převedeme (zakódujeme) nějakým způsobem na přirozené číslo x (např. pomocí známého ASCII kódu) a nechť je pro jednoduchost

---

RNDr. Michal Křížek, DrSc. (1952), Matematický ústav AV ČR, Žitná 25, 115 67 Praha, e-mail: krizek@math.cas.cz

Předneseno na 6. setkání učitelů matematiky všech typů a stupňů škol, Mariánské Lázně, 21. – 23. října 1998, za podpory grantu ME 148 (1998) MŠMT ČR.

$x < n$. Šifrovanou zprávu označme symbolem x^*. Je to přirozené číslo splňující nerovnost $x^* < n$ jednoznačně definované kongruencí [1])

$$x^* \equiv x^e \bmod n,$$

kterou v roce 1976 navrhli W. Diffie a M. Hellman. Šifrovací exponent e (od angl. slova encryption) a n jsou veřejně známá přirozená čísla. Při dešifrování se opět definuje přirozené číslo $(x^*)\hat{} < n$ tak, aby

$$(x^*)\hat{} \equiv (x^*)^d \bmod n.$$

Dešifrovací exponent d (od angl. slova decryption) ale veřejně znám není. Volí se tak, aby $de \equiv 1 \bmod \varphi(n)$, kde $\varphi(n)$ je hodnota Eulerovy funkce, která je definována jako počet těch přirozených čísel nepřevyšujících n, jež jsou nesoudělná s n.

Věta. *Jsou-li e a $\varphi(n)$ nesoudělná, pak $(x^*)\hat{} = x$, tj. zašifrovaná zpráva je po dešifrování totožná s původní zprávou x.*

Důkaz (viz např. [13]) je založen na kongruenci $x^{\varphi(n)} \equiv 1 \bmod n$, kterou pro nesoudělná x a n odvodil L. Euler (1707–1783), aniž tušil, jaké obrovské uplatnění bude mít.

Hlavní trik metody RSA spočívá v tom, že vynásobit dvě velká prvočísla trvá na běžném osobním počítači jen zlomek sekundy, zatímco zpětně rozložit tento součin na dva prvočinitele by trvalo pomocí nejlepších známých metod a nejmodernějších počítačů mnohem déle, než je celkové stáří vesmíru. Bez znalosti prvočísel p a q nelze v „rozumné době“ vypočítat $\varphi(n)$, a tedy ani dešifrovací exponent d.

Ilustrační příklad na metodu RSA je uveden např. v [13]. Zde se také lze dočíst, co je tzv. *digitální podpis*, jenž je založen na rovnosti $(x\hat{})^* = x$. Jeho stupeň spolehlivosti je mnohem vyšší než notářsky ověřený podpis či otisky prstů. Digitální podpisy hrají též důležitou roli při projektování počítačových systémů odolávajících nežádoucím vstupům a manipulacím, ochraně dat před „nepovolanými čtenáři“, proti falzifikaci nebo destrukci rozličných souborů.

Nedlouho po vzniku metody RSA vznikly ve Spojených státech RSA Laboratories, kde se studují nové směry v kryptografii založené na šifrování pomocí velkých prvočísel. Na adresách `http://www.ica.cz` nebo `http://digitalid.verisign.com` je informace, jak se používá metoda RSA např. v našich bankách. Více o moderních metodách šifrování se lze dočíst v [6, 28, 29, 31].

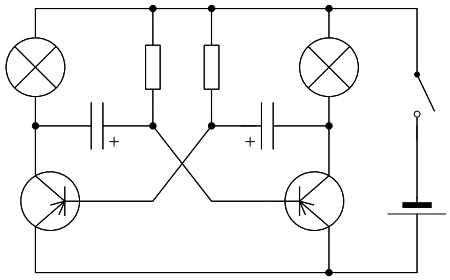
2. Teorie grafů

Nejprve připomeňme, že *obyčejný graf* je dvojice (V, E), kde V je množina vrcholů (uzlů), E je množina hran a každé dva vrcholy spojuje nejvýše jedna hrana. Pro jednoduchost předpokládejme, že obě množiny jsou konečné.

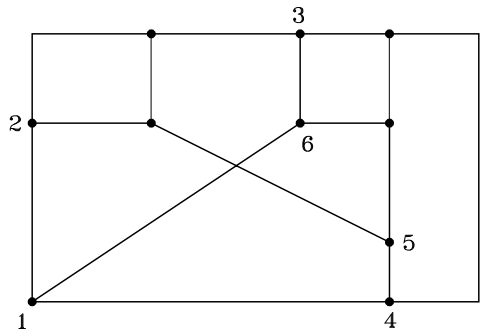
[1]) Zápis $j \equiv k \bmod n$ znamená, že $k - j$ je dělitelné n beze zbytku.

Pod pojmem graf se tedy zde nemíní graf reálné funkce. Množství praktických aplikací teorie grafů lze nalézt v [18, 19, 25, 27], např. stanovení celkového počtu izomerů uhlovodíku C_kH_{2k+2}, problém optimální cesty z vrcholu A do B v ohodnoceném grafu, problém obchodního cestujícího atd.

Graf se nazývá *rovinný*, jestliže existuje takové jeho nakreslení, že se žádné dvě hrany nekříží. Je-li navíc „souvislý“ a je-li v, e, n postupně počet jeho vrcholů, hran a stěn[2]), pak platí známý Eulerův vztah $v + n = e + 2$, který se používá např. v metodě konečných prvků. Připomeňme ještě, že v roce 1976 K. Appel a W. Haken vyřešili pomocí počítače zajímavý problém čtyř barev z teorie rovinných grafů, tj. dokázali, že každou mapu lze obarvit nejvýše čtyřmi barvami tak, že žádné dva sousední státy nejsou obarveny stejnou barvou.



Obr. 1



Obr. 2

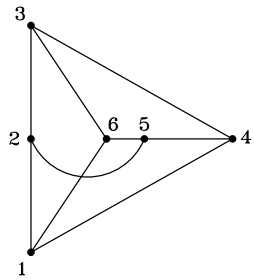
Teorii rovinných grafů lze použít při návrhu integrovaných obvodů nebo desek s plošnými spoji. Ilustrujme to na jednoduchém příkladě. Na obrázku 1 je schéma elektrického obvodu pro dvoužárovkový blikač. Vzniká otázka, zda existuje takové nakreslení odpovídajícího grafu z obrázku 2, že se žádné dva vodiče nekříží. Pro řešení použijeme následující větu (viz [16, 19]) pocházející od C. Kuratowského z roku 1930, jejíž důkaz není vůbec triviální.

Věta. *Obyčejný graf je rovinný právě tehdy, když neobsahuje část izomorfní s dělením*[3]) *grafu* K_5 *nebo* $K_{3,3}$.

Připomínáme, že K_5 je graf s pěti vrcholy, které jsou všechny vzájemně propojeny (jako pravidelný pětiúhelník se všemi úhlopříčkami), graf $K_{3,3}$ je nakreslen na obrázku 3 a pojem „izomorfní“ zde pro jednoduchost chápejme intuitivně jako „ekvivalentní (totožný)“. Izomorfní grafy se často považují za dvě kopie téhož matematického objektu. Snadno nahlédneme, že vynecháním neočíslovaných vrcholů a příslušných slabě nakreslených hran z grafu na obrázku 2 dostaneme graf izomorfní s grafem z obrázku 3. Graf na obrázku 2 tedy není rovinný.

[2]) Tato terminologie je do značné míry motivovaná teorií mnohostěnů. Graf je souvislý, jestliže pro každé dva vrcholy existuje cesta (spojení) — viz [19].

[3]) Dělení grafu znamená, zhruba řečeno, že alespoň jednu hranu rozdělíme dalšími vrcholy (pro přesnou definici viz [19]).



Obr. 3

Pro komplikovanější elektrické obvody existují algoritmy, které rozhodnou, zda je příslušný graf rovinný, a které minimalizují počet překřížení, pokud graf rovinný není. Tyto algoritmy též navrhují odpovídající nakreslení plošných spojů. Jestliže je počet překřížení vodičů příliš velký, používají se dvojstranné plošné spoje. Jindy se vystačí s přemostěním vodičů pomocí elektrotechnických součástek.

Připomeňme ještě, že *kružnice* je souvislý graf, z jehož každého vrcholu vycházejí právě dvě hrany. Souvislý rovinný graf neobsahující kružnici se nazývá *strom*. Takové grafy se velice dobře prohledávají a mají mnoho aplikací. Například adresáře v operačních systémech DOS a Windows mají stromovou strukturu. Brněnský profesor O. Borůvka (1899–1995) se kdysi zabýval metodou, jak propojit několik desítek moravských měst elektrickým vedením tak, aby celá trasa byla co nejkratší, a tím náklady na její stavbu minimální. Dnes se tento problém nazývá hledání minimální kostry (napnutého stromu) v ohodnoceném grafu, viz [27].

3. Teorie grup

Grupa je trojice $(G, 1, *)$, kde G je množina, na níž je definována operace „násobení $*$“, která je asociativní, s neutrálním prvkem 1 a ke každému prvku z G existuje právě jeden prvek inverzní.

E. Galois (1811–1832) na základě konečných grup permutací dokázal, že algebraické rovnice stupně alespoň 5 nejsou obecně řešitelné pomocí odmocnin. Stejný výsledek získal nedlouho předtím N. H. Abel (1802–1829) pro rovnice 5. stupně. V práci [7] se poukazuje na to, že kvarky, z nichž jsou složeny protony a neutrony, se dají popsat pomocí jisté podgrupy transformací Rubikovy kostky. Grupy lze použít i pro vytváření rozmanitých ornamentálních vzorů (viz [21]). Řada dalších zajímavých aplikací teorie grup při studiu kmitů molekul, v krystalografii, ve fyzice a chemii je obsahem knížek [1, 17]. Teorie grup byla též použita k důkazu Velké Fermatovy věty.

Kdysi se pro kontrolu správnosti dat na 8-stopých děrných páskách používala tzv. parita (tj. osmá krajní stopa se doplňovala tak, aby počet dírek byl v každém řádku sudý). O něco komplikovaněji jsou chráněny ISBN[4]) kódy knih skládající se z deseti

[4]) ISBN kódy mají tvar: jazyk – nakladatelství – identifikační číslo knihy – kontrolní cifra x_{10}.

cifer $x_1, x_2, \ldots, x_{10}$. Poslední cifra se volí tak, aby číslo $x_1 + 2x_2 + 3x_3 + \cdots + 10x_{10}$ bylo dělitelné jedenácti. Podobně se pro ověření správnosti velkých datových souborů používají různé kontrolní součty, rodná čísla od roku 1954 jsou dělitelná 11 aj. Takto sice snadno můžeme zjistit, že v daném souboru vznikla chyba, ale obecně nevíme, který bit se přenesl (zobrazil) nesprávně. Pomocí teorie grup však můžeme tento nedostatek odstranit. Stručně si popíšeme *metodu samoopravujících se kódů* (viz [11, 29, 32]), která se dnes používá například pro přenos dat z meziplanetárních sond. Poněkud odlišnou verzi této metody poprvé použil R. W. Hamming v roce 1947 na tehdejších reléových počítačích, aby ošetřil následky jejich značně nespolehlivosti.

Definice. *Hammingova vzdálenost* $\operatorname{dist}(u, v)$ *mezi vektory* $u = (u_1, u_2, \ldots, u_n)$ *a* $v = (v_1, v_2, \ldots, v_n)$, $u_i, v_i \in \{0, 1\}$, *je počet míst, kde se* u *liší od* v.

Například pro $n = 3$ je $\operatorname{dist}(000, 110) = 2$ nebo $\operatorname{dist}(010, 101) = 3$. Jednoduchý samoopravující se kód můžeme zapsat pomocí následujících osmi *kódových slov* délky $n = 7$:

$$\begin{array}{l} 0000000 \\ 0010111 \\ 1001011 \\ 1100101 \\ 1110010 \\ 0111001 \\ 1011100 \\ 0101110 \end{array} \qquad (1)$$

Přenášená informace se rozdělí do skupin po třech bitech. Povšimněme si, že první 3 bity (cifry) v každém řádku (1) jsou vzájemně různé a žádná jiná trojice bitů už neexistuje. Zbylé 4 bity jsou voleny tak, aby Hammingova vzdálenost mezi libovolnými dvěma řádky byla 4. Každé 3 bity přenášené informace se tedy jednoznačně doplní o další 4 bity podle (1).

Pokud při přenosu informace dojde ke změně jednoho bitu v nějakém kódovém slovu, bude jeho Hammingova vzdálenost od původního kódového slova 1, zatímco od ostatních slov 3 nebo 5. Tak se okamžitě zjistí, který bit se špatně přenesl. Při ztrátě dvou ze sedmice bitů se pouze pozná, že došlo k chybě.

Všimněme si, že se nenulové prvky v (1) postupně cyklicky posunují vždy o jeden bit vpravo. Tvoří tzv. cyklickou podgrupu tělesa $\mathrm{GF}(2^7)$, jejíž násobení lze snadno definovat pomocí multiplikativní tabulky [17] (GF je zkratka od angl. Galois field).

4. Teorie funkcí

Rozsáhlý přehled funkcí vyskytujících se v aplikacích je uveden v [22]. Jejich praktické použití jsme podali např. v [8]. V této kapitole stručně popíšeme, jak studium funkcí přispělo ke vzniku matematických základů *počítačové tomografie* (viz [2, 9]).

Při vyšetření v počítačovém tomografu je lidské tělo z různých stran prozařováno rentgenovým (popř. gama) zářením. Protože kosti pohlcují více záření než měkké

tkáně, detektor naměří v různých směrech obecně různý úbytek intenzity záření. Tyto projekce lze v jednom řezu těla popsat funkcí $p = p(\ell, \vartheta)$, kde ℓ charakterizuje vodorovnou polohu detektoru a ϑ úhel natočení těla (pro podrobný popis viz [9]). Předpokládejme, že $f = f(r, \varphi)$ je ve standardních polárních souřadnicích odpovídající neznámá funkce absorpce záření, která vlastně vypovídá o rozložení lidských orgánů ve studovaném řezu.

V roce 1917 J. Radon odvodil následující inverzní formuli (viz [9])

$$f(r,\varphi) = \frac{1}{2\pi^2} \int_0^{\pi} \int_{-\infty}^{\infty} \frac{-1}{\ell - r\cos(\varphi - \vartheta)} \frac{\partial p}{\partial \ell}(\ell, \vartheta)\, \mathrm{d}\ell\, \mathrm{d}\vartheta. \tag{2}$$

Pro výpočet (2) se používá známá Fourierova[5]) transformace

$$\big(\mathcal{F}(q)\big)(t) = \int_{-\infty}^{\infty} q(x)\, \mathrm{e}^{2\pi \mathrm{i} x t}\, \mathrm{d}x \qquad (\mathrm{i} \text{ — imaginární jednotka}), \tag{3}$$

definovaná pro měřitelné funkce q splňující nerovnost $\int_{-\infty}^{\infty} |q(x)|\, \mathrm{d}x < \infty$, a dále následující tvrzení (viz [22]).

Věta. *Jsou-li funkce q_1 a q_2 absolutně integrovatelné na intervalu $(-\infty, \infty)$, pak $\mathcal{F}(q_1 * q_2) = \mathcal{F}(q_1)\mathcal{F}(q_2)$, kde symbol $*$ značí konvoluci.*

Na počítači se určité integrály aproximují sumami, což vede na diskrétní Fourierovu transformaci [4], která je dosti časově náročná. Naštěstí v roce 1965 J. W. Cooley a J. W. Tukey vynalezli tzv. *rychlou diskrétní Fourierovu transformaci* (viz [3]), která je velmi nenáročná na počet prováděných aritmetických operací. Ta nám pak umožňuje v reálném čase sledovat pohybující se orgány (např. plíce, srdce).

Aproximace vztahů (2), (3), rychlá Fourierova transformace apod., bez nichž je počítačová tomografie nemyslitelná, jsou skryté v softwarovém vybavení tomografů, což bohužel širší veřejnost většinou nevidí a bere to jako samozřejmost. EMR tomografy založené na principu magnetické rezonance jsou vybaveny analogickým softwarem.

5. Teorie pravděpodobnosti

Jako příklad možnosti praktického uplatnění teorie pravděpodobnosti představíme *metodu Monte Carlo* pro řešení parciálních diferenciálních rovnic. Hledejme dvakrát spojitě diferencovatelnou funkci u splňující následující rovnice

$$\Delta u = 0 \quad \text{v } \Omega, \tag{4}$$

$$u = g \quad \text{na } \partial\Omega, \tag{5}$$

kde $\Omega \subset R^n$ je omezená oblast s hranicí $\partial\Omega$, $\Delta = \sum_{k=1}^{n} \partial^2/\partial x_k^2$ je Laplaceův operátor a g je spojitá funkce zadaná na $\partial\Omega$. Vztahy (4)–(5) popisují rozložení teploty

[5]) J. B. J. Fourier (1768–1830), francouzský matematik, zabýval se především matematickou fyzikou.

v oblasti Ω, průhyb elastické membrány, kroucení tyče aj. Předpokládejme pro jednoduchost, že $n = 2$ a že lze vyšetřovanou oblast vykrýt čtvercovou sítí (pro obecné sítě a obecnou eliptickou rovnici s proměnnými koeficienty viz [26, 33]). Předpokládejme dále, že se po hranách sítě náhodně pohybuje nějaká částice od pevného vnitřního uzlu X. K předem stanovenému sousednímu uzlu Y částice dorazí s pravděpodobností $\frac{1}{4}$. Odtud se opět náhodně vydá k jednomu ze sousedů uzlu Y atd. Jakmile částice poprvé dorazí k hranici $\partial\Omega$, označíme příslušný bod hranice ξ_X, tj. ξ_X je náhodná veličina. Pro dostatečně velké m opakujme m krát tento pokus s částicí náhodně se pohybující od bodu X. Pak pomocí zákona velkých čísel lze pro (slabé) řešení u problému (4)–(5) dokázat (viz [33]) následující tvrzení.

Věta. *Označíme-li E střední hodnotu, pak* $u(X) \doteq Eg(\xi_X) \approx \dfrac{1}{m}\displaystyle\sum_{j=1}^{m} g(\xi_X^j)$.

Všimněme si, že metoda Monte Carlo neklade téměř žádné nároky na paměť počítače. Pro simulaci pohybu částice v síti se používají generátory náhodných a pseudonáhodných čísel. Metodu Monte Carlo lze snadno zobecnit na vícerozměrné problémy, kde pro $n \gg 1$ může být účinnější než numerické metody. Jinou verzi této pravděpodobnostní metody lze použít i pro testování prvočíselnosti [30] či hledání prvočíselných rozkladů [20].

6. Teorie diferenciálních rovnic

Uvažujme opět problém (4)–(5) a označme ∇u gradient řešení u. Pak platí následující *Dirichletův princip*[6]):

Věta. *Jestliže u řeší* (4)–(5)*, pak minimalizuje tzv. Dirichletův integrál*

$$I(v) = \int_\Omega (\nabla v)^\top \nabla v \,\mathrm{d}x \tag{6}$$

mezi všemi funkcemi, které mají spojité první parciální derivace a splňují (5).

Podobný princip (minima potenciální energie) platí i pro stacionární rovnice pružnosti, gravitačního pole, vedení tepla, Maxwellovy či Stokesovy rovnice apod. Povšimněme si, že Dirichletův integrál (6) obsahuje jen první derivace, což je velice příznivé pro numerické aproximace. Přesné řešení u lze totiž přesně analyticky vyjádřit jen v několika málo speciálních případech.

7. Teorie aproximace

Jako příklad numerické aproximace problému (4)–(5) uvedeme *metodu konečných prvků*, kterou v roce 1943 navrhl R. Courant pro $n = 2$. Tehdy se ještě nepoužívaly

[6]) P. G. L. Dirichlet (1805–1859), německý matematik, zabýval se teorií čísel a matematickou analýzou.

elektronické počítače, a proto se na tuto metodu pozapomnělo. Zhruba o deset let později byla znovu objevena americkými leteckými inženýry. U nás se začala používat v šedesátých letech pro výpočet pevnosti přehrad. Jednou z předností této metody je to, že umožňuje na počítači simulovat řadu fyzikálních procesů, a tím nahrazuje nákladné technické modely (prototypy) nebo složitá měření.

Základní myšlenka metody konečných prvků spočívá v tom, že se nejprve trianguluje vyšetřovaná oblast Ω, tj. rozdělí se na konečný počet jednoduchých podoblastí (trojúhelníků, čtyřúhelníků, popř. čtyřstěnů, pětistěnů apod.). Poté se minimalizuje stejný funkcionál (6) na konečněrozměrné množině spojitých a po částech polynomiálních funkcí nad triangulací, které aproximují (5). Vhodnou volbou bázových funkcí lze tuto úlohu převést na řešení soustavy lineárních algebraických rovnic (viz (7)), jejíž matice je „řídká“, tj. obsahuje většinou nulové prvky, což snižuje nároky na paměť počítače a počet prováděných aritmetických operací. Vyřešením této soustavy dostaneme koeficienty linární kombinace bázových funkcí, které určují přibližné řešení úlohy (4)–(5). V roce 1968 dokázal konvergenci této metody brněnský profesor M. Zlámal (1924–1997).

Metoda konečných prvků se používá pro výpočet průběhu chemických reakcí, průhybů nosníků a desek, oteplení vysokonapěťových transformátorů a motorů, obtékání lopatek turbín, zjišťování pevnosti vysokotlakých nádob apod. Její hlavní výhodou je, že na počítači lze celý proces zautomatizovat:

1. interpolace vstupních dat,
2. generování triangulací,
3. sestavení soustavy algebraických rovnic,
4. vyřešení soustavy algebraických rovnic,
5. zhlazení numerického řešení,
6. aposteriorní odhady chyby (viz [12]),
7. grafické znázornění výsledků.

Při praktickém programování těchto sedmi bodů se používá celá řada rozmanitých teoretických výsledků. Například pro bod 2 lze použít větu:

Věta. *Pro každý mnohostěn existuje rozklad na čtyřstěny.*

Její důkaz (viz [15]) je konstruktivní, čehož lze využít při programování trojrozměrných úloh. Navíc čtyřstěny lze konstruovat tak, že délky jejich hran jsou menší než předem zadané kladné číslo a každá stěna libovolného čtyřstěnu z rozkladu je stěnou jiného čtyřstěnu anebo podmnožinou hranice mnohostěnu.

8. Teorie matic

V této kapitole si připomeneme některé důležité teoretické výsledky týkající se řešení soustavy lineárních algebraických rovnic

$$Ax = b, \tag{7}$$

kde A je regulární matice typu $N \times N$ a $b \in R^N$. Řešení soustavy (7) známou Gaussovou eliminační metodou vyžaduje přibližně $\frac{2}{3}N^3$ aritmetických operací. V roce 1952 M. R. Hestenes a E. Stiefel publikovali *metodu sdružených gradientů*, která konverguje k řešení (7) v N krocích algoritmu, je-li A symetrická. Její podrobný popis a další vlastnosti lze nalézt v [15, 22]. Tato metoda dlouho zůstávala nepovšimnuta, protože vyžadovala přibližně $2N^3$ operací pro „plné“ matice. O 15 let později se ale přišlo na to, že konverguje velice rychle (viz [5], popř. [10]), pokud je matice A pozitivně definitní (tj. $x^\top Ax > 0$ pro $x \neq 0$), což je v řadě technických aplikací splněno.

Věta. *Nechť A symetrická a pozitivně definitní matice. Pak $\overline{x}$ je řešením* (7) *právě tehdy, když minimalizuje funkcionál $J(x) = \frac{1}{2}x^\top Ax - b^\top x$ na prostoru R^N.*

Při jednotlivých iteracích metody sdružených gradientů se funkcionál J minimalizuje na podprostorech, jejichž dimenze postupně vzrůstá.

Jak již bylo řečeno, při použití metody konečných prvků je matice A řídká. V tomto případě metoda sdružených gradientů potřebuje řádově jen N paměťových buněk počítače. Matice A se v průběhu celého výpočtu nemění, zatímco při eliminaci se matice soustavy mění a navíc se ztrácí její řídkost.

V důsledku velké rychlosti konvergence metody sdružených gradientů lze ukončit iterační proces mnohem dříve než po N krocích (když iterační chyba je zhruba rovna diskretizační chybě). Pro trojrozměrné úlohy vyžaduje Gaussova eliminace řádově $N^{7/3}$ operací, zatímco metoda sdružených gradientů řádově jen $N^{4/3}$ operací a tzv. *metoda sdružených gradientů s předpodmíněním* řádově dokonce jen $N^{7/6}$ operací (viz [15]). Při dnes běžně na PC dosahované rychlosti milion aritmetických operací za sekundu si posledně jmenovaná metoda vyžádá pro $N = 10^6$ řádově desítky sekund strojového času. Naproti tomu Gaussova metoda s $\frac{2}{3}N^3$ operacemi by spotřebovala zhruba 20 000 let pro plnou matici, vzniklou např. pomocí klasické Galerkinovy metody, a výpočtový čas pro známé Cramerovo pravidlo[7]) by byl ještě o mnoho řádů větší.

V současnosti se zkoumají metody více sítí, které vyžadují řádově jen $N \log N$ operací, což umožňuje řešit soustavy o mnoha milionech neznámých.

9. Teorie optimalizace

Bouřlivý rozvoj numerických metod si vyžádala teorie optimalizace, která má široké uplatnění v ekonomii (např. optimalizace distribuce zboží). Pomocí optimalizačních technik lze stanovit i ekonomickou dráhu vesmírné sondy, tj. kdy a na jak dlouho mají být zapáleny její motory, aby dosáhla cíle co možno nejúspornější cestou.

Teorie optimalizace také umožňuje navrhnout tvar strojní součásti tak, aby měla minimální váhu nebo aby na jejím povrchu bylo minimální mechanické napětí. Takový

[7]) Kdybychom příslušné determinanty počítali přímo z definice, která vyžaduje provést $N!$ součtů součinů N čísel, pak by pro milion rovnic bylo zapotřebí více než $10^{5000000}$ let strojového času (viz Stirlingův vzorec v [22]).

přístup se nazývá *tvarová optimalizace*. Spočívá v hledání oblasti Ω_{opt}, která minimalizuje daný kriteriální (účelový) funkcionál $\mathcal{J}$ na množině přípustných oblastí U_{ad}, tj.

$$\mathcal{J}(\Omega_{\text{opt}}) = \min_{\Omega \in U_{\text{ad}}} \mathcal{J}(\Omega).$$

V [15] se metodou konečných prvků hledá přibližné řešení této úlohy pro „optimální" návrh tvaru elektrických strojů. V konečné fázi se hledá minimum (popř. maximum) spojité funkce $J : R^N \to R^1$. Zde lze v některých případech uplatnit následující *Eulerovu nutnou podmínku* pro extrém.

Věta. *Jestliže J má v $\overline{x}$ lokální extrém a $\nabla J(\overline{x})$ existuje, pak $\nabla J(\overline{x}) = 0$.*

10. Teorie informace

Praktické aplikace v této oblasti jsou více než evidentní (viz např. [24]). Proto se zmíníme jen o jednom významném objevu.

Kniha proměn, která vznikla v Číně zhruba v 8. stol. př. n. l., obsahuje obrázek skládající se z 8×8 políček (viz [14, str. 224]). Uvnitř každého z nich je 6 horizontálních čar. Přerušená čára znamená starý čínský princip *jin* a plná princip *jang*. *Jin* je spojováno s Měsícem, vlhkostí, tmou, zemí, ženou a pasivitou, *jang* naproti tomu se Sluncem, suchem, světlem, nebesy, mužem a aktivitou. Významný německý filozof a matematik G. W. Leibniz (1646–1716) spojoval tento obrázek s objevem dvojkové soustavy. Budeme-li totiž místo přerušené čáry uvažovat nulu a místo plné čáry jedničku, pak symboly v políčkách lze jednoznačně interpretovat jako čísla $0, 1, 2, \ldots, 63$ zapsaná ve dvojkové soustavě.

I když staří Číňané neprováděli se symboly *jin* – *jang* žádné aritmetické ani logické operace, nelze jim upřít prioritu ve znázornění čísel zapsaných ve dvojkové soustavě. Tento fenomenální objev našel praktické uplatnění až v dnešní době počítačů, tj. téměř o 28 století později. Počítače totiž zobrazují a zpracovávají veškerou informaci (včetně čísel) právě ve dvojkové soustavě. Je to nejjednodušší způsob, jak v elektronických obvodech počítače toto zpracování realizovat. A tak i fungování celosvětové sítě internet, e-mailu, faxu, digitálních kamer a fotoaparátů, kompaktních disků CD, mobilních telefonů apod. je vlastně založeno na principech *jin* ($= 0$) a *jang* ($= 1$).

Závěrem mi dovolte poděkovat RNDr. J. Chlebounovi, CSc., RNDr. A. Šolcové a Mgr. J. Němcovi, kteří svými cennými připomínkami přispěli ke zlepšení textu. Příště se zaměříme na zajímavé aplikace teorie množin, teorie distribucí, teorie chaosu, teorie katastrof aj.

L i t e r a t u r a

[1] Bishop, D. M.: *Group theory and chemistry.* Clarendon Press, Oxford 1973.
[2] Buchštaber, V. M., Gindikin, S. G.: *Od Cavalieriho principu k tomografu.* PMFA *29* (1984), 196–210.

[3] Cooley, J. W., Tukey, J. W.: *An algorithm for the machine calculation of complex Fourier series.* Math. Comp. *19* (1965), 297–301.
[4] Čížek, V.: *Diskrétní Fourierova transformace a její použití.* SNTL, Praha 1981.
[5] Daniel, J. W.: *The conjugate gradient method for linear and nonlinear operator equations.* SIAM J. Numer. Anal. *4* (1967), 10–26.
[6] Grošek, O., Porubský, Š.: *Šifrovanie — algoritmy, metody, prax.* Grada, Praha 1992.
[7] Hofstadter, D. R.: *Mathemagical themes.* Scient. Amer. *247* (1982), 18–30.
[8] Chleboun, J., Kříž ek, M.: *Křivky kolem nás.* Rozhledy mat.-fyz. *76* (1999).
[9] Jelínek, J., Segeth, K., Overton, T. R.: *Three-dimensional reconstruction from projections.* Apl. Mat. *30* (1985), 92–109.
[10] Kaniel, S.: *Estimates for some computational techniques in linear algebra.* Math. Comp. *20* (1966), 369–378.
[11] Klarner, D. A. (ed.): *The mathematical gardner.* Wadsworth Internat., Belmont 1981.
[12] Kříž ek, M.: *Padesát let metody konečných prvků.* PMFA *37* (1992), 129–140.
[13] Kříž ek, M.: *Metoda RSA pro šifrování zpráv pomocí velkých prvočísel.* Rozhledy mat.-fyz. *75* (1998), 101–107.
[14] Kříž ek, M., Liu, L.: *Matematika ve starověké Číně.* PMFA *42* (1997), 223–233.
[15] Kříž ek, M., Neittaanmäki, P.: *Mathematical and Numerical Modelling in Electrical Engineering: Theory and Applications.* Kluwer, Dordrecht 1996.
[16] Kuratowski, C.: *Sur le problème des courbes gauches en topologie.* Fund. Math. *15* (1930), 271–283.
[17] Litzman, O., Sekanina, M.: *Užití grup ve fyzice.* Academia, Praha 1982.
[18] Nečas, J.: *Grafy a jejich použití.* SNTL, Praha 1978.
[19] Nešetřil, J.: *Teorie grafů.* SNTL, Praha 1979.
[20] Pollard, J. M.: *A Monte Carlo method for factorization.* BIT *15* (1975), 331–334.
[21] Pradlová, J.: *Ornamentální vzory — frýzy.* Rozhledy mat.-fyz. *72* (1995), 121–125.
[22] Rektorys, K.: *Přehled užité matematiky.* Prometheus, Praha 1995.
[23] Rivest, R. L., Shamir, A., Adelman, L. M.: *A method for obtaining digital signatures and public key cryptosystems.* Comm. ACM *21* (1978), 120–126.
[24] Roman, S.: *An introduction to coding and information theory.* Springer-Verlag, New York 1996.
[25] Rosen, K. H.: *Discrete mathematics and its applications.* Mc-Graw Hill 1994.
[26] Sabelfeld, K. K.: *Monte Carlo methods in boundary value problems.* Springer Series in Comput. Physics 1991.
[27] Sedláček, J.: *Úvod do teorie grafů.* Academia, Praha 1981.
[28] Schneier, B.: *Applied cryptography.* Wiley, New York 1993.
[29] Schroeder, M. R.: *Number Theory in Science and Communication.* Springer, Berlin 1986.
[30] Solovay, R., Strassen, V.: *A fast Monte-Carlo test for primality.* SIAM J. Comput. *6* (1977), 84–85.
[31] Stallings, W.: *Network and internetwork security principles and practice.* Prentice Hall, New Jersey 1995.
[32] Thompson, T. M.: *From error-correcting codes through sphere packings to simple groups.* Math. Assoc. Amer. 1983.
[33] Zhu, Q., Lin, Q., Liu, L.: *Monte Carlo finite element method.* Sborník semináře: Programy a algoritmy numerické matematiky *8*, MÚ AV ČR, Praha, 1996, 210–217.