RECENZII

ISRAEL GOHBERG, PETER LANCASTER, LEIBA RODMAN, *Invariant Subspaces of Matrices with Applications,* Classics in Applied Mathematics 51, SIAM , 2006, XXI + 692 p., ISBN 0-89871-608-X.

Linear algebra is one of the fundamental domains of pure and applied mathematics. Although it is already a classical domain of mathematics, it is still developing and most of its new ideas and research directions are inspired by subjects in applied mathematics, especially in systems theory and computational mathematics.

The present monograph considers the fundamental notion of invariant subspace of a linear operator in finite dimensional space. The importance of invariant subspaces becomes clearer in the linear systems theory, in problems of controllability, feedback controllability and stabilization, etc. The text thus provides to the reader a systematic treatment of this notion and of various theoretical aspects. Organization of the material is in four parts, each composed of several chapters.

The first part (Chapters 1–8) describes the fundamental properties of invariant subspaces, Jordan forms and more specific topics, such as coinvariant and semiinvariant subspaces, matrix polynomials, the case of transformations between different spaces and rational matrix functions. Applications are given, in the last chapter of this part, to time invariant linear differential systems.

The second part of the book (Chapters 9–12) develops the algebraic aspects of the theory, studying characterisations of the invariant subspaces, as well as the relation with the operators commuting with the given operator and, more generally, with algebras of transformations. The theory is revisited in the framework of real operators.

The third part (Chapters 13–17) deals with topological aspects concerning invariant subspaces. After introducing a metric structure on the set of invariant subspaces, various problems of stability under small perturbations are investigated.

The last part of the book (Chapters 18–20) studies analytic families of operators depending on a complex parameter, and the dependence of their invariant subspaces. The study also includes the dependence of irreducible subspaces, Jordan forms and Jordan bases.

In conclusion, the book represents a valuable monograph useful for a broad audience, from undergraduate students to postgraduate students and researchers.

Cătălin-George Lefter

DARIO CATALANO, RONALD CRAMER, IVAN DAMGÅRD, GIOVANNI DI CRESCENZO, DAVID POINTCHEVAL, TSUYOSCHI TAKAGI, *Contemporary Cryptology,* Birkhäuser Verlag, Basel, Boston, Berlin, 2005,viii + 237 p., ISBN-10: 3-7643-7294-X, ISBN-13: 978-3-7643-7294-1.

The growing importance of modern cryptology and the multidisciplinarity of the subject have motivated, during the last decade, the organization of a multitude of workshops, conferences and intensive courses. This volume includes the expanded version of the lectures on *Advanced Course on Contemporary Cryptology* organized by Centre de Recerca Matemàtica in Barcelona at the Universitat Politècnica de Catalunya.

The material is structured into five independent themes: Efficient distributed computation modulo a shared secret, Multiparty computation, Foundations of modern cryptology, Provable security for public-key schemes, and Efficient and secure public key cryptosystems.

The first chapter, "Efficient distributed computation modulo a shared secret", written by D. Catalano (ENS Paris), contains several algorithms that can be combined to allow a set of participants to generate shared RSA keys without assuming the existence of a trusted dealer. This situation is required in several cryptography protocols, when all participants use the same RSA modulus, yet they are not assumed to know the factorization.

R. Cramer (CWI Amsterdam) and I. Darmgård (University of Aarhus) discuss several concepts related to the notion of secure multiparty computation, survey several general results and present techniques for building secure multiparty protocols, showing how they imply secure multiparty computation.

The third theme approached in the volume, developed by G. Di Crescenzo (Telcordia Technologies, USA), refers to aspects on "Foundations of modern cryptography": one-way functions, pseudo-random generators, pseudo-random functions, solution techniques, zero-knowledge protocols.

In the next chapter, D. Pointcheval (ENS Paris) presents practical asymmetric protocols with corresponding security proofs. The protocols cover the main goals of the public-key cryptography: confidentiality (with public-key encryption schemes) and authentication (with digital signatures).

The last part of the volume, written by T. Takagi (Future University – Hakodate), provides efficient algorithms applied to RSA and to elliptic curves cryptosystems. The algorithms concern integer arithmetic, fast variants of RSA, efficient coordinate systems for elliptic curves, attacks related to efficient implementation (implementation attack, side channel attack, zero-valued point attack) and countermeasures against them.

The volume contains some interesting material on several topics of contemporary cryptography. Even if it requires some basic knowledge in the subject, it can be recommended as a valuable introduction in the themes selected for this text.

Răzvan Liţcanu

TYN MYINT-U, LOKENATH DEBNATH, *Linear Partial Differential Equations for Scientists and Engineers*, Fourth Edition, Birkhäuser, Boston, 2007, xxii+ 778 p. , ISBN 0-8176-4393-1.

This book is the fourth revised edition of a monograph, very well received worldwide, concerning the theory and applications of linear PDEs. The authors provide fundamental concepts, underlying principles, a wide range of applications, and various methods of solution to PDEs.

The work is divided into 15 chapters, an Appendix on special functions and their properties, and a rich bibliography, composed of standard texts and reference books, alongwith selected classical and recent papers.

The introductory chapter presents the historical development of the domain of partial differential equations, then basic concepts and definitions are provided.

Chapter 2 treats the construction and geometrical interpretation of the first order, quasi-linear and linear, partial differential equations and their solution, by using the Lagrange method of characteristics and its generalizations.

Chapter 3 describes the physical deduction of the mathematical models of waves in an elastic medium, heat conduction in solids, and of the Laplace, Burgers, Schrödinger and Korteweg-de Vries equations.

Chapter 4 deals with the classification and reduction of second-order linear equations in two independent variables to canonical form.

Chapter 5 studies Cauchy problems for hyperbolic partial differential equations, particularly for wave equations. The final sections of this chapter are devoted to spherical and cylindrical wave equations.

Chapter 6 covers Fourier series and integrals with their applications.

Chapter 7 is devoted to the method of separation of variables, exemplified on the vibrating string, on the heat conduction problem, on Laplace and beam equations.

Chapter 8 treats eigenvalue problems and special functions. The authors present Sturm-Liouville systems, Bessel's and Legendre's equations and functions, as well as Green's functions for ordinary differential equations.

Chapter 9 deals with boundary value problems for two-dimensional elliptic partial differential equations, particularly for the Laplace equation on a circle or a rectangle. Chapter 10 is concerned with higher-dimensional boundary-value problems, such as the Laplace equation on a cube, cylinder or sphere, or with three-dimensional wave and heat equations.

Chapter 11 describes the method of Green's functions for solving boundary-value problems in partial differential equations in two or more dimensions. Two of the examples analysed are Dirichlet's problem for the Laplace and Helmholtz operator.

Chapter 12 is concerned with the Fourier, Laplace, Hankel, and Mellin integral transforms. A separate section is devoted to fractional partial differential equations.

Chapter 13 presents nonlinear partial differential equations, such as the nonlinear wave equations, Whitham's equations, or the traffic flow model. Other topics discussed are shock waves, solitons for the Korteweg-de Vries equation, and solitary waves for the nonlinear Schrödinger equations.

Chapter 14 deals with numerical and approximation approaches to the solutions of the many partial differential equations problems which cannot be solved analytically. The authors treat numerical methods based on explicit and implicit finite difference approximations, variational methods and the Euler-Lagrange equations, the Rayleigh-Ritz, Galerkin, and Kantorovich methods of approximation. The final section presents the finite element method.

Chapter 15 contains tables of integral Fourier, Laplace and Hankel transforms.

Each chapter ends with a set of exercises, totalizing over 900 worked examples and exercises dealing with problems in fluid mechanics, gas dynamics, optics, plasma physics, elasticity, biology, and chemistry. Solutions and hints to selected exercises are provided.

The book is useful not only as a textbook for courses in PDEs or in advanced engineering mathematics, but also to graduate students and researchers in applied mathematics, mathematical physics, and engineering.

Adriana-Ioana Lefter

S.S. SRITHARAN (editor), *Optimal Control of Viscous Flow*, SIAM, Philadelphia, 1998, xi + 198 p., ISBN 0-89871-406-0.

The book, based on the contributions of eleven renowned specialists in the mathematical theory of control for Navier-Stokes equations, presents various technical issues of this subject.

Chapter 1, written by S.S. Sritharan, is an introduction to the deterministic and stochastic control of the Navier-Stokes evolution system. The deterministic control part reviews the existence theorems for optimal controls, the Pontryagin maximum principle and the adjoint equation, dynamic programming and the Hamilton-Jacobi equation, while the stochastic control section treats stochastic dynamic programming with complete and partial observations and nonlinear filtering.

In Chapter 2, Max D. Gunzburger, L. Steven Hou and Thomas P. Svobodny analyse an abstract constrained optimization problem, which is then applied to the control of fluids. The existence of optimal solutions, of Lagrange multipliers and the regularity of optimal solutions are studied.

Chapter 3, elaborated by Viorel Barbu, is concerned with the feedback control of time dependent Stokes flows. The author studies the dual Hamilton-Jacobi equations associated with the dynamic programming equations, with applications to optimal control of viscous flows.

Chapter 4 treats an optimal control problem of three dimensional unsteady incompressible flows. The author, Eduardo Casas, considers the problem of minimizing the turbulence within the flow, which can be done by minimizing an integral involving the vorticity. An existence theorem for optimal control is formulated, along with necessary conditions for optimality in terms of adjoint equations.

Frédéric Abergal and Roger Temam present in Chapter 5 an optimal control technique for the high frequency modes in turbulence. They consider time-dependent two- and three-dimensional flows and steady three-dimensional flows. The corresponding systems of optimality conditions are derived by means of the adjoint state equation.

In Chapter 6, A.V. Fursikov studies two problems: the global unique solvability of the three-dimensional Navier-Stokes equations for a dense set of forcing data and the problem of work minimization when the flow is speeded up to a prescribed velocity.

Chapter 7, by Yuh-Roung Ou, is devoted to minmax compensator designs for flow control in a driven cavity and to active control of unsteady flows past a circular cylinder at low Reynolds numbers. Computational results are presented.

S.S. Ravindran treats in Chapter 8 a sequential quadratic programming method for the numerical approximation of optimal Dirichlet control problems associated with steady Navier-Stokes equations.

The book is addressed to engineers and mathematicians.

Adriana-Ioana Lefter

LAWRENCE HUBERT, PHIPPS ARABIE, JACQUELINE MEULMAN, *The Structural Representation of Proximity Matrices with MATLAB*, SIAM, Philadelphia, 2006, xvi+214 p., ISBN 0-89871-607-1.

The book is intended to present and illustrate the use of functions (M-files) within a MATLAB computational environment, to perform a variety of structural representations for proximity information assumed available on a set of objects. The proximity information analyzed may be grouped in two cathegories: one-mode proximity data, defined between the objects of a single set, and two-mode proximity data, defined between the objects of two distinct sets.

The volume is divided into 11 chapters, grouped in three main sections, each based on the general class of representations under consideration.

Part I discusses optimization problems posed by linear unidimensional scaling, (Chapter 1), linear multidimensional scaling (Chapter 2), circular unidimensional scaling (Chapter 3) and linear unidimensional scaling for two-modes proximity data (Chapter 4). All over, the city-block metric is used as the major representational device.

Part II deals with characterizations based on various graph-theoretic tree structures, such as ultrametrics and additive trees. Chapter 5 is concerned with fitting and finding ultrametrics in the L_2 -norm, and with graphical representation of ultrametrics. Chapter 6 treats fitting and finding an additive tree in the L_2 -norm, decomposing additive trees and their graphical representation. Chapter 7 describes fitting of multiple tree structures (ultrametrics and additive trees) to a symmetric proximity matrix, while chapter 8 presents fitting and finding for two-mode rectangular ultrametrics and additive trees.

Part III concerns the representation of proximity matrices by structures dependent solely on order, accent being laid on anti-Robinson forms. Chapters 9 and 10 study anti-Robinson and circular anti-Robinson matrices (either strongly or not), respectively. The topics are: fitting and finding in the L_2 -norm for these matrices, graphical representation of the above structures and representation through multiple anti-Robinson matrices. Finally, chapter 11 treats anti-Robinson matrices for two-mode proximity data.

The volume also includes a list of figures, a list of tables and an appendix, providing the description and the syntax of 67 functions (M-files) used to find and fit computationally the structures presented in the text. An extensive bibliography complements the material.

The book is written for applied statisticians, data analysts, bioinformaticians, chemometricians, psychometricians, industrial engineers, quantitative psychologists, behavioural and social scientists.

Adriana-Ioana Lefter

MARK S. GOCKENBACH, *Understanding and Implementing the Finite Element Method,* SIAM (Society for Industrial and Applied Mathematics), Philadelphia, 2006, xvi+363 p., ISBN: 0-89871-614-4 (pbk.).

The finite element method is the most powerful general-purpose technique for computing accurate solutions to partial differential equations.

This book explains how to write a finite element code from scratch. In addition, it comes with a collection of MATLAB programs implementing the ideas presented in the book. The four parts of the book illustrates very well this general explanation.

In Part I, an overview of the theoretical basis of the finite element method is given. In fact, quite a large number of finite element methods, sharing common features, yet with important differences, exists. The author focuses on the *Galerkin* finite element method for steady state boundary value problems, that is, problems describing equilibrium in various systems.

Part II approaches the computer implementation of finite elements. The author presents the technical theorems, such as the necessary interpolation theory for piecewise polynomials, showing how they fit into the convergence theory. To make the discussion as concrete as possible, it initially focuses on the common case of piecewise linear functions defined on triangles (linear Lagrange triangles).

A finite element method reduces a boundary value problem for a linear partial differential equation (PDE) to a system of linear algebraic equations, written in matrix-vector form as $KU=F$, that should be solved. The finding of this system of equations is presented in Part I, while the algorithms in Part II show how to compute matrix K and vector F.

Part III discusses both direct and iterative algorithms for solving a large system like $KU=F$. One reason explaining the success of the finite element method is that piecewise polynomials result in a sparse stiffness matrix K, that is, a matrix in which most of the entries are zero. This makes it possible to solve the system $KU=F$ when the number of unknowns is very large. The first chapter of this part gives a brief overview of the direct methods for solving sparse systems, known as producing the exact solution in a finite number of steps. This first chapter was included in the book mainly to provide a context for understanding the advantages of the iterative methods. A detailed discussion on direct algorithms is beyond the scope of this book. A number of different iterative algorithms computing a sequence of approximate solutions that converges to the exact solution is described in Chapters 11 to 13.

In Part IV, the author discusses the various components of an adaptive finite element algorithm, which automatically creates a mesh suited for a problem at hand. The first chapter of this part explains the algorithms for the local refinement of meshes and a strategy for choosing the elements to be refined. The author also presents a simple but expensive error estimator, applied to form a complete adaptive algorithm. Several examples show the advantage of the adaptive approach.

Many practical error estimators have been proposed. The last chapter of the book describes such estimators; two of them are explicit and other one is implicit. Several examples of problems with singular solutions are given. Adaptive finite element methods are particularly effective on such problems.

Exercises are provided in the end of each chapter. Some of these are theoretical, some ask the student to apply the code provided with the text, others require programming to extend the capabilities of the code. Beyond the given exercises, there is probably no better way to understand the finite element method than to rewrite the MATLAB codes in another programming language. In the process of translating the code into a different syntax, and particularly in testing and debugging, the details should be mastered.

The bibliography lists the books and papers directly used by the author in writing this manuscript.

This practical book should provide an excellent foundation for those who wish to delve into advanced texts on the subject, including advanced undergraduates and beginning graduate students in mathematics, engineering, and physical sciences.

Ion Al. Crăciun

GÉRARD MEURANT, *The Lanczos and Conjugate Gradient Algorithms. From Theory to Finite Precision Computations,* SIAM (Society for Industrial and Applied Mathematics), Philadelphia, 2006, xv+365 p., ISBN: 13: 978-0-898716-16-0, ISBN: 10: 0-89871-616-0.

The Lanczos algorithm and the conjugate gradient (CG) are among the most fascinating numerical algorithms. This book discusses, in a comprehensive way, the use of these methods for computing the eigenvalues of a symmetric matrix A and for solving the linear algebraic systems $Ax=b$.

The book presents some old and new results on the Lanczos and CG algorithms in both exact and finite arithmetic precision.

Chapter 1, devoted to the Lanczos algorithm in exact arithmetic, describes the mathematical properties of this algorithm, while Chapter 2 derives the CG algorithm from the Lanczos one.

Chapter 3 gives a historical perspective on the Lanczos and CG algorithms in finite arithmetic precision. The author first recalls the classical model of finite precision arithmetic and then derives some results on rounding errors for the operations involved in the Lanczos and CG algorithms. These results, to be used in the next chapters, are summarized and illustrated by some of the most important results obtained over the years, by different people, for the Lanczos and CG algorithms in finite precision arithmetic. Main contributions to these fields brought by C. Paige and A. Greenbaum. The author also briefly reviews the works of J. Grcar, H. Simon, Z. Strakôs, J. Cullum and R. Willoughly, V. Druskin, and L. Knizhnerman. The book and papers of P.N. Parlett have also been very influential over the last 30 years.

Chapter 4 is devoted to some new results on the Lanczos algorithm in finite arithmetic precision.

Chapter 5 studies CG in finite precision arithmetic, and the relationship of Lanczos and CG algorithms in finite precision is analyzed.

Chapter 6 deals with the problem of estimating the maximum attainable accuracy. It is well known that, when performing a large enough number of iterations at some points, the norms of the residual $b - Ax^k$ and the error stagnate. The level of stagnation depends on the matrix and on the initial vector norms. The author also describes some ways to slightly improve the maximum attainable accuracy.

Chapter 7 shows that the expressions for the A-norm of the error derived in Chapter 2 are still valid in finite precision arithmetic up to small perturbation terms. Results for the l_2 norm of error are also obtained.

Chapter 8 is concerned with the modification to be made in the results of the previous chapters, when CG is used as a preconditioned algorithm.

Chapter 9 deals with various topics that would not fit naturally in the previous chapters. The first one is the choice of the starting vector for CG. Then, the author describes certain variants of CG, some of them being used for solving several linear systems, sequentially, with the same matrix *A*, but with different right-hand sides.

Although the main audience of this book includes researchers in numerical linear algebra and, more generally, in numerical analysis, it could be equally of interest to engineers, computational scientists, and physicists interested in linear algebra, numerical analysis, and partial differential equations. Engineers and scientists using the Lanczos algorithm to compute eigenvalues and the CG algorithm to solve linear systems, and researchers in the Krylov subspace methods for symmetric matrices, especially those concerned with floating point error analysis, could find information in this book. Moreover, it can be used in advanced courses about iterative methods or as an example of the study of a well-known numerical method in finite precision arithmetic.

All computations were done with the MATLAB version 6 software on a PC, some of them using the Symbolic Toolbox, which uses a Maple kernel for extended precision computations.

Ion Al. Crăciun

GERDA DE VRIES, THOMAS HILLEN, MARK LEWIS, JOHANNES MŰLLER, BIRGITT SCHŐNFISCH, *A Course in Mathematical Biology: Quantitative Modeling with Mathematical and Computational Methods*, Mathematical Modeling and Computation, SIAM (Society for Industrial and Applied Mathematics), Philadelphia, 2006, xii+309 p., ISBN: 0-89871-612-8.

The field of mathematical biology is rapidly growing. Questions on infectious diseases, heart attacks, cell signaling, cell movement, ecology, environmental changes, and genomics are now being analyzed with mathematical and computational methods. This book, including all aspects of modern mathematical modeling, is specifically designed to introduce undergraduate students to problems solving in the context of biology.

The volume is structured in three parts: (I) analytical modeling techniques, (II) computational modeling techniques, (III) problem solving.

Part I covers the basic analytical modeling techniques. The formulation of models using difference equations, differentials equations, probability theory, cellular automata, as well as model validation and parameter estimation, are discussed. Stress is laid on the modeling process and qualitative analysis, rather than on explicit solutions techniques, which can be found in other textbooks. Classical models for disease, movement, and population dynamics are derived from the first principles. Each solution provides a number of biologically motivated exercises.

Part II introduces the computational tools used in the modeling of biological problems. Students are guided through symbolic and numerical calculations with Maple. Many of the examples and exercises of this part relate directly to the models discussed in Part I.

Part III provides 25 open-ended research projects from epidemiology, ecology, and physiology. Each project is formulated in a most accessible manner to students. In most cases, questions will guide the student through the modeling process. These problems can be used as a basis for extended investigation, for example, as a term project or as a team project. This part concludes with a detailed presentation of two projects (cell competition and the chemotactic paradox) based on solutions developed by teams of undergraduate students, who participated in one of workshops organized by the authors of this textbook.

The book is accompanied by a Web site that contains solutions to most of the exercises, and a tutorial for the implementation of the computational modeling techniques. Calculations can be done in modern computing languages such as Maple, Mathematica, and MATLAB.

Intended for upper-level undergraduate students in mathematics or similar quantitative sciences, this book is also appropriate for beginning graduate students in biology, medicine, ecology, and other sciences. It will also be of interest to researchers entering the field of mathematical biology.

Ion Al. Crăciun

TONY F. CHAN, JIANHONG (JACKIE) SHEN, *Image Processing and Analysis: Variational, PDE, Wavelet and Stochastic Methods*, SIAM, Philadelphia, 2005, xxi+ 400 p., ISBN 0-89871-589-X.

The book develops the mathematical foundation of modern image processing and low-level computer vision, and presents a general framework from the analysis of image structures and patterns to their processing. The authors cover the four most powerful classes of mathematical tools in contemporary image analysis and processing and explore their intrinsic connections and integration. Three key aspects are dealt with: modelling, model analysis, and computation or simulation.

The material is divided into 7 chapters. It also contains a list of figures, an index and a bibliography covering more than 300 titles.

The first chapter is an introductory one, overviewing the field and introducing the scopes and structures of the book.

Chapter 2 provides the general mathematical, physical and statistical background for modern image analysis and processing, making the book more self-contained. It treats elements of differential geometry of curves and surfaces in two and three dimensions, functions with bounded variation (BV), thermodynamics and statistical mechanics, a general framework of the Bayesian estimation theory, linear and nonlinear filtering and diffusion, wavelets and multiresolution analysis.

Chapter 3 studies several generic ways to model and represent images, such as deterministic image models, wavelets and multiscale representation, lattice and random-field representation, level-set representation, and the Mumford-Shah free boundary image model.

The last four chapters are concerned with models and computation of most common lower-level image processing tasks, such as denoising, deblurring, inpainting or interpolation, and segmentation, respectively.

After discussing the origins, physics and models of noise, Chapter 4 deals with linear denoising, data-driven optimal filtering, wavelet shrinkage denoising, variational denoising based on bounded variation image model, denoising *via* nonlinear diffusion and scale-space theory, denoising salt-and-pepper noise, multichannel TV denoising.

Chapter 5 reviews the physical origins and mathematical models of blur and then presents deblurring with Wiener filters, deblurring of bounded variation images with known point spreading function and variational blind deblurring with unknown point spreading function.

Chapter 6 studies several inpainting (image interpolation) models based upon the Bayesian, variational, PDE, and wavelet approaches and contains applications of inpainting techniques in digital and information technologies. The authors treat, for example, inpainting of Sobolev images, of bounded variation images (*via* the TV Radon measure), of piecewise smooth images (*via* Mumford and Shah), inpainting *via* Euler's elasticas and curvatures, inpainting with missing wavelet coefficients, inpainting of Gibbs/Markov random fields.

Finally, Chapter 7 discusses several important and interconnected models pertinent to the segmentation task, such as active contours, the Geman and Geman's intensity-edge mixture model, and Mumford and Shah's free boundary model.