Applications of Mathematics

Book Reviews

Applications of Mathematics, Vol. 47 (2002), No. 5, 459--460

Persistent URL: http://dml.cz/dmlcz/134507

BOOK REVIEWS

J. M. Cooper: INTRODUCTION TO PARTIAL DIFFERENTIAL EQUATIONS WITH MATLAB. Birkhäuser-Verlag, Boston-Basel-Berlin, 1998, 560 pages. ISBN 3-7643-3967-5, price DM 138,–.

This advanced textbook reference is an introduction to partial differential equations covering the traditional subjects of the heat equation, the wave equation and the Laplace equation in the traditional manner using the method of separation of variables. The title may be misleading a bit for the interested reader as MATLAB serves only as an exercise tool here. Nevertheless, the extensive use of MATLAB in the exercises for computation and graphical display of solutions should be highly appreciated. Moreover, many of the numerical methods discussed in the book shortly have been implemented in MATLAB codes available by ftp from the Birkhauser Boston Web Site.

The book differs from similar textbooks not only in using MATLAB. To give a more varied, up-to-date treatment of the subject, the following topics are also included and discussed in a more or less detailed way: nonlinear equations (in particular, nonlinear first-order equations), dispersive wave equations and the Schrödinger equation, discrete and fast Fourier transform. Solutions to selected exercises from extensive exercise sets accompanying each chapter and a self-contained overview of MATLAB basics can be found in the appendix.

The book is organized as follows. Chapter 1 reviews the preliminaries from calculus, vector spaces and linear operators, and gives some basic facts about ordinary differential equations. The study of partial differential equations begins in Chapter 2 with the first-order equations. The overall style of this chapter is typical for the whole book. The author starts with the general linear PDE's, then nonlinear conservation laws are discussed and their linearization, followed by a section on the weak solutions. Then, a selected numerical method is introduced (the finite-difference method in this case). The chapter is concluded with a discussion of an applied problem (a conservation law for cell dynamics). Chapters 3 and 4 treat the diffusion and the heat equations, Chapter 5 is devoted to "waves again". For instance, the equations of gas dynamics, the vibrating string, or a nonlinear wave equation are discussed here. Chapter 6 introduces the reader to Fourier series and the Fourier transform. Dispersive wave equations, some quantum mechanics, and the Schrödinger equation are the subject of Chapter 7. The heat and wave equations in higher dimensions are studied in Chapter 8, elliptic PDE's in Chapter 9. Chapter 10 describes numerical methods for higher dimensions.

This is an interesting, atypical textbook in the field. By no means it is a textbook on just the theory of PDE's or the numerical methods for their solution. In any case, it is worth a look as it may serve as an excellent resource for classroom or self-study purposes. It will be useful for anyone trying to understand PDE's and their applications or learning to use modern PDE methods. Finally, we note that a second printing with corrections is now available.

Petr Přikryl

Igor Shparlinski: NUMBER THEORETIC METHODS IN CRYPTOGRAPHY. COMPLEXITY LOWER BOUNDS. Birkhaüser-Verlag, Basel-Berlin-Boston, 1999, 192 pages. ISBN 3-7643-5888-2, price DM 138,–.

Essentially all cryptographic systems that are relevant for practice are based on number-theoretical functions, thus number theory plays a key role in cryptography. Another important field for cryptography is the complexity theory. Unfortunately, the means for proving hardness of problems that are currently available in complexity theory are very weak and thus one cannot prove security of the systems. The book of Shparlinski studies what one can do with the current number-theoretical and complexity-theoretical methods. The book starts with a review and some proofs of auxiliary results, such as sums of characters over finite fields, some of them being quite useful also in related fields of combinatorics and theoretical computer science. Then the author proves many results on various approximations of some cryptographic functions, in particular the discrete logarithm and the Diffie-Hellman function. These results are then applied to derive complexity lower bounds. The complexity lower bounds are proven for the weak models, the only ones for which one is able to prove such bounds. So this does not have any impact on cryptography, but it is the best that one can currently do. The book should be very useful for researchers working in cryptography and complexity theory, as they can learn a lot of useful number-theoretical tools. It may also be useful for number theorists, as they can learn number-theoretical problems relevant for cryptography.

Pavel Pudlák

Kwok-Yan Lam, Igor Shparlinski, Huaxiong Wang and Chaoping Xing (eds.): CRYPTOGRAPHY AND COMPUTATIONAL NUMBER THEORY. Birkhäuser-Verlag, Basel-Berlin-Boston, 2001, 392 pages. ISBN 3-7643-6510-2, price DM 196,–.

This is the proceedings of the Workshop on Cryptography and Computational Number Theory, CCNT'99, held in Singapore in 1999. It consists of 13 papers on Computational Number Theory and 14 on Cryptography. The topics of the papers range from cryptographic systems and attacks on the existing systems to integer factorization and analytical number theory. A specialist in the filed may be interested in original up to date results. A non-specialist may enjoy survey papers, eg., Mihalesscu's *Algorithms for Generating, Testing and Proving Primes* or Gollmann's *Autentification—Myths and Misconceptions.*

Pavel Pudlák