

## REVIEWS AND DESCRIPTIONS OF TABLES AND BOOKS

The numbers in brackets are assigned according to the American Mathematical Society classification scheme. The 2000 Mathematics Subject Classification can be found in print starting with the 1999 annual index of *Mathematical Reviews*. The classifications are also accessible from [www.ams.org/msc/](http://www.ams.org/msc/).

**4[33C45]**—*Chebyshev polynomials*, by J. C. Mason and D. C. Handscomb, Chapman & Hall/CRC, Boca Raton, FL, 2002, xiii+341 pp., \$99.95, ISBN 0-8493-0355-9

The book presents a wide panorama of the applications of Chebyshev polynomials to scientific computing. The authors work with four kinds of Chebyshev polynomials instead of the two usual ones: each of them is, up to a multiplicative constant, equal to a Jacobi polynomial  $J_n^{\alpha,\beta}$  for  $\alpha$  and  $\beta$  equal to either  $-\frac{1}{2}$  or  $\frac{1}{2}$ . The main properties of these polynomials are of course recalled; however, the main originality of the book is that each of them is accompanied by a sequence of applications to different computational algorithms. The most standard ones are weighted numerical integration (see chapter 8), construction of best polynomial approximations (see chapters 3 and 4) or spectral type methods (see chapters 9 and 10). The importance of the fast Fourier transform to enhance the efficiency of the algorithms is explained for most applications. But a large number of lesser-known results are also presented, such as the acceleration of convergence for the iterative solution of a linear system in chapter 3, and the solution of integral equations of Fredholm type in chapter 9. These polynomials can also be defined on the complex variable, as illustrated in chapter 1, and a further application of this concerns trees and number theory. The history of all these methods and algorithms is recalled via the first references on the subject. The quoted references cover the second half of the nineteenth century—P. L. Chebyshev was born in 1821—and the whole twentieth century, and testify to the deep knowledge of the authors on the subject.

The book is very clearly written and is a pleasure to read. Examples inserted in the text allow one to test his or her ability to understand and use the methods, which are described in detail, and each chapter ends with a section full of very pedagogical problems. The only drawback of the book is that the level of the intended reader is rather difficult to determine since it combines rather elementary notions, the definition of a vector space in chapter 3 for instance, with very recent and sophisticated methods. However, I am sure that anyone who is not allergic to relearning the definition of a vector space could discover new clever uses of Chebyshev polynomials in this book.

CHRISTINE BERNARDI

*E-mail address:* [bernardi@ann.jussieu.fr](mailto:bernardi@ann.jussieu.fr)

**5[65Mxx, 65C20, 65Dxx, 65-02, 76-xx]**—*Level set methods and dynamic implicit surfaces*, by Stanley Osher and Ron Fedkiw, Applied Mathematical Sciences, 153, Springer-Verlag, New York, 2003, xiii+273 pp., hardcover \$79.95, ISBN 0-387-95482-1

Level set methods have successfully been used for a wide range of applications since the pioneering paper of Osher and Sethian [1]. This book is an excellent introduction to the field, allowing newcomers to quickly grasp the key ideas. It also covers, in sufficient detail, the level set approach to several problems arising in image processing and computational physics. The book is broken up into four parts.

The first part introduces the idea of implicit surface representation. This is the key section for students and new researchers to the field. It covers the basic ideas of implicit surface representation, normal vectors, curvature, and signed distance functions. This is even a nice reference for researchers already familiar with level set methods.

The second part deals specifically with level set methods, namely the partial differential equations associated with motion of surfaces represented implicitly. The requisite numerical methods and several examples are also covered in this section. Again, this is extremely useful to newcomers to the field.

Applications from image processing and computer vision compose the third part of the book. Topics covered include image restoration, image segmentation, and reconstruction of surfaces given unstructured data points.

In the fourth part, the authors give an overview of hyperbolic conservation laws, before moving on to several applications in computational fluid dynamics. Specifically covered are level set methods for two-phase (compressible and incompressible) fluid flow, and level set approaches to treating discontinuities such as shocks, detonations, flames, and phase changes. Fluid-solid and liquid-gas interactions, free surface flow and heat flow methods using level set ideas are also presented.

There are many other applications of the level set method to image processing and computational physics (as of the date of this review, [1] has been cited nearly 1000 times), but these serve as good examples in the field. This book is suitable for researchers interested in modeling interface motion, and would be an excellent book for a graduate level course in mathematics/engineering/science.

#### REFERENCES

- [1] S. Osher and J. Sethian, *Fronts propagating with curvature-dependent speed: algorithms based on Hamilton-Jacobi formulations*, J. Comput. Phys. **79** (1988), 12-49.

TARIQ ASLAM

DX-2: DETONATION PHYSICS TEAM  
MAIL STOP P952  
LOS ALAMOS NATIONAL LABORATORY  
LOS ALAMOS, NEW MEXICO 87545  
E-mail address: aslam@lanl.gov

**6[41-02, 41A63, 41A30, 41A05, 65-02]**—*Radial basis functions: theory and implementations*, by M. D. Buhmann, Cambridge Monographs on Applied and

Computational Mathematics, 12, Cambridge University Press, Cambridge, 2003, x+259 pp., \$65.00, ISBN 0-521-63338-9

In many applications it is important to be able to approximate data depending on data with a large number of inputs and no particular structure. Examples include neural networks, partial differential equations, and terrain modelling. Methods such as piecewise polynomial approximation, which work well in low space dimension or on data sets with structure, become significantly less successful in higher space dimension. Radial basis function approximation has come to the fore in such applications because of its simple computational form and because, remarkably, the interpolation problem is solvable in arbitrarily high space dimension for a wide variety of basis functions with only mild conditions on the position of the data points.

There are a number of good survey papers in the literature [2, 3, 6] as well as an excellent introduction in the book by Cheney and Light [4]. However, the time is ripe for a book expounding the key principles in radial basis approximation. This is such a book. It is a carefully written work by one of the most influential researchers in the area. It concentrates on theoretical aspects of radial approximation, as this is where the main interest of the author lies. Constant reference is made, however, to important applications, and the point is made that a good understanding of the theory leads to wise choice of basis functions in particular applications.

This book is accessible to the reader who wishes to receive a grounding in radial basis approximation theory, and is certainly one that should be recommended to graduate students working in this area. It is also a useful reference for the active radial basis researcher. There is also a significant amount of information for those who have a general interest in approximation theory.

In the first chapter we are introduced to the approximating spaces  $S \subset \mathbf{C}(\mathbb{R}^d)$ , the continuous functions on  $\mathbb{R}^d$ ,  $d \geq 1$ . Given a (possibly infinite) set of points  $\Xi \in \mathbb{R}^d$ , and a univariate function  $\phi$ ,

$$S = \left\{ \sum_{\xi \in \Xi} \alpha_{\xi} \phi(|\cdot - \xi|) : \alpha_{\xi} \in \mathbb{R} \right\},$$

where  $|\cdot|$  denotes the Euclidean distance. Common choices of  $\phi(r)$  include  $r^2 \log r$ , the thin-plate spline;  $(r^2 + c^2)^{1/2}$ ,  $c > 0$  a parameter, the multiquadric;  $e^{-\beta r^2}$ ,  $\beta > 0$  a parameter, the Gaussian; a family of compactly supported functions. In some instances, depending on the particular choice of  $\phi$ , a low-dimensional polynomial subspace may also be added to  $S$ .

A key notion running through the theory and hence this book is that of *positive definiteness*, or, more generally, conditional positive definiteness. The function  $\phi$  is conditionally strictly positive definite if the quadratic form

$$\sum_{\xi, \eta \in \Xi} c_{\xi} c_{\eta} \phi(|\xi - \eta|) > 0,$$

for all  $c_{\xi}$ ,  $\xi \in \Xi$ , not all zero, which satisfy some polynomial annihilation condition. If this condition is empty, we say that  $\phi$  is strictly positive definite.

The author considers a number of different approximation methods, interpolation, quasi-interpolation, wavelets and least squares methods. Interpolation is the main approximation method considered in this book, and is explored both when  $\Xi$

is the scaled multi-integer grid  $h\mathbb{Z}^d$ ,  $h > 0$ , and when  $\Xi$  is a finite set of scattered points.

In the third chapter the special case of univariate multiquadric interpolation on the integer grid is considered as it provides the essence of the general case which is described in Chapter 4. Of course, the question of existence of interpolants is central here, and Fourier techniques are exploited to give affirmative answers to this question for a wide range of conditionally strictly positive definite basis functions.

In Chapter 5 the author looks at interpolation when  $\Xi$  is a finite set of scattered data points, the case which is most applicable to real world problems. Fourier transform technology is again used to show that the interpolation problem is solvable, under very mild restrictions, for conditionally strictly positive definite basis functions, and it is this guarantee of a unique interpolant that has made radial basis interpolation such an attractive proposition.

A variational theory underpins the analysis of convergence of radial basis interpolation, these interpolants being the minimal (semi)norm interpolants from some reproducing kernel Hilbert space. Thus, the radial basis approximations often satisfy some physical minimisation principle, making them excellent candidates for approximation in real application. The author does a fine job of elaborating the variational theory, and at the same time gives an excellent survey of the contributions of other authors in this area. A conclusion of the analysis is that radial basis functions provide optimal convergence orders in the appropriate setting, another point in their favour.

Even though radial basis interpolants exist and are good approximators, we still have to compute them. The interpolation equations are typically full and ill conditioned. Lower bounds on the 2-norm of the interpolation matrices are established at the end of the fifth chapter.

To solve the interpolation equations in a reasonable time, one needs to employ a preconditioned iterative method. A number of such methods now exist, and in Chapter 7 the author discusses the well-known Beatson, Faul, Goodsell, Powell algorithm, which may be viewed as a Krylov subspace method. An important part of this algorithm is a preconditioning step, involving the computation of almost Lagrange functions, which are 1 at a particular point, zero at a number of locally selected points, and (hopefully) small at all other data points.

Another key component of computation with radial basis functions is a fast evaluation scheme. Later in Chapter 7 the author describes a development, by Newsam and Beatson [1] of the multipole algorithm of Greengard and Rokhlin [5], tuned for the thin-plate spline. Fast evaluation for all of the commonly used radial basis functions is possible, making the complexity of computation of a radial basis interpolant at  $N$  data points of order  $N \log N$ .

Another way to avoid having to invert full and ill-conditioned linear systems is to use compactly supported radial basis functions. These are also very useful for the solution of partial differential equations. The main issue here is that such functions cannot be positive definite in all space dimensions, so the construction of such functions, and the space dimension in which they are positive definite, has received much recent interest. In Chapter 6 there is a very complete survey of the construction of such functions, and this would be a very good place for anyone to start if they wished to gain an understanding of this interesting area of radial basis function research.

There are also chapters on least squares approximation and the construction of wavelets.

I would recommend this book to anyone interested in learning about radial basis functions, most especially theoretical aspects. This is also a book for radial basis function practitioners who want a reference detailing the main theoretical approaches in radial approximation theory. It also contains a very good bibliography which points the reader to a large part of the important literature in this very important and growing area of modern approximation theory research.

## REFERENCES

- [1] R. K. Beatson and G. N. Newsam, *Fast evaluation of radial basis functions: I*, *Comput. Math. Appl.* **24** (1992), 7–19.
- [2] M. D. Buhmann, *Radial basis functions*, *Acta Numerica* **9** (2000), 1–37.
- [3] N. Dyn, “Interpolation and approximation by radial and related functions”, in *Approximation Theory VI. Vol. I*, C. K. Chui, L. L. Schumaker, and J. D. Ward (eds.), Academic Press, Boston, MA, 1989, pp. 211–234.
- [4] E. W. Cheney and W. A. Light, *A Course in Approximation Theory*, Brooks, Pacific Grove, California.
- [5] L. Greengard and V. Rokhlin, *A fast algorithm for particle simulations*, *J. Comput. Phys.* **73** (1987), 325–348.
- [6] M. J. D. Powell, “The theory of radial basis function approximation in 1990”, in *Advances in Numerical Analysis II: Wavelets, Subdivision Algorithms, and Radial Basis Functions*, W. A. Light (ed.), Oxford University Press, New York, 1992, pp. 105–210.

JEREMY LEVESLEY

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE  
LEICESTER UNIVERSITY  
LEICESTER, LE1 7RH, ENGLAND  
*E-mail address:* j11@mcs.le.ac.uk

**7[11K45, 11T71, 11Yxx, 68Q17, 94-02]**—*Cryptographic applications of analytic number theory*, by I. Shparlinski, *Progress in Computer Science and Applied Logic*, 22, Birkhäuser Verlag, Basel, 2003, viii+411 pp., \$109, ISBN 3-7643-6654-0

This is a greatly expanded and updated version of the author’s book *Number theoretic methods in cryptography* (Birkhäuser Verlag, Basel, 1999). As in the earlier book, the emphasis is on rigorous lower bounds on the complexity of cryptologic problems that are established by means of bounds for character sums and for the number of solutions of equations and congruences. The present book also uses sieve methods and lattice reduction algorithms as additional tools.

The first part of the book presents a detailed exposition of the background in algebra, number theory, and complexity theory that is needed for the book. Part II of the book basically follows the lines of the corresponding part of the earlier book and deals with the interpolation and approximation of the discrete logarithm in finite prime fields by polynomials over appropriate finite fields, the bitwise approximation of the discrete logarithm by Boolean functions, and analogous problems for the interpolation and approximation by real or complex polynomials. Part III on the Diffie-Hellman problem contains the corresponding material in the earlier book, but also a new chapter on the bit security of the Diffie-Hellman secret key.

The remaining parts of the book offer mostly new material. Part IV studies properties such as uniformity of distribution, high linear complexity, and bit security for various cryptographic schemes (RSA, XTR, LUC, NTRU, DSA, ElGamal). Part V on pseudorandom numbers contains results on period length, uniformity of distribution, and linear complexity for pseudorandom number generators such as the power generator, the  $1/M$  generator, the inversive congruential generator, and the subset sum generator. Part VI presents applications to some other algorithmic, cryptographic, and complexity-theoretic problems and, in particular, a proof of the beautiful result that for any nonlinear function modulo a prime either its arithmetic depth or its Boolean depth is large. The book concludes with a long list of open problems and a substantial bibliography.

This monograph is essential reading for anybody interested in the rigorous complexity analysis of cryptologic problems. The book is also a treasure trove of powerful technical tools that are bound to lead to further deep complexity results in the future.

H. NIEDERREITER

*E-mail address:* nied@math.nus.edu.sg

**8[94A60, 11T71, 11Y16]**—*RSA and public-key cryptography*, by R. A. Mollin, Discrete Mathematics and Its Applications, Chapman & Hall/CRC, Boca Raton, FL, 2002, xii+291 pp., \$79.95, ISBN 1-58488-338-3

This textbook is a welcome addition to the existing cryptographic literature. Instead of trying to produce a universal manual covering all possible (and impossible) aspects of cryptography, the author concentrates and provides an in-depth treatment of a single topic, the RSA cryptosystem. The matter is traced from its number theoretic roots up to practical protocols, which one can rarely find in more traditional cryptographic textbooks. It provides all the necessary preliminaries, such as primality testing and integer factorisation algorithms. Additionally, such practically important issues as timing and power attacks as well as small public exponent attacks are described. The last three chapters of the book give a treatment of several practical applications of RSA, including such very recently emerged applications as digital cash, electronic commerce, and WLAN (wireless local area network).

The book also contains a carefully selected set of exercises with solutions to the odd-numbered ones.

IGOR SHPARLINSKI

*E-mail address:* igor@comp.mq.edu.au