REVIEWS AND DESCRIPTIONS OF TABLES AND BOOKS

The numbers in brackets are assigned according to the American Mathematical Society classification scheme. The 1980 Mathematics Subject Classification (1985 Revision) can be found in the December index volumes of Mathematical Reviews.

13[45–02, 45L10, 65R20].—A. N. TIKHONOV & A. V. GONCHARSKY (Editors), *Ill-Posed Problems in the Natural Sciences*, Advances in Science and Technology in the USSR, Mathematics and Mechanics Series (translated from the Russian by M. Bloch), "Mir", Moscow, 1987, 344 pp., $21\frac{1}{2}$ cm. Price $9.95.

And now remains that we find
out the cause of this effect.
Shakespeare: HAMLET

The theory of numerical methods for integral equations of the first kind has been under vigorous development for a quarter of a century. Such equations provide the most natural mathematical expression for many inverse problems in science and technology. Although specific instances of inverse problems have been around for some time (studies of the temperature of the early earth by Fourier and Kelvin, and Bernoulli's investigation of the inhomogeneous vibrating string come to mind), an awareness of some of the common features and main difficulties of inverse problems has emerged remarkably slowly.

The reluctance to recognize the reality and significance of inverse problems is partially rooted in philosophy and history. For generations, mathematical physics was dominated by the Laplacian view that the business of natural philosophy is the precise determination of effects from causes which evolve continuously over time or space. The future-directed and outward-looking viewpoint was dominant. Thus in the "direct" problems of classical mathematical physics each cause leads to a unique effect which depends continuously on the cause. This Laplacian mindset led to Hadamard's extreme position that any realistic problem in mathematical physics must have a unique solution which depends continuously on the data of the problem. Hadamard called such problems correctly set. The term well-posed is now more common, and problems not in this class have come to be known, somewhat darkly, as ill-posed.

The demands of science and technology in recent decades have brought to the fore many problems which are inverse to the classical direct problems, that is, problems which may be interpreted as finding the cause of a given effect. Included among such problems are many questions in remote sensing or indirect measurement

0025-5718/89 $1.00 + $.25 per page

such as the determination of characteristics of an inaccessible region from measurements on its boundary, the determination of system parameters from input-output measurements, and the reconstruction of past events from measurements of the present state. In these problems the viewpoint is inward-looking or past-directed. Very often, in the direct problem the transition from cause to effect is accomplished by a compact integral operator and hence the associated inverse problem is ill-posed, as the inverse of a compact operator is unbounded. This ill-posedness raises serious questions about the computation and interpretation of approximate solutions, particularly since in practical circumstances the observed effects, as measured quantities, are inherently imprecise, and even small observational errors can be magnified greatly by the discontinuous solution operator. This discontinuity often becomes apparent very quickly in wild numerical instability which emerges when conventional numerical methods are used on ill-posed integral equations of the first kind.

A numerical method for ill-posed integral equations of the first kind, now known as regularization, which replaces the first-kind integral equation by an approximating well-posed equation of the second kind was first published by D. L. Phillips (1962). For the matrix case, Levenberg had earlier (1944) proposed a closely related idea, known as damped least squares, for solving a linearized version of a nonlinear least squares problem. However, it was a seminal paper of A. N. Tikhonov in 1963 that launched a rapid development of the theory of regularization for numerical solution of ill-posed problems by the Soviet school, led by Academician Tikhonov. Effective application of this method is a delicate balancing act that involves the choice of regularization parameters, smoothing norms, and approximating subspaces and the incorporation of a priori information about the solution.

The book under review is a collection of fifteen papers on the theory of regularization for ill-posed problems and the application of the method of regularization to the numerical solution of specific ill-posed inverse problems in the natural sciences. All of the papers are by Soviet mathematicians who are associated with Tikhonov's school. The first three papers are devoted to the mathematical theory of regularizing algorithms, including questions related to the solution of linear algebraic systems with approximate data, a survey of the general theory of regularizing algorithms in Hilbert spaces, and an article with a distinct topological flavor on the regularization of the computation of function values with approximately specified arguments. The remaining thirteen chapters all deal with specific inverse problems in the natural sciences. There are three papers on geophysical inverse problems, including problems in electrodynamic prospecting, seismology, gravimetry and magnetometry. Additional papers on inverse problems in plasma diagnostics, astro-physics, inverse scattering, medical tomography, and various problems in optics round out the volume. In each of these papers the physical background of the problem is examined, the main problem is cast as an integral or operator equation of the first kind, the implementation of the regularization method is discussed and the results of the numerical calculations are displayed, usually in graphical form.

In this book, leading Soviet experts provide hard-to-find information on an eclectic collection of ill-posed problems in the natural sciences. The unifying thread is the use of the regularization method to solve these problems numerically. The very low purchase price is a genuine incentive for those interested in inverse problems and numerical analysis to add this little book to their personal libraries.

C. W. GROETSCH

Department of Mathematical Sciences
University of Cincinnati
Cincinnati, Ohio 45221-0025

14[65–04, 65F05].—THOMAS F. COLEMAN & CHARLES VAN LOAN, *Handbook for Matrix Computations*, Frontiers in Applied Mathematics, Vol. 4, SIAM, Philadelphia, PA, 1988, vii+264 pp., 23 cm. Price: Softcover $24.00.

No course in numerical linear algebra is complete without laboratory assignments. There are three good reasons for this. First, the coding of efficient matrix algorithms cannot be learned in an armchair; one must actually write programs. Second, students who have not made computer runs generally believe that rounding errors are like cooties—only other people get them. Finally, this is one of the few courses where the instructor can insist on cleanly coded, well-documented programs that would be suitable for distribution in a computation center.

Unfortunately, it is not enough to give a student an assignment and a due date. Even if the student already knows a programming language, there are tricks to making it do matrix computations efficiently. Students should be encouraged to use the Basic Linear Algebra Subprograms, which, however, have complicated calling sequences with forbidding parameters. The calling sequences for the standard matrix packages, LINPACK and EISPACK, are even worse. Finally, if the instructor decides to use an interactive package, the student must learn what is essentially a new language. Helping the student master these details can eat heavily into time better spent deriving and analyzing algorithms.

The authors of this handbook have circumvented these problems by providing their students with a small book that sets out the details in concise form. It is assumed that the reader has been exposed to a high-level programming language and has had one semester of linear algebra. The book consists of four chapters. The first is an introduction to FORTRAN. The second leads the reader through the Basic Linear Algebra Subprograms (BLAS) for performing vector operations. The third is an introduction to LINPACK, a collection of subroutines for computing and applying matrix decompositions. The last chapter is an introduction to MATLAB, an interactive system for manipulating matrices. Interesting exercises are interspersed throughout the book. Let us look at each chapter in turn.

Although they are not dogmatic about it—they make a gracious nod toward the language C—the authors have chosen FORTRAN as the language of their handbook. This makes sense. Not only is most scientific computation done in FORTRAN, but FORTRAN is the language in which the best matrix packages are coded. The chapter contains a detailed description of how arrays are arranged in memory and how they appear to subroutines. This material, which is of paramount importance in matrix computations, is slighted in most treatments of FORTRAN.

The section on programming tips is well thought out. People coming from richer languages will especially appreciate the hints for implementing constructions such as **while** loops in FORTRAN.

The BLAS are a collection of FORTRAN subprograms to perform vector operations, e.g., inner products or the addition of the multiple of one vector to another. Their power lies in the fact that the "vector" can be a column or row of an array. Thus they provide a way of coding matrix algorithms at the vector rather than the scalar level. Here the BLAS are introduced in stages, with examples illustrating their use. This chapter could have been better coordinated with the previous chapter. For example, there is no reference back to the material on arrays; the reader is left to figure out on his own how the BLAS get inside a matrix. Again, in the section on programming tips the authors stress the need to avoid overflows by scaling. Then they proceed to ignore their own good advice in Example 2.2-1.

LINPACK is a collection of FORTRAN subroutines to perform various matrix computations, all loosely associated with linear systems or linear least squares. The package follows the modern trend in numerical linear algebra by first computing a matrix decomposition, which then is used as a platform for solving a number of problems. The authors are particularly good at leading the reader through the complicated calling sequences for the subroutines. However, the chapter is flawed in two ways. First, no summary is provided at the end of the chapter, so that the experienced user who merely wants to be reminded of the calling sequences finds himself forever thumbing between the index and the text. Second, the authors drop the reader *in medias res.* A couple of pages explaining the philosophy and organization of LINPACK and defining the decompositions it uses—they are not likely to be treated in the prerequisite semester of linear algebra—would make this section much more comprehensible to the novice.

MATLAB is a system for manipulating matrices at a high level. For example to solve the least squares problem of minimizing $\|b - Ax\|^2$, where $\|\cdot\|$ is the Euclidean norm, one simply enters

$$x = A\backslash b.$$

With this much power at their fingertips, students of numerical linear algebra can experiment in a way that would have been impossible less than a decade ago. The introduction to MATLAB given here is very clean; in fact, I prefer it to MATLAB's own documentation. The one important omission is the indispensible **save** and **load** commands, which allow the user to walk away from a session and later pick up where he left off.

Another omission, which is much more serious, is that of a chapter on the EISPACK routines for eigenvalue calculations. The failure to treat this very important aspect of matrix computations detracts greatly from the value of the book.

Nonetheless, it *is* a valuable book. As a reference work it is conveniently bound and attractively formatted, and for everyday work, exclusive of occasional fine points, it replaces at least three bulkier manuals. It is also a useful supplement to a course on numerical linear algebra. However, some polishing would make it more accessible to the tyro, and I hope the authors will undertake the job in revision.

G. W. S.

15[90–02].—FERENC FORGÓ, *Nonconvex Programming*, Akadémiai Kiadó, Budapest, 1988, 188 pp., $24\frac{1}{2}$ cm. Price $24.00.

The general field of finite-dimensional optimization has largely been cultivated in areas concerned with linear, integer, and convex problems, although there are also major subfields associated with stochastic, dynamic, and nondifferentiable problems.

The term "Nonconvex Programming" is generally meant to apply to optimization problems dealing with a continuous objective function and a closed constraint region (often described by continuous functions, especially linear). Such problems have traditionally been treated by algorithms developed for convex problems, often started from several different points with the hope that one will lead to a true global optimum.

There has, however, been a significant amount of work done in the last 15–20 years in the development of methods which specifically apply to problems which have proper local solutions but whose global solution is required. This book is the first to attempt a broad and extensive summary of the various aspects of those algorithms which *guarantee* to produce such global optimizers.

Integer problems, methods based on random search and unconstrained global optimization algorithms are not covered.

Chapter 1 is an especially well-written summary of the basic results of convex optimization, and Chapter 2 is devoted to the geometric notions of convex hulls and envelopes. The three basic approaches to nonconvex programming are enumeration (direct and implicit), branch and bound, and cutting plane methods. These are summarized in Chapter 3.

One of the oldest and most studied of the nonconvex problems is that of maximizing a convex function over a polytope, and there are probably a dozen distinct algorithms that have been proposed for its solution. Some of the earlier of these are detailed in Chapter 4, while Chapter 5 discusses the basic ideas involved in treating problems whose constraint region is described (at least in part) by "reverse convex constraints", i.e., inequality constraints involving convex functions which are not to be smaller than a given constant.

Chapters 6 and 7 address methods for the largest set of nonconvex problems, including the separable and quadratic varieties. The important Fixed Charge Problem is treated in Chapter 8, while the concluding part of the book collects some isolated topics such as closed form solutions and decomposition.

While there are (understandably) a number of important topics not covered, and while there are virtually no insights into the computational efficiencies of the algorithms, this book is remarkable for the sheer extent of the items covered, and the skill with which the author covers them. The list of 113 references is also outstanding.

JAMES E. FALK

Department of Operations Research
George Washington University
Washington, D. C. 20052

16[26–02, 26D15, 26B25].—P. S. BULLEN, D. S. MITRINOVIĆ & P. M. VASIĆ, *Means and Their Inequalities*, Mathematics and Its Applications (East European Series), Kluwer, Dordrecht, 1988, xix + 459 pp., $24\frac{1}{2}$ cm. Price $89.00.

A mean of the positive values $a_1, \ldots, a_n$ is a function $F(a_1, \ldots, a_n)$ whose value lies between the smallest and largest of its arguments. Weighted means depend also on positive weights $w_1, \ldots, w_n$ with $\sum w_i = 1$. By far the most important means are the arithmetic and geometric means, $\sum w_i a_i$ and $\prod a_i^{w_i}$. These two, together with the harmonic mean $(\sum w_i a_i^{-1})^{-1}$, occupy nearly a quarter of the book under review. It is a very comprehensive survey of nearly everything that has been published on mean values, as illustrated by 52 proofs of the fundamental inequality stating that the geometric mean does not exceed the arithmetic mean. The bibliography fills 63 pages and contains approximately a thousand entries, clear evidence that the current revision of the Mathematics Subject Classification needs a better pigeonhole for means than the 1985 version provides.

Almost another quarter of the book is occupied by the power mean $(\sum w_i a_i^r)^{1/r}$, which includes the geometric mean when $r \to 0$ as well as the arithmetic and harmonic means. Its increase with r generalizes the inequality of arithmetic and geometric means, and its other properties include the inequalities of Cauchy, Hölder, and Minkowski. While the power mean is homogeneous in $a_1, \ldots, a_n$, a further generalization called the quasi-arithmetic mean, $\phi^{-1}[\sum w_i \phi(a_i)]$ with ϕ continuous and strictly monotonic, is not homogeneous unless $\phi(x)$ is a linear function of x^r or $\log x$. Other main topics are symmetric means like $[(a_1a_2 + a_1a_3 + a_2a_3)/3]^{1/2}$, means constructed in various esoteric ways, iterated means like Gauss's arithmetic-geometric mean, and finally integral means of functions. Means of operators are mentioned but not discussed. There is a list of notations and symbols and an index of authors but no subject index.

For anyone doing research on mean values or looking for an inequality between means, the book is a splendid reference work in spite of many misprints, a photographically reduced typescript with small characters, and the absence of boldface or large headings that would make it easier to navigate. One or more proofs of nearly every theorem are given expertly in a consistent notation with careful attention to conditions of equality. Above all, the reader will find many references to published papers that he would be very unlikely to discover otherwise. Because applications to other branches of mathematics are rarely mentioned, he may get the impression that inequalities for mean values have become a somewhat ingrown field of research without a strong sense of future directions. This impression will perhaps be proved incorrect by a complementary volume of applications, comments, and further results, now being prepared by the senior author (D.S.M.) and two collaborators.

B. C. C.

17[65–06, 65D30, 65D32].—H. BRASS & G. H. HÄMMERLIN (Editors), *Numerical Integration III*, International Series of Numerical Mathematics, Vol. 85, Birkhäuser, Basel, 1988, xiv + 325 pp., 24 cm. Price $60.50.

These are the proceedings of the third conference on numerical integration held at the Oberwolfach Mathematics Research Institute November 8–14, 1987. (The proceedings of the 1978 and 1981 conferences were published in Volumes 45 and 57 of the same series.) There are 28 papers, about three quarters of which deal with one-dimensional integration. The great variety of topics addressed during this conference can be gathered from the following list of key words: Computation of convolution integrals, Stieltjes integrals, and principal value integrals; Gauss and Chebyshev type quadrature rules; optimal quadrature; product integration; positivity of interpolatory rules; error estimation and convergence acceleration; theorems of Bernstein-Jackson type; cubature formulae with minimal or almost minimal number of knots; criteria for constructing multidimensional integration rules; quasi-Monte Carlo methods; lattice rules. The volume concludes with a traditional section on open problems.

W. G.

18[11A41, 11Y05, 11Y11].—HIDEO WADA, *Computers and Prime Factorization* (Japanese), Yūsei Publishers, Tōkyō, 1987, 190 pp., 21 cm. Price Yen 1800.

Most methods of obtaining the prime factorization of a given natural number have two steps. In the first step one decides whether the integer is prime or composite. In the second step one finds a nontrivial factor of the integer, if it is composite. The complete prime factorization is produced by performing the two steps recursively while composite factors remain. This book is an introduction to modern algorithms for these two steps.

To decide whether a large integer n is prime or not, one often checks whether it satisfies the conclusion of Fermat's Little Theorem, $b^{n-1} \equiv 1 \pmod{n}$, for some b. If this congruence fails and n is relatively prime to b, then n is definitely composite and we try to factor it. If the congruence holds, then n is almost certain to be prime and we use a *prime-proving algorithm* to show rigorously that n is prime. Rigorous tests for primeness are still much slower than probabilistic ones.

The book begins with some preliminaries from elementary number theory: Euclid's algorithm, congruences and Euler's totient function. The first algorithm after Euclid's is trial division, the only algorithm which factors and proves primality as well (for small integers). The next algorithm, fast modular exponentiation, is used for a simple prime-proving algorithm based on the converse of Fermat's Little Theorem: If $n-1 = p_1^{e_1} \cdots p_r^{e_r} \cdot m$, where $m < \sqrt{n}$, and if for each i in $1 \le i \le r$ there exists an a_i for which $a_i^{n-1} \equiv 1 \pmod{n}$ but $\gcd(a_i^{(n-1)/p_i} - 1, n) = 1$, then n is prime. Fast exponentiation is also a component of Pollard's two-step $p-1$ factoring algorithm. His Monte Carlo factoring algorithm and the $p+1$ factoring algorithm are presented here, too.

After stating the quadratic reciprocity law, the author tells how to solve quadratic congruences quickly in many cases. This ability is needed for initializing the quadratic sieve factoring algorithm. A later chapter gives details of the multiple-polynomial quadratic sieve algorithm from Silverman [5]. Quadratic reciprocity is used also to derive the tests of Pépin and Lucas for the primality of Fermat and Mersenne numbers, respectively.

The theory of continued fractions of quadratic surds is applied to solving Pell's equation and to factoring integers by the continued fraction method of Morrison and Brillhart. We learn also how to express a prime as a sum of two or four squares.

The beautiful elliptic curve factoring algorithm of H. W. Lenstra, Jr. is described, beginning from the addition formula for the Jacobian elliptic function $\operatorname{sn} x$. The book offers a taste of the fast prime-proving algorithm of Adleman and Rumely. Gauss sums are discussed in this connection, following the treatment in Cohen and Lenstra [1].

A short chapter describes codes, ciphers and the Rivest-Shamir-Adleman public key cryptosystem.

Algorithms are given for extended-precision integer arithmetic, including fast multiplication by the FFT and the Strassen-Schönhage method. At the end of the book, C programs are provided for multiprecise arithmetic and for all algorithms which were described fully earlier in the text. Although the programs have no comments, they are explained carefully.

This book is a fine introduction to the subject for a beginner. It covers a lot of ground in 190 pages. It contains the first treatment of the elliptic curve factoring algorithm in a book and only the second treatment (after that in Riesel [4]) of the Adleman-Rumely primality test. The book takes a practical approach to the subject. It is intended for those who would write fast computer programs to factor and test primality. It does not say much about methods whose interest is only theoretical, such as Dixon's factoring algorithm [2] or Miller's primality test [3] which depends on the Riemann Hypothesis.

S. S. WAGSTAFF, JR.

Department of Computer Sciences
Purdue University
West Lafayette, Indiana 47907

1. H. COHEN & H. W. LENSTRA, JR., "Primality testing and Jacobi sums," *Math. Comp.*, v. 42, 1984, pp. 297–330.

2. JOHN D. DIXON, "Asymptotically fast factorization of integers," *Math. Comp.*, v. 36, 1981, pp. 255–260.

3. GARY MILLER, "Riemann's hypothesis and tests for primality," *J. Comput. System Sci.*, v. 13, 1976, pp. 300–317.

4. HANS RIESEL, *Prime Numbers and Computer Methods for Factorization*, Birkhäuser, Boston, 1985. (Review **3**, *Math. Comp.*, v. 48, 1987, pp. 439–440.)

5. ROBERT D. SILVERMAN, "The multiple polynomial quadratic sieve," *Math. Comp.*, v. 48, 1987, pp. 329–339.

19[11–06, 11B37, 11B39].—A. N. PHILIPPOU, A. F. HORADAM & G. E. BERGUM (Editors), *Applications of Fibonacci Numbers*, Kluwer, Dordrecht, 1988, xx + 213 pp., $24\frac{1}{2}$ cm. Price \$79.00/Dfl.145.00.

This book contains nineteen full length papers from among the twenty-five papers presented at the Second International Conference on Fibonacci Numbers and Their Applications held at San Jose State University, San Jose, California, U.S.A., August 13–16, 1986. While the underlying theme of this conference is the theory and application of linear recurring sequences, the contents of these proceedings are quite varied. Some indication of this diversity is afforded by the following sample of titles: Recurrences Related to the Bessel Functions, Primitive Divisors of Lucas Functions, Fibonacci Numbers and Groups, Asveld's Polynomials $p_j(N)$, Covering the Integers with Linear Recurrences.

H. C. W.