11. ______, *The quadratic sieve factoring algorithm*, Advances in Cryptology (T. Beth, N. Cot and I. Ingemarsson, eds.), Springer Lecture Notes in Computer Science **209** (1985), 169–182.

12. ______, *Fast, rigorous factorization and discrete logarithm algorithms*, Discrete Algorithms and Complexity (D. S. Johnson, T. Nishizeki, A. Nozaki and H. S. Wilf, eds.), Academic Press, Orlando, Florida, 1987, pp. 119–143.

13. M. O. Rabin, *Probabilistic algorithms for testing primality*, J. Number Theory **12** (1980), 128–138.

14. J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64–94.

15. R. J. Schoof, *Elliptic curves over finite fields and the computation of square roots* mod p, Math. Comp. **44** (1985), 483–494.

16. R. Solovay and V. Strassen, *A fast Monte-Carlo test for primality*, SIAM J. Comput. **6** (1977), 84–85; erratum, ibid. **7** (1978), 118.

17. V. Strassen, *Einige Resultate über Berechnungskomplexität*, Jahresber. Deutsch. Math.-Verein **78** (1976/77), 1–8.

Carl Pomerance

BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 18, Number 1, January 1988
©1988 American Mathematical Society
0273-0979/88 $1.00 + $.25 per page

Monotone iterative techniques for nonlinear differential equations, by G. S. Ladde, V. Lakshmikantham, and A. S. Vatsala, Pitman Publishing Company, Boston, London, Melbourne, 1985, x + 236 pp., $110.00. ISBN 0-273-08707-X

The monotone method and its associated upper-lower solutions for nonlinear partial differential equations have been given extensive attention in recent years. The method is popular because not only does it give constructive proof for existence theorems but it also leads to various comparison results which are effective tools for the study of qualitative properties of solutions. The monotone behavior of the sequence of iterations is also useful in the treatment of numerical solutions of various boundary value and initial boundary value problems. Recognizing its immense value to nonlinear problems, the authors repeatedly apply the monotone method and the idea of upper-lower solutions to various first- and second-order partial differential equations. To illustrate the basic idea of the monotone method, let us consider a typical elliptic boundary value problem in the form

$$-L[u] = f(x,u) \text{ in } \Omega, \qquad B[u] = h(x) \text{ on } \partial\Omega,$$

where L is a uniformly elliptic operator in a bounded domain Ω and B is a linear boundary operator on $\partial\Omega$. Suppose there exists an ordered pair of upper and lower solutions v and w, that is, v and w are smooth functions with $v \geqslant w$ such that

$$-L[v] \geqslant f(x,v) \text{ in } \Omega, \qquad B[v] \geqslant h(x) \text{ on } \partial\Omega,$$

and w satisfies the reversed inequalities. Then by using v and w as two distinct initial iterations one can construct two sequences $\{v_k\}$ andn $\{w_k\}$ from the iteration process

$$\begin{aligned} -L[u_k] + cu_k &= cu_{k-1} + f(x, u_{k-1}) && \text{in } \Omega, \\ B[u_k] &= h(x) && \text{on } \partial\Omega. \end{aligned}$$

The function $c \equiv c(x)$ is taken as any upper bound of $(-\partial f/\partial u)$ for $v \geqslant u \geqslant w$. Based on the property of upper and lower solutions, one establishes that the sequence $\{v_k\}$ is monotone nonincreasing and the sequence $\{w_k\}$ is monotone nondecreasing, and both sequences converge to a solution (say $\bar{u}$ and $\underline{u}$, respectively) of the problem. The monotone property of these sequences leads to the relation

$$w \leqslant w_k \leqslant w_{k+1} \leqslant \underline{u} \leqslant \bar{u} \leqslant v_{k+1} \leqslant v_k \leqslant v \quad \text{in } \bar{\Omega}$$

for every k. When $\bar{u} = \underline{u}$, there is a unique solution in the sector $\langle w, v\rangle$ between w and v; otherwise the problem has multiple solutions.

The above technique has been repeatedly used in the book for the treatment of other types of differential equations and boundary conditions. This includes the three basic types of second-order elliptic, parabolic, and hyperbolic equations where the function f depends on u as well as on ∇u, the gradient of u. It also covers a class of first-order equations and periodic boundary conditions. A major advance of this technique is the extension of the idea of upper-lower solutions to coupled systems of a finite number of parabolic and elliptic equations. For coupled systems of equations, whether parabolic or elliptic, the definition of upper-lower solutions depends on the quasimonotone property of the "reaction function" f in the system, and is often coupled. When an ordered pair of coupled upper-lower solutions v, w exists, the Leray-Schauder theory can be used to prove the existence of a solution in the sector $\langle w, v\rangle$. Based on the quasimonotone property of the reaction function one can also construct two sequences which are monotone. Although these two sequences converge to some limits $\bar{u}$ and $\underline{u}$, it is not certain that $\bar{u}$ or $\underline{u}$ is a solution of the problem except in the very special case where every component of the vector function f is quasimonotone nondecreasing. For a parabolic system of two equations where f is not dependent on the gradient of u these two limits coincide and their common value is the unique solution. An unanswered question is whether the same is true for the general system, especially when the problem involves a system of elliptic equations. For this reason the authors refer to $\bar{u}$ and $\underline{u}$ as a "quasi-solution", distinguishing them from a true solution. It is interesting and important to know whether a quasi-solution is (or is not) a true solution without severe restrictions. To the knowledge of this reviewer this is still an open problem.

The book is divided into five chapters. The first two chapters are devoted to two-point boundary value problems, in both the scalar case and the case of a finite system. In each case the existence problem is examined using the method of upper-lower solutions and monotone iterations. Periodic and terminal boundary conditions are included in the discussion. Chapter 3 is concerned with elliptic equations, and Chapter 4 with parabolic equations. A major part of these two chapters is devoted to the existence problem for systems where the nonlinear reaction function depends on u as well as on ∇u. These two chapters cover the main theme of the book and they deserve special attention. The final chapter treats the hyperbolic equation of first order. Here the method of upper-lower solutions is shown to be useful for the construction of a Lyapunov function. The book is self-contained, with an appendix giving most of the necessary material from the theory of linear partial differential equations. The bibliography is extensive, and it leads the reader to various references for more detailed discussions on related subjects.

Although there are some minor points which need more explanation or clarification, the book is well written and is a much needed and timely addition to the current literature, especially in the area of nonlinear reaction-diffusion systems. Despite the distinct characteristics among second-order elliptic, parabolic and hyperbolic equations, the authors have successfully established a unified approach and cast these problems into the same framework of monotone technique. This book may well stimulate further research in other areas of differential and integral equations and related fields. In fact, the monotone method and its associated upper and lower solutions have already been used for the treatment of numerical solutions of nonlinear parabolic and elliptic equations. It is likely that both the analytical techniques and the numerical schemes will receive even greater attention in various applied sciences.

C. V. Pao

BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 18, Number 1, January 1988
©1988 American Mathematical Society
0273-0979/88 $1.00 + $.25 per page

K-theory for operator algebras, by Bruce Blackadar, Mathematical Sciences Research Institute Publications, vol. 5, Springer-Verlag, New York, Berlin, Heidelberg, London, Paris, Tokyo, 1986, 338 pp., $28.00. ISBN 0-387-96391-x

The development of K-theory has been one of the great unifying forces in mathematics during the past thirty years, bringing together ideas from geometry, algebra, and operator theory in fruitful and often unexpected ways, and stimulating each of these subjects through the importation of insights and techniques from other areas.

It is commonly agreed that K-theory originated with the work of Grothendieck in the late 1950s in which he proved a generalized Riemann-Roch