Strengths of the book include the demystification of some components of REDUCE as well as its implementation in LISP, and pointers to research papers and books with further details.

This text is recommended for serious REDUCE users as well as for the casual REDUCE user interested in learning more about the system.

RICHARD J. FATEMAN

Computer Science Division, EECS Dept.
University of California
Berkeley, CA 94720

31[65-06, 68-06].—ROBERT E. O'MALLEY, JR. (Editor), *ICIAM* 91: *Proceedings of the Second International Conference on Industrial and Applied Mathematics*, SIAM, Philadelphia, PA, 1992, xviii+391 pp., 26 cm. Price $61.50.

The conference in the title, sponsored internationally by 12 societies of Applied, Industrial and Computational Mathematics, was held July 8–12, 1991, in Washington, D.C. Part I of the proceedings contains the text of 17 invited presentations, Part II an account of over 160 minisymposia organized in 29 chapters according to subject areas.

The authors and titles of the invited papers in Part I are: J. M. Ball, Dynamic energy minimization and phase transformations in solids; G. I. Barenblatt, Intermediate asymptotics in micromechanics; M. Brady, Computer vision: mathematics and computing; R. Coifman, Y. Meyer & V. Wickerhauser, Adapted wave form analysis, wavelet-packets and applications; A. R. Conn, N. Gould & Ph. L. Toint, Large-scale nonlinear constrained optimization; C. N. Dawson & M. F. Wheeler, Time-splitting methods for advection-diffusion-reaction equations arising in contaminant transport; W. Eckhaus, On modulation equations of the Ginzburg-Landau type; A Fasano, Modelling the solidification of polymers: an example of an ECMI cooperation; M. Grötschel, Discrete mathematics in manufacturing; F. L. Chalot & T. J. R. Hughes, Analysis of hypersonic flows in thermochemical equilibrium by application of the Galerkin/least-squares formulation; N. Karmarkar, Interior-point methods in optimization; P. L. Lions, Viscosity solutions and optimal control; M. Mimura, Dynamics of patterns, waves, and interfaces from the reaction-diffusion aspect; J. D. Murray, Complex pattern formation in embryology: models, mathematics, and biological implications; G. Ruget, Trends in radar architectures; D. J. Wallace, Massively parallel computing: status and prospects; H. Yserentant, Hierarchical bases.

A useful feature in Part II is a list of suggested reading appended to each chapter.

The volume, which is attractively sprinkled with photographs of speakers and participants, ends with an author index and a list of attendees.

W. G.

32[65C10, 68Q15, 94A60].—NOAM NISAN, *Using Hard Problems to Create Pseudorandom Generators*, An ACM Distinguished Dissertation 1990, The MIT Press, Cambridge, MA, 1992, x+43 pp., $23\frac{1}{2}$ cm. Price $20.00.

This book is a slightly revised version of the author's doctoral dissertation written under the supervision of R. Karp at Berkeley. It deals with pseudoran-

dom bit generation for cryptographic purposes in the sense of A. Yao, M. Blum, and S. Micali, that is, the problem of finding functions which stretch a short string of truly random bits into a long string of bits which looks random to observers having limited computational power. This problem is closely linked with issues of computational complexity. The author presents two different constructions of pseudorandom bit generators that relate to given complexity classes. The first construction is of a general type and produces bit strings that look random to any algorithm from a complexity class C using an arbitrary function that is hard for C. In particular, using the known lower bounds for constant-depth circuits, this construction yields unconditionally proven pseudorandom bit generators for constant-depth circuits. The second construction, which does not rely on any unproven hypothesis, produces bit strings that look random to all Logspace machines.

H. N.

33[65C05, 65D32].—NANCY FLOURNOY & ROBERT K. TSUTAKAWA (Editors), *Statistical Multiple Integration*, Contemporary Mathematics, Vol. 115, American Mathematical Society, Providence, RI, 1991, xii+276 pp., $25\frac{1}{2}$ cm. Price $71.00.

This collection of articles arose from the AMS–IMS–SIAM Joint Summer Research Conference on Statistical Multiple Integration which was held at Humboldt University, Arcata, California, in 1989. The emphasis in these papers is on Monte Carlo methods and analytic approximation methods. Articles of particular interest for numerical analysts are those by D. K. Kahaner on existing software for multidimensional numerical integration, by A. Genz on subregion adaptive algorithms, by M. Mascagni on the implementation of algorithms for high-dimensional numerical integration on massively parallel computers, and by M.-S. Oh on importance sampling.

H. N.

34[11–06, 11B37, 11B39].—G. E. BERGUM, A. N. PHILIPPOU & A. F. HORADAM (Editors), *Applications of Fibonacci Numbers*, Vol. 4, Kluwer, Dordrecht, 1991, xxiv+313 pp., $24\frac{1}{2}$ cm. Price $99.00/Dfl.180.

This book consists of thirty-three papers from among the thirty-eight papers presented at the Fourth International Conference on Fibonacci Numbers and their Applications held at Wake Forest University, Winston-Salem, NC from July 30–August 3, 1990. The theme of these Conferences is wider than that suggested by their title; in fact, they are devoted to the theory and application of linear recurring sequences in general. The papers are very diverse, discussing the occurrence of these sequences in such settings as: algebra, combinatorics, graph theory, geometry, number theory, probability, and even electronics.

H. C. W.