Information, communication, circuits

semigroup theory, abstract differential equations in linear spaces, integral equations and interpolation theory. Existence of optimal controls is established for arbitrary control sets by means of a general theory of relaxed controls.

Giorgio PICCI, David S. GILLIAM, (Editors). — **Dynamical systems, control, coding computer vision: new trends, interfaces, and interplay.** — Progress in systems and control theory, vol. 25. — Un vol. relié, 16×24, de VI, 493 p. — ISBN 3-7643-6060-7. — Prix: SFr. 168.00. — Birkhäuser, Basel, 1999.

This volume contains expanded versions of talks delivered by leading experts at the Mathematical Theory of Networks and Systems Symposium (MTNS 98) in Padova, Italy, in July 1998. Systems, control, and network theory have permeated the development of much of present-day technology. The theory has developed from the early phase of its history when the basic tools were elementary complex analysis, Laplace transform, and linear differential equations, to the present day, where the mathematics ranges widely from functional analysis, PDEs, abstract algebra, stochastic processes and differential geometry. This book is a collection of essays devoted in part to the growing interaction of these disciplines with coding, computer vision, and hybrid systems.

Martin SCHECHTER. — **Linking methods in critical point theory.** — Un vol. relié, 16,5×24,5, de XVI, 294 p. — ISBN 0-8176-4095-9. — Prix: SFr. 98.00. — Birkhäuser, Boston, 1999.

Many non-linear problems in the physical and social sciences can be reduced to finding critical points (minima, maxima, and minimax points) of functionals (real-valued functions on various spaces). Much of the activity in the calculus of variations is devoted to finding such points, although a more difficult problem is finding critical points that are neither maxima nor minima. Until recently there was no organized procedure for producing such points. In this work, Schechter briefly reviews the issue of critical points from the old "linking" viewpoint and then studies the theory in light of a new concept of "linking subsets" which he helped introduce. New theorems are proved and applied to the solution of subcritical problems on bounded domains.

Ian S. SHAW. — **Fuzzy control of industrial systems: theory and applications.** — Un vol. relié, 16,5×24,5, de XXIII, 192 p. — ISBN 0-7923-8249-8. — Prix: Dfl. 260.00. — Kluwer Academic Publishers, Dordrecht, 1998.

This volume has been planned as an introductory textbook on intelligent control systems such as fuzzy logic and neurofuzzy systems. The objective was to create a linkage between an undergraduate text and a practical guide for experienced engineers wishing to upgrade their knowledge. To this end, both theoretical as well as practical design aspects are presented. Included are generic aspects of fuzzy systems with an emphasis on the many degrees of freedom and its practical design implications, modeling and systems identification techniques based on fuzzy rules, parametrized rules and relational equations... etc.

Information, communication, circuits

Ian F. BLAKE, Gadiel SEROUSSI & Nigel P. SMART. — **Elliptic curves in cryptography.** — London Mathematical Society lecture note series, vol. 265. — Un vol. broché, 15×23, de XV, 204 p. — ISBN 0-521-65374-6. — Prix: £24.95. — Cambridge University Press, Cambridge, 1999.

In the past few years elliptic curve cryptography has moved from a fringe activity to a major challenger to the dominant RSA/DSA systems. Elliptic curves offer major advances on older

systems such as increased speed, less memory and smaller key sizes. As digital signatures become more and more important in the commercial world the use of elliptic-curve-based signatures will become all pervasive. This book summarizes knowledge built up within Hewlett-Packard over a numbers of years, and explains the mathematics behind practical implementations of elliptic curve systems.

S.C. COUTINHO. — **The mathematics of ciphers: number theory and RSA cryptography.** — Un vol. relié, 16×24, de XV, 196 p. — ISBN 1-56881-082-2. — Prix: US$30.00. — A.K. Peters, Natick, Massachusetts, 1999.

Revised and updated since its publication in Portuguese in 1997, this highly accessible book is an introduction to the algorithmic aspects of number theory and its applications to cryptography. Accompanied by historical anecdotes, the familiar topics of number theory are defined and explored. The author takes the reader on a leisurely journey through this fascinating field, culminating in a visit to the RSA cryptosystem, the best known and one of the most widely used public key cryptosystems invented in 1978.