polynomial codes," *IEEE Trans. Inform. Theory*, vol. IT-17, May 1971, pp. 322–331.

[7] L. D. Rudolph, "Geometric configuration and majority-logic decodable codes," M.E.E. thesis, Univ. Oklahoma, Norman, 1964.

[8] B. Elspas, "The theory of autonomous linear sequential networks," *IRE Trans. Circuit Theory*, vol. CT-6, Mar. 1959, pp. 45–60.

[9] C. L. Chen, "Computer results on the minimum distance of some binary cyclic codes," *IEEE Trans. Inform. Theory* (Corresp.), vol. IT-16, May 1970, pp. 359–360.

[10] N. Q. Duc and L. V. Skattebol, "Algorithms for majority-logic check equations of maximal-length codes," *Electron. Lett.*, vol. 5, Nov. 1969, pp. 577–579.

[11] E. R. Berlekamp, *Algebraic Coding Theory*. New York: McGraw-Hill, 1968.

Book Review

An Introduction to Error-Correcting Codes—Shu Lin (Englewood Cliffs, N.J.: Prentice-Hall, 1970, 330 pp., $12.95).

There has long been a communication gap between coding theorists and practicing communication engineers. Thus one can only welcome this book by Prof. Shu Lin of the Hawaiian coding coterie, which marks the first serious effort to heal this breach. Our view is that Lin has succeeded as much as is possible at this time. Communication engineers will be disappointed that this book is of little help in choosing the right code for a particular application; the choice of a code depends upon so many factors that it will remain an art for some time to come. Coding theorists will decry Lin's omission of the elegant algebraic theory that has given coding its great aesthetic appeal. Yet the fact remains that the reader who wishes to acquire a working knowledge of the most practical coding schemes, but who has a minimal background in algebra, will find this book his best source.

In the preface the author states his penchant for "clarity of exposition," and he serves the reader well in this regard. At times, indeed, clarity is carried to absurdity with attempts to explain the unexplainable—as in Fig. 10.1 entitled "A general convolutional encoder," which shows only a box labelled "Convolutional Encoder." We defer further general comments on the text until after our chapter-by-chapter discussion.

The first chapter is a brief but adequate discussion of the communications problem and the place of coding therein. At one point, the author achieves something of an information-theory first (crediting too much to Shannon!) by citing Shannon as the source for the *exponential* decrease of error probability with code constraint length.

In Chapter 2 the author compresses into 20 pages enough algebra, largely without proofs, so that the reader can learn to do calculations in the finite field $GF(2^m)$. In an unfortunate oversight, he neglected to point out on page 15 that the polynomial $p(X)$ used as a modulus must be irreducible, but the remainder of the treatment is excellent. It is especially pleasant to see the emphasis on vector spaces, rather than groups and rings, as the natural structures for coding theory. An annoying misprint on page 20 has "$1 \cdot 1 = 1^2 = 0$," which will certainly confuse the reader who has just mastered the fact that $1 + 1 = 0$. We hasten to add that the book is amazingly free of typographical errors; we found less than a dozen in a fairly careful reading.

Chapter 3 is a very readable introduction to linear block codes and their associated generator and parity-check matrices. A treatment with proofs of cosets and standard arrays is given, but unaccountably there is no mention of the fact that the coset is invariant to the choice of the coset leader. This fact, which is easily proved from the results on hand, is essential to proper understanding of the standard array as a decoding table. It is also strange, in light of the first chapter, that no mention is made of the crucial fact that linear codes are sufficiently rich to satisfy the coding theorem.

Chapter 4 is devoted to the important special case of cyclic codes and succeeds in avoiding the algebraic morass that strangles most treatments of this subject. The coding theorist, who will not find much new in this book, will be treated to a simple and elegant development of the k-stage encoder for cyclic codes. One notational preference, namely, using $(v_0,v_1,\cdots,v_{n-1})$ rather than $(v_{n-1},v_{n-2},\cdots,v_0)$ for code vectors, results in some confusion as to which is the first digit. On page 64 we find "... the first k digits of each codeword are the unaltered information digits...," while on page 69 we are told that "... the last k symbols ... will be taken as information symbols."

Chapter 5 is entitled "Error-Trapping Decoding for Cyclic Codes." By error-trapping, the author means cyclic shifting until the errors are confined to the parity positions in the block. The general error-trapping decoder of Fig. 5.3 and its explanation are overcomplicated by the choice of reading the received digits into the low rather than the high end of the syndrome register; moreover, the latter choice is made for all the examples later in the chapter. This chapter should be an interesting one for the communication engineer since error trapping is often the simplest effective decoding method to implement, particularly for burst correction. The author also gives considerable and proper attention to Kasami's error-trapping decoder for the Golay code; it is the simplest way to decode this code, which is of great theoretical and practical interest.

In Chapter 6 we are given a guided tour, entirely without proofs, through the land of BCH codes and the Berlekamp decoding algorithm. The tour should be adequate for the engineer who wants to know only what must be done and is not interested in why. But we also suspect that such an engineer would like the book's table of n, k, and t for all primitive BCH codes of length 1023 and less to be expanded by inclusion of the generator polynomial $g(X)$ and the parity-check polynomial $h(X)$, which he will need to know to implement the code.

Chapter 7 discusses majority-logic decoding of cyclic codes as an effective practical technique for many short codes. The reader should be alerted to an important simplification that can be made in all the Type *I* majority-logic decoders given in this chapter. For syndrome resetting, the output of the majority gate should be fed only to the adder at the input end of the syndrome register so as to complement the contents of the first stage whenever an error is corrected. This follows from the fact that the error after shifting has the form X^n, which equals 1 modulo $g(X)$. It is easily seen from Figs. 7.3, 7.5, and 7.7 that this is the net effect of the extra and unnecessary set of tap connections, corresponding to $\rho(X)$, that the author has included. There is also an important, and common, conceptual error in this chapter. The author states that L-step orthogonalization may require an inordinately large number of majority-logic gates and claims on page 171 that "... the complexity of an L-step majority-logic decoder is an exponential function of L." This is not true since as we clearly pointed out[1] earlier, one never needs more than k majority-logic elements to do the entire decoding.

Cyclic burst-correcting codes are treated in Chapter 8 with the

Fire codes and the Burton codes receiving good coverage. The use of interlacing is discussed with exceptional clarity. Chapter 9 extends this treatment to codes for the simultaneous correction of bursts and random errors. Product codes, Reed–Solomon $GF(2^m)$ codes as binary codes, and concatenated codes all come in for mention and are all good candidates for practical applications. Unfortunately, the author fails to make adequately clear that by "simultaneous correction" he means correction of the error whether it is a burst pattern or a random-error pattern, but not both in conjunction.

The last four chapters are devoted to convolutional codes, a much greater and welcome proportion of the text than in previous books on coding. Convolutional codes are introduced in Chapter 10, a veritable thicket of notation. The author employs only the matrix notation for convolutional codes. Our opinion is that the use of the D-transform notation in conjunction with some matrix notation makes for the simplest reading. On a minor point, the reader will be puzzled to find the encoded digits rather than the received digits as the input to the syndrome-forming circuit of Fig. 10.6. Chapter 11 contains a good treatment of all the known practical random-error-correcting convolutional codes, namely, the self-orthogonal codes, Massey's trial-and-error orthogonalizable codes, the uniform codes, and the Wyner–Ash single-error-correcting codes. The coding theorist is warned against the incomplete statement on page 257 that "Massey has shown that the L-step orthogonalization process for block codes does not apply to convolutional codes." Massey showed this only for the case $k = 1$.

In Chapter 12 on burst correction, the author wisely eschews the optimum but impractical Berlekamp–Preparata codes in favor of the suboptimum but practical Iwadare codes. This chapter also has a fair treatment of diffuse codes and the Gallager probabilistic burst-correcting scheme. In the 13th and last chapter, the author gives a brief introduction to sequential decoding, which has proved to be the most practical of any decoding method for random errors. Most readers will find the discussion inadequate and will want to dig deeper into the references. Only the Fano algorithm is discussed; our view is that the Zigangirov–Jelinek stack algorithm would have been a better choice, being the simpler to explain and of equal practical importance. Nonetheless, it is refreshing to see any coverage at all of sequential decoding in a book on algebraic coding.

Returning to generalities, we found the book to be attractively printed and illustrated. However, we were puzzled by the decision to put references at the end of each chapter rather than collected at the end of the book where they would be easier to find. Also, the choice of references is not always clear, for those at the end of a chapter are not necessarily cited therein, and some of the noncited references are quite inaccessible literature. The danger of anticipation is shown by several references to the still-awaited Peterson second edition as a 1970 book. It must be said in the matter of references that the author is generous in crediting the work of others.

Each chapter has a set of exercises, most of which are straightforward. However, some of the problems at the end of the early chapters will be very difficult for the reader who has only this book as background. It should also be mentioned that only binary codes are treated in this book. The resultant carelessness with signs will make it hard to build the more general case on this book as a base.

The large question remains: who will use this book? Our opinion is that it is not suited for a text in a course on coding unless the instructor is sufficiently steeped in coding theory to fill in the numerous missing details. The most likely use for this book is as a source for self-study and reference by the communication engineer who requires some knowledge of coding, but has neither the time nor the inclination to tackle the deeper treatises of Peterson and Berlekamp.

James L. Massey
Dep. Elec. Eng.
Univ. Notre Dame
Notre Dame, Ind. 46556

[1] J. L. Massey, *Threshold Decoding*. Cambridge, Mass.: M.I.T. Press, 1963, p. 100.

James L. Massey received the B.S. degree from the University of Notre Dame, Notre Dame, Ind., in 1956 and the S.M. and Ph.D. degrees from the Massachussets Institute of Technology, Cambridge, in 1960 and 1962, all in electrical engineering. From 1956 to 1959, he was a Communications Officer in the U.S. Marine Corps. Since 1962 he has been on the faculty of the University of Notre Dame. He has worked primarily in coding and systems and has published a score of papers in these fields. His monograph, "Threshold Decoding," received the 1964 paper award of the Group on Information Theory. He served as Chairman of the Group in 1969. He was elected a Fellow of the IEEE in 1971.

BOOKS RECEIVED

Compiled by Thomas M. Cover

Adapting to Innovation, D. Elizur (Jerusalem: Jerusalem Academic Press, 1970, 215 pp., $5.00).

Applied Probability Models With Optimization Applications, S. M. Ross (San Francisco: Holden-Day, 1970, 198 pp., $12.95).

Detection, Estimation and Modulation Theory, Part 2—Nonlinear Modulation Theory, H. L. Van Trees (New York: Wiley, 1971, 349 pp., $17.95). To be reviewed.

Empirical Bayes Methods, J. S. Maritz (New York: Barnes and Noble, 1970, 159 pp., $8.00).

Frequency Analysis Periodicity Detection in Hearing, R. Plomp and G. Smoorenburg, Eds. (Leiden, Netherlands: Sijthoff, 1971, 482 pp., $16.95).

Fundamental Research Statistics for the Behavioral Sciences, J. T. Roscoe (New York: Holt, Rinehart and Winston, 1969, 336 pp., $9.95).

Geometric Measure Theory, H. Federer (New York: Springer, 1969, 676 pp., $29.50).

Introduction to Probability and Statistics, M. Goldman (New York: Harcourt, Brace and World, 1970, 546 pp., $11.50).

Introductory Mathematical Statistics, E. Kreyszig (New York: Wiley, 1970, 470 pp., $12.50).

Linear Optimal Control, B. D. O. Anderson and J. B. Moore (Englewood Cliffs, N.J.: Prentice-Hall, 1971, 399 pp., $14.95).

Linear Programming, S. I. Gass (New York: McGraw-Hill, 1969, 358 pp., $14.50).

Mathematical Methods of Optimal Control, V. Boltyanskii (New York: Holt, Rinehart and Winston, 1971, 272 pp., $12.50).

Mathematical Psychology, C. Coombs, R. Dawes, and A. Tversky (Englewood Cliffs, N.J.: Prentice-Hall, 1970, 419 pp., $10.95).

Mathematics for the Social and Behavioral Sciences: Probability, Calculus and Statistics, B.Gelbaum and J. March (Philadelphia, Pa.: Saunders, 1969, 337 pp., $8.75).

Mathematics in the Behavioral and Social Sciences, J. Bishir and D. Drewes (New York: Harcourt, Brace and World, 1970, 714 pp., $10.95).

The Mathematics of Experimental Design and Patterns and Configurations in Finite Spaces, vol. 1, S. Vajda (New York: Hafner, 1967, 118 pp., $4.75).

The Mathematics of Experimental Design and Patterns and Configuration in Finite Spaces, vol. 2, S. Vajda (New York: Hafner, 1967, 127 pp., $4.95).

A Nonparametric Introduction to Statistics, C. H. Kraft and C. van Eeden (New York: Macmillan, 1968, 342 pp., $9.95).

Optimal Control of Systems Governed by Partial Differential Equations, J. L. Lions (New York: Springer, 1970, 430 pp., $21.50). Translated from the French by S. K. Mitter.

Order Statistics, H. David (New York: Wiley, 1970, 272 pp., $13.95).

Probability and Statistical Inference, R. Krutchkoff (New York: Gordon and Breach, 1970, 291 pp., $12.50).

Probability, Inference, and Decision, vol. 1, W. Hays and R. Winkler