Book Reviews

Information Theory, Robert Ash. (Interscience Tracts in Pure and Applied Mathematics, Interscience Publishers, a division of John Wiley & Sons, New York, N. Y., 1965. 339 pp., $13.50.)

Professor Ash's remark in the Preface that this book was written "··· in a style suitable for first-year graduate students in mathematics and the physical sciences···" should not be taken too seriously. The material is indeed largely self-contained, but the pace and depth of treatment are such that a heavy dose of mathematical maturity is required of the reader. It must be added that this is a very scholarly treatise which will generously reward the reader for his time spent in its mastery. Theorems are precisely stated and rigorously proved (except for a few minor lapses such as on page 112, where it is erroneously argued that pairwise independence of components implies pairwise independence of the entire code words), and historical credits are carefully traced. It is striking evidence to the genius of Claude Shannon that the broad coverage provided by the eight chapters of this book fails to exhaust the concepts introduced in Shannon's 1948 paper; e.g., there is no mention of Shannon's important concept of the rate-distortion function for an information source.

In Chapter One, "A Measure of Information," Ash derives the uncertainty function from a set of intuitive axioms and gives several interpretations of $H(X)$. The interpretation in terms of typical sequences is particularly well done. In Chapter Two, "Noiseless Coding," Ash treats the main features of the noiseless coding theorem including Huffman's construction for optimal codes. This chapter is complicated by Ash's formidable proof of the validity of an algorithmic test for unique decipherability. This material could have been relegated to an appendix (or omitted altogether) with little loss, since a major conclusion of the chapter is that the conditions for unique decipherability coincide with those for the existence of instantaneous (or prefix) codes. Thus codes that are uniquely decipherable but noninstantaneous would seem to be of little theoretical or practical interest.

Chapter Three, "The Discrete Memoryless Channel," is an elegant presentation of the noisy coding theorem for the DMC. Ash isolates the important aspects in his "Fundamental Lemma," which lies at the root of all the coding theorems proved in this book. As has become standard, the coding theorems in this and the later chapters are all stated in terms of word error probabilities for *block* codes. (Tree codes are nowhere considered in this book—a significant omission, since Ash co-authored one of the fundamental papers on the theory of recurrent codes which are linear tree codes.) The danger in restricting attention to blocks of channel digits is that one may ignore the fact that the quantities of real interest are the source digits. Ash shows his awareness of this point on page 84, where he takes pains to point out the rather obvious fact that if the block error probability is λ_n, then the average number of errors per source digit is at worst λ_n. "Thus by reducing λ_n toward zero we are in fact achieving reliable transmission." However, Ash ignores the logical converse conclusion that showing that λ_n approaches one is not in fact showing that transmission is unreliable, but only that at least one error must occur in the nR source digits that are associated with the block codeword. This consideration casts a shadow upon the worth of block codeword converses of the noisy coding theorem. An appreciation of this point may be found in Gallager.[1]

Chapter Four, "Error Correcting Codes," is a concise introduction to coding techniques for the binary symmetric channel. Parity-check codes are treated along the lines of Slepian's group-theoretic approach, and the sufficiency of parity-check codes for achieving the coding theorem is shown. Some misleading phraseology mars this chapter, e.g., "error of magnitude e" instead of the common "pattern of e errors," and "corrector" in place of the customary "syndrome." The material on binary block codes is continued in Chapter Five, "Further Theory of Error Correcting Codes," which treats of cyclic parity-check codes and arrives at the Bose-Chaudhuri-Hocquenghem codes as its *pièce de résistance.* This

[1] R. G. Gallager, "Information theory," in *The Mathematics of Physics and Chemistry*, H. Margenau and G. Murphy, Eds., vol. 2. Princeton, N. J.: Van Nostrand, 1964.

chapter contains a novel realization of the finite field $GF(2^m)$ as the set of 2^m matric polynomials of degree $m - 1$ or less in T, where T is any binary square matrix whose minimal polynomial is irreducible and of degree m. The T matrices associated with feedback shift registers are studied and cyclic codes are defined in terms of these matrices. This chapter provides an excellent treatment of shift register behavior, but a somewhat complicated approach to cyclic codes. The standard purely algebraic approach to cyclic codes seems more direct and transparent, but Ash's alternative formulation will provide additional insight to the reader already schooled in the algebraic approach.

Chapter Six, "Information Sources," is a compilation of material on Markov information sources superior to any other known to this reviewer. The book would be worth having for this chapter alone. This material leads naturally into Chapter Seven, "Channels with Memory," which is also well done. Wolfowitz's notion of λ-capacity and its relation to weak and strong converses of the coding theorem is clearly and simply presented. An unfortunate example on page 214 may confuse the reader who probes too deeply. There the operation of Blackwell's "trapdoor channel" is described commencing at some point when the source is in state a_1 and the channel is in state s_{10}—a situation that can never be attained physically.

In Chapter Eight, "Continuous Channels," Ash attacks the Gaussian channel with the artillery of operators in Hilbert space (the relevant theory is summarized in the Appendix). Ash calls into question Shannon's celebrated formula, $W \log (1 + M/NW)$, for the band-limited Gaussian white noise channel, claiming that it gives only a lower bound. However, Ash's objection is itself open to objection since Shannon explicitly required that both the signal and the noise be band-limited. Ash insists on time-limiting the signal and band-limiting the noise. One could argue that Ash must pass his time-limited signal through an ideal band-pass filter (admittedly such filters are physically unrealizable, but the whole problem is in a rather artificial arena) before it becomes an acceptable input for Shannon's channel. This reviewer, at the risk of being labeled naïve, cannot see that the question is worth all the fuss that it has received in this book and in several recent papers.

To summarize this reviewer's impressions, this book is an ambitious effort by a skilled theoretician. It will be a welcome addition to the library of anyone seriously interested in the foundations of Information Theory. Because of its wide coverage of the field, it will make an excellent text for a graduate course in Information Theory when used by a teacher who can impart a good intuitive appreciation for its contents. Some important points are relegated to exercises, but this is more than justified by the inclusion of complete solutions in the text. These will be a valuable self-study aid for the reader who wishes to test his mastery of the material. The book is remarkably free of misprints; the few found by this reviewer are easily corrected from the context. Readability suffers somewhat from the practice of merging many equations into the textual passages, but this tactic may have been necessary to keep the volume to manageable size.

James L. Massey
Dept. of Elec. Engrg.
University of Notre Dame
Notre Dame, Ind.

Random-Process Simulation and Measurements, G. A. Korn. (McGraw-Hill Book Co., New York, N. Y., 1966. 15 + 234 pp. $12.50.)

For thousands of years randomness was something to be avoided as far as possible (except in gambling games!). Only recently has a more creative attitude toward randomness emerged, especially in the fields of communication and automatic control. Not only has randomness invaded the theoretical aspects of these fields, but also the practical parts. Thus it is now necessary to be able to measure, produce and design for random behavior.

A good book on this topic has been needed for some time. As the author states in the preface

> This volume describes modern techniques utilizing analog, digital, and hybrid-analog-digital computers for random-process studies. It attempts a unified treatment of much material otherwise scattered over many publications and research reports, and adds previously unpublished material based on the writer's own research and lectures. Instrumentation and procedures are described as well as the underlying theory, and it is hoped that this book will be useful to a wide variety of engineers and scientists working in the areas of control, guidance, communication, detection, and instrument design.

The book is scholarly in the sense of having many references to the relevant literature, and in the sense that the author is a master of his subject matter. Unfortunately, it is hard reading in many places, but the importance of the material (plus the references) will make the effort to master it worthwhile.

The first chapter, "Mathematical Description of Random Processes," gives a very concise presentation of the background material, while the second, " A Review of Computer Techniques," presents the author's principal tool. To those who think that the digital computer is supreme, this chapter, as well as Chapter 8, will come as a surprise; the analog and the hybrid analog-digital computers are developing rapidly.

Again from the preface,

> Chapter 3 describes *analog-computer implementation of statistical input-output relations for linear systems*, including time-variable linear systems obtained through perturbation of nonlinear state or trajectory equations. A new and simplified derivation of modified-adjoint-system setups is presented; since the modified-adjoint system yields system mean-square error in a single computer run, the practical importance of this technique has been greatly enhanced by the modern iterative analog computer, which permits direct iterative parameter optimization.

Chapter 4, "Direct Simulation of Random Phenomena: Introduction to Monte-Carlo Techniques and Noise Generators," contains a good discussion of the matter with a sensible discussion of pseudo-random number generators and their uses.

The "Measurement of Time and Sample Averages, Correlation Functions, and Amplitude Distributions" is covered in Chapter 5, while Chapter 6 presents a mathematical theory of quantization effects that is so often ignored in practice. (Perhaps a bit more on "companding" would have been a help here.)

Chapter 7 deals with the difficult and important topic of "Measurement of Spectral Densities, Fourier Components, and System Response" in a better fashion than do most books on the topic.

Chapter 8 closes with "Special Techniques and Applications." The book is based on the author's extensive experience in the field and thus gives the book a unique, practical flavor that the poor engineer who has to do something will appreciate.

Richard W. Hamming
Bell Telephone Labs., Inc.
Murray Hill, N. J.

Principles of Communication Engineering, J. M. Wozencraft and I. M. Jacobs. (John Wiley & Sons, Inc., New York, N. Y., 1965.)

This is indeed a welcome addition to the communication theory literature and should be required reading for all graduate students majoring in communication theory and for advanced communication system designers. In particular, this work is the first formal effort to unite the converging disciplines of detection theory and information or coding theory, a natural union which has heretofore been ignored by far too many engineers and researchers concentrating on one or the other area. Besides this major contribution, the authors have made a valiant effort to maintain the presentation at a level suitable for the first-year graduate student with only a minor loss in generality and significance of results.

After an introductory chapter in which the plan of the book and some of the authors' basic philosophy is revealed, the next two chapters are devoted totally to an introduction to the theory of probability and random processes. As such they are fairly standard and typical of textbooks which provide the necessary introductory material before proceeding to the more advanced central topic of the