14. M. Metivier, *The stochastic integral with respect to processes with values in a reflexive Banach space*, Theor. Probability **19** (1974), 758–787.

15. M. Metivier and G. Pistone, *Une formule d'isométrie pour l'intégrale stochastique Hilbertienne et équations d'évolution linéaires stochastiques*, Z. Wahrscheinlichkeitstheorie und Verw. Gebiete **33** (1975), 1–18.

16. P. A. Meyer, *A decomposition theorem for supermartingales*, Illinois J. Math. **6** (1962), 193–205.

17. ______, *Intégrales stochastiques*. IV, Lecture Notes in Math., vol. 39, Springer-Verlag, Berlin and New York, 1967, pp. 142–162.

18. ______, *Un cours sur les intégrales stochastiques*, Lecture Notes in Math., vol. 511, Springer-Verlag, Berlin and New York, 1976, pp. 245–400.

19. ______, *Intégrales Hilbertiennes*, Lecture Notes in Math., vol. 581, Springer-Verlag, Berlin and New York, 1977, pp. 446–461.

20. R. E. A. C. Paley, N. Wiener and A. Zygmund, *Notes on random functions*, Math. Z. **37** (1933), 647–668.

21. J. Pellaumail, *Sur l'intégrale stochastique et la décomposition de Doob-Meyer*, Asterique **9** (1973), 1–125.

22. P. E. Protter, *Markov solutions of stochastic differential equations*, Z. Wahrscheinlichkeitstheorie und Verw. Gebiete **41** (1977), 39–58.

23. ______, *A comparison of stochastic integrals*, Ann. Probability (to appear).

24. R. L. Stratonovich, *A new representation for stochastic integrals and equations*, SIAM. J. Control **4** (1966), 362–371.

25. N. Wiener, *Differential-space*, J. Math. and Physics **2** (1923), 131–174.

PHILIP PROTTER

BULLETIN OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 84, Number 6, November 1978

The theory of information and coding: A mathematical framework for communication, by Robert J. McEliece, Addison-Wesley, London, Amsterdam, Don Mills, Ontario, Sydney, Tokyo, 1977, xvi + 302 pp., $21.50.

In the beginning (30 years ago) were Shannon and Hamming, and they took two different approaches to the coding problem. Shannon showed that the presence of random noise on a communications channel did not, by itself, impose any nonzero bound on the reliability with which communications could be transmitted over the channel. Given virtually any statistical description of the channel noise, one could compute a number C, called the channel capacity, which is a limit on the rate at which information can be transmitted across the channel. For any rate $R < C$, and any $\varepsilon > 0$, one could concoct codes of rate R which would allow arbitrarily long blocks of information to be transmitted across the noisy channel in such a way that the entire block could be correctly received with probability greater than $1 - \varepsilon$. Shannon's results were astounding and, at first, counterintuitive. However, they opened an area of study which has continued until this day. Modern practitioners of the "Shannon theory" continue to study questions of what performance is theoretically possible and what is not when one is free to use asymptotically long codes. The major activity in this area in the last few years has been related to questions about networks of channels, and broadcast channels, in which the same transmitted information is corrupted by different types of noise before being received by many different receivers. The main emphasis of this subject continues to be on the channel, and the methods of study are predominantly statistical.

At the same time that Shannon was studying the desirable properties of very long codes, Hamming began a study of very short codes. His most famous example was a code which specified how to append 3 check bits to 4 information bits in such a way that a single error in any of the 7 bits could be corrected. Hamming's work marked the beginning of a subject which has become known as "algebraic coding theory". Modern practitioners of this discipline continue to emphasize the codes rather than the channel. Code lengths are always finite, and often quite short, and their implementation is often of more concern than performance in some statistically complicated noise environment. The methods of "algebraic coding theory" are predominantly combinatorial and statistical. Galois fields often play an important role. The receiver of a noisy encoded message is typically faced with a decoding problem: he must somehow use the code's redundancy to decide where the errors occurred so that they can be corrected. This computational problem, generally ignored in the Shannon theory, becomes tractable for certain algebraic codes precisely because the codes have been constructed in a sophisticated way which allows the decoder to set up a system of simultaneous nonlinear equations over a Galois field, and to associate the locations of the errors with the solutions to these equations. However, the performance of the best algebraic codes devised to date falls far short of the codes whose existence has been proved by the Shannon theory.

For the past 30 years, the statistical school of information theory and the algebraic school of coding theory have gone their separate ways. Although there have been a few schizophrenics (e.g., Forney and this reviewer) who have worked on both sides of the fence, current erudite papers on coding theory are now classified as either "Shannon theory" or "algebraic coding", and there is a near-zero incidence of overlap. It has become traditional for every textbook in either field to include a highly condensed summary of the other, but despite this tradition, present-day researchers can still be sociologically partitioned into two highly specialized camps, each relatively ignorant of the other. This dichotomy has not impeded applications; many digital engineers have gone ahead and successfully implemented (72, 64) Hamming codes for their semiconductor memories in blissful ignorance of all relevant branches of theory!

McEliece's new book is probably the first to treat both historical approaches to the coding problem at a level intelligible to the novice. As befits the title, "encyclopedia", the coverage is very broad. The uniformly high standard of intelligibility appropriate for an "introductory" treatment is maintained throughout, even on those topics to which McEliece has himself made major contributions. McEliece's own theorems are simplified and condensed down to the same or an even smaller amount of printed space than is devoted to other theorems of comparable importance. Rare indeed is the book whose author exhibits such intellectual modesty!

Of course, a lot of things in this book might have been done differently.

Had the book been written primarily for mathematicians, the section on the Golay code might have been expanded to include the relationship between the Golay code and the Leech lattice (a packing of spheres in 24-dimensional Euclidean space which serves as an illustration of an excellent code for the Gaussian channel and as a point of connection with finite group theory, since the Leech lattice is the object which is preserved by Conway's group of order 8, 315, 553, 613, 086, 720, 000).

Had the book been written primarily for communication engineers, it might have included a more detailed overview of the current implementation costs for various types of decoders. Recent breakthroughs in the architecture of decoders, as well as recent and projected developments in the technology of large-scale integrated digital circuits, have resulted in enormous decreases in the costs of implementing decoders for long algebraic codes. In the reviewer's opinion, threshold decoding is no longer a promising area for further work because long algebraic codes already provide much better performance for at most slightly greater cost. Sequential decoding is even less competitive. A book directed primarily toward an audience of communication engineers might have also presented a more detailed (and admittedly controversial) examination of the relative merits of current block decoders vs. current convolutional decoders. Although McEliece's book gives a nice description of the suitability of Viterbi (convolutional) decoders for transmitting voice or pictures over white Gaussian noise channels, it does not discuss the numerous other factors which can now tip the scales in favor of long block codes. For example, jamming noise or burst noise from any source both cause considerably more problems for convolutional decoders than for long block decoders. High information rates or high performance requirements also favor long block codes.

Had the book been written a year later, it would have surely included Lovasz' very recent elegant solution to Shannon's classic problem of zero-error capacity, and some of the many exciting extensions of that result which McEliece himself has been pursuing in recent weeks.

However, had any of these "post facto" suggestions been pursued very far, *The theory of information and coding* would not be the broadly oriented, timely, introductory, superbly accessible encyclopedia that it is.

E. R. BERLEKAMP

BULLETIN OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 84, Number 6, November 1978

Matroid theory, by D. J. A. Welsh, Academic Press, London, New York, San Francisco, 1976, xi + 433 pp., $38.00

The term "matroid" was coined by Hassler Whitney in the 1930s to describe a system with an abstract linear dependence relation. He took as a model the linearly independent sets of column vectors of a matrix over a field. Thus a matroid consists of a finite set E and a distinguished collection $\mathcal{S}$ of subsets (called *independent* sets) of E having the properties

(I_1) Any subset of a member of $\mathcal{S}$ belongs to $\mathcal{S}$;

(I_2) Any two members of $\mathcal{S}$ which are maximal in a subset of S of E have the same cardinality.

If $S \subseteq E$ and $\rho(S)$ denotes the common cardinality of the sets of $\mathcal{S}$ which