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
© American Mathematical Society 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 $\mathfrak{S}$ of subsets (called *independent* sets) of E having the properties

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

(I_2) Any two members of $\mathfrak{S}$ 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 $\mathfrak{S}$ which