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 $\mathcal{E}$ of subsets (called *independent* sets) of E having the properties

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

(I_2) Any two members of $\mathcal{E}$ 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 $\mathcal{E}$ which are maximal in S, then ρ is a rank function on the subsets of E having the properties

(R_1) $0 \leq \rho(S) \leq |S|$;

(R_2) If $S \subseteq T$, then $\rho(S) \leq \rho(T)$;

(R_3) $\rho(S \cup T) + \rho(S \cap T) \leq \rho(S) + \rho(T)$.

The rank function ρ abstracts the notion of the dimension of the subspace spanned by a set of vectors. Furthermore the rank function can be used to define the matroid. Namely, if ρ is a rank function on the subsets of E satisfying (R_1)–(R_3), then the subsets S for which $\rho(S) = |S|$ are the independent sets of a matroid.

If ρ is the rank function of a matroid on the set E and $S \subseteq E$, let $\bar{S}$ consist of the elements x of E such that $\rho(S \cup \{x\}) = \rho(S)$. Then $S \rightarrow \bar{S}$ is a closure operator on the subsets of E having the exchange property.

(C_1) If $x \in \overline{S \cup \{y\}}$ and $x \notin \bar{S}$, then$y \in \overline{S \cup \{x\}}$.

Conversely, if $S \rightarrow \bar{S}$ is a closure operator defined on the subsets S of E satisfying (C_1), then the subsets S such that $x \notin \overline{S - \{x\}}$ for all $x \in S$ are the independent set of a matroid.

Finally, the closed subsets S for which $\bar{S} = S$ form a lattice under set inclusion. The closures of the one-element subsets are the atoms of the lattice and each closed subset is the join of the atoms which it contains. If S is closed and $x \notin S$, then by (C_1) the closure of $S \cup \{x\}$ covers S. Hence the lattice of closed subsets is a semimodular point lattice. Such a lattice is called a *geometric* lattice since its elements are the analogue of flats in a geometry and ρ plays the role of a dimension function. It should be noted that if E is the set of atoms of geometric lattice, the subsets S of E such that $x \not\leq \bigvee (S - x)$ all $x \in S$ are the independent sets of a matroid.

Almost immediately after Whitney introduced matroids, G. Birkhoff noted that the study of matroids was essentially equivalent to the study of geometric lattices. A year or two later, Saunders Mac Lane observed that the matroid axioms were satisfied by the notion of algebraic independence in field extensions and went on to generalize the ideas to infinite systems. Apart from some studies of geometric lattices by the reviewer in the 1940s there was little activity until the late 1950s when W. Tutte published his fundamental papers on matroids and graphs. Whitney had observed that the edge set of a graph becomes a matroid if the independent sets of edges are the sets containing no cycles. This matroid is called the *cycle* matroid of the graph and matroids which arise in this manner are said to be *graphic*. Exploiting this relationship between matroids and graphs, Tutte established a number of deep results. In particular, he gave an intrinsic characterization of graphic matroids. The work of Tutte stimulated a lively investigation of matroids from a graph theoretic viewpoint.

The first hint of possible applications of matroid theory to combinatorics came in the early 1940s with R. Rado's discovery of an analogue for matroids of P. Hall's theorem on representatives of sets. A couple of decades later, Edmonds and Fulkerson showed that the partial transversals of a family of subsets of a finite set can be taken as the independent sets of a matroid. From this observation came a variety of applications of matroid theory to combinatorial problems related to covering, packing, and transversal theory.

For example, a typical result states that a matroid E is the union of k independent sets if and only if $k\rho(S) \geqslant |S|$ for all subsets S of E. In the late 1960s and early 1970s, G. Rota and his associates undertook a broad range development of combinatorial theory from a matroid perspective. An important feature of this approach is the geometric framework in which many combinatorial problems are placed. Thus many geometric combinatorial properties of vector spaces have been shown to have matroid analogues.

Most of the investigations in the 1950s and 1960s were directed toward the basic problem of characterizing the classes of matroids arising from specific applications. In fact, Whitney posed the problem of characterizing those matroids which can be represented as matroids formed from a set of vectors of a vector space. This is a coordinatization problem which is still unsolved, although a number of characterizations have been given for specific fields. As mentioned above, Tutte provided a deep and elegant characterization of graphic matroids. A truly satisfactory characterization of transversal graphs has not been found although there are a number of results relating this characterization problem to other representation problems. In addition to the characterization problems there has been a continuing effort to use matroid techniques to simplify and extend a variety of combinatorial results.

The first half of Welsh's book is devoted to developing the elementary properties of matroids, describing the standard examples, and giving an account of the results of the investigations summarized in the previous paragraphs. The author tends to present the simpler proofs and refer the reader to the literature for the more difficult proofs. Although this is a fairly common practice it has the disadvantage of frequently disguising the relative importance of the results. This is particularly true when a rather minor theorem is included because it has a short and elegant proof. Fortunately, Welsh does make a point of emphasizing the more important contributions to the theory whether or not proofs are given. As far as subject matter is concerned, the first half of the book, while more up-to-date, covers much the same ground as the book, *On the foundations of combinatorial theory*: *Combinatorial geometries*, by Crapo and Rota. While Crapo and Rota adopt a geometric, lattice theoretic approach, Welsh sticks as strictly as possible to matroid-theoretic methods. Indeed, the presentation gives the impression that he would have preferred avoiding lattice theory altogether. However, there are important problem areas, for example, the Unimodality and Logarithmic Concavity Conjectures for the Whitney numbers, which are most naturally approached from a lattice point of view. Furthermore, questions of structure are usually handled more effectively in a lattice framework. As an introduction to the subject, the reader will probably find that the choice between the two approaches is largely a matter of taste.

The second half of the book is more technical in nature treating a variety of topics currently being investigated. In some cases the connection with matroid theory proper is a bit tenuous. Furthermore the selection of some topics clearly reflects the special interests of the author. Nevertheless, it does provide a sampling of the many different directions which current research is taking.

The book is not without some deficiencies. In each of the portions which the reviewer read carefully, a number of minor misprints and errors were found. Thus the reader should be warned to proceed with some care. Some of the terminology adopted by the author is unfortunate. For example, the term "simple" is used to describe matroids which have been trivially reduced by identifying mutually dependent elements. However, this term when applied to geometric lattices means something quite different. Since matroids and geometric lattices are so closely related, this terminology could lead to some confusion.

As in many recent books, the sets of exercises tend to be miscellaneous collections of results which the author decided not to include in the main body of the text. They vary in difficulty from trivialities to results which were only obtained through a major research effort. Unless the reader is an expert in the field he may find it hard to distinguish these two categories. Exercises make a significant contribution to a book at this level when they stimulate the reader's interest and provide him with an attractive opportunity to test his understanding of the material. In order to do this, the exercises should be carefully selected with regard to interest, subject matter content, and level of difficulty. Unfortunately, the exercise sets in this volume do not show this kind of careful preparation.

In spite of these shortcomings, this account of the present status of matroid theory will be a useful resource for both the novice and the expert in this subject area.

R. P. DILWORTH

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

The theory of error-correcting codes. I and II, by F. J. MacWilliams and N. J. A. Sloane, North-Holland, Amsterdam, New York, Oxford, 1977, ix + 762 pp., $50.95.

The first few sentences of the preface are as follows: "Coding theory began in the late 1940s with the work of Golay, Hamming and Shannon. Although it has its origins in an engineering problem, the subject has developed by using more and more sophisticated mathematical techniques. It is our goal to present the theory of error-correcting codes in a simple, easily understandable manner, and yet also to cover all the important aspects of the subject." The authors have been eminently successful in attaining their goal. For this reason these volumes are excellent as a text. They are also excellent as a reference for people working in coding as well as other mathematicians who are interested in applications of algebra or combinatorics or just interested in this new, fascinating subject. Since Shannon first demonstrated, using probabilistic methods, that one could communicate as reliably as desired by using long enough error-correcting codes, much work has gone into this subject by both mathematicians and electrical engineers. This has resulted in the construction and analysis of various codes and families of codes and the devising of practical decoding algorithms. It has also resulted in a growing mathematical theory of error-correcting codes which uses techniques from a variety of different areas as well as its own techniques.