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.

Due to the great activity in coding in the last thirty years and the exciting nature of the developments, there is now a great body of material on this subject. Even though there are other excellent books on coding [1]-[3], [5], [6], and [7] (to name some of them), much appears here in book-form for the first time. In order to indicate a portion of the topics covered, I will describe how these volumes can be used for courses in coding. The authors suggest chapters and parts of chapters for an introductory course and a secondary course for mathematicians and similar courses for engineers. They also describe what could be covered in an advanced course. I have taught two courses in coding for mathematicians somewhat near to the authors' suggestions using chapters from their book, and I have been very pleased with both the exposition and the materials covered. The student taking the elementary course does not need an extensive algebraic background as the various concepts used are discussed in the text. Indeed, such a course is an interesting, motivated introduction to modern algebra and provides many illuminating examples. I would judge the first course to be suitable for undergraduates with a course in linear algebra or more advanced students and the second course for upper level undergraduates or graduate students. There are many good exercises throughout the volumes with difficult ones labelled as such. In addition, the authors list many open research problems in relevant sections which enhances the value of the courses for graduate students looking for a thesis topic. This clearly is also very useful for a research worker in coding or someone just interested in the open problems in this subject.

Before describing the contents of the course for mathematicians, I present some terminology. A code (really a block code) consists of a set of vectors of a fixed length n with components in a finite field F. If $F = GF(2)$, the code is binary. The most widely used codes are binary and these volumes are primarily about binary codes although many of the results are stated for a general F. If v is a vector in the code a set of k of the positions in v are considered as information positions and the rest are redundancy positions which are added to the information positions so that the original message can be recovered if it is garbled when transmitted over a communications channel or stored in a computer. The process of adding the redundancy is called encoding and is usually not difficult. The process of recovering the original message is called decoding and is, in general, quite difficult, a challenge many have responded to by the construction of ingenious decoding algorithms. If the set of code vectors forms a k-dimensional vector subspace, the code is called a linear (n, k) code. The weight of a vector is the number of nonzero components it has and the minimum weight of a code, denoted by d, is the weight of the nonzero vector of smallest weight. The weight distribution of a code is the number of vectors in it of any given weight. The group of a binary code is the set of all permutations of the coordinate positions which send the code into itself.

Here is an abbreviated description of the two courses for mathematicians given both to demonstrate the contents of the books and to describe the courses. The elementary courses start with the first chapter which is a very readable introduction to the subject giving its practical origins, many examples including the Hamming codes, fundamental properties of linear codes, and the important Shannon theorem. This latter theorem is just stated, not proved, and the more accessible Gilbert-Varshamov theorem, demonstrating the existence of "good" linear codes, is proved. Since the single error-correcting Hamming codes were constructed, the next topic is the construction of a double error-correcting B.C.H. code of length 16 which motivates the use of $GF(16)$. This leads naturally to a description of how to construct any finite field and how to compute in it. Also general properties of these fields are given. This material is necessary for the study of the family of cyclic codes. This is one of the earliest families of codes investigated due to their easy encoding. They have quite a nice theory because of their relationship to ideals in a certain polynomial ring. This leads to a description of these codes in terms of factors of $x^n - 1$ over $GF(2)$. The practical B.C.H. codes, which are cyclic, are discussed next utilizing constructions based on finite fields. The course ends with a discussion of Reed-Muller codes which in general are not as good as B.C.H. codes but which are relatively easy to decode due to their relation to finite geometries.

The second course begins with nonlinear codes and their construction from various designs such as Hadamard designs. It also introduces the famous linear, binary Golay code and demonstrates how the nonlinear Nordstrom-Robinson code can be derived from it. If C is a linear code, $C^{\perp}$ the dual code, is the subspace of all vectors orthogonal, with respect to the usual inner product, to the vectors in C. It is an important result of coding theory that there are equations relating the weight distribution of C to that of $C^{\perp}$. When $C = C^{\perp}$, C is called self-dual, and these relations are constraints on the weight distribution of C. The next part of the course on the MacWilliams identities covers this, also MacWilliams identities for nonlinear codes.

The course then proceeds to the discussion of t-designs and their relation to codes. These are very interesting combinatorial configurations when they exist particularly for $t \geqslant 3$. No t-designs are known for $t > 5$ and until recently few 4 and 5 designs were known. It is quite surprising that 4 and 5 (also 1, 2, and 3) designs were found in codes. Many of these were found in self-dual codes. However, even if a t-design exists somewhere, its existence, in general, is very difficult to demonstrate. This demonstration is given by the Assmus-Mattson theorem which provides criteria on the weight distribution of a code and its dual code which ensure that certain t-designs are held by vectors of certain weights in the code. The designs are found in self-dual codes via this theorem is due to the fact that many have relatively few distinct nonzero weights. Another situation when designs can be found in codes is when the code is perfect. It is known that spheres of radius $[(d - 1)/2]$ about codewords are disjoint and when all vectors in the space are contained in these spheres, the code is called perfect. When such codes exist, they are very good, i.e. intrinsically capable of correcting many errors so an intriguing problem in coding was to find perfect codes. It is not hard to show that perfect codes can only exist for certain values of n, k, and d, and it was this observation which led Marcel Golay to construct his perfect codes, a (23, 12) triple error-correcting binary code and an (11, 6) double error-correcting ternary code. These remarkable codes have as groups the Mathieu groups M_{23} and $Z_2 \cdot M_{11}$, contain 5-designs, and have important connections with the new simple, sporadic groups [4]. It is now known (van Lint and Tietevainen) that these are the only parameters possible for multiple error-correcting codes over any field. This latter theorem is proved in the text but only stated and discussed in the course.

Next come the Reed-Solomon codes. After this the family of quadratic-residue codes are covered. These are cyclic codes whose construction is given by the quadratic residues over $GF(p)$ where p, a prime, is the length of the code. For moderate p, it is known that these are quite good codes and for all p the group of the extended codes contains $\mathrm{PSL}_2(p)$. The Golay codes can be expressed as quadratic residue codes. Next is a discussion of current results on bounds, a basic problem in coding. It can be shown that if d is the minimum distance of a code, then the code can correct $[(d-1)/2]$ errors. Hence it is desirable to know what is the maximum number, $A(n, d)$, of codewords in any code (linear or nonlinear) of length n and minimum distance d. Upper and lower bounds are given. The course ends with Gleason's theorem giving generators for the weight distributions of self-dual codes. This is done from the point of view of invariant theory.

As the authors note there is much left over for an advanced course. There is more material on the topics mentioned in addition to a discussion of association schemes, first introduced in statistics but which is a natural combinatorial setting for certain problems in coding. The list of topics mentioned above is not a complete list and more codes are contained in the books than are given here. Further, these topics are pursued in great depth. I believe the coverage of topics is excellent and these courses provide the student with an up-to-date account of the subject.

Although these volumes cover a great deal of material, much of it in book form for the first time, the authors had to exclude some topics which were included in their original plan. Even so, this represents a major scholarly effort as is attested by the bibliography of more than fourteen hundred references. In addition there is a short bibliography and historical notes at the end of each chapter. These volumes are very well-written with many nice exercises and open research problems. I am sure they will be widely used as both a text and reference work.

References

1. E. R. Berlekamp, *Algebraic coding theory*, McGraw-Hill, New York, 1968.

2. I. F. Blake and R. C. Mullin, *The mathematical theory of coding*, Academic Press, New York, 1975.

3. P. J. Cameron and J. H. van Lint, *Graph theory, coding theory, and block designs*, London Math. Soc. Lecture Notes Series, No. 19, Cambridge Univ. Press, London, 1975.

4. J. H. Conway, *Three lectures on exceptional groups*, in Finite Simple Groups, M. B. Powell and G. Higman (Eds.), Academic Press, New York, 1971, pp. 215–247.

5. S. Lin, *An introduction to error-correcting codes*, Prentice-Hall, Englewood Cliffs, N. J., 1970.

6. J. H. van Lint, *Coding theory*, Springer, New York, 1971.

7. W. W. Peterson and E. J. Weldon, Jr., *Error correcting codes*, 2nd ed., M.I.T. Press, Cambridge, Mass., 1972.

Vera Pless