BULLETIN OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 82, Number 1, January 1976

# BOOK REVIEWS

*The mathematical theory of coding*, by Ian F. Blake and Ronald C. Mullin, Academic Press, New York, 1975, 356+xi pp., $28.00.

The aim of this book is best expressed by the authors as follows:

"The subject of coding theory, for both discrete and continuous channels, has developed rapidly over the past twenty-five years with the application of more and more diverse algebraic and combinatoric methods. The aim of this book is to present a unified treatment of these mathematical ideas and their use in the construction of codes. It is not at all concerned with the practical matters of code implementation, and the subject of decoding is considered only insofar as it relates to the mathematical ideas involved. In many instances we have purposely chosen for a problem an approach that is mathematically more advanced than required in order to expose the reader to as wide a scope of concepts as possible, within the context of coding."

The extremely rapid development of coding theory over the past twenty-five years, the many facets of mathematics occurring in these developments, and the subsequent important relationships with these areas of mathematics make this book a welcome and timely addition. It covers the important developments in algebraic coding theory until the most recent times and introduces the new subject of codes for the Gaussian channel. In order to exhibit the scope of this book, we describe some of the topics covered.

The first chapter presents an extensive introduction to finite fields, and polynomials and vector spaces over finite fields. Cyclic codes, B.C.H. codes, Reed-Muller codes, and the group of a code are discussed. This chapter also covers the polynomial approach to coding. The second chapter covers various combinatorial structures and related codes. Among these are finite geometries, their groups, the various codes based on some type of finite geometry, and majority-logic decoding. Other combinatorial structures covered which are related to codes are balanced incomplete block design, latin squares, Steiner triple systems and Hadamard matrices. The related codes are the quadratic residue codes, symmetry codes, other self-dual and quasi-cyclic codes, and perfect codes. The MacWilliams equations and the Pless identities relating the weight distribution of a code to that of its orthogonal code are given in Chapter 1 and the Gleason polynomials which generate the weight enumerators of self-dual codes (over GF(2) and GF(3)) are introduced in Chapter 2. Chapter 3 continues the rich connections of combinatorial structures with codes starting with a discussion of t-designs and relations to perfect codes, nearly perfect codes, balanced codes and equidistant codes. The Assmus-Mattson theorem giving a criteria for codes to contain a $t$-design is presented. Many of the topics in this chapter are discussed from an interesting and unusual point of view, that of matroids. The fourth chapter discusses semisimple rings and places cyclic codes and

abelian codes in this context. Chapter 5 gives a survey of the theory of group representations from the linear algebra point of view, and the last chapter utilizes this theory to construct codes for the Gaussian channel.

Only an introductory knowledge of modern algebra is needed to understand this book. The topics mentioned above are all developed and most of the theorems are proved. In addition, at the end of each chapter there are interesting exercises, many of which advance the theory. The more difficult exercises contain references. Comments are provided at the end of each chapter and an extensive set of references are at the end of the book. This book should provide a valuable tool for those mathematicians who have recently become interested in investigating some of the open problems in error-correcting codes as well as those already in the field. Areas requiring further investigation are noted in this book. This book could be a basis for an advanced undergraduate or graduate course in combinatorics, coding theory, or applications of modern algebra.

VERA PLESS

*Braids, links, and mapping class groups*, by Joan S. Birman, based on lecture notes by James Cannon, Annals of Mathematics Studies, No. 82, Princeton University Press, Princeton, New Jersey, 1975, 228+ix pp., $8.50.

Talleyrand is supposed to have said that nobody could know the full sweetness of life who had not lived before the French Revolution. One may say that nobody can know the full charm of topology who had to learn it after it became rigorous. Artin's first paper (published in 1925) on the theory of braids is a perfect and lasting monument of this charm. It is a paper containing almost exclusively ideas and results but practically no machinery. Birman's monograph gives a nearly complete account not only of Artin's results but also of the numerous important applications, later developments and generalizations of the theory of braids, many of which are due to the author. Her presentation is, of course, completely rigorous, but it is remarkable that she has been able to preserve much of the appeal to geometric intuition which helped to make Artin's paper so attractive.

The book is written in a concise but lucid style. The prerequisites are a solid knowledge of basic algebraic topology and familiarity with the elements of the theory of presentations of groups. Many more specialized concepts and theorems (as, for instance, the free differential calculus of R. Fox), are developed in detail and sometimes with new proofs. For some theorems, only an outline of the proof or only a survey is given. These cases are fully covered by references to the literature.

The first chapter begins with the definition of the pure (or unpermuted) braid group of a manifold $M$ of dimension $>2$ as the fundamental group of the space

$$F_{0,n}M = \left\{ (z_1, \cdots, z_n) \in \prod_{i=1}^{n} M / z_i \neq z_j \qquad \text{if } i \neq j \right\}$$