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