Review of the book

"Finite Fields"

by Rudolf Lidl and Harald Niederreiter
Cambridge University Press, 2008

ISBN: 978-0-521-06567-2

Edoardo Persichetti
University of Warsaw
September 2013

1 Summary of the review

In this review I present the book "Finite Fields" by Rudolf Lidl and Harald Niederreiter. This volume gives a comprehensive coverage of the theory of finite fields and its most important applications such as combinatorics and coding theory.

2 Summary of the book

The theory of finite fields is a fascinating and important branch of algebra with many diverse applications. This book is the first to offer a dedicated treatment of the subject, providing a solid basis for a detailed study of finite fields. The authors assume as a prerequisite only a basic background in linear algebra.

3 Main Review

The volume is divided in nine medium-sized chapters, plus a short final chapter that contains a variety of tables. Chapter 1 is introductory, and features all the algebraic notions necessary for reading through the book. These include basics of groups, rings and fields, polynomials, and field extensions.
Moving on to Chapter 2, the authors start defining the structure of finite fields. The chapter presents all the principal methods for characterizing, representing and constructing finite fields, and it culminates with a milestone result in the theory, which is Wedderburn's theorem.
Having defined finite fields in detail, the book proceeds to introduce polynomials over finite fields. Chapter 3 contains accurate definitions of primitive and irreducible polynomials, and a long digression on linearized polynomials. A small separate section is dedicated to the special case of binomials and trinomials.
The last notions of this first part of the book are given in Chapter 4. This is a short chapter about the factorization of the polynomials, both over small and large finite fields, including a section on the calculation of roots.
Chapter 5 begins a new topic, namely that of exponential sums. The fundamental tools are described here, such as characters, and Gauss and Jacobi sums. The chapter also features a section on character sums with polynomial arguments, and some additional results on character sums.
Equations over finite fields are discussed in Chapter 6. The chapter begins with definitions and some classical

results, and proceeds then to describe some special classes of equations, namely quadratic forms and diagonal equations. The last section provides a detailed description of the Stepanov-Schmidt method for solving equations.
In Chapter 7 the authors go back to polynomials, presenting the particular category of permutation polynomials (polynomials whose associated polynomial functions are permutations over a certain finite field). An accurate characterization is given, starting from basic criteria and including special types, exceptional polynomials and polynomials in several indeterminates.
Another important topic is illustrated in Chapter 8: linear recurring sequences. These special sequences, such as feedback shift registers and impulse response sequences, find applications in coding theory and other areas. Families, characterization and distribution properties of these sequences are described in the last part of the chapter.
The final chapter, Chapter 9, is entirely dedicated to the main applications of finite fields. Among these, the most important is certainly coding theory. General linear codes and cyclic codes are therefore presented at the beginning of the chapter. Other applications mentioned in this chapter include finite geometries, combinatorics and linear modular systems.
As already noted, Chapter 10 consists of a few pages about computation in finite fields, and an extensive collection of tables relative to finite fields. Table A contains lists of all the non-zero elements of the fields $\mathbb{F}_q$, for $q \leq 128$. Table B is relative to the so-called *Jacobi's logarithm*. Tables C-F are relative to irreducible and primitive polynomials.

4 Style of the book

The book is rigorous but not hard to read, and it is presented in a very fluent style. Every chapter begins with a short description of the specific topic that will be presented, and features accurate definitions and theorems, and useful examples. The most cumbersome proofs are, for simplicity, omitted.
At the end of each chapter there are two extra sections. The first contains rather lengthy but interesting notes that provide further explanation and a historical perspective on the topics just presented. The second features several exercises, ranging from routine problems to, as is common practice, proofs that were not given in the main body, and material not covered in the chapter itself. All these aspects contribute in making the book appealing as a textbook for a Finite Field course.

5 Would you recommend the book?

The book provides an extensive treatment of the theory of finite fields. Its simple and reader-friendly style, and the inclusion of many worked examples and exercises make it suitable not only as a reference volume for the topic, but also as a textbook for a dedicated course. I highly recommend the book to any person interested in the theory of finite fields and its applications.

The reviewer is a Post-doc at University of Warsaw, Poland.