Review of the book

"Handbook of Finite Fields"

by Gary L. Mullen and Daniel Panario
CRC Press, Taylor & Francis Group, 2013

ISBN: 9781439873786

Jorge Nakahara Jr

1 Summary of the review

I this report I present my review on the "Handbook of Finite Fields" by Gary Mullen and Daniel Panario. It is an encyclopedic volume with an extensive overview of the subject of finite fields. The content is quite technical and requires a considerable background in abstract algebra and discrete mathematics to fully appreciate the magnitude of its coverage. Each chapter (and section within chapters) provide short surveys of different, up-to-date topics in finite field theory.

2 Summary of the book

This handbook provides a comprehensive and up-to-date overview of the theory of finite fields, including historical accounts of the origins of the subject, dating back to Evariste Galois in the 18th and 19th centuries.
This handbook is the result of a 3-year project involving 88 researchers (including the authors).
This single volume is divided into 3 parts, contains 17 contributed chapters totaling 1068 pages, useful pointers to computer algebra systems (e.g. GP-Pari, Matlab, ...) with capabilities to operate on finite fields. These references to computer software packages are quite instructive to practitioners and students willing to get some hands-on experience with the algebraic structure of finite fields.
Part I contains two chapters. The first chapter tells the history of finite fields during the 18th and 19th centuries, highlighting the contributions and insights of Evariste Galois. Chapter 2 lists some elementary properties of finite fields, providing a little background for the rest of the handbook. Also, several tables of polynomials are provided for computational issues involving finite fields.

Part II contains eleven chapters. Chapters 3 and 4 describe irreducible and primitive polynomials; chapter 5 describes several kinds of bases over finite fields, such as polynomial and normal bases; chapter 6 describes character and exponential sums over finite fields; chapter 7 discusses solutions of equations over finite fields; chapter 8 covers permutation and exceptional polynomials in one or several variables; chapter 9 discusses planar functions and Dickson polynomials, Boolean, APN, PN, bent and kappa polynomials; it finishes with a discussion on Schur's conjecture; chapter 10 discusses sequences over finite fields as well as transforms, LFSRs and maximal length sequences, correlation, autocorrelation, and linear complexity of sequences; chapter 11 deals with various kinds of finite field algorithms including formulas for polynomial counting, irreducible techniques, factorization of polynomials in one and several variables and the discrete logarithm problem; chapter 12 describes elliptic and hyperelliptic curves over finite fields; rational points on curves are considered as well as towers and zeta functions over finite fields; chapter 13 discusses relations between integers and polynomials, matrices over finite fields, linear algebra and related computational topics, as well as classical groups over finite fields, and Carlitz and Drinfeld modules.

Part III contains four chapters. Chapter 14 discusses latin squares and the polynomial method, applications of primitive polynomials over finite fields and Ramanujan and expander graphs. Chap. 15 deals with algebraic coding theory, LDPC codes, turbo code, algebraic geometric codes, raptor codes and polar codes. Chap. 16 discusses cryptographic algorithms, elliptic and hyperelliptic curve cryptosystems. Chap. 17 deals with finite fields in biology, quantum information theory, applications in orthogonal codes, binary sequences with small aperiodic auto-correlation, and sequences with small Hamming correlation.

3 What is the book like (style)?

The style of this book is very technical and advanced, mathematically and computationally. This book systematically lists hundreds of theorems, lemmas and contributions from 88 authors and different sources, but no proofs are provided. Rather, an extensive bibliography with 3084 references is cited for readers interested in the proofs and further details. It is comprehensive in scope and presents state-of-the-art results.

Problems are sparsely interleaved with the theory, but, again, no proofs are provided.

Various tables of polynomials and other primitives are included. These tables as well as examples, make some theorems more concrete and easy to understand.

This work is not a textbook. Considerable background in abstract algebra and discrete mathematics is needed to fully grasp and appreciate the theory presented. Sometimes, numerical examples are provided to instantiate some constructions.

The setting of this book is not elementary, as in a textbook. Rather, it is aimed at readers with an advanced background. It may serve as an excelent reference work for post-graduate courses.

This book is not meant (and it is not ideal) to be read from chapter 1 until chapter 17 in sequential order. Although there is some dependency between chapters, each chapter (or section) is more or less self contained, and deals with especific topics. It is a reference work, and as such it makes more sense to browse the chapter/section *'a la carte*, according to the particular interests of each reader.

The authors make available additional resources in
http://people.math.carleton.ca/∼daniel/hff/

4 Would you recommend this book?

This book serves as a comprehensive reference (and maybe the only commercially available) work to researchers, post-docs, PhD students and practitioners (e.g. engineers, programmers) interested in the theory and applications of finite fields. There are separate sections on applications of finite fields in cryptography, coding theory (error-correcting codes), combinatorics, biology, quantum information theory, etc.

An important contribution of this handbook is the extensive bibliography with 3084 entries, providing a comprehensive list of sources for proofs, theorems, properties and tables not explicitly included in the text.

The font used in this book is quite small, maybe 9pt or less, which makes reading difficult at times, e.g. distinguishing subscripts and superscripts in several mathematical notations.