Review of the book

"Algebraic Function Fields and Codes (2nd Edition)"

by Henning Stichtenoth

Springer, 2008

ISBN: 978-3-540-76877-7

Steven Galbraith
Department of Mathematics, The University of Auckland, New Zealand

June 17, 2010

1 Summary of the review

Algebraic geometry is a major branch of mathematics and the theory of curves over finite fields is a sub-topic with important applications in cryptography and coding theory. In particular, elliptic and hyperelliptic curves are a building block for many public key cryptosystems, and algebraic geometry codes have applications both in coding theory and cryptography.
Stichtenoth's book is the canonical modern textbook for the field-theoretic formulation of the theory of curves over finite fields. The book is carefully written, develops the theory rigorously from first principles, and contains elegant algebraic proofs of a number of very important facts. The original version of the book has been widely used by researchers and this second edition is sure to be also frequently referenced.

2 Summary of the book

There are many applications in cryptography and coding theory of algebraic curves over finite fields. Working over finite fields requires special care compared with "classical" algebraic geometry over $\mathbb{C}$, for at least 2 reasons. First, there are certain phenomena (such as inseparability) which arise in characteristic p and which do not arise in characteristic zero. Second, one must pay close attention to the field of definition of objects.
There are two languages in which the theory of curves over finite fields can be expressed. The geometric language speaks of points, curves, rational maps etc. These concepts can also be expressed in field-theoretic language as valuations (equivalently, places), function fields, field homomorphisms (of a certain type) and so on. Both languages express the same theory, and there are pros and cons of each formulation. The geometric approach is used in the books of Weil, Fulton, Mumford, Hartshorne and others, while the field-theoretic language is used in the books of Chevalley, Eichler, Artin and Deuring.
Stichtenoth's book is the canonical modern textbook for the field-theoretic formulation of the theory of curves over finite fields, and in particular those aspects relevant for coding theory. We now briefly summarise the contents of the book.

- Chapter 1 gives some basic theory of function fields and their valuations. The weak approximation theorem for valuations is a key tool. This chapter gives a proof of the Riemann Roch theorem.
- Chapter 2 gives a brief survey of error correcting codes from curves over finite fields.
- Chapter 3 is about extensions of function fields (which corresponds to rational maps between curves in the geometric language). The Hurwitz genus formula is proved.
- Differentials are given in Chapter 4.

- Chapter 5 is about the zeta function. The famous Hasse-Weil theorem (the Riemann hypothesis for function fields) is proved.
- Chapter 6 studies some particular function fields, such as those associated with elliptic and hyperelliptic curves.
- Chapter 7 discusses Ihara's constant $A(q)$, which is an asymptotic measure, as the genus grows, of the number of points on curves of genus g over a field of q elements. The chapter then surveys research on the topic of large values for $A(q)$ within certain families of curves (which lead to codes with good properties).
- Chapters 8 and 9 give further discussion about codes based on curves.
- The appendices briefly summarise some basic concepts in field theory and algebraic geometry.

The main changes in the second edition are the addition of exercises at the end of each chapter, the addition of a small number of new examples, and the addition/expansion of some sections and chapters. In particular, there is a new chapter (Chapter 7) on asymptotic bounds for the number of places in towers of extensions of function fields. That said, the majority of the text is essentially unchanged from the first edition and, conveniently, many theorems have the same numbering in the new edition as they had in the first edition.

3 What is the book like (style)?

Stichtenoth's textbook gived a clear and modern introduction to the field-theoretic formulation of the theory of curves over finite fields. The book is carefully written, develops the theory rigorously from first principles, and contains elegant algebraic proofs of a number of very important facts.
The style is formal and rather dense, with relatively few examples. This second edition has exercises, which are a valuable addition to the book, though solutions to the exercises are not given.
The strength of the book, to me, has always been that it contains self-contained and simple proofs of a number of fundamental results in the theory. For example, Theorem 1.4.11 gives, as far as I know, the simplest self-contained proof in the literature of the important theorem that the degree of the divisor of a function on a curve is zero. Similarly, Chapter 5 gives an easily accessible proof of the Hasse-Weil theorem and related results about zeta functions of curves.
The main weaknesses of the first edition of the book remain in the second edition. In particular, the early part of the book is rather economical with non-trivial examples, and almost no geometric motivation or intuition is given (Appendix B gives the dictionary between the field-theoretical language and the geometric language, but only over an algebraically closed field). For this reason, students who want to learn algebraic geometry using the book will be advised to also read a book with a more geometric point of view, such as the book of Fulton or books by Reid, Hartshorne or Washington. Another weakness is that, despite the major focus in the book on error correcting codes, relatively little is actually said about codes, decoding algorithms (apart from Section 8.5, which is still at a rather high level), or practical issues in coding theory. Instead, the presence of coding theory is mainly to provide motivation for the study of curves over finite fields with many rational points.

4 Would you recommend this book?

This book is published as a Springer Graduate Text in Mathematics, and this is an appropriate indication of the intended audience. The reader is required to have a solid background in algebra (for example, having taken a serious course in groups, rings and fields and preferably with Galois theory). The reader is also assumed to have the mathematical maturity to be able to absorb large amounts of detail without needing too many signposts about where the subject is headed. In this sense, the book is appropriate for beginning PhD students, or Masters students doing projects in the subject.
The book is an excellent companion for students learning the theory of curves, though I would also recommend reading a book which gives a more geometric point of view (such as Fulton's book) in parallel.

For researchers in the field the book is a very convenient reference for proofs and definitions, and I consult my copy of the first edition frequently.
Since this is a book review for the IACR I feel obliged to remark that the book does not contain any details about public key cryptography using curves over finite fields, or about applications of algebraic geometry codes in cryptography. In particular, readers who wish to learn about topics of major interest in elliptic curve cryptography, such as the Weil pairing or isogenies, will find no mention of these subjects in Stichtenoth's book. This should not be taken as a criticism, as the author's purpose is clear and his goal is successfully achieved.
Similarly, the book is not appropriate as a general introduction to error correcting codes. Students who wish to learn coding theory are advised to look at, for example, the book by van Lint. They can move on to Stichtenoth when they need to learn more about codes from curves.

The reviewer is a Senior Lecturer at the Department of Mathematics at the University of Auckland, New Zealand.