DE GRUYTER

Harald Niederreiter, Alina Ostafe,
Daniel Panario, Arne Winterhof (Eds.)

ALGEBRAIC CURVES AND FINITE FIELDS

CRYPTOGRAPHY AND OTHER APPLICATIONS

RADON SERIES ON COMPUTATIONAL AND APPLIED MATHEMATICS 16

DE G

Algebraic Curves and Finite Fields

Cryptography and Other Applications

Edited by
Harald Niederreiter
Alina Ostafe
Daniel Panario
Arne Winterhof

DE GRUYTER

Mathematics Subject Classification 2010
05, 11, 12, 14, 68, 94

ISBN 978-3-11-031788-6
e-ISBN 978-3-11-031791-6
ISSN 1865-3707

Library of Congress Cataloging-in-Publication Data
A CIP catalog record for this book has been applied for at the Library of Congress.

Bibliographic information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at http://dnb.dnb.de.

Typesetting: le-tex publishing services GmbH, Leipzig
Printing and binding: CPI books GmbH, Leck
♾ Printed on acid-free paper
Printed in Germany

www.degruyter.com

Harald Niederreiter, Alina Ostafe, Daniel Panario, Arne Winterhof (Eds.)
Algebraic Curves and Finite Fields

Radon Series on Computational and Applied Mathematics

Volume 16

Introduction

This book contains survey articles based on some invited lectures of two workshops of the *RICAM Special Semester on Applications of Algebra and Number Theory*:

- Algebraic Curves over Finite Fields (November 11–15, 2013).
- Emerging Applications of Finite Fields (December 9–13, 2013).

These workshops brought together some of the worldwide most prominent researchers in the area of finite fields and their applications. Some classical as well as very new problems on curves and other aspects of finite fields were addressed, with emphasis on their diverse applications.

Finite fields are the meeting point of algebra, number theory, computer science, combinatorics, cryptography, to mention just a few. The book describes some of the most recent achievements in theory and applications of finite fields with a focus on curves and cryptography.

The theory of algebraic curves (or function fields) has its origins in number theory. However, many applications of curves were found in different areas such as coding theory, sphere packings and lattices, sequence design, quasi-Monte Carlo methods, and cryptography. The use of algebraic curves often led to better results than those within classical approaches.

The book presents some new developments and stimulates the interaction between different application areas as well as the continuous quest for new applications. The main application area of curves (or function fields) is coding theory. The chapter of Bassa, Beelen, and Nguyen gives an overview of known and new techniques for constructing good towers of function fields. The chapter of Giuletti and Korchmáros surveys recent results and open problems on curves with many automorphisms, while the survey of Achter and Pries presents results and open questions about the p-ranks and Newton polygons for curves in positive characteristic. The chapter of Villa-Salvador contains the proof of an analogue in positive characteristic of the Kronecker–Weber theorem that the maximal Abelian extension of the rationals is the union of all cyclotomic number fields. The chapters of Carlet and Guilley respectively Pott, Schmidt, and Zhou deal with Boolean functions and related topics as side-channel attacks and difference sets. The chapter of Cheon, Kim, and Song discusses a modification of the discrete logarithm problem which is the basis for the security of the Diffie–Hellman public key exchange. The chapter of Steinfeld gives an overview of recent developments on the NTRU and related cryptosystems. The chapter of Helleseth surveys known results on nonlinear shift registers which are very attractive alternatives to linear ones. Finally, the chapter of Pausinger and Topuzoğlu studies permutation polynomials of finite fields for constructing uniformly distributed permuted Halton sequences for quasi-Monte Carlo integration.

All these chapters were reviewed and we wish to thank the anonymous referees for their precious help.

We also like to thank the program chairs of the two workshops, Henning Stichtenoth and Igor Shparlinski, as well as Annette Weihs and Wolfgang Forsthuber for administrative support and all the speakers of the workshops listed below who contributed with excellent talks and made the workshop a great success: Nurdagül Anbar, Peter Beelen, Herivelto Borges, Cicero Carvalho, Ignacio Cascudo, Iwan Duursma, Arnaldo Garcia, Olav Geil, Massimo Giulietti, Clemens Heuberger, Gabor Korchmáros, Aristides Kontogeorgis, Florian Luca, Rachel Pries, Luciane Quoos-Conte, Christophe Ritzenthaler, Gabriel Villa-Salvador, Chaoping Xing, Alexey Zaytsev (algebraic curves) and Andreas Bender, Claude Carlet, Jung Hee Cheon, Pierrick Gaudry, Alexey Glibichuk, Tor Helleseth, Doowon Koh, Swastik Kopparty, Winnie Li, Ferruh Özbudak, Oliver Roche-Newton, Alexander Pott, Nitin Saxena, Ilya Shkredov, Ron Steinfeld, Ming Su, Julia Wolf (finite fields).

More details on this special semester can be found on the webpage www.ricam.oeaw.ac.at/specsem/specsem2013/.

We also thank the Radon Institute for Computational and Applied Mathematics (RICAM) of the Austrian Academy of Sciences for financial support.

Linz, December 2013

Harald Niederreiter,
Alina Ostafe,
Daniel Panario,
Arne Winterhof

Contents

Jeffrey D. Achter and Rachel Pries

Generic Newton polygons for curves of given p-rank

Abstract: We survey results and open questions about the p-ranks and Newton polygons of Jacobians of curves in positive characteristic p. We prove some geometric results about the p-rank stratification of the moduli space of (hyperelliptic) curves. For example, if $0 \leq f \leq g-1$, we prove that every component of the p-rank $f+1$ stratum of $\mathcal{M}_g$ contains a component of the p-rank f stratum in its closure. We prove that the p-rank f stratum of $\overline{\mathcal{M}}_g$ is connected. For all primes p and all $g \geq 4$, we demonstrate the existence of a Jacobian of a smooth curve of genus g, defined over $\overline{\mathbb{F}}_p$, whose Newton polygon has slopes $\{0^{g-4}, 1/4, 3/4, 1^{g-4}\}$. We include partial results about the generic Newton polygons of curves of given genus g and p-rank f.

Keywords: Newton polygon, curve, Jacobian, p-rank, moduli space

Mathematics Subject Classification 2010: 11G20, 11M38, 14H10, 14H40, 14L05, 11G10

Jeffrey D. Achter, Rachel Pries: Department of Mathematics, Colorado State University, Fort Collins, CO 80523, USA, email: achter@math.colostate.edu, pries@math.colostate.edu

1 Introduction

Suppose C is a smooth projective curve of genus g defined over a finite field $\mathbb{F}_q$ of characteristic p. Then its zeta function has the form $Z_{C/\mathbb{F}_q}(T) = L_{C/\mathbb{F}_q}(T)/[(1-T)(1-qT)]$ for some polynomial $L_{C/\mathbb{F}_q}(T) \in \mathbb{Z}[T]$. The Newton polygon ν of C is that of $L_{C/\mathbb{F}_q}(T)$; it is a lower convex polygon in $\mathbb{R}^2$ with endpoints $(0,0)$ and $(2g,g)$. Its slopes encode important information about C and its Jacobian.

Given a curve $C/\mathbb{F}_q$ of genus g, there are methods to compute its Newton polygon. After some experiments, it becomes clear that the typical Newton polygon has slopes only 0 and 1. For small g and p, the other possible Newton polygons do occur, but rarely, leading us to the following question.

Question 1.1. *Does every Newton polygon of height $2g$ (satisfying the obvious necessary conditions) occur as the Newton polygon of a smooth curve defined over a finite field of characteristic p for each prime p?*

The answer to this question is unknown, although one now knows that every integer f such that $0 \leq f \leq g$ occurs as the length of the line segment of slope 0 for the Newton

The first author is supported in part by Simons Foundation grant 204164. The second author is supported in part by NSF grant DMS-11-01712

polygon of a curve in each characteristic p [12]. As an example, we consider the first open case, when $g = 4$ and ν has slopes $1/4$ and $3/4$. We confirm in Lemma 5.3 that this Newton polygon occurs for a curve of genus 4 for each prime p using a unitary Shimura variety of type $U(3, 1)$.

The main idea in this chapter is that the occurrence of a certain Newton polygon for a curve of small genus can be used to prove the occurrence of new Newton polygons for smooth curves for every larger genus. As an application, we prove in Corollary 5.6 that the Newton polygon ν_g^{g-4} having $g - 4$ slopes of 0 and 1 and four slopes of $1/4$ and $3/4$ occurs as the Newton polygon of a smooth curve of genus g for all primes p and all $g \geq 4$.

The key condition above is that the curve must be smooth, because it is easy to produce singular curves with decomposable Newton polygons by clutching together curves of smaller genus. In order to deduce results about Newton polygons of smooth curves from results about Newton polygons of singular curves, we rely on geometric methods from [2]. It turns out that one of the best techniques to determine the existence of a curve whose Jacobian has specified behavior is to study the geometry of the corresponding loci in $\mathcal{M}_g$, the moduli space of smooth proper curves of genus g.

More precisely, the p-rank f and Newton polygon are invariants of the p-divisible group of a principally polarized Abelian variety. The stratification of the moduli space $\mathcal{A}_g$ by these invariants is well understood, in large part because of work of Chai and Oort. Let $\mathcal{A}_g$ be the moduli space of principally polarized Abelian varieties of dimension g. The Torelli map $\tau\colon \mathcal{M}_g \hookrightarrow \mathcal{A}_g$, which sends a curve to its Jacobian, allows us to define the analogous stratifications on $\mathcal{M}_g$. For dimension reasons, this gives a lot of information when $1 \leq g \leq 3$ and very little information when $g \geq 4$. For example, in most cases it is not known whether the p-rank f stratum $\mathcal{M}_g^f$ is irreducible.

In Section 2, we review the fundamental definitions and properties of the p-rank and Newton polygon. In Section 3, we review the p-rank and Newton polygon stratifications of $\mathcal{A}_g$. Since degeneration is one of the few techniques for studying stratifications in $\mathcal{M}_g$, in Section 4.1 we recall the Deligne–Mumford compactification of $\mathcal{M}_g$, and explain how it interacts with the p-rank stratification.

In Section 4.2, we review a theorem that we proved about the boundary of the p-rank strata $\mathcal{M}_g^f$ of $\mathcal{M}_g$ in [2]. Using this, we prove that $\overline{\mathcal{M}}_g^f$ is connected for all $g \geq 2$ and $0 \leq f \leq g$ (Corollary 4.5). For $f \geq 1$, we also prove that every component of $\mathcal{M}_g^f$ contains a component of $\mathcal{M}_g^{f-1}$ in its closure (Corollary 4.4).

In Section 5, we consider the finer stratification of $\mathcal{M}_g$ by Newton polygon. We consider a Newton polygon ν_g^f which is the most generic Newton polygon of an Abelian variety of dimension g and p-rank f. The expectation is that the generic point of every component of $\mathcal{M}_g^f$ represents a curve with Newton polygon ν_g^f. We prove that this expectation holds in the first nontrivial case when $f = g-3$ in Corollary 5.5 and prove a slightly weaker statement when $f = g - 4$ in Corollary 5.6.

The discrete invariants associated with these stratifications seem to influence arithmetic attributes of curves over finite fields, such as automorphism groups and maximality. One should note, however, that this relationship is somewhat subtle. On one hand, many exceptional curves turn out to be *supersingular*, meaning that Newton polygon is a line segment of slope $1/2$. For example, it is not hard to prove that a curve which achieves the Hasse–Weil bound over a finite field must be supersingular. On the other hand, the p-rank stratification is in some ways "transverse" to other interesting loci in $\mathcal{M}_g$, illustrated by the fact that a randomly chosen Jacobian of genus g and p-rank f behaves like a randomly selected principally polarized Abelian variety of dimension g. In Sections 4.4 and 5, we discuss open questions and conjectures on these topics.

2 Structures in positive characteristic

Consider a principally polarized Abelian variety X of dimension g defined over a field K of characteristic $p > 0$. If $N \geq 2$ is relatively prime to p, then the N-torsion group scheme $X[N]$ is étale, and $X[N](\overline{K}) \cong (\mathbb{Z}/N)^{\oplus 2g}$ depends only on the dimension of X. In contrast, $X[p]$ is *never* reduced, and there is a range of possibilities for the geometric isomorphism class of $X[p]_{\overline{K}}$ and, *a fortiori*, the p-divisible group $X[p^\infty] := \lim_{\to n} X[p^n]$. In this section, we review some attributes of $X[p]$ and $X[p^\infty]$, with special emphasis on the case where X is the Jacobian of a curve over a finite field.

2.1 The p-rank

The p-rank of X is the rank of the "physical" p-torsion of X. More precisely, it is the integer f such that

$$X[p](\overline{K}) \cong (\mathbb{Z}/p)^{\oplus f} . \tag{2.1}$$

We will see below (2.2.3) that $0 \leq f \leq g$. The Abelian variety X is said to be ordinary if its p-rank is maximal, i.e. $f = g$.

Specifying a K-point of $X[p]$ is equivalent to specifying a homomorphism $X[p] \to (\mathbb{Z}/p)$ of group schemes over K, and thus one may also define f by

$$f = \dim_{\mathbb{F}_p} \mathrm{Hom}_{\overline{K}}(X[p], (\mathbb{Z}/p)) .$$

Now, $X[p]$ is a self-dual group scheme, and the dual of $(\mathbb{Z}/p)$ is the nonreduced group scheme $\boldsymbol{\mu}_p$, the kernel of Frobenius on the multiplicative group $\mathbb{G}_m$. Consequently, it is equivalent to define the p-rank of X as

$$f = \dim_{\mathbb{F}_p} \mathrm{Hom}_{\overline{K}}(\boldsymbol{\mu}_p, X[p]) .$$

(This last formulation is convenient for defining the p-rank of semi-Abelian varieties and semistable curves.)

If X is the Jacobian of a smooth, projective curve C, then the p-rank equals the maximum rank of a p-group which occurs as the Galois group of an unramified cover of C [20, Corollary 4.18].

2.2 Newton polygons

2.2.1 Newton polygon of a curve over a finite field

Let $C/\mathbb{F}_q$ be a smooth, projective curve of genus g. Then its zeta function

$$Z_{C/\mathbb{F}_q}(T) = \exp\left(\sum_{k\geq 1} \#C(\mathbb{F}_{q^k})T^k/k\right)$$

is a rational function of the form

$$Z_{C/\mathbb{F}_q} = \frac{L_{C/\mathbb{F}_q}(T)}{(1-T)(1-qT)}$$

where $L_{C/\mathbb{F}_q}(T) \in \mathbb{Z}[T]$ is a polynomial of degree $2g$. The L-polynomial factors over $\overline{\mathbb{Q}}$ as

$$L_{C/\mathbb{F}_q}(T) = \prod_{1\leq j\leq 2g} (1-\alpha_j T)\,,$$

where the roots can be ordered so that

$$\alpha_j\alpha_{g+j} = q \text{ for each } 1 \leq j \leq g\,. \tag{2.2}$$

Each α_j has Archimedean size $\sqrt{q}$; for each $\iota\colon \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$, one has $\left|\iota(\alpha_j)\right| = \sqrt{q}$. In contrast, there is a range of possibilities for the p-adic valuations of the α_j. The Newton polygon of C (or of its Jacobian X) is a combinatorial device which encodes these valuations.

Let $\mathbb{K}$ be a field with a discrete valuation v, and let $h(T) = \sum a_i T^i \in \mathbb{K}[T]$ be a polynomial. The Newton polygon of $h(T)$ is defined in the following way.

In the plane, graph the points $(i, v(a_i))$, and form its lower convex hull. This object is called the Newton polygon of h. Equivalently, it suffices to track the multiplicity $e(\lambda)$ with which each slope λ occurs in the diagram. Thus, we will often record a Newton polygon as the function

$$\begin{aligned} \mathbb{Q} &\longrightarrow \mathbb{Z}_{\geq 0} \\ \lambda &\longmapsto e(\lambda)\,, \end{aligned}$$

which, to each λ, assigns the length of the projection of the "slope λ" part of the Newton polygon onto its first coordinate. This function encodes the valuation of the roots of