ALGEBRA AND APPLICATIONS

Arnaldo Garcia
Henning Stichtenoth
(Editors)

Topics in Geometry, Coding Theory and Cryptography

Springer

Topics in Geometry, Coding Theory and Cryptography

Algebra and Applications

Volume 6

Algebra and Applications aims to publish well written and carefully refereed monographs with up-to-date information about progress in all fields of algebra, its classical impact on commutative and noncommutative algebraic and differential geometry, K-theory and algebraic topology, as well as applications in related domains, such as number theory, homotopy and (co)homology theory, physics and discrete mathematics.
Particular emphasis will be put on state-of-the-art topics such as rings of differential operators, Lie algebras and super-algebras, group rings and algebras, C*algebras, Kac-Moody theory, arithmetic algebraic geometry, Hopf algebras and quantum groups, as well as their applications. In addition, Algebra and Applications will also publish monographs dedicated to computational aspects of these topics as well as algebraic and geometric methods in computer science.

Topics in Geometry, Coding Theory and Cryptography

Edited by

Arnaldo Garcia
Instituto de Matematica Pura e Aplicada (IMPA),
Rio de Janeiro, Brazil

and

Henning Stichtenoth
University of Duisburg-Essen, Germany and
Sabanci University, Istanbul, Turkey

Springer

A C.I.P. Catalogue record for this book is available from the Library of Congress.

ISBN-10 1-4020-5333-9 (HB)
ISBN-13 978-1-4020-5333-7 (HB)
ISBN-10 1-4020-5334-4 (e-book)
ISBN-13 978-1-4020-5334-4 (e-book)

Published by Springer,
P.O. Box 17, 3300 AA Dordrecht, The Netherlands.

www.springer.com

Printed on acid-free paper

Contents

Foreword

The theory of algebraic function fields has a long history. Its origins are in number theory, and there are close interrelations with other branches of pure mathematics such as algebraic geometry or compact Riemann surfaces. In fact, the study of algebraic function fields is essentially equivalent to the study of algebraic curves. These relations have been well-known for a long time.

Around 1980 V. D. Goppa came up with a brilliant idea of constructing error-correcting codes by means of algebraic function fields over finite fields. These codes are now known as *geometric Goppa codes* or *algebraic geometry codes* (AG *codes*). The key point of Goppa's construction is that one gets information about the code parameters (length, dimension, minimum distance of the code) in terms of geometric and arithmetic data of the function field (number of rational places, genus). Goppa's method can be seen as a "simple" generalization of the construction of Reed-Solomon codes: one just replaces the evaluation of polynomials in one variable at elements of a finite field (which is used for the definition of Reed-Solomon codes) by evaluating functions of a function field at some of its rational places. A basic role is then played by the Riemann-Roch theorem.

Soon after Goppa's discovery, M. A. Tsfasman, S. G. Vladut and T. Zink constructed families of AG codes of increasing length whose asymptotic parameters are better than those of all previously known infinite sequences of codes and which beat the Gilbert-Varshamov bound - a bound which is well-known in coding theory and which is a classical measure for the performance of long codes. The proof of the Tsfasman-Vladut-Zink result uses two main tools: Goppa's construction of AG codes and the existence of curves or function fields (more specifically: classical or Drinfeld modular curves) over a finite field having large genus and many rational places.

Cyclic codes have a natural representation as *trace codes*, and one can associate with each codeword of a trace code an Artin-Schreier function field. Properties of this function field (specifically the number of rational places) reflect properties of the corresponding cyclic code (namely the weights of codewords and subcodes). In this way one gets another link between codes and function fields which is entirely different from Goppa's.

In 1985, N. Koblitz invented cryptosystems which are based on elliptic curves (or elliptic function fields) over a finite field. These cryptosystems are very powerful and attracted much attention; they created a new and very lively area of research (*elliptic curve cryptography*) and brought together researchers from pure mathematics (number theory, arithmetic geometry) and applied mathematics and engineering (cryptography). Similar as in the case of coding theory, this interaction proved fruitful for both sides, posing new problems and leading to many interesting practical and theoretical results.

The above-mentioned applications of function fields in constructing good long codes (due to Goppa and to Tsfasman-Vladut-Zink) and in constructing powerful cryptosystems via elliptic or hyperelliptic curves are now well-known. However, most mathematicians and engineers are not so familiar with many other, entirely different applications of function fields. To mention some of them: dense *sphere packings* in high-dimensional spaces; sequences with *low discrepancy*; *multiplication algorithms* in finite fields; the construction of *nonlinear codes* whose asymptotic parameters are even better than the Tsfasman-Vladut-Zink bound; the construction of good *hash families*. In all these cases the use of function fields leads to better results than those of classical approaches.

In this book we present five survey articles on some of these new developments. Most of the material is directly related to the interactions between function fields and their various applications; in particular the structure and the number of rational places of function fields are always of great significance. When choosing the topics, we also tried to focus on material which has not yet been presented in books or review articles. So, for instance, we did not include chapters about elliptic curve cryptography or about AG codes. There are numerous interconnections between the individual articles. Wherever applications are pointed out, a special effort has been made to present some background concerning their use. For the convenience of the reader, we have included an appendix which summarizes the basic definitions and results from the theory of algebraic function fields.

We give now a brief summary of the five chapters. More detailed descriptions are given in the introduction of each chapter.

Chapter 1. *Towers of Algebraic Function Fields over Finite Fields, by Arnaldo Garcia and Henning Stichtenoth.* In this chapter, the authors give a comprehensive survey of their work on explicit towers of algebraic function fields having many rational places. This concept provides a more elementary and explicit approach than class field towers and towers from modular curves. Towers with many rational places play a crucial role in many "asymptotic" constructions, such as error-correcting codes (Tsfasman-Vladut-Zink), low-discrepancy sequences (Niederreiter-Xing), and other applications of function fields in cryptography (see Chapter 2). Several examples of asymptotically good recursive towers are presented in detail. The proofs for the behaviour of the genus in wild towers are considerably simplified, compared to the proofs in the original papers.

Chapter 2. *Function Fields over Finite Fields and Their Applications to Cryptography, by Harald Niederreiter, Huaxiong Wang and Chaoping Xing.* This survey article focuses on several recent, less well-known applications of function fields – specifically, function fields with many rational places – in cryptography and combinatorics. Many of these applications are due to the authors. Among the topics are constructions of authentication codes, frameproof codes, perfect hash families, cover-free families and pseudorandom sequences of high linear complexity.

Chapter 3. *Artin-Schreier Extensions and Their Applications, by Cem Güneri and Ferruh Özbudak.* Extensions of function fields of Artin-Schreier type provide many examples of function fields having many rational places; this makes them very interesting for coding theory. In this chapter, several other applications of Artin-Schreier extensions are discussed, among them to the famous Weil bound for character sums, to weights of trace codes and to generalizations of cyclic codes.

Chapter 4. *Pseudorandom Sequences, by Alev Topuzoğlu and Arne Winterhof.* Various constructions of pseudorandom sequences are based on function fields, see Chapters 2 and 5. Therefore, some background material on the theory of pseudorandom sequences is presented in Chapter 4. In particular, the important concept of linear complexity and some related measures for the performance of pseudorandom sequences are discussed in this chapter.

Chapter 5. *Group Structure of Elliptic Curves over Finite Fields and Applications, by Ram Murty and Igor Shparlinski.* Motivated by applications of

elliptic curves to cryptography, the structure of the group of $\mathbb{F}_q$-rational points of an elliptic curve has attracted much attention. In particular it is an important feature for cryptographic applications if this group is cyclic or if it contains a large cyclic subgroup. The authors give a survey of recent results on this topic. Techniques from many branches of number theory and algebraic geometry are used in this chapter.

Each chapter begins with a detailed introduction, giving an overview of its contents and also giving some applications and motivation. It is clear that we do not want to present all proofs here. However, whenever possible, some typical proofs are provided. Our aim is to stimulate further research on some promising topics at the border line between pure and applied mathematics; therefore each chapter contains also an extensive list of references of recent research papers.

Some of the authors (A. Garcia, H. Niederreiter, I. Shparlinski, H. Stichtenoth, A. Winterhof and C. Xing) visited Sabancı University in Istanbul (Turkey) during the years 2002-2005, where they presented part of the material of this volume. It is our pleasure to thank our hosts at Sabancı University for their support and hospitality.

January 2006

Arnaldo Garcia, Henning Stichtenoth

Chapter 1

EXPLICIT TOWERS OF FUNCTION FIELDS OVER FINITE FIELDS

Arnaldo Garcia and Henning Stichtenoth

1. Introduction

The purpose of this review article is to serve as an introduction and at the same time, as an invitation to the theory of towers of function fields over finite fields. More specifically, we treat here the case of explicit towers; i.e., towers where the function fields are given by explicit equations. The asymptotic behaviour of the genus and of the number of rational places in towers are important features for applications to coding theory and to cryptography (cf. Chapter 2).

The interest in solutions of algebraic equations over finite fields has a long history in mathematics, especially when the equations define a one-dimensional object (a curve or, equivalently, a function field). The major result of this theory is the Hasse-Weil theorem which gives in particular an upper bound for the number of rational points in terms of the genus of the curve and of the cardinality of the finite field.

The Hasse-Weil theorem is equivalent to the validity of Riemann's Hypothesis for the Zeta function associated to the curve by E. Artin, in analogy with the classical situation in Number Theory. This upper bound of Hasse-Weil is sharp, and the curves attaining this bound are called maximal curves. Y. Ihara was the first to notice that the Hasse-Weil bound can be improved for curves of high genus, and he gave in particular an upper bound for the genus of maximal curves in terms of the cardinality of the finite field.

We will use here the language of function fields; i.e., we will be closer to Number Theory than to Algebraic Geometry. Hence the concepts we will deal with are function fields, field extensions, traces, norms, valuations, places, ratio-

A. Garcia and H. Stichtenoth (eds.), Topics in Geometry, Coding Theory and Cryptography, 1–58.

nal places, ramification indices and inertia degrees, tame and wild ramification, etc.

Denote by $\mathbb{F}_q$ the finite field of cardinality q. For a function field F over $\mathbb{F}_q$ we denote by $N(F)$ its number of $\mathbb{F}_q$-rational places and by $g(F)$ its genus. The upper bound of Hasse-Weil is

$$N(F) \leq 1 + q + 2\sqrt{q} \cdot g(F),$$

and Ihara showed that if the equality holds above then $2g(F) \leq q(q-1)$.

The following real number

$$A(q) := \limsup_{g(F)\to\infty} N(F)/g(F),$$

where F runs over all function fields over the field $\mathbb{F}_q$, was introduced by Ihara. It is of fundamental importance for the theory of function fields over a finite field, since it gives information about how many rational places a function field $F/\mathbb{F}_q$ of large genus can have.

In order to investigate the quantity $A(q)$, it is natural to study towers of function fields over $\mathbb{F}_q$; i.e., one considers sequences $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ of function fields F_i over $\mathbb{F}_q$ with $F_0 \subseteq F_1 \subseteq F_2 \subseteq \ldots$ with the property $g(F_i) \to \infty$. It can be seen easily that the limit of the tower

$$\lambda(\mathcal{F}) := \lim_{n\to\infty} N(F_n)/g(F_n)$$

always exists (see Section 3), and it is clear that the estimate below holds:

$$0 \leq \lambda(\mathcal{F}) \leq A(q).$$

As follows from the Hasse-Weil bound, we have that $A(q) \leq 2\sqrt{q}$. Based on Ihara's ideas, this bound was improved by Drinfeld-Vladut who showed that

$$A(q) \leq \sqrt{q} - 1.$$

But even before this bound of Drinfeld-Vladut was obtained, Ihara (and independently Tsfasman-Vladut-Zink) proved that if q is a square then $A(q) \geq \sqrt{q} - 1$. We thus have the equality

$$A(q) = \sqrt{q} - 1, \text{ if } q \text{ is a square.}$$

The proofs given by Ihara and Tsfasman-Vladut-Zink use the fact that certain modular curves have many rational points. However these curves are in general not easy to describe by explicit equations. Another approach due to J.-P. Serre uses class field theory in order to prove the existence of curves of arbitrary high genus with sufficiently many rational points. Also this construction is not

explicit. Our purpose here is to stimulate the investigation of explicit towers of function fields over finite fields; i.e., the function fields of the towers should be given explicitly by algebraic equations. The concept of explicit towers was first introduced in 1995 in the paper [20].

These notes are organized as follows:

- Section 2 contains basic concepts such as towers of function fields and their limits; recursive towers and the corresponding pyramids; tame and wild ramification in towers; linear codes and their parameters. In Section 2 one also finds:
  - The statement of the fundamental Hasse-Weil theorem (Theorem 2.3).
  - Serre's "explicit formulae" for bounding the number of rational places in a function field (Proposition 2.4).
  - The Drinfeld-Vladut bound (Theorem 2.5).
  - The Tsfasman-Vladut-Zink theorem connecting the asymptotics of function fields with the asymptotics of linear codes (Theorem 2.7).
  - Abhyankar's lemma which is an important tool to study the behaviour of the genus in recursive towers (Theorem 2.11).
- Section 3 is devoted to the investigation of the behaviour of the genus and of the number of rational places in towers of function fields over finite fields. It contains the following notions: the genus and the splitting rate of a tower; subtowers; asymptotically good and asymptotically optimal towers; ramification locus and splitting locus of a tower. In Section 2 one also finds:
  - A proof that the limit of a tower exists (Definition 3.4).
  - The limit of a subtower is at least as big as the limit of the tower (Proposition 3.6).
  - A sufficient condition which ensures that the genus of a tower is finite (Theorem 3.8 and Corollary 3.9).
  - A sufficient condition which ensures that a tower has finite ramification locus (Proposition 3.10).
  - A sufficient condition which ensures the existence of completely splitting places (Proposition 3.13).
  - A sufficient condition which ensures that a polynomial $f(X, Y)$ does define a recursive tower (Proposition 3.14).
- In Section 4 we investigate some interesting recursive tame towers, in which every step F_{n+1}/F_n is a Kummer extension. It contains the following subsections:

- Section 4.1: The optimal tower $\mathcal{T}_1$ over $\mathbb{F}_4$ which is given recursively by the equation $Y^3 = X^3/(X^2 + X + 1)$.
- Section 4.2: For $r \geq 2$ and $q = \ell^r$, the tower $\mathcal{T}_2$ over $\mathbb{F}_q$ which is defined recursively by the equation

$$Y^m = (X + 1)^m - 1 \text{ with } m = (q - 1)/(\ell - 1).$$

  This tower gives a very simple proof that $A(q) > 0$ if q is not a prime number.
- Section 4.3: For $q = p^2$ and p an odd prime number, the optimal tower $\mathcal{T}_3$ over $\mathbb{F}_q$ given recursively by the equation

$$Y^2 = (X^2 + 1)/2X.$$

  This tower corresponds to the modular curves $X_0(2^n)$ and it reveals some remarkable properties of Deuring's polynomial.

We also mention in Section 4 some other interesting towers from the papers [3, 14, 24, 33, 37].

- Section 5 is devoted to recursive wild towers. Especially interesting are wild towers where every step F_{n+1}/F_n is an Artin-Schreier extension, since some of the best towers known in the literature are of this type. We present here a simple method which allows a unified treatment of the genus behaviour of several towers of Artin-Schreier type (Lemma 5.1). Section 5 contains the following subsections:
  - Section 5.1: The optimal tower $\mathcal{W}_1$ over $\mathbb{F}_q$ with $q = \ell^2$, which is defined recursively by the equation

$$Y^\ell + Y = X^\ell/(X^{\ell-1} + 1).$$

    A complete proof for the optimality of the tower $\mathcal{W}_1$ is given and this proof is much simpler than the original one in [21].
  - Section 5.2: The optimal tower $\mathcal{W}_2$ over $\mathbb{F}_q$ with $q = \ell^2$, which is the first explicit example in the literature attaining the Drinfeld-Vladut bound [20].
  - Section 5.3: The optimal tower $\mathcal{W}_3$ over $\mathbb{F}_q$ with $q = \ell^2$, which is given recursively by the equation

$$(Y - 1)/Y^\ell = (X^\ell - 1)/X.$$

  - Section 5.4: The tower $\mathcal{W}_4$ over the field with eight elements, which is recursively given by

$$Y^2 + Y = X + 1 + 1/X.$$

This tower was first introduced in [30], and we give here a much simpler proof for its asymptotic behaviour.

- Section 5.5: The tower $\mathcal{W}_5$ over the cubic field $\mathbb{F}_q$ with $q = \ell^3$ which is defined recursively by the equation

$$Y^\ell - Y^{\ell-1} = 1 - X - X^{-(\ell-1)}.$$

The tower $\mathcal{W}_5$ generalizes the tower $\mathcal{W}_4$ of Section 5.4, and its limit $\lambda(\mathcal{W}_5) \geq 2(\ell^2 - 1)/(\ell + 2)$ gives the best known lower bound for Ihara's quantity $A(\ell^3)$.

- Section 6 contains some miscellaneous results on towers, among them a couple of conditions which easily show sometimes that a given tower is asymptotically bad (Theorem 6.2, Theorem 6.3 and Theorem 6.6). This section has the following subsections:

  - Section 6.1: In a tower $(F_0, F_1, F_2, \ldots)$ of function fields, the growth of the genus $g(F_n)$ depends on the behaviour of the different degrees of the extensions F_n/F_{n-1}. This interrelation is explored in Theorem 6.1 and Theorem 6.2 where sufficient conditions are given for the tower to have finite or infinite genus.
  - Section 6.2: Skew towers are asymptotically bad. This means: if the equation $f(X, Y) = 0$ which defines a recursive tower has unequal degrees in the variables X and Y, then the tower is asymptotically bad (Theorem 6.3).
  - Section 6.3: Here the concept of the dual tower of a recursive tower is introduced; if the ramification loci of the tower and of its dual tower are distinct, then the tower is bad (Theorem 6.6).
  - Section 6.4: This subsection contains a classification result on recursive towers defined by an Artin-Schreier equation of prime degree p of the form

$$Y^p + aY = \psi(X),$$

with $a \in \mathbb{F}_q^\times$ and with a rational function $\psi(X) \in \mathbb{F}_q(X)$. If such a tower is asymptotically good, then the function $\psi(X)$ must have a very specific form (Theorem 6.8).

2. Towers and Codes

Throughout this Chapter we denote by $\mathbb{F}_q$ the finite field with q elements and by $p = \mathrm{char}(\mathbb{F}_q)$ its characteristic. We are interested in function fields over $\mathbb{F}_q$ (briefly, $\mathbb{F}_q$-function fields) having many rational places with respect to the genus. For basic concepts and facts about algebraic function fields (such as the

definitions of function fields, places, divisors, rational places, genus, ramification, and Riemann-Roch theorem, Hurwitz genus formula, etc.) we refer to the Appendix or to [48]. For an $\mathbb{F}_q$-function field F we always assume throughout that $\mathbb{F}_q$ is the full constant field of F; i.e., that $\mathbb{F}_q$ is algebraically closed in F.

We denote by $N(F)$ the number of rational places and by $g(F)$ the genus of an $\mathbb{F}_q$-function field F, and we will be mainly interested in the behaviour of the ratio $N(F)/g(F)$ for function fields of large genus. To investigate this behaviour, Ihara [31] introduced the following quantity $A(q)$:

$$A(q) = \limsup_{g(F)\to\infty} N(F)/g(F),$$

where F runs over all function fields over $\mathbb{F}_q$. To deal with this quantity $A(q)$ one is naturally led to towers of function fields.

Definition 2.1. A *tower $\mathcal{F}$ over $\mathbb{F}_q$* (or an *$\mathbb{F}_q$-tower*) is an infinite sequence $\mathcal{F} = (F_0, F_1, F_2, ...)$ of function fields $F_i/\mathbb{F}_q$ such that

i) $F_0 \subsetneqq F_1 \subsetneqq F_2 \subsetneqq \ldots \subsetneqq F_n \subsetneqq \ldots$;

ii) each extension F_{n+1}/F_n is finite and separable;

iii) the genera satisfy $g(F_n) \to \infty$ as $n \to \infty$.

For an $\mathbb{F}_q$-tower $\mathcal{F}$ the following limit does exist (see Section 3):

$$\lambda(\mathcal{F}) = \lim_{n\to\infty} N(F_n)/g(F_n).$$

It is clear from the definitions that one has

$$0 \le \lambda(\mathcal{F}) \le A(q).$$

Definition 2.2. The real number $\lambda(\mathcal{F})$ is called the *limit* of the $\mathbb{F}_q$-tower $\mathcal{F}$. The tower $\mathcal{F}$ is called *asymptotically good* if it has a positive limit $\lambda(\mathcal{F}) > 0$. If $\lambda(\mathcal{F}) = 0$ then $\mathcal{F}$ is said to be *asymptotically bad*.

It is not easy in general to construct asymptotically good towers, and it is an even harder task to construct towers over finite fields with large limits. These are the main concerns of this Chapter.

We start by deriving an upper bound for $A(q)$, the so-called Drinfeld-Vladut bound. It states that

$$A(q) \le \sqrt{q} - 1. \tag{2.1}$$

This bound is then also an upper bound for the limit of towers; i.e., the following inequality holds for all $\mathbb{F}_q$-towers $\mathcal{F}$:

$$\lambda(\mathcal{F}) \le \sqrt{q} - 1.$$

In order to prove the upper bound in (2.1) for $A(q)$ we will need the following theorem due to Hasse and Weil, which is the central result of the theory of function fields over finite fields. It is equivalent to the validity of the Riemann Hypothesis in this context, cf. [48, p.169]. Hasse [29] proved it for elliptic function fields (i.e., for $g(F) = 1$), and Weil [61] proved it in the general case. For other proofs of the Hasse-Weil theorem we refer to [10] and [47].

We need some notation: for a function field $F/\mathbb{F}_q$, let $F^{(r)} := F \cdot \mathbb{F}_{q^r}$ be the constant field extension of F of degree r, and let $N_r(F) := N(F^{(r)})$ be the number of $\mathbb{F}_{q^r}$-rational places of the function field $F^{(r)}$ over $\mathbb{F}_{q^r}$. The Hasse-Weil theorem can be stated in the following form:

Theorem 2.3. (Hasse-Weil) *Let F be an $\mathbb{F}_q$-function field of genus $g(F) = g$. Then there exist complex numbers $\alpha_1, \alpha_2, \ldots, \alpha_{2g} \in \mathbb{C}$ with the following properties:*

i) They can be ordered in such a way that

$$\alpha_{g+i} = \bar{\alpha}_i \text{ for } i = 1, \ldots, g.$$

ii) The polynomial $L(t) := \prod_{i=1}^{2g}(1 - \alpha_i t)$ has integer coefficients. It follows in particular that each α_i is an algebraic integer.

iii) For all $r \geq 1$ we have

$$N_r(F) = q^r + 1 - \sum_{i=1}^{2g} \alpha_i^r.$$

iv) The absolute value of α_i is

$$|\alpha_i| = \sqrt{q} \text{ for } i = 1, \ldots, 2g.$$

The elements $\alpha_i^{-1} \in \mathbb{C}$ are the roots of the Zeta function associated to the function field $F/\mathbb{F}_q$. From item iv) and item iii) with $r = 1$, one gets the so-called Hasse-Weil bound

$$N(F) \leq q + 1 + 2\sqrt{q} \cdot g(F).$$

This bound implies immediately that $A(q) \leq 2\sqrt{q}$. For the proof of the Drinfeld-Vladut bound (2.1) we make use of Serre's "explicit formulae":

Proposition 2.4. (Serre) (see [49]). *Let $0 \neq h(X) \in \mathbb{R}[X]$ be a polynomial with non-negative coefficients and with $h(0) = 0$. Suppose that the associated rational function $H(X)$, which is defined as*

$$H(X) = 1 + h(X) + h(X^{-1}),$$

satisfies the condition

$$H(\beta) \geq 0 \text{ for all } \beta \in \mathbb{C} \text{ with } |\beta| = 1.$$

Then for any function field $F/\mathbb{F}_q$ we have

$$N(F) \leq 1 + \frac{h(q^{1/2})}{h(q^{-1/2})} + \frac{g(F)}{h(q^{-1/2})}.$$

Proof. Let F be a function field over $\mathbb{F}_q$ with $g(F) = g$, and let $\alpha_1, \alpha_2, \ldots, \alpha_{2g}$ be the associated complex numbers, ordered as in item i) of Theorem 2.3. For simplicity we set $N_r(F) = N_r$ and in particular $N(F) = N_1$. Write

$$h(X) = \sum_{r=1}^{m} c_r X^r,$$

with $c_r \in \mathbb{R}$ and $c_r \geq 0$ for all r. Then we have

$$N_r = 1 + q^r - \sum_{i=1}^{g} (\alpha_i^r + \bar{\alpha}_i^r),$$

by item iii) of Theorem 2.3; hence

$$\begin{aligned} N_r \cdot q^{-r/2} &= q^{-r/2} + q^{r/2} - \sum_{i=1}^{g} ((\alpha_i q^{-1/2})^r + (\bar{\alpha}_i q^{-1/2})^r) \\ &= q^{-r/2} + q^{r/2} - \sum_{i=1}^{g} (\beta_i^r + \bar{\beta}_i^r), \end{aligned} \tag{2.2}$$

with $\beta_i = \alpha_i q^{-1/2}$. By item iv) of Theorem 2.3, the complex numbers β_i have absolute value $|\beta_i| = 1$, so $\bar{\beta}_i = \beta_i^{-1}$. We now multiply Equation (2.2) by the coefficient c_r of $h(X)$ and we sum up for $r = 1, \ldots, m$, to obtain

$$\sum_{r=1}^{m} N_r \cdot c_r \cdot q^{-r/2} = h(q^{-1/2}) + h(q^{1/2}) + g - \sum_{i=1}^{g} H(\beta_i), \tag{2.3}$$

as follows from the definition of the rational function $H(X)$. We then rewrite Equation (2.3) as follows

$$N_1 \cdot h(q^{-1/2}) = h(q^{-1/2}) + h(q^{1/2}) + g - R,$$

with

$$R = \sum_{i=1}^{g} H(\beta_i) + \sum_{r=1}^{m} (N_r - N_1) c_r q^{-r/2}.$$

Since $N_r \geq N_1$, $c_r \geq 0$ and $H(\beta_i) \geq 0$, it follows that $R \geq 0$ and hence

$$N_1 \cdot h(q^{-1/2}) \leq h(q^{-1/2}) + h(q^{1/2}) + g.$$

□

Now we can prove:

Theorem 2.5. (Drinfeld-Vladut bound) (see [12]). *The following bound holds:*

$$A(q) \leq \sqrt{q} - 1.$$

In particular we have for any tower $\mathcal{F}$ over $\mathbb{F}_q$:

$$\lambda(\mathcal{F}) \leq \sqrt{q} - 1.$$

Proof. For each $m \in \mathbb{N}$ with $m \geq 2$ we consider the polynomial $h_m(X) \in \mathbb{R}[X]$ which is given by

$$h_m(X) = \sum_{r=1}^{m} \left(1 - \frac{r}{m}\right) \cdot X^r. \tag{2.4}$$

The key point of the proof of Theorem 2.5 is the following equality

$$h_m(X) = \frac{X}{(X-1)^2} \cdot \left(\frac{X^m - 1}{m} + 1 - X\right), \tag{2.5}$$

which we prove in Lemma 2.6 below. For the associated rational function $H_m(X)$ we then get

$$\begin{aligned} H_m(X) &= 1 + h_m(X) + h_m(X^{-1}) \\ &= 1 + \frac{X}{(X-1)^2}\left(\frac{X^m - 1}{m} + 1 - X\right) \\ &\quad + \frac{X^{-1}}{(X^{-1}-1)^2}\left(\frac{X^{-m} - 1}{m} + 1 - X^{-1}\right) \qquad (2.6) \\ &= \frac{X}{(X-1)^2} \cdot \frac{X^m + X^{-m} - 2}{m} \\ &= \frac{2 - (X^m + X^{-m})}{m(X-1)(X^{-1}-1)}. \end{aligned}$$

For any complex number $\beta \neq 1$ with $|\beta| = 1$, the numbers $(\beta - 1)(\beta^{-1} - 1)$ and $2 - (\beta^m + \beta^{-m})$ are positive real numbers. Hence the hypothesis in Proposition 2.4 is satisfied; i.e., we have $H_m(\beta) \geq 0$ for all $\beta \in \mathbb{C}$ with

$|\beta| = 1$. It follows from Proposition 2.4 that for any function field F over $\mathbb{F}_q$ with genus $g(F) > 0$ the following inequality holds for all $m \geq 2$

$$\frac{N(F)}{g(F)} \leq \frac{1}{h_m(q^{-1/2})} + \frac{1}{g(F)} \cdot \left(1 + \frac{h_m(q^{1/2})}{h_m(q^{-1/2})}\right). \tag{2.7}$$

Using again Equation (2.5) we see that

$$\lim_{m\to\infty} \frac{1}{h_m(q^{-1/2})} = \sqrt{q} - 1.$$

Let $\epsilon > 0$ be a real number and choose $n = n(\epsilon)$ such that

$$\frac{1}{h_n(q^{-1/2})} \leq \sqrt{q} - 1 + \epsilon/2.$$

Choose $g_0 = g_0(\epsilon, n)$ such that

$$\frac{1}{g_0} \cdot \left(1 + \frac{h_n(q^{1/2})}{h_n(q^{-1/2})}\right) < \epsilon/2.$$

Then we conclude from (2.7) with $m = n = n(\epsilon)$ that for all function fields $F/\mathbb{F}_q$ with $g(F) \geq g_0$,

$$\frac{N(F)}{g(F)} \leq (\sqrt{q} - 1 + \epsilon/2) + \epsilon/2 = \sqrt{q} - 1 + \epsilon.$$

□

We still have to prove Equation (2.5):

Lemma 2.6. *For all $m \geq 2$ the following identity holds:*

$$\sum_{r=1}^{m} \left(1 - \frac{r}{m}\right) \cdot X^r = \frac{X}{(X-1)^2} \cdot \left(\frac{X^m - 1}{m} + 1 - X\right).$$

Proof. We set

$$f(X) := \sum_{r=1}^{m} X^r = \frac{X^{m+1} - X}{X - 1};$$

then we have

$$\frac{X \cdot f'(X)}{m} = \sum_{r=1}^{m} \frac{r}{m} \cdot X^r,$$

and therefore

$$\sum_{r=1}^{m} \left(1 - \frac{r}{m}\right) \cdot X^r = f(X) - \frac{X \cdot f'(X)}{m}$$

$$= \frac{X}{X-1} \cdot (X^m - 1) - \frac{X}{m} \cdot \frac{(X-1)((m+1)X^m - 1) - (X^{m+1} - X)}{(X-1)^2}$$

$$= \frac{X}{(X-1)^2} \cdot \left(\frac{X^m - 1}{m} + 1 - X\right).$$

□

The interest in the quantity $A(q)$ also arose from applications of function fields to coding theory, cf. [48, 54]. The Tsfasman-Vladut-Zink theorem establishes a close connection between the asymptotics of $\mathbb{F}_q$-function fields (represented by the quantity $A(q)$) and the asymptotics of codes over $\mathbb{F}_q$. Some connections to cryptography are discussed in Chapter 2. For further connections to other areas we refer to [2, 40, 41, 44, 50, 52, 59].

Let us briefly recall the connection to coding theory. A linear code C over $\mathbb{F}_q$ of length $n = n(C)$ is a linear subspace of $\mathbb{F}_q^n$. The dimension $k = k(C)$ of C is its dimension as a vector space over $\mathbb{F}_q$. An important parameter of a linear code $C \neq \{0\}$ is its minimum distance $d = d(C)$, which is defined by

$$d = \min \{\mathrm{wt}(c) \mid c \in C \text{ and } c \neq 0\},$$

where for a nonzero vector $c = (c_1, \ldots, c_n) \in \mathbb{F}_q^n$ its weight $\mathrm{wt(c)}$ is given by

$$\mathrm{wt}(c) = \#\{i \mid 1 \leq i \leq n \text{ and } c_i \neq 0\}.$$

A linear code C over $\mathbb{F}_q$ of length $n = n(C)$, dimension $k = k(C)$ and minimum distance $d = d(C)$ is briefly called an $[n, k, d]$-code, and the integers n, k and d are called the parameters of the code. In order to compare codes of different lengths, one also introduces relative parameters of the code C as follows:

- the *transmission rate* $R(C)$, given by $R(C) = k(C)/n(C)$.
- the *relative minimum distance* $\delta(C)$, given by $\delta(C) = d(C)/n(C)$.

We then get a map $\varphi : \{\mathbb{F}_q\text{-linear codes}\} \to [0,1] \times [0,1]$ by setting

$$C \xrightarrow{\varphi} (\delta(C), R(C)).$$

For a real number $\delta \in [0,1]$ we consider the accumulation points of the image of the map φ on the vertical line $X = \delta$. The largest second coordinate of