



ELSEVIER

Available online at www.sciencedirect.com

SCIENCE @ DIRECT®

FINITE FIELDS
AND THEIR
APPLICATIONS

Finite Fields and Their Applications 11 (2005) 434–450

<http://www.elsevier.com/locate/ffa>

Asymptotics for the genus and the number of rational places in towers of function fields over a finite field

Arnaldo Garcia^{a,1}, Henning Stichtenoth^{b,c,*}

^a*IMPA-Instituto de Matematica Pura e Aplicada, Estrada Dona Castorina 110,
22460-320 Rio de Janeiro, RJ, Brazil*

^b*Universität Duisburg-Essen, Campus Essen, FB Mathematik, 45117 Essen, Germany*

^c*Sabancı University, MDBF, Orhanli, 34956 Tuzla, Istanbul, Turkey*

Received 2 November 2004; revised 31 March 2005

Communicated by G.L. Mullen

Available online 2 June 2005

Abstract

We discuss the asymptotic behaviour of the genus and the number of rational places in towers of function fields over a finite field.

© 2005 Elsevier Inc. All rights reserved.

Keywords: Tower of function fields; Genus; Rational places; Curves with many points

1. Introduction

Y. Ihara and Y.I. Manin discovered independently that the classical Hasse–Weil bound for the number of rational points on a curve over a finite field can be improved substantially if the genus of the curve is large with respect to the cardinality of the underlying finite field.

* Corresponding author. Universität Duisburg-Essen, Campus Essen, FB Mathematik, 45117 Essen, Germany. Fax: +49 201 183 2426.

E-mail addresses: garcia@impa.br (A. Garcia), stichtenoth@uni-essen.de, henning@sabanciuniv.edu (H. Stichtenoth).

¹A. Garcia was partially supported by PRONEX CNPq # 662408/1996-9 (Brazil).

Manin’s proof is based on coding theory. In his paper [13] with the title “What is the maximum number of points on a curve over \mathbb{F}_2 ?” he recalls Goppa’s construction of error-correcting codes using algebraic curves over a finite field (these codes are nowadays known as algebraic geometric codes), and he shows then that well-known bounds for the parameters of codes (like the Mc Eliece–Rodemich–Rumsey–Welch bound) imply an improvement of the Hasse–Weil upper bound

$$N(\chi) \leq q + 1 + 2g(\chi)\sqrt{q} \tag{1.1}$$

for $q = 2$ or 3 and large genus. Here χ denotes a non-singular, absolutely irreducible, projective algebraic curve over the finite field \mathbb{F}_q , and $N(\chi)$ (resp. $g(\chi)$) is the number of \mathbb{F}_q -rational points (resp. the genus) of χ .

While Manin’s arguments work only for $q = 2$ and $q = 3$, Ihara’s results hold for all q . In his short note “Some remarks on the number of rational points on algebraic curves over finite fields” he introduces, for any prime power q , the real number (see [11])

$$A(q) := \limsup_{\chi} N(\chi)/g(\chi),$$

where χ runs over all non-singular, absolutely irreducible, projective curves over the field \mathbb{F}_q with genus $g(\chi) > 0$. It follows immediately from the Hasse–Weil bound (1.1) that $A(q) \leq 2\sqrt{q}$. Ihara’s first result is that one has the much stronger estimate

$$A(q) \leq (\sqrt{8q + 1} - 1)/2. \tag{1.2}$$

The idea of his proof is very simple: Let $N_r(\chi)$ denote the number of rational points on χ over the field \mathbb{F}_{q^r} , for each $r \geq 1$. The Hasse–Weil bound for χ/\mathbb{F}_q and for χ/\mathbb{F}_{q^2} and the trivial observation that $N(\chi) = N_1(\chi)$ is less or equal to $N_2(\chi)$ yield easily the proof of Inequality (1.2).

It turns out to be much harder to obtain non-trivial lower bounds $C > 0$ for $A(q)$. To this end one has to provide an infinite sequence $(\chi_n)_{n \geq 0}$ of curves χ_n/\mathbb{F}_q such that $\lim_{n \rightarrow \infty} N(\chi_n)/g(\chi_n) \geq C$. Ihara proved in [11] already the fundamental result

$$A(q) \geq \sqrt{q} - 1 \quad \text{for square cardinalities } q, \tag{1.3}$$

by showing that certain (Shimura-) modular curves have sufficiently many \mathbb{F}_q -rational points, when q is a square. The Inequality (1.3) was again proved by Tsfasman et al. [17,18], and these authors showed that (1.3) implies an improvement of the Gilbert–Varshamov bound (which is a fundamental bound in coding theory) for all square cardinalities $q \geq 49$.

Refining Ihara’s method, Drinfeld and Vladut [3] improved Inequality (1.2) further and showed that

$$A(q) \leq \sqrt{q} - 1 \quad \text{for all } q. \tag{1.4}$$

In particular it follows from (1.3) and (1.4) that

$$A(q) = \sqrt{q} - 1, \quad \text{if } q \text{ is a square.} \tag{1.5}$$

For non-squares $q = p^{2m+1}$ much less is known about $A(q)$. Based on classified towers and the Golod–Shafarevic theorem, Serre [15] proved that

$$A(q) \geq c \log q > 0 \tag{1.6}$$

with some constant $c > 0$, independent of q (see also [14]). For $q = p^3$ (p a prime number), Zink [20] proved the lower bound

$$A(p^3) \geq \frac{2(p^2 - 1)}{p + 2}. \tag{1.7}$$

He obtained Inequality (1.7) by using degenerations of Shimura modular surfaces.

All above-mentioned results on lower bounds for $A(q)$ are based on deep methods from number theory and algebraic geometry (classified towers, classical modular curves, Shimura modular curves and surfaces, Drinfeld modular curves). Moreover, most sequences $(\chi_n)_{n \geq 0}$ of curves χ_n/\mathbb{F}_q with $\lim_{n \rightarrow \infty} N(\chi_n)/g(\chi_n) > 0$ which were constructed by those methods are far from being explicit. However, for applications (e.g., in coding theory or cryptography) one needs curves over \mathbb{F}_q with large genus and many rational points, which are given by explicit equations and such that their rational points are given explicitly by coordinates.

Following an attempt by Feng, Rao and Pellikaan, Garcia and Stichtenoth published in 1995 the first explicit example of a sequence $(\chi_n)_{n \geq 0}$ of curves over \mathbb{F}_q with $q = \ell^2$ and $\lim_{n \rightarrow \infty} N(\chi_n)/g(\chi_n) = \sqrt{q} - 1$, hence attaining the Drinfeld–Vladut bound (1.4) (see [6]). In subsequent papers, these ideas were further developed (see [7–9]). For explicit equations for certain modular curves we refer to [4]. Our approach is, in comparison with all others mentioned above, fairly elementary and explicit.

The aim of this paper is to explain our construction of infinite sequences of curves, by presenting one typical example in detail. We will use the language of algebraic function fields which is essentially equivalent to that of algebraic curves. We assume only some basic facts from the theory of function fields: the main tool is ramification theory in finite extensions.

2. Preliminaries and notations

Our reference for the theory of algebraic function fields is the book [16]. We fix now some notations which will be used throughout this paper:

- \mathbb{F}_q the finite field with cardinality q .
- p the characteristic of \mathbb{F}_q .
- F, E, F_n, \dots algebraic function fields (in one variable) over \mathbb{F}_q . We always assume that \mathbb{F}_q is the full constant field of F (resp. E, F_n, \dots).
- $g(F)$ the *genus* of the function field F .
- P, Q, \dots places of a function field.
- $\deg P$ the *degree* of the place P . In particular, the place is said to be *rational* (or \mathbb{F}_q -*rational*) if $\deg P = 1$.
- v_P the (normalized) discrete valuation associated with the place P .
- $\mathbb{P}(F)$ the set of places of F .
- $N(F) = N(F/\mathbb{F}_q)$ the number of \mathbb{F}_q -rational places of F .

Let E/F be a finite algebraic extension of function fields over \mathbb{F}_q . For any place $P \in \mathbb{P}(F)$ there are finitely many places $Q \in \mathbb{P}(E)$ lying above P . We then write $Q|P$ and denote by

- $e(Q|P)$ the *ramification index* of $Q|P$,
- $f(Q|P)$ the *inertia degree* of $Q|P$.

Then $\deg Q = f(Q|P) \deg P$, and we have the *fundamental equality*

$$\sum_{Q|P} e(Q|P)f(Q|P) = [E : F]. \tag{2.1}$$

The place $P \in \mathbb{P}(F)$ is said to be

- ramified* in E/F if $e(Q|P) > 1$ for some $Q|P$,
- wildly ramified* in E/F if $\gcd(e(Q|P), q) > 1$ for some $Q|P$,
- tame* in E/F if it is not wildly ramified,
- totally ramified* in E/F if $e(Q|P) = [E : F]$ for some $Q|P$ (it follows from

Eq. (2.1) that Q is then the only place above P and that $\deg Q = \deg P$, completely splitting in E/F if there are exactly $m = [E : F]$ distinct places $Q_1, \dots, Q_m \in \mathbb{P}(E)$ lying above P . Then $\deg Q_i = \deg P$ for all $Q_i|P$, as follows from Eq. (2.1).

From the fundamental equality (2.1) we also conclude an estimate for the number of rational places of E/\mathbb{F}_q :

$$t[E : F] \leq N(E) \leq [E : F]N(F), \tag{2.2}$$

where t is the number of rational places of F which are completely splitting in the extension E/F .

In addition we assume now that the extension E/F is separable. Then the following formula due to Hurwitz relates the genera of E and F :

$$2g(E) - 2 = [E : F](2g(F) - 2) + \deg \text{Diff}(E/F). \tag{2.3}$$

Here $\text{Diff}(E/F)$ denotes the *different* of E/F which is a divisor of the function field E/\mathbb{F}_q :

$$\text{Diff}(E/F) = \sum_{P \in \mathbb{P}(F)} \sum_{Q|P} d(Q|P)Q.$$

The integer $d(Q|P)$ is called the *different exponent* of $Q|P$, and Dedekind’s different theorem asserts that

$$d(Q|P) \geq e(Q|P) - 1 \tag{2.4}$$

with equality if and only if $Q|P$ is tame; i.e., if and only if the characteristic p does not divide $e(Q|P)$.

We will need some results about the behaviour of places in the composite of two function fields. So we consider now a finite extension E/F of the function field F/\mathbb{F}_q and two intermediate fields $F \subseteq E_i \subseteq E$ (for $i = 1, 2$) such that E is the composite field $E = E_1E_2$. Let $Q \in \mathbb{P}(E)$ be a place of E , and let $Q_i = Q|_{E_i}$ and $P = Q|_F$ be the places below Q in E_i and in F . Then the following results hold (see [16, Ch. III]).

(a) If $e(Q_1|P) = 1$ and $e(Q_2|P) = [E_2 : F]$, then it follows that $e(Q|Q_1) = e(Q_2|P) = [E : E_1]$ and $e(Q|Q_2) = 1$. Moreover, if \mathbb{F}_q is algebraically closed in E_1 , then it is also algebraically closed in the field E . (2.5)

(b) If P is completely splitting in E_2/F , then the place Q_1 splits completely in E/E_1 . (2.6)

The assertion in (2.5) is a special case of Abhyankar’s lemma (see [16, Prop. III.8.9]).

3. Basic theory of towers of function fields

As we pointed out in the Introduction, we want to construct explicitly sequences $(F_i)_{i \geq 0}$ of function fields F_i/\mathbb{F}_q such that $g(F_i) \rightarrow \infty$ and $\limsup_{i \rightarrow \infty} N(F_i)/g(F_i)$ is large. By the Drinfeld–Vladut bound (1.4) we always have that

$$\limsup_{i \rightarrow \infty} N(F_i)/g(F_i) \leq A(q) \leq \sqrt{q} - 1 \tag{3.1}$$

and any sequence with $\limsup_{i \rightarrow \infty} N(F_i)/g(F_i) > 0$ yields by (3.1) a non-trivial lower bound for $A(q)$. We will not consider arbitrary infinite sequences of function fields but we will focus on towers only.

Definition 3.1. A tower of function fields over \mathbb{F}_q is an infinite sequence $\mathcal{F} = (F_0, F_1, F_2, \dots)$ of function fields F_i/\mathbb{F}_q having the following properties:

- (i) $F_0 \subseteq F_1 \subseteq F_2 \subseteq \dots$, and for each $n \geq 1$ the extension F_n/F_{n-1} is separable of degree $[F_n : F_{n-1}] > 1$.
- (ii) $g(F_j) > 1$ for some $j \geq 0$.

It is clear by the Hurwitz genus formula (2.3) that $g(F_i) \rightarrow \infty$ for $i \rightarrow \infty$. As we will show, the limit $\lim_{i \rightarrow \infty} N(F_i)/g(F_i)$ exists for any tower $\mathcal{F} = (F_0, F_1, F_2, \dots)$ over \mathbb{F}_q .

Lemma 3.2. Let $\mathcal{F} = (F_i)_{i \geq 0}$ be a tower of function fields over \mathbb{F}_q . Then the two sequences

$$(N(F_i)/[F_i : F_0])_{i \geq 0} \quad \text{and} \quad (g(F_i)/[F_i : F_0])_{i \geq 0}$$

are convergent, with

$$0 \leq \lim_{i \rightarrow \infty} N(F_i)/[F_i : F_0] < \infty \quad \text{and} \quad 0 < \lim_{i \rightarrow \infty} g(F_i)/[F_i : F_0] \leq \infty.$$

Proof. (i) For $i \geq 1$ we have

$$\frac{N(F_i)/[F_i : F_0]}{N(F_{i-1})/[F_{i-1} : F_0]} = \frac{N(F_i)}{[F_i : F_{i-1}]N(F_{i-1})} \leq 1$$

by (2.2). The sequence $(N(F_i)/[F_i : F_0])_{i \geq 0}$ is therefore monotonously decreasing, hence convergent.

(ii) Choose $j \geq 0$ such that $g(F_j) > 1$. As in item (i) one shows that the sequence $((g(F_i) - 1)/[F_i : F_0])_{i \geq j}$ is monotonously increasing, using the Hurwitz genus formula (2.3). Hence the sequence $((g(F_i) - 1)/[F_i : F_0])_{i \geq 0}$ converges in $\mathbb{R} \cup \{\infty\}$, and the sequence $(g(F_i)/[F_i : F_0])_{i \geq 0}$ has the same limit. \square

Now the following definitions make sense:

Definition 3.3. For a tower $\mathcal{F} = (F_i)_{i \geq 0}$ of function fields over \mathbb{F}_q we define

$$v(\mathcal{F}/F_0) := \lim_{i \rightarrow \infty} N(F_i)/[F_i : F_0], \text{ the splitting rate of } \mathcal{F}/F_0$$

and

$$\gamma(\mathcal{F}/F_0) := \lim_{i \rightarrow \infty} g(F_i)/[F_i : F_0], \text{ the genus of } \mathcal{F}/F_0.$$

By Lemma 3.2 we have that

$$0 \leq v(\mathcal{F}/F_0) < \infty \text{ and } 0 < \gamma(\mathcal{F}/F_0) \leq \infty.$$

Corollary and Definition 3.4. *The limit of the tower \mathcal{F} ,*

$$\lambda(\mathcal{F}) := \lim_{i \rightarrow \infty} N(F_i)/g(F_i),$$

exists and one has

$$\lambda(\mathcal{F}) = v(\mathcal{F}/F_0)/\gamma(\mathcal{F}/F_0).$$

Hence it follows that $\lambda(\mathcal{F}) > 0$ if and only if $v(\mathcal{F}/F_0) > 0$ and $\gamma(\mathcal{F}/F_0) < \infty$.

Proof. Since

$$\frac{N(F_i)}{g(F_i)} = \frac{N(F_i)/[F_i : F_0]}{g(F_i)/[F_i : F_0]},$$

all assertions follow from Lemma 3.2. \square

The inequality $0 \leq \lambda(\mathcal{F}) \leq A(q)$ motivates the following definition:

Definition 3.5. The tower $\mathcal{F} = (F_i)_{i \geq 0}$ of function fields over \mathbb{F}_q is said to be

- asymptotically good*, if $\lambda(\mathcal{F}) > 0$;
- asymptotically bad*, if $\lambda(\mathcal{F}) = 0$;
- asymptotically optimal*, if $\lambda(\mathcal{F}) = A(q)$.

By Corollary 3.4 a tower is asymptotically good if and only if its splitting rate is positive and its genus is finite. Therefore we study these two properties separately and give simple sufficient conditions for them to hold.

Definition 3.6. Let $\mathcal{F} = (F_i)_{i \geq 0}$ be a tower over \mathbb{F}_q . We define two sets of places in the function field F_0 :

$$V(\mathcal{F}/F_0) := \{P \in \mathbb{P}(F_0) \mid P \text{ is ramified in } F_n/F_0 \text{ for some } n \geq 1\}, \text{ and}$$

$$S(\mathcal{F}/F_0) := \{P \in \mathbb{P}(F_0) \mid P \text{ is a rational place which splits completely in all extensions } F_n/F_0\}.$$

The set $V(\mathcal{F}/F_0)$ is called the *ramification locus* of \mathcal{F}/F_0 , and $S(\mathcal{F}/F_0)$ is the *completely splitting locus* of \mathcal{F}/F_0 .

Lemma 3.7. Suppose that $\mathcal{F} = (F_i)_{i \geq 0}$ is a tower over \mathbb{F}_q , whose completely splitting locus $S(\mathcal{F}/F_0)$ is non-empty. Then

$$v(\mathcal{F}/F_0) \geq t > 0,$$

with $t := |S(\mathcal{F}/F_0)|$.

Proof. Let $P \in S(\mathcal{F}/F_0)$; then there are $[F_n : F_0]$ rational places in $\mathbb{P}_0(F_n)$ lying above P , for any $n \geq 0$. Hence $N(F_n) \geq t[F_n : F_0]$, and the lemma follows immediately from the definition of $v(\mathcal{F}/F_0)$. \square

Now we give a sufficient condition for the genus $\gamma(\mathcal{F}/F_0)$ to be finite.

Lemma 3.8. Let $\mathcal{F} = (F_i)_{i \geq 0}$ be a tower over \mathbb{F}_q . Suppose that the following conditions hold:

- (1) the ramification locus $V(\mathcal{F}/F_0)$ is finite;
- (2) all extensions F_n/F_0 are tame.

Then the genus $\gamma(\mathcal{F}/F_0)$ is finite. More precisely,

$$\gamma(\mathcal{F}/F_0) \leq g(F_0) + (s - 2)/2,$$

where $s := \sum_{P \in V(\mathcal{F}/F_0)} \deg P$.

Proof. Let $P \in \mathbb{P}(F_0)$ and $Q \in \mathbb{P}(F_n)$ with $Q|P$. Then the different exponent $d(Q|P)$ is equal to $e(Q|P) - 1$, since the extension F_n/F_0 is tame. We obtain therefore

$$\begin{aligned} \deg \text{Diff}(F_n/F_0) &= \sum_{P \in V(\mathcal{F}/F_0)} \sum_{Q|P} d(Q|P) \deg Q \\ &\leq \sum_{P \in V(\mathcal{F}/F_0)} (\sum_{Q|P} e(Q|P) f(Q|P)) \deg P \\ &= [F_n : F_0]s \end{aligned}$$

with $s = \sum_{P \in V(\mathcal{F}/F_0)} \deg P$. The Hurwitz genus formula gives now

$$2g(F_n) - 2 \leq [F_n : F_0](2g(F_0) - 2 + s)$$

and the assertion of Lemma 3.8 follows. \square

Corollary 3.9. *Let $\mathcal{F} = (F_i)_{i \geq 0}$ be a tower over \mathbb{F}_q satisfying the following conditions:*

- (1) *the ramification locus $V(\mathcal{F}/F_0)$ is finite;*
- (2) *all extensions F_n/F_0 are tame;*
- (3) *the completely splitting locus $S(\mathcal{F}/F_0)$ is non-empty.*

Then the tower is asymptotically good.

4. A simple example

In this section we present in detail a very simple example of an optimal tower over the field with 9 elements. The analysis of this particular tower is typical for many other examples of asymptotically good towers, see Section 5 below. The tower $\mathcal{F} = (F_0, F_1, F_2, \dots)$ is defined as follows: $F_0 := \mathbb{F}_9(x_0)$ is the rational function field over \mathbb{F}_9 , and for all $n \geq 1$ let $F_n = F_{n-1}(x_n)$, where x_n satisfies the equation

$$x_n^2 = \frac{x_{n-1}^2 + 1}{2x_{n-1}}. \tag{4.1}$$

We must first show that the sequence of function fields (F_0, F_1, F_2, \dots) is in fact a tower over the field \mathbb{F}_9 ; in particular we have to show that $F_i \subsetneq F_{i+1}$ and that \mathbb{F}_9 is algebraically closed in F_i , for all $i \geq 0$. Before proving this, we study the “basic function field” corresponding to Eq. (4.1); this is the function field

$$F = \mathbb{F}_9(x, y), \quad \text{with } y^2 = \frac{x^2 + 1}{2x}. \tag{4.2}$$

We also fix an element $\delta \in \mathbb{F}_9$ with $\delta^2 = -1$. The following notation will be useful. Let E/\mathbb{F}_q be a function field and $Q \in \mathbb{P}(E)$ be a place of E . Let $z \in E$ and $\alpha \in \mathbb{F}_q \cup \{\infty\}$. Then for $\alpha \in \mathbb{F}_q$ we write $z = \alpha$ (at Q) if Q is a zero of $z - \alpha$, and $z = \infty$ (at Q) if Q is a pole of z .

Lemma 4.1. *Let $F = \mathbb{F}_9(x, y)$ be defined by Eq. (4.2). Then we have:*

- (i) *$[F : \mathbb{F}_9(x)] = [F : \mathbb{F}_9(y)] = 2$, and \mathbb{F}_9 is the full constant field of F .*
- (ii) *In the extension $F/\mathbb{F}_9(x)$, exactly the places with $x = 0$, $x = \infty$ and $x = \pm\delta$ are ramified.*
- (iii) *Let $Q \in \mathbb{P}(F)$ be the place with $x = \infty$ (by item (ii) there exists exactly one such place). Then $y = \infty$ (at Q), and Q is unramified in $F/\mathbb{F}_9(y)$.*

Proof. Clear from the theory of Kummer extensions of algebraic function fields (see [16, Prop. III.7.3]). \square

Corollary 4.2. *Let $F_0 = \mathbb{F}_9(x_0)$, and for all $n \geq 1$ let $F_n = F_{n-1}(x_n)$, where x_n satisfies Eq. (4.1). Then the following holds:*

- (i) *$[F_n : F_0] = 2^n$, for all $n \geq 0$.*

- (ii) The pole of x_0 is totally ramified in the extension F_n/F_0 , and \mathbb{F}_9 is algebraically closed in F_n .
- (iii) Let $Q \in \mathbb{P}(F_n)$ be the pole of x_0 in F_n (which is unique by item (ii)). Then Q is unramified in the extension $F_n/\mathbb{F}_9(x_n)$.

Proof. The case $n = 1$ is clear from Lemma 4.1, and we assume that the corollary holds for n . Let $Q \in \mathbb{P}(F_{n+1})$ be a pole of x_0 in F_{n+1} , and denote by Q_1, Q_2 and P the places below Q in the fields $F_n, \mathbb{F}_9(x_n, x_{n+1})$ and $\mathbb{F}_9(x_n)$. Then Q_1 is the pole of x_0 in F_n and (by induction hypothesis) $e(Q_1|P) = 1$, and P is the pole of x_n in $\mathbb{F}_9(x_n)$. Moreover Q_2 is a simple pole of x_{n+1} , and $Q_2|P$ is totally ramified. Now we apply (2.5) (Abhyankar’s lemma) and obtain all assertions for the case $n + 1$. \square

For the rest of this section we consider the sequence $\mathcal{F} = (F_0, F_1, F_2, \dots)$ of function fields over \mathbb{F}_9 which is defined by Eq. (4.1). Note that we have not proved yet that \mathcal{F} is indeed a tower, since we haven’t shown that $g(F_j) \geq 2$ for some j . Thus will be done in Lemma 4.3 below.

For $\alpha \in \mathbb{F}_9$ we denote by $P_\alpha \in \mathbb{P}(F_0)$ the zero of $x_0 - \alpha$ and by P_∞ the pole of x_0 in the rational function field $F_0 = \mathbb{F}_9(x_0)$. Recall that $\delta \in \mathbb{F}_9$ is an element with $\delta^2 = -1$.

Lemma 4.3. *With notations as above, we have:*

- (i) The four places P_0, P_∞, P_δ and $P_{-\delta}$ are totally ramified in the extension F_2/F_0 , and the genus of F_2 is at least $g(F_2) \geq 3$.
- (ii) In the extension F_5/F_0 also the places P_1 and P_{-1} are ramified.

Proof. (i) The assertion about ramification follows easily from Lemma 4.1 and (2.5), and then the Hurwitz genus formula (2.3) for the extension F_2/F_0 gives

$$2g(F_2) - 2 \geq 4(-2) + 4(4 - 1) = 4,$$

hence $g(F_2) \geq 3$. In fact it is easily shown that $g(F_2) = 3$.

(ii) Since we will not need this result, we leave the proof to the reader (use Lemma 4.1 again!). \square

We are now going to determine the ramification locus and the genus of the above tower (see Def. 3.6).

Lemma 4.4. *Let $\mathcal{F} = (F_i)_{i \geq 0}$ be the tower over \mathbb{F}_9 which is defined by Eq. (4.1). Then we have:*

- (i) The ramification locus of \mathcal{F}/F_0 is the set $V(\mathcal{F}/F_0) = \{P_\alpha \mid \alpha \in A\}$, with $A = \{0, \infty, \pm 1, \pm \delta\}$, and hence $|V(\mathcal{F}/F_0)| = 6$.
- (ii) The genus of \mathcal{F}/F_0 satisfies $\gamma(\mathcal{F}/F_0) \leq 2$.

Proof. (i) Let A be as above, and consider a place $P \in V(\mathcal{F}/F_0)$. Then for some $n \geq 1$ there exists a place $Q \in \mathbb{P}(F_n)$ such that $Q|P$ and Q is ramified over F_{n-1} . Considering F_n as the composite field of F_{n-1} and $\mathbb{F}_9(x_{n-1}, x_n)$ over $\mathbb{F}_9(x_{n-1})$, we conclude from (2.5) (Abhyankar’s lemma) that Q is ramified in $\mathbb{F}_9(x_{n-1}, x_n)/\mathbb{F}_9(x_{n-1})$, and then it follows from Lemma 4.1 that $x_{n-1} = 0$ or ∞ or $\pm\delta$ at Q . We have therefore $x_{n-1} = \alpha \in A$, for some $\alpha \in A$.

Suppose now that $x_i = \beta \in A$ at the place Q , for some $1 \leq i \leq n - 1$. If we can show that this implies $x_{i-1} = \gamma \in A$ at Q , it will follow that $V(\mathcal{F}/F_0)$ is contained in the set $\{P_\alpha | \alpha \in A\}$, and in particular that $|V(\mathcal{F}/F_0)| \leq 6$. Now we see from Eq. (4.1)

$$x_i^2 = \frac{x_{i-1}^2 + 1}{2x_{i-1}},$$

that

$$\begin{aligned} x_i = 0 \text{ at } Q &\Rightarrow x_{i-1} \in \{\pm\delta\} \text{ at } Q, \\ x_i = \infty \text{ at } Q &\Rightarrow x_{i-1} \in \{0, \infty\} \text{ at } Q, \\ x_i = \pm 1 \text{ at } Q &\Rightarrow x_{i-1} = 1 \text{ at } Q, \\ x_i = \pm\delta \text{ at } Q &\Rightarrow x_{i-1} = -1 \text{ at } Q. \end{aligned}$$

This proves our claim that $V(\mathcal{F}/F_0) \subseteq \{P_\alpha | \alpha \in A\}$. From item (ii) of Lemma 4.3 follows equality (but in the following we need only the inclusion “ \subseteq ”).

(ii) Follows from item (i) and Lemma 3.8. Note that we have just used that the cardinality of $V(\mathcal{F}/F_0)$ is at most 6. \square

Now we consider the completely splitting locus $S(\mathcal{F}/F_0)$ and the splitting rate $v(\mathcal{F}/F_0)$.

Lemma 4.5. *Let $\mathcal{F} = (F_i)_{i \geq 0}$ be the tower over \mathbb{F}_9 which is defined by Eq. (4.1). Then we have:*

- (i) *The completely splitting locus of \mathcal{F}/F_0 is $S(\mathcal{F}/F_0) = \{P_\beta \mid \beta \in B\}$, with $B = \{1 + \delta, 1 - \delta, -1 + \delta, -1 - \delta\}$, and hence $|S(\mathcal{F}/F_0)| = 4$.*
- (ii) *The splitting rate of \mathcal{F}/F_0 satisfies $v(\mathcal{F}/F_0) \geq 4$.*

Proof. (i) One checks that for $x = \beta \in B$ the equation

$$y^2 = \frac{x^2 + 1}{2x} = \frac{\beta^2 + 1}{2\beta}$$

has both roots in the set B (here one uses that $p = 3$). It follows by induction (using (2.6)) that the places P_β with $\beta \in B$ split completely in the tower \mathcal{F} . For $\alpha \in (\mathbb{F}_9 \cup \{\infty\}) \setminus B$, the place P_α belongs to the ramification locus $V(\mathcal{F}/F_0)$ by Lemma 4.4, and therefore $P_\alpha \notin S(\mathcal{F}/F_0)$. This proves item (i).

(ii) This follows from item (i) and Lemma 3.7. Note that here we have just used that $|S(\mathcal{F}/F_0)| \geq 4$. \square

Theorem 4.6. *The tower $\mathcal{F} = (F_i)_{i \geq 0}$ over the field \mathbb{F}_9 which is defined by Eq. (4.1) has the limit*

$$\lambda(\mathcal{F}) = 2 = \sqrt{9} - 1;$$

so it attains the Drinfeld–Vladut bound, and it is therefore an asymptotically optimal tower over \mathbb{F}_9 .

Proof. Since $\lambda(\mathcal{F}) = v(\mathcal{F}/F_0)/\gamma(\mathcal{F}/F_0)$ (see Corollary 3.4), we get from Lemmas 4.4 and 4.5 that $\lambda(\mathcal{F}) \geq 4/2 = 2$. On the other hand, the Drinfeld–Vladut bound (1.4) gives the estimate $\lambda(\mathcal{F}) \leq 2$, and so we obtain that $\lambda(\mathcal{F}) = 2$. \square

Remark 4.7. One can consider the tower \mathcal{F} given by Eq. (4.1) over the field \mathbb{F}_{p^2} , for any odd prime number p . Fixing an element $\delta \in \mathbb{F}_{p^2}$ with $\delta^2 = -1$ one can easily see that Lemma 4.4 holds also for $p > 3$, and hence that

$$\gamma(\mathcal{F}/F_0) \leq 2 \quad \text{for all } p \geq 3. \tag{4.3}$$

The determination of the completely splitting locus $S(\mathcal{F}/F_0)$ is for arbitrary prime numbers $p \geq 3$ much harder than in the special case $p = 3$. One can prove that

$$|S(\mathcal{F}/F_0)| = 2(p - 1). \tag{4.4}$$

It follows from (4.4) that the splitting rate $v(\mathcal{F}/F_0)$ satisfies $v(\mathcal{F}/F_0) \geq 2(p - 1)$, therefore

$$\lambda(\mathcal{F}) = v(\mathcal{F}/F_0)/\gamma(\mathcal{F}/F_0) \geq p - 1.$$

This lower bound for $\lambda(\mathcal{F})$ is equal to the Drinfeld–Vladut bound, and so the tower \mathcal{F} given by Eq. (4.1) is in fact asymptotically optimal over the quadratic fields \mathbb{F}_{p^2} , for all prime numbers $p \geq 3$.

The analysis of the set $S(\mathcal{F}/F_0)$ involves the so-called Deuring polynomial $H_p(X) \in \mathbb{F}_p[X]$ which is defined by

$$H_p(X) = \sum_{j=0}^{(p-1)/2} \binom{(p-1)/2}{j}^2 X^j.$$

The key point of this analysis is to show that all roots of the equation $H_p(\beta^4) = 0$ are in \mathbb{F}_{p^2} and that

$$S(\mathcal{F}/F_0) = \{P_\beta \mid H_p(\beta^4) = 0\}. \tag{4.5}$$

We proved these assertions for $p = 3$ in Lemma 4.5 (note that $H_3(X^4) = X^4 + 1$). For $p = 5$ one has $H_5(X^4) = X^8 - X^4 + 1 \in \mathbb{F}_5[X]$ and we leave it to the reader as an exercise to prove (4.5) in this case. For $p = 7$ one has to consider the polynomial $H_7(X^4) = X^{12} + 2X^8 + 2X^4 + 1$ over the field \mathbb{F}_{49} , and already in this case it is non-trivial to prove (4.5) directly. For general $p \geq 3$ we refer to [8, Section 5].

5. Further examples

In this section, we present some further examples of recursively defined towers \mathcal{F} over a finite field \mathbb{F}_q . We say that a tower $\mathcal{F} = (F_0, F_1, F_2, \dots)$ over \mathbb{F}_q is *defined recursively* by the equation

$$\varphi(y) = \psi(x) \tag{5.1}$$

(with rational functions $\varphi(Y), \psi(X)$ with coefficients in \mathbb{F}_q) if the following conditions hold:

- (i) $F_0 = \mathbb{F}_q(x_0)$ is the rational function field over \mathbb{F}_q , and for all $i \geq 0$,

$$F_{i+1} = F_i(x_{i+1}) \text{ with } \varphi(x_{i+1}) = \psi(x_i).$$

- (ii) $[F_{i+1} : F_i] = \deg \varphi(Y)$, for all $i \geq 0$.

For instance, the tower \mathcal{F} over \mathbb{F}_9 that we analyzed in Section 4, is recursively defined by the equation $y^2 = (x^2 + 1)/2x$.

Remark 5.1. Observe that it is not clear a priori, if an equation $\varphi(y) = \psi(x)$ defines a tower: it can happen that the equation $\varphi(Y) = \psi(x_i)$ becomes reducible over the field $F_i = \mathbb{F}_q(x_0, \dots, x_i)$ for some $i \geq 0$, or that the constant field of $\mathbb{F}_q(x_0, \dots, x_i)$ is larger than \mathbb{F}_q . Therefore one has to investigate in every specific case if a particular Eq. (5.1) actually defines a tower.

Example 5.2. (Towers of Fermat type, see Garcia and Stichtenoth [8] and Wulftange [19]). A tower over \mathbb{F}_q which is defined recursively by the equation

$$y^m = a(x + b)^m + c, \quad \text{with } a, b, c \in \mathbb{F}_q \text{ and } (m, q) = 1 \tag{5.2}$$

is called a *Fermat tower* over \mathbb{F}_q . One can show that Eq. (5.2) defines a tower if and only if $m > 1$ and $abc \neq 0$. The condition $(m, q) = 1$ ensures that Fermat towers are tame; i.e., all extensions F_n/F_0 are tame. For specific values of m, a, b and c , Fermat towers have nice properties, e.g.

- (a) If $q \equiv 1 \pmod m$ and $a = 1$, then the pole P_∞ of x_0 in F_0 splits completely in the Fermat tower \mathcal{F} ; hence $v(\mathcal{F}/F_0) \geq 1$, by Lemma 3.7.
- (b) There are examples of Fermat towers with finite ramification locus.

We point out two special cases of Fermat towers:

Example 5.3 (see Garcia et al. [9]). Let $q = p^e$ with $e > 1$ and $m = (q - 1)/(p - 1)$. Then the Fermat tower \mathcal{F}/\mathbb{F}_q which is defined recursively by the equation

$$y^m = 1 - (x + 1)^m \tag{5.3}$$

is asymptotically good; its limit satisfies $\lambda(\mathcal{F}) \geq 2/(q - 2)$. In fact, it is easily seen that in this specific case the ramification locus satisfies $V(\mathcal{F}/F_0) \subseteq \{P_\alpha | \alpha \in \mathbb{F}_q\}$ and hence it has cardinality at most q . Moreover the pole of x_0 splits completely in \mathcal{F} . We then conclude from Lemmas 3.7 and 3.8 that

$$\lambda(\mathcal{F}) \geq 2/(q - 2) > 0.$$

Note that Example 5.3 gives an easy proof for all non-prime q of the fact that $A(q) > 0$ (see the Introduction, Eq. (1.6)).

Example 5.4 (see Garcia et al. [9]). Let $\ell \geq 3$ and $q = \ell^2$ be a square. Then the Fermat tower \mathcal{F} over \mathbb{F}_q which is defined by

$$y^{\ell-1} = 1 - (x + 1)^{\ell-1} \tag{5.4}$$

is asymptotically good over \mathbb{F}_q , with $\lambda(\mathcal{F}) \geq 2/(\ell - 2)$. In fact, in this example one shows easily that the ramification locus satisfies $V(\mathcal{F}/F_0) \subseteq \{P_\alpha | \alpha \in \mathbb{F}_\ell\}$ and that the pole of x_0 splits completely over \mathbb{F}_{ℓ^2} .

Observe that Example 5.3 yields an optimal tower over \mathbb{F}_4 , and Example 5.4 yields an optimal tower over the field \mathbb{F}_9 . For other applications of Lemmas 3.7 and 3.8 we refer to [8].

Now we will consider some wild (i.e., non-tame) towers.

Example 5.5 (see Garcia and Stichtenoth [7]). Let $q = \ell^2$ be a square, and let $\mathcal{F} = (F_i)_{i \geq 0}$ be the tower over \mathbb{F}_q which is recursively defined by

$$y^\ell + y = x^\ell / (x^{\ell-1} + 1). \tag{5.5}$$

One can easily determine the ramification locus $V(\mathcal{F}/F_0)$ and the completely splitting locus $S(\mathcal{F}/F_0)$ in this case:

$$V(\mathcal{F}/F_0) = \{P_\infty\} \cup \{P_\alpha \mid \alpha^\ell + \alpha = 0\},$$

and

$$S(\mathcal{F}/F_0) = \{P_\beta \mid \beta \in \mathbb{F}_q \text{ and } \beta^\ell + \beta \neq 0\}.$$

It follows that the splitting rate satisfies $v(\mathcal{F}/F_0) \geq \ell^2 - \ell$. However, it is much harder to determine the genus $\gamma(\mathcal{F}/F_0)$, since in case of wild ramification one has in general no control on the different exponents. A very careful analysis of the ramification behaviour of this tower shows that $\gamma(\mathcal{F}/F_0) = \ell$, and therefore $\lambda(\mathcal{F}) \geq (\ell^2 - \ell)/\ell = \ell - 1$. Now it follows from the Drinfeld–Vladut bound that we have equality $\lambda(\mathcal{F}) = \ell - 1$; i.e., the tower \mathcal{F} which is defined by Eq. (5.5) is optimal over the field \mathbb{F}_{ℓ^2} .

We remark that the tower in Example 5.5 is closely related to the optimal towers over \mathbb{F}_q (with $q = \ell^2$) which were considered in [1,6]. Its interpretation as a Drinfeld modular tower was established in [5].

If q is not a square, it seems to be harder to find towers over \mathbb{F}_q with “large” limits. The tower in Example 5.3 is asymptotically good over \mathbb{F}_q for each non-prime q , but the limit $\lambda(\mathcal{F}) \geq 2/(q - 2)$ is rather small. We give now two other examples of wild towers with large limits, over finite fields with cubic cardinality.

Example 5.6 (see van der Geer and van der Vlugt [10]). This is a wild tower over the field with eight elements; it is recursively defined by the equation

$$y^2 + y = x + 1 + 1/x \quad \text{over } \mathbb{F}_8. \tag{5.6}$$

It is not difficult to determine the ramification locus $V(\mathcal{F}/F_0)$ and the completely splitting locus $S(\mathcal{F}/F_0)$:

$$V(\mathcal{F}/F_0) = \{P_\alpha \mid \alpha = \infty \text{ or } \alpha \in \mathbb{F}_4\} \quad \text{and} \quad S(\mathcal{F}/F_0) = \{P_\beta \mid \beta \in \mathbb{F}_8 \setminus \mathbb{F}_2\}.$$

The difficult part here is to investigate the behaviour of the ramified places, since they are all wildly ramified. One can show that $\gamma(\mathcal{F}/F_0) = 4$ and hence that $\lambda(\mathcal{F}) \geq 3/2$; this is just Inequality (1.7) for $p = 2$.

Example 5.7 (see Bezerra et al. [2]). The equation

$$(1 - y)/y^\ell = (x^\ell + x - 1)/x \tag{5.7}$$

defines a very interesting recursive tower \mathcal{F} over the field \mathbb{F}_q with $q = \ell^3$ (one can easily show that for $\ell = 2$ this tower is the same as the tower of Example 5.6). There are $\ell(\ell + 1)$ rational places of F_0/\mathbb{F}_q which split completely in the tower \mathcal{F} (but one does not see them as easily as in the towers of Examples 5.2–5.6). For $\ell \neq 2$ the extensions F_{i+1}/F_i in this tower are non-galois, and ramification is very complicated: some places are tamely ramified, others are wild, and the computation of the different

exponents is rather involved. The result of a careful analysis gives

$$\gamma(\mathcal{F}/F_0) = \ell(\ell + 2)/(2\ell - 2)$$

and therefore

$$\lambda(\mathcal{F}) = v(\mathcal{F}/F_0)/\gamma(\mathcal{F}/F_0) \geq 2(\ell^2 - 1)/(\ell + 2).$$

So the tower in Example 5.7 attains Zink’s lower bound (1.7) for $A(p^3)$ (in case $\ell = p$ is a prime), and it also proves the bound

$$A(\ell^3) \geq 2(\ell^2 - 1)/(\ell + 2) \text{ for all prime powers } \ell.$$

Problem 5.8. We finish this paper with an obvious problem: Find asymptotically good recursive towers with large limits over any finite field \mathbb{F}_q . For example, can one produce towers \mathcal{F} over \mathbb{F}_q with $q = p^{2n+1}$ such that the limit $\lambda(\mathcal{F})$ is close to a constant multiple of p^n ? How to find explicit equations leading to recursive towers \mathcal{F} with positive limit $\lambda(\mathcal{F}) > 0$ over prime fields \mathbb{F}_p ?

References

- [1] J. Bezerra, A. Garcia, A tower with non-Galois steps which attains the Drinfeld–Vladut bound, *J. Number Theory* 106 (2004) 142–154.
- [2] J. Bezerra, A. Garcia, H. Stichtenoth, An explicit tower of function fields over cubic finite fields and Zink’s lower bound, Manuscript, 2004.
- [3] V.G. Drinfeld, S.G. Vladut, Number of points of an algebraic curve, *Funct. Anal.* 17 (1983) 53–54.
- [4] N. Elkies, Explicit modular towers, Proceedings of the 35th Annual Allerton Conference on Communication, Control and Computing, Urbana, IL, 1997.
- [5] N. Elkies, Explicit towers of Drinfeld modular curves, in: C. Casacuberta et al. (Ed.), European Congress of Mathematics (Barcelona, 2000), vol. II, Birkhäuser, Basel, 2001.
- [6] A. Garcia, H. Stichtenoth, A tower of Artin–Schreier extensions of function fields attaining the Drinfeld–Vladut bound, *Invent. Math.* 121 (1995) 211–222.
- [7] A. Garcia, H. Stichtenoth, On the asymptotic behaviour of some towers of function fields over finite fields, *J. Number Theory* 61 (1996) 248–273.
- [8] A. Garcia, H. Stichtenoth, On tame towers over finite fields, *J. Reine Angew. Math.* 557 (2003) 53–80.
- [9] A. Garcia, H. Stichtenoth, M. Thomas, On towers and composita of towers of function fields over finite fields, *Finite Fields Appl.* 3 (1997) 257–274.
- [10] G. van der Geer, M. van der Vlugt, An asymptotically good tower of function fields over the field with eight elements, *Bull. London Math. Soc.* 34 (2002) 291–300.
- [11] Y. Ihara, Some remarks on the number of rational points of algebraic curves over finite fields, *J. Fac. Sci. Univ. Tokyo* 28 (1981) 721–724.
- [12] W.-C.W. Li, Modularity of asymptotically optimal towers of function fields, in: K.Q. Feng, H. Niederreiter, C.P. Xing (Eds.), Coding, Cryptography and Combinatorics, Birkhäuser, Basel, 2004, pp. 51–65.
- [13] Y.I. Manin, What is the maximal number of points on a curve over \mathbb{F}_2 ?, *J. Fac. Sci. Univ. Tokyo* 28 (1981) 715–720.

- [14] H. Niederreiter, C.P. Xing, *Rational Points on Curves Over Finite Fields: Theory and Applications*, Cambridge University Press, Cambridge, 2001.
- [15] J.-P. Serre, Sur le nombre des points rationnelles d'une courbe algébrique sur une corps fini, *C. R. Acad. Sci. Paris* 296 (1983) 397–402.
- [16] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer Universitext, Berlin, Heidelberg, New York, 1993.
- [17] M.A. Tsfasman, S.G. Vladut, *Algebraic–Geometric Codes*, Kluwer Academic Publishers, Dordrecht, Boston, London, 1991.
- [18] M.A. Tsfasman, S.G. Vladut, T. Zink, Modular curves, Shimura curves and Goppa codes, better than the Varshamov–Gilbert bound, *Math. Nachr.* 109 (1982) 21–28.
- [19] J. Wulftange, On the construction of some towers over finite fields, in: G.L. Mullen, et al. (Eds.), *Finite Fields and Applications*, Lecture Notes in Computer Science, vol. 2948, Springer, Berlin, 2004, pp. 154–165.
- [20] T. Zink, Degeneration of Shimura surfaces and a problem in coding theory, in: L. Budach (Ed.), *Fundamentals of Computation Theory*, Lecture Notes in Computer Science, vol. 199, Springer, Berlin, 1985, pp. 503–511.