ON TAME TOWERS OVER FINITE FIELDS

ARNALDO GARCIA AND HENNING STICHTENOTH

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

Subject classification. 11G, 11R, 14H

1. Introduction

The theory of equations over finite fields is a basic topic in classical number theory. Its foundations were laid (among others) by Fermat, Euler, Lagrange, Gauss and Galois. The object of the first investigations in this theory were congruences of the special form

$$y^2 \equiv f(x) \quad \text{(modulo a prime number)},$$

where $f(x)$ is a rational function with integer coefficients. Assuming an analogue of Riemann's hypothesis for the zeta function that he introduced, E. Artin conjectured an upper bound for the number of solutions for such congruences. The general solution of that conjecture was given by A. Weil (the elliptic case being settled before by H. Hasse), and it can be stated as follows: Let F be a function field over the finite field $\mathbb{F}_q$ with q elements, let $N(F)$ denote its number of $\mathbb{F}_q$-rational places and $g(F)$ denote its genus. Then the celebrated theorem of A. Weil [23] states that the following inequality holds

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

Ihara [13] noticed that one has a strict inequality above if $g(F) > \sqrt{q}(\sqrt{q}-1)/2$. Setting

$$N_q(g) = \max\{N(F) \mid F \text{ is a function field over } \mathbb{F}_q \text{ with } g(F) = g\}$$

and

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

one has the following result on the asymptotic behaviour of the number of $\mathbb{F}_q$-rational places (the so-called Drinfeld-Vladut bound [2]):

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

For tables describing the behaviour of $N_q(g)$ for small values of q and g we refer to [10]. Using class field theory, J.-P. Serre [17] showed that $A(q) > 0$, for any

Both authors were partially supported by GMD/CNPq and the first author also by PRONEX # 41.96.0883.00 (Brazil).

prime power q (see also [15]). Using modular curves, Ihara [13] (see also [20]) showed that

$$A(q^2) = q - 1, \quad \text{for any } q.$$

Using the above equality (for $q \geq 7$), Tsfasman-Vladut-Zink [20] observed that one can then construct an infinite sequence of algebraic geometric codes with limit parameters above the so-called Gilbert-Varshamov bound. In order to construct explicitly such an infinite sequence of codes, one needs an infinite sequence of algebraic function fields $(F_i)_{i\geq 0}$ over $\mathbb{F}_{q^2}$ that is given by explicit equations and satisfies $\lim_{i\to\infty} N(F_i)/g(F_i) = q - 1$, see [6], [7] and [3].

The subject of this paper is an analysis of the asymptotic behaviour of the number of $\mathbb{F}_q$-rational places in tame towers of function fields over $\mathbb{F}_q$. Section 2 gives basic definitions and results on towers over $\mathbb{F}_q$ and it points out that tame towers are specially interesting if they have the following two properties (see Theorem 2.24):

- The tower is of finite ramification type.
- The tower is completely splitting over $\mathbb{F}_q$.

In Section 3 we investigate those two properties for towers of Fermat type (see Definition 3.3), and in Section 4 we investigate them for towers of quadratic extensions. In Section 5 we show that the tower over $\mathbb{F}_{p^2}$ (p an odd prime number) defined recursively by the following equation

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

attains the Drinfeld-Vladut bound. This tower is related to the modular tower $X_0(2^n)$ whose recursive defining equation was given by Elkies [3] (see Remarks 5.9 and 5.10). Our proof is more elementary and also describes explicitly the set Ω of $\mathbb{F}_{p^2}$-rational places that are splitting completely in the tower. It has also led to two new properties of Deuring's polynomial $H(X) \in \mathbb{F}_q[X]$ (see Definition 5.4) whose roots describe the supersingular elliptic curves in Legendre form. These two properties are

1) The roots of $H(X)$ are fourth powers in $\mathbb{F}_{p^2}$.
2) $H(X^4) = X^{p-1} \cdot H\left(\left(\frac{X^2+1}{2X}\right)^2\right)$.

The proof of Property 1) is due to H. G. Rück; it is given in an appendix of this paper. It was noticed by M. Zieve that Property 1) also follows from Property 2) and the fact that the roots of $H(X)$ are in $\mathbb{F}_{p^2}$.

2. Towers over $\mathbb{F}_q$

In this section we discuss some general properties of towers of function fields that are independent of the specific representation of the tower.

Definition 2.1. A *tower over* $\mathbb{F}_q$ is an extension field $\mathcal{T} \supseteq \mathbb{F}_q$ having the following properties:

i) The transcendence degree of $\mathcal{T}/\mathbb{F}_q$ is one.

ii) The field $\mathbb{F}_q$ is algebraically closed in $\mathcal{T}$.
iii) The field extension $\mathcal{T}/\mathbb{F}_q$ is not finitely generated.

The notation $F < \mathcal{T}$ will always mean a function field F with $\mathbb{F}_q \subseteq F \subseteq \mathcal{T}$; i.e., $F/\mathbb{F}_q$ is a finitely generated field extension of $\mathbb{F}_q$ (with transcendence degree one) contained in the tower $\mathcal{T}$.

Any tower $\mathcal{T}$ over $\mathbb{F}_q$ can be described as follows: Choose a function field $F < \mathcal{T}$. Then there is an infinite sequence of function fields $F_i < \mathcal{T}$ such that

$$F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \dots \text{ and } \mathcal{T} = \bigcup_{i=0}^{\infty} F_i.$$

We say that $\mathcal{T}$ is *represented by the sequence* $(F_0, F_1, F_2, \dots)$. Note that the degrees $[F_{i+1} : F_i]$ are finite, since the extensions F_{i+1}/F_i are finitely generated and algebraic.

Definition 2.2. A tower $\mathcal{T}$ over $\mathbb{F}_q$ is said to be *separable* if there exists a function field $F < \mathcal{T}$ such that the (infinite) extension $\mathcal{T}/F$ is separable.

It is clear that a tower can be represented by various sequences of function fields. In order to compare two sequences $(F_0, F_1, F_2, \dots)$ and $(E_0, E_1, E_2, \dots)$ representing the same tower $\mathcal{T}$, the following simple observation is often useful: For each $i \geq 0$ there is some $j = j(i) \geq 0$ such that $F_i \subseteq E_j$. As an example how to use this reasoning, we state the following lemma.

Lemma 2.3. *For a tower $\mathcal{T}/\mathbb{F}_q$, the following conditions are equivalent:*
i) *The tower $\mathcal{T}$ is separable.*
ii) *There exists an element $x \in \mathcal{T} \setminus \mathbb{F}_q$ such that the extension $\mathcal{T}/\mathbb{F}_q(x)$ is separable.*
iii) *There exists a sequence $(F_0, F_1, F_2, \dots)$ representing $\mathcal{T}$ such that the extensions F_{i+1}/F_i are separable for almost all $i \geq 0$ (i.e., except for finitely many).*
iv) *For each sequence $(F_0, F_1, F_2, \dots)$ representing $\mathcal{T}$, almost all extensions F_{i+1}/F_i are separable.*

Proof. Obvious. □

Let $\mathcal{T}$ be any tower over $\mathbb{F}_q$ and let $(F_0, F_1, F_2, \dots)$ be any sequence representing the tower $\mathcal{T}$. The extensions F_n/F_0 can be splitted in two subextensions $F_0 \subseteq E_n \subseteq F_n$, where E_n/F_0 is separable and F_n/E_n is purely inseparable. The field E_n is uniquely determined by these conditions and it can be obtained as follows: Let $p = \text{char}(\mathbb{F}_q)$ and let p^{a_n} be the degree of inseparability of the extension F_n/F_0, then

$$E_n = F_n^{p^{a_n}}.$$

Setting $\mathcal{S} := \bigcup_{i=0}^{\infty} E_i$, we see that $\mathcal{S}/F_0$ is separable and $\mathcal{T}/\mathcal{S}$ is purely inseparable. Moreover the field E_n is isomorphic to F_n, for each $n \geq 0$. For this reason we will only consider separable towers over $\mathbb{F}_q$.

Let $g(F)$ denote the genus of a function field $F/\mathbb{F}_q$.

Proposition 2.4. *Let $\mathcal{T}$ be a separable tower over $\mathbb{F}_q$.*

i) *For any sequence $(F_0, F_1, F_2, \dots)$ representing $\mathcal{T}$, the sequence of rational numbers $(g(F_i)/[F_i : F_0])_{i \geq 0}$ is convergent in $\mathbb{R} \cup \{\infty\}$.*

ii) *Given two sequences $(F_0, F_1, F_2, \dots)$ and $(E_0, E_1, E_2, \dots)$ that represent $\mathcal{T}$, with $E_0 = F_0$, then*

$$\lim_{i \to \infty} \frac{g(F_i)}{[F_i : F_0]} = \lim_{i \to \infty} \frac{g(E_i)}{[E_i : E_0]}.$$

Proof. i) If $g(F_i) \leq 1$ for all $i \geq 0$, then $\lim_{i\to\infty}(g(F_i)/[F_i : F_0]) = 0$. Hence we can assume that $g(F_n) \geq 2$ for some $n \in \mathbb{N}$. Moreover we can assume that F_{i+1}/F_i is separable for all $i \geq n$, by Lemma 2.3. For $i \geq n$ we then have by Hurwitz' genus formula:

$$\begin{aligned} g(F_{i+1}) - 1 \ &= [F_{i+1} : F_i] \cdot (g(F_i) - 1) + \tfrac{1}{2} \deg \operatorname{Diff}(F_{i+1}/F_i) \\ &\geq \frac{[F_{i+1} : F_0]}{[F_i : F_0]} \cdot (g(F_i) - 1), \end{aligned}$$

where $\deg \operatorname{Diff}(E/F)$ denotes the degree of the different divisor. The sequence of rational numbers $((g(F_i) - 1)/[F_i : F_0])_{i \geq n}$ is therefore non-decreasing, hence the limit

$$\lim_{i \to \infty} \frac{g(F_i)}{[F_i : F_0]} = \lim_{i \to \infty} \frac{g(F_i) - 1}{[F_i : F_0]}$$

exists in $\mathbb{R} \cup \{\infty\}$.

ii) The case $g(F_i) \leq 1$ for all $i \geq 0$ is trivial, so we consider the case where $g(F_n) \geq 2$ and $\mathcal{T}/F_n$ is separable, for some $n \geq 0$. Let $H_i = F_i \cdot E_i$ be the compositum of F_i and E_i. For each $i \geq 0$, there exists some $j \geq i$ such that $F_i \subseteq H_i \subseteq F_j$, and as in the proof of item i), we see that the inequalities below hold (for all $i \geq n$):

$$\frac{g(F_i) - 1}{[F_i : F_0]} \leq \frac{g(H_i) - 1}{[H_i : F_0]} \leq \frac{g(F_j) - 1}{[F_j : F_0]}.$$

Since $F_0 = E_0$, it follows that

$$\lim_{i \to \infty} \frac{g(F_i)}{[F_i : F_0]} = \lim_{i \to \infty} \frac{g(H_i)}{[H_i : F_0]} = \lim_{i \to \infty} \frac{g(E_i)}{[E_i : E_0]}.$$

□

Definition 2.5. Let $\mathcal{T}$ be a separable tower over $\mathbb{F}_q$ and let F be a function field contained in $\mathcal{T}$. Choose a sequence $(F_0, F_1, F_2, \dots)$ representing $\mathcal{T}$ with $F_0 = F$. The we call

$$\gamma_F(\mathcal{T}) := \lim_{i \to \infty} \frac{g(F_i)}{[F_i : F]}$$

the *F-genus of the tower $\mathcal{T}$*.

Note that $\gamma_F(\mathcal{T})$ is well-defined as follows from Proposition 2.4, and moreover $0 \leq \gamma_F(\mathcal{T}) \leq \infty$. It is obvious from the proof of Proposition 2.4 that

$$\gamma_F(\mathcal{T}) = 0 \Leftrightarrow g(E) \leq 1 \text{ for each } E < \mathcal{T}.$$

The F-genus $\gamma_F(\mathcal{T})$ depends not only on the tower $\mathcal{T}$ but also on the function field F. The next lemma explains this dependence on the function field:

Lemma 2.6. *Let $\mathcal{T}$ be a separable tower over $\mathbb{F}_q$ and let $E, F < \mathcal{T}$ be two function fields contained in $\mathcal{T}$. Let $H < \mathcal{T}$ be such that $E \subseteq H$ and $F \subseteq H$. Then*

$$[H : F] \cdot \gamma_F(\mathcal{T}) = [H : E] \cdot \gamma_E(\mathcal{T}).$$

Proof. Choose a sequence $(H, H_1, H_2, \dots)$ representing $\mathcal{T}$; then the sequences $(F, H, H_1, H_2, \dots)$ and $(E, H, H_1, H_2, \dots)$ represent $\mathcal{T}$ as well. It follows from the definitions that

$$\gamma_F(\mathcal{T}) = \lim_{i\to\infty} \frac{g(H_i)}{[H_i : F]} = \frac{1}{[H : F]} \cdot \lim_{i\to\infty} \frac{g(H_i)}{[H_i : H]} = \frac{1}{[H : F]} \cdot \gamma_H(\mathcal{T}),$$

and similarly $\gamma_E(\mathcal{T}) = \gamma_H(\mathcal{T})/[H : E]$. Hence

$$\gamma_F(\mathcal{T}) \cdot [H : F] = \gamma_H(\mathcal{T}) = \gamma_E(\mathcal{T}) \cdot [H : E].$$

□

As a consequence of Lemma 2.6 we see that the property "$\gamma_F(\mathcal{T}) < \infty$" depends only on the tower $\mathcal{T}$; i.e., it is independent of the particular function field $F < \mathcal{T}$ chosen.

Definition 2.7. Let $\mathcal{S}$ and $\mathcal{T}$ be two towers over $\mathbb{F}_q$. We say that $\mathcal{S}$ is a *subtower* of $\mathcal{T}$ if we have $\mathcal{S} \subseteq \mathcal{T}$.

Lemma 2.8. *Let $\mathcal{S} \subseteq \mathcal{T}$ be two towers over $\mathbb{F}_q$. Assume that the tower $\mathcal{S}$ is separable and that the extension $\mathcal{T}/\mathcal{S}$ is also separable. Then $\mathcal{T}$ is a separable tower and, for each function field $F < \mathcal{S}$, one has*

$$\gamma_F(\mathcal{S}) \leq \gamma_F(\mathcal{T}).$$

Proof. We can assume that $F < \mathcal{S}$ is a function field such that $\mathcal{S}/F$ is separable. Then there exist two sequences $(F = F_0, F_1, F_2, \dots)$ resp. $(F = E_0, E_1, E_2, \dots)$ that represent $\mathcal{S}$ resp. $\mathcal{T}$, with $F_i \subseteq E_i$ for all $i \geq 0$. The lemma follows easily by considering these two sequences (cf. the proof of Proposition 2.4 i)). □

Proposition 2.9. *Let $\mathcal{S} \subseteq \mathcal{T}$ be two separable towers over $\mathbb{F}_q$ such that the extension $\mathcal{T}/\mathcal{S}$ is finite and separable. Then, for any function field $F < \mathcal{S}$, we have:*

$$\gamma_F(\mathcal{S}) < \infty \Leftrightarrow \gamma_F(\mathcal{T}) < \infty.$$

Proof. $\Leftarrow$: This implication follows from Lemma 2.8.
$\Rightarrow$: Since $\mathcal{T}/\mathcal{S}$ is finite and separable, there exists an element $z \in \mathcal{T}$ such that $\mathcal{T} = \mathcal{S}(z)$. Choose a sequence $(F = F_0, F_1, F_2, \dots)$ which represents $\mathcal{S}$ and let $E_i = F_i(z)$. Then the sequence $(E_0, E_1, E_2, \dots)$ represents the tower $\mathcal{T}$. The minimal polynomial of z over $\mathcal{S}$ has coefficients in F_n for some $n \geq 0$. Hence for

all $i \geq n$ we have $[E_i : F_i] = [E_n : F_n] = [\mathcal{T} : \mathcal{S}]$. By Castelnuovo's inequality [19, III.10.3] we have the estimate (for all $i \geq n$):

$$g(E_i) \leq [E_i : E_n] \cdot g(E_n) + [\mathcal{T} : \mathcal{S}] \cdot g(F_i) + ([E_i : E_n] - 1) \cdot ([\mathcal{T} : \mathcal{S}] - 1).$$

Setting $H := F_n$, we obtain

$$\frac{g(E_i)}{[E_i : H]} \leq \frac{g(E_n)}{[E_n : H]} + \frac{g(F_i)}{[F_i : H]} + 1.$$

Hence $\gamma_H(\mathcal{T}) \leq \gamma_H(S) + g(E_n)/[E_n : H] + 1$, and we have then shown that

$$\gamma_H(S) < \infty \Rightarrow \gamma_H(\mathcal{T}) < \infty.$$

Now the result follows from Lemma 2.6. □

Remark 2.10. i) The proof of Proposition 2.9 shows: The extension $\mathcal{T}/\mathcal{S}$ is of finite degree if and only if there is some function field $E < \mathcal{T}$ such that $\mathcal{T} = E \cdot \mathcal{S}$. This means that if $\mathcal{S}$ is represented by the sequence $(F_0, F_1, F_2, \dots)$ then $\mathcal{T}$ is represented by the sequence of composita $(E \cdot F_0, E \cdot F_1, E \cdot F_2, \dots)$.

ii) Under certain hypotheses one can prove a formula relating the F-genera $\gamma_F(\mathcal{S})$ and $\gamma_F(\mathcal{T})$, which is similar to the Hurwitz genus formula [9, Theorem 3.6].

Given a function field F in a tower $\mathcal{T}$, we will say that a property holds for each E/F (resp. for some E/F) if it holds for each (resp. for some) field E contained in the tower $\mathcal{T}$ and with a finite degree over the field F.

Definition 2.11. Let $\mathcal{T}$ be a separable tower over $\mathbb{F}_q$.

i) The tower $\mathcal{T}$ is called *totally ramified* if there exist a function field $F < \mathcal{T}$ and a place P of F which is totally ramified in each E/F.

ii) The tower $\mathcal{T}$ is called *tame* if there exists a function field $F < \mathcal{T}$ such that the extension E/F is tame for each E/F (i.e., all ramification indices are relatively prime to the characteristic). Otherwise, the tower $\mathcal{T}$ is said to be *wild.*

In this paper we will be dealing with tame towers. As for some interesting wild towers we refer to [6] and [7].

Definition 2.12. Let $\mathcal{T}$ be a separable tower over $\mathbb{F}_q$ and let $F < \mathcal{T}$. The *F-ramification locus* of $\mathcal{T}$ is defined to be

$$V_F(\mathcal{T}) := \{P \in \mathbb{P}_F \mid P \text{ ramifies in } E, \text{ for some } E/F\},$$

where $\mathbb{P}_F$ denotes the set of places of the function field F.

Note that in a purely inseparable extension of function fields over $\mathbb{F}_q$, all places are totally ramified. Hence the F-ramification locus is infinite if $\mathcal{T}/F$ is not separable.

Lemma 2.13. *Let $\mathcal{T}$ be a separable tower over $\mathbb{F}_q$ and let $E, F < \mathcal{T}$ be function fields such that $\mathcal{T}/F$ and $\mathcal{T}/E$ are both separable extensions. Then one has:*

$$V_F(\mathcal{T}) \text{ is finite } \Leftrightarrow V_E(\mathcal{T}) \text{ is finite.}$$

Proof. We can assume that $F \subseteq E < \mathcal{T}$ where E/F is a finite separable extension (otherwise, we replace E by the compositum $H = E \cdot F$). As only finitely many places are ramified in E/F, the assertion

$$V_F(\mathcal{T}) \text{ is finite } \Leftrightarrow V_E(\mathcal{T}) \text{ is finite}$$

is now obvious. □

Definition 2.14. A separable tower $\mathcal{T}$ over $\mathbb{F}_q$ is said to be of *finite ramification type* if there exists a function field $F < \mathcal{T}$ such that $V_F(\mathcal{T})$ is a finite set.

Proposition 2.15. *If $\mathcal{T}$ is a tame tower over $\mathbb{F}_q$ of finite ramification type, then $\gamma_H(\mathcal{T}) < \infty$ for each $H < \mathcal{T}$. More precisely: if $F < \mathcal{T}$ is a function field in $\mathcal{T}$ such that E/F is tame, for each E/F, then we have:*

$$\gamma_F(\mathcal{T}) \leq g(F) + \frac{s-2}{2},$$

where

$$s := \sum_{P \in V_F(\mathcal{T})} \deg P.$$

Proof. Let E/F be a tame extension of finite degree. The degree of the different of E/F is bounded by $\deg \mathrm{Diff}(E/F) \leq s \cdot [E:F]$, therefore

$$2g(E) - 2 \leq [E:F](2g(F) - 2 + s).$$

Dividing both sides of this inequality by $2 \cdot [E:F]$ and letting $[E:F] \to \infty$, we obtain the desired result. □

For a function field $F/\mathbb{F}_q$ we denote by $N(F)$ its number of $\mathbb{F}_q$-rational places.

Proposition 2.16. *Let $\mathcal{T}$ be a tower over $\mathbb{F}_q$.*

i) *For any sequence $(F_0, F_1, F_2, \dots)$ representing $\mathcal{T}$, the sequence of rational numbers $(N(F_i)/[F_i : F_0])_{i \geq 0}$ is non-increasing and, in particular, it is convergent.*

ii) *Given two sequences $(F_0, F_1, F_2, \dots)$ and $(E_0, E_1, E_2, \dots)$ that represent $\mathcal{T}$, with $E_0 = F_0$, then*

$$\lim_{i \to \infty} \frac{N(F_i)}{[F_i : F_0]} = \lim_{i \to \infty} \frac{N(E_i)}{[E_i : E_0]}.$$

Proof. i) Follows from the fact that $N(F_{i+1}) \leq [F_{i+1} : F_i] \cdot N(F_i)$.

ii) Similar to the proof of Proposition 2.4 ii). □

We can now give the following definition:

Definition 2.17. For a tower $\mathcal{T}$ over $\mathbb{F}_q$ and a function field $F < \mathcal{T}$, we call

$$\nu_F(\mathcal{T}) := \lim_{i \to \infty} \frac{N(F_i)}{[F_i : F_0]}$$

the *F-splitting rate* of the tower $\mathcal{T}$, where $(F_0, F_1, F_2, \dots)$ is any sequence representing $\mathcal{T}$ with $F_0 = F$.

It follows immediately that the F-splitting rate of $\mathcal{T}$ satisfies

$$0 \leq \nu_F(\mathcal{T}) \leq N(F).$$

As for the F-genus $\gamma_F(\mathcal{T})$ (cf. Lemma 2.6) one shows the following lemma on the splitting rate.

Lemma 2.18. *Let $\mathcal{T}$ be a tower over $\mathbb{F}_q$, and let $E, F, H < \mathcal{T}$ be function fields with $E \subseteq H$ and $F \subseteq H$. Then we have:*

$$[H : F] \cdot \nu_F(\mathcal{T}) = [H : E] \cdot \nu_E(\mathcal{T}).$$

Definition 2.19. A tower $\mathcal{T}$ over $\mathbb{F}_q$ is said to be *completely splitting* if there exist a function field $F < \mathcal{T}$ and a $\mathbb{F}_q$-rational place P of F which splits completely in each E/F.

The next lemma is trivial (observe Lemma 2.18).

Lemma 2.20. *Let $\mathcal{T}/\mathbb{F}_q$ be a completely splitting tower. Then for each $H < \mathcal{T}$ on has $\nu_H(\mathcal{T}) > 0$. More precisely, choose $F < \mathcal{T}$ such that the integer*

$$t := \{P \in \mathbb{P}_F \mid \deg P = 1 \text{ and } P \text{ splits completely in } E, \text{ for each } E/F\}$$

is strictly positive. Then we have

$$\nu_F(\mathcal{T}) \geq t.$$

In what follows we will only consider separable towers $\mathcal{T}$ over $\mathbb{F}_q$ whose F-genus $\gamma_F(\mathcal{T})$ is strictly positive for some (hence for all) $F < \mathcal{T}$. Recall that this condition holds if and only if there is a function field $H < \mathcal{T}$ with genus $g(H) > 1$. From Lemmas 2.6 and 2.18 we have (for all $E, F < \mathcal{T}$) the equality

$$\frac{\nu_F(\mathcal{T})}{\gamma_F(\mathcal{T})} = \frac{\nu_E(\mathcal{T})}{\gamma_E(\mathcal{T})}.$$

Hence we define:

Definition 2.21. For a separable tower $\mathcal{T}$ over $\mathbb{F}_q$, we call the real number

$$\lambda(\mathcal{T}) := \nu_F(\mathcal{T})/\gamma_F(\mathcal{T})$$

the *limit of the tower $\mathcal{T}$*, with F being any function field contained in $\mathcal{T}$.

In other words, for any sequence $(F_0, F_1, F_2, \dots)$ representing $\mathcal{T}$ the limit $\lambda(\mathcal{T})$ is given by

$$\lambda(\mathcal{T}) = \lim_{i \to \infty} N(F_i)/g(F_i).$$

Theorem 2.22. *For any separable tower $\mathcal{T}$ over $\mathbb{F}_q$ one has*

$$0 \leq \lambda(\mathcal{T}) \leq \sqrt{q} - 1.$$

Proof. The assertion $\lambda(\mathcal{T}) \geq 0$ is trivial; the upper bound $\lambda(\mathcal{T}) \leq \sqrt{q} - 1$ is the well-known Drinfeld-Vladut bound, cf. [2]. □

Definition 2.23. A separable tower $\mathcal{T}$ over $\mathbb{F}_q$ is said to be *asymptotically good* (resp. *asymptotically bad*, resp. *asymptotically optimal*) if $\lambda(\mathcal{T}) > 0$ (resp. $\lambda(\mathcal{T}) = 0$, resp. $\lambda(\mathcal{T}) = \sqrt{q} - 1$).

It is clear from Definition 2.21 that the tower $\mathcal{T}$ is asymptotically good if and only if $\nu_F(\mathcal{T}) > 0$ and $\gamma_F(\mathcal{T}) < \infty$ (for some $F < \mathcal{T}$). The next theorem gives a lower bound for the limit $\lambda(\mathcal{T})$ which will often be used in the next sections, see also [9].

Theorem 2.24. *Let $\mathcal{T}$ be a tame tower over $\mathbb{F}_q$ having the following properties:*

1) *The tower $\mathcal{T}$ is of finite ramification type.*
2) *The tower $\mathcal{T}$ is completely splitting.*

Then the tower $\mathcal{T}$ is asymptotically good. More precisely, let $F < \mathcal{T}$ be a function field such that $\mathcal{T}/F$ is tame and completely splitting. Then the limit $\lambda(\mathcal{T})$ satisfies the inequality

$$\lambda(\mathcal{T}) \geq \frac{2t}{2g(F) + s - 2},$$

where t is the number of $\mathbb{F}_q$-rational places of F that split completely in $\mathcal{T}/F$, and s is the degree of the F-ramification locus $V_F(\mathcal{T})$; i.e.,

$$s = \sum_{P \in V_F(\mathcal{T})} \deg P.$$

Proof. Follows from Proposition 2.15 and Lemma 2.20. □

Definition 2.25. A tower $\mathcal{T}$ over $\mathbb{F}_q$ is said to be *Galois* if there is some function field $F < \mathcal{T}$ such that the (infinite) extension $\mathcal{T}/F$ is Galois.

Being Galois is a strong property of a tower. For instance, one can prove a partial converse of Theorem 2.24 for Galois towers.

Theorem 2.26. *Let $\mathcal{T}$ be an asymptotically good Galois tower over $\mathbb{F}_q$. Then the tower $\mathcal{T}$ is completely splitting and it is of finite ramification type.*

Proof. Choose a function field $F < \mathcal{T}$ such that $\mathcal{T}/F$ is Galois, and assume that the F-ramification locus $V_F(\mathcal{T})$ is infinite. Then there exists an infinite sequence of distinct places $P_1, P_2, \ldots$ of F and a sequence of Galois extensions $E_i/F (i = 1, 2, \ldots)$ such that the sequence $(F, E_1, E_2, \ldots)$ represents the tower $\mathcal{T}$, and moreover each of the places $P_1, \ldots, P_n$ is ramified in the extension E_n/F.

For $i = 1, \ldots, n$ let Q_i be a place of E_n above P_i, and denote by e_i (resp. f_i, resp. d_i) the ramification index (resp. the residue class degree, resp. the different exponent) of Q_i over P_i. Then the degree of the different of E_n/F satisfies

$$\begin{aligned} \deg \mathrm{Diff}(E_n/F) &\geq \sum_{i=1}^{n} \frac{[E_n : F]}{e_i f_i} \cdot d_i \cdot \deg Q_i \\ &= [E_n : F] \cdot \sum_{i=1}^{n} \frac{d_i}{e_i} \deg P_i \geq [E_n : F] \cdot \sum_{i=1}^{n} \frac{e_i - 1}{e_i} \\ &\geq \frac{n}{2} \cdot [E_n : F]. \end{aligned}$$

The Hurwitz genus formula for the extension E_n/F now gives

$$2g(E_n) - 2 \geq [E_n : F] \cdot (2g(F) - 2) + \frac{n}{2} \cdot [E_n : F].$$

Dividing by $[E_n : F]$ and letting $n \to \infty$, we obtain that $\gamma_F(\mathcal{T}) = \infty$, hence $\lambda(\mathcal{T}) = \nu_F(\mathcal{T})/\gamma_F(\mathcal{T}) = 0$. This contradiction proves that the tower $\mathcal{T}$ is of finite ramification type.

Now we want to show that the tower is completely splitting. Again we choose a function field $F < \mathcal{T}$ such that $\mathcal{T}/F$ is Galois, and we choose a sequence $(F, E_1, E_2, \dots)$ which represents the tower $\mathcal{T}$ and has the property that all extensions E_i/F are Galois. Let M denote the set of $\mathbb{F}_q$-rational places of F. For $P \in M$ and for each $i \geq 1$, let $a_i(P)$ denote the number of $\mathbb{F}_q$-rational places of E_i lying above P, and set

$$\mu(P) := \lim_{i \to \infty} \frac{a_i(P)}{[E_i : F]}.$$

Then the F-splitting rate $\nu_F(\mathcal{T})$ is given by

$$\nu_F(\mathcal{T}) = \sum_{P \in M} \mu(P).$$

Since we have that $\nu_F(\mathcal{T}) > 0$, we conclude that there is a $\mathbb{F}_q$-rational place P of F with $\mu(P) > 0$. This place P cannot be inert in any extension E_i/F, hence

$$a_i(P) = \frac{[E_i : F]}{e_i},$$

where e_i is the ramification index of the place P in E_i/F. Thus

$$0 < \mu(P) = \lim_{i \to \infty} \frac{1}{e_i}.$$

It follows that there is some $n \geq 0$ such that $e_i = e_n$, for each $i \geq n$, so the places of E_n lying above P are $\mathbb{F}_q$-rational, and they split completely in the tower. □

Remark 2.27. Let $\mathcal{T}$ be a Galois tower over $\mathbb{F}_q$ with the property that for some function field $F < \mathcal{T}$ the infinite extension $\mathcal{T}/F$ is abelian. Then the tower is asymptotically bad, see [5] and [4].

3. Towers of Fermat type

Many interesting towers $\mathcal{T}$ over $\mathbb{F}_q$ can be defined recursively in the following manner:

Definition 3.1. We say that the tower $\mathcal{T}$ is *defined by the equation* $\psi(y) = \varphi(x)$ if $\psi(y)$ and $\varphi(x)$ are two rational functions over $\mathbb{F}_q$ such that

$$\mathcal{T} = \mathbb{F}_q(x_0, x_1, x_2, \dots) \quad \text{with} \quad \psi(x_{i+1}) = \varphi(x_i) \quad \text{for all} \quad i \geq 0.$$

Of course, setting $F_i = \mathbb{F}_q(x_0, \dots , x_i)$ one has that the sequence $(F_0, F_1, F_2, \dots)$ represents the tower $\mathcal{T}$.

Remark 3.2. For a rational function $\varphi(x) = f(x)/g(x)$, where $f(x), g(x) \in \mathbb{F}_q[x]$ with $(f(x), g(x)) = 1$, we define its degree as

$$\deg \varphi = \max\{\deg f, \deg g\}.$$

We will always consider here towers over $\mathbb{F}_q$ that are defined recursively by an equation $\psi(y) = \varphi(x)$ with balanced degrees (i.e., with $\deg \psi = \deg \varphi$). Otherwise the tower is easily seen to be asymptotically bad (see [8]).

In this section we will consider towers $\mathcal{F}$ over $\mathbb{F}_q$ which are defined by the equation

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

Definition 3.3. A tower $\mathcal{F}$ over $\mathbb{F}_q$ defined by Equation $(*)$ is said to be a *tower of Fermat type* or a *Fermat tower* if the following Hypothesis (A) holds.

Hypothesis (A). For each $i \geq 0$, the field $\mathbb{F}_q$ is algebraically closed in F_i and we have $[F_{i+1} : F_i] = m$.

We first give two results showing that Equation $(*)$ defines a Fermat tower under certain conditions.

Proposition 3.4. *Let $a, b, c \in \mathbb{F}_q^*$ with*

$$a \cdot b^m + c = 0, \ \textit{where } (m, q) = 1.$$

Then Equation $(*)$ defines a tower of Fermat type; i.e., we have that Hypothesis (A) does hold.

Proof. Consider the equation

$$y^m = a(x+b)^m + c, \ \text{with } a, b, c \in \mathbb{F}_q^* \text{ and } ab^m + c = 0.$$

We then see that $x = 0$ is a simple zero of the right hand side and hence it ramifies totally in the function field extension $\mathbb{F}_q(x, y)/\mathbb{F}_q(x)$. The unique place above $x = 0$ is then a simple zero for the function y. Since the tower is defined recursively by Equation $(*)$, we then conclude that the place of F_0 corresponding to $x_0 = 0$ is totally ramified in F_n, for each $n \geq 1$. Now Hypothesis (A) follows immediately. □

In case $a \cdot b^m + c \neq 0$, the following result gives sufficient conditions for Hypothesis (A) to hold. We denote by $\bar{\mathbb{F}}_q$ an algebraic closure of $\mathbb{F}_q$.

Proposition 3.5. *Let $a, b, c \in \mathbb{F}_q^*$ with $a \cdot b^m + c \neq 0$. Suppose that there exist two elements $\alpha, \beta \in \bar{\mathbb{F}}_q$ such that*

$$a \cdot (\alpha + b)^m + c = 0 \ \ \textit{and} \ \ a \cdot (\beta + b)^m + c = \alpha^m = \beta^m.$$

Then Equation $(*)$ defines a Fermat tower; i.e., we have that Hypothesis (A) does hold.

Proof. If follows from the assumptions that

1) We have $\alpha \neq 0, \beta \neq 0$ and $\alpha \neq \beta$.

2) There is a unique place P_i of F_i with $x_0(P_i) = x_1(P_i) = \ldots = x_i(P_i) = \beta$.
3) There is a unique place Q_i of F_i such that $x_0(Q_i) = x_1(Q_i) = \ldots = x_{i-1}(Q_i) = \beta$ and $x_i(Q_i) = \alpha$.
4) The place Q_i is a simple zero of $a \cdot (x_i + b)^m + c$.

By induction we then see that the place Q_i ramifies totally in the extension F_{i+1}/F_i, for each $i \geq 0$. Now Hypothesis (A) follows immediately. □

Remark 3.6. Equation $(*)$ does not define recursively a tower if $abc = 0$. However it seems plausible that Hypothesis (A) does hold whenever one has that $abc \neq 0$.

We give now a very simple condition which implies that many towers of Fermat type are completely splitting.

Proposition 3.7. *Suppose that Equation $(*)$ defines a Fermat tower $\mathcal{F}$ over $\mathbb{F}_q$ and assume moreover that*

$$q \equiv 1 \bmod m \quad \textit{and} \quad a = a_1^m, \ \textit{for some } a_1 \in \mathbb{F}_q^*.$$

Then the tower $\mathcal{F}$ is completely splitting; more precisely, the pole of x_0 in F_0 splits completely in the tower $\mathcal{F}$.

Proof. Let Q be a pole of x_0 in F_i, then Q is also a pole of x_i. We obtain from Equation $(*)$ that

$$\left(\frac{x_{i+1}}{x_i}\right)^m = a\left(1 + \frac{b}{x_i}\right)^m + \frac{c}{x_i^m}.$$

Modulo Q this yields the congruence

$$\left(\frac{x_{i+1}}{x_i}\right)^m \equiv a \bmod Q,$$

which has m distinct roots in $\mathbb{F}_q$ as follows from the assumptions. Thus the place Q splits completely in the extension F_{i+1}/F_i. □

Now we investigate some Fermat towers which are of finite ramification type.

Proposition 3.8. *Let l be a power of the characteristic of $\mathbb{F}_q$ and let $q = l^r$ with $r \geq 2$. Assume that the equation*

$$y^{(q-1)/(l-1)} = a \cdot (x + b)^{(q-1)/(l-1)} + c, \ \textit{with } a, c \in \mathbb{F}_l^* \textit{ and } b \in \mathbb{F}_q^*,$$

defines a Fermat tower $\mathcal{F}$ over $\mathbb{F}_q$. Then the tower $\mathcal{F}$ is of finite ramification type; more precisely, one has that

$$V_{F_0}(\mathcal{F}) = \{P \in \mathbb{P}_{F_0} \mid x_0(P) = \alpha \textit{ for some } \alpha \in \mathbb{F}_q\}.$$

Proof. We set for simplicity $m := (q-1)/(l-1)$. Note that the map $\gamma \mapsto \gamma^m$ (for $\gamma \in \mathbb{F}_q$) is the norm map from $\mathbb{F}_q$ to $\mathbb{F}_l$. Consider a place P of F_0 which is ramified in the tower $\mathcal{F}$. Then there exists an index $n \geq 0$ and a place Q of F_n lying above P which ramifies in the extension F_{n+1}/F_n. Since

$$x_{n+1}^m = a(x_n + b)^m + c,$$

the ramification theory of Kummer extensions (see [19, III.7.]) shows that

$$a(x_n(Q)+b)^m + c = 0.$$

Since $a, c \in \mathbb{F}_l \setminus \{0\}$, we conclude that $(x_n(Q)+b)^m \in \mathbb{F}_l$ and hence that $x_n(Q) \in \mathbb{F}_q$, since m is the norm exponent. In the same manner we obtain from the equation

$$x_n^m = a(x_{n-1}+b)^m + c$$

that $x_{n-1}(Q) \in \mathbb{F}_q$ and then, by induction, that $x_0(Q) \in \mathbb{F}_q$. As the place Q lies above P, we have then shown that $x_0(P) = x_0(Q) = \alpha \in \mathbb{F}_q$. □

Proposition 3.9. *Let l be a power of the characteristic of $\mathbb{F}_q$ and let $q = l^r$ with $r \geq 1$. Then the equation*

$$y^{l-1} = -(x+b)^{l-1} + 1, \text{ with } b \in \mathbb{F}_l^*,$$

defines a Fermat tower $\mathcal{F}$ over $\mathbb{F}_q$. Moreover this tower $\mathcal{F}$ is of finite ramification type and we have that

$$V_{F_0}(\mathcal{F}) = \{P \in \mathbb{P}_{F_0} \mid x_0(P) = \alpha, \text{ for some } \alpha \in \mathbb{F}_l\}.$$

Proof. The assertion that the equation defines a Fermat tower follows from Proposition 3.4. The assertion about the ramification locus $V_{F_0}(\mathcal{F})$ follows with the same reasonings used in the proof of Proposition 3.8. □

Combining the above results we obtain some asymptotically good towers of Fermat type (see also [9]).

Theorem 3.10. *Let l be a power of the characteristic of $\mathbb{F}_q$ and let $q = l^r$ with $r \geq 2$. Assume that the equation*

$$y^{(q-1)/(l-1)} = a \cdot (x+b)^{(q-1)/(l-1)} + c, \text{ with } a, c \in \mathbb{F}_l^* \text{ and } b \in \mathbb{F}_q^*,$$

defines a Fermat tower $\mathcal{F}$ over $\mathbb{F}_q$ (e.g., see Proposition 3.4). Then the tower $\mathcal{F}$ is asymptotically good and its limit satisfies

$$\lambda(\mathcal{F}) \geq \frac{2}{q-2}.$$

Proof. Since $m = (q-1)/(l-1)$ is the norm exponent in the extension $\mathbb{F}_q/\mathbb{F}_l$ and since $a \in \mathbb{F}_l^*$ we have

$$a = a_1^m, \text{ for some } a_1 \in \mathbb{F}_q^*.$$

The result now follows from Propositions 3.7 and 3.8. □

Theorem 3.11. *Let l be a power of the characteristic of $\mathbb{F}_q$ and let $q = l^r$ with $r \geq 1$. Assume that*

$$r \equiv 0 \bmod 2 \quad \text{or} \quad l \equiv 0 \bmod 2.$$

Then the equation

$$y^{l-1} = -(x+b)^{l-1} + 1, \text{ with } b \in \mathbb{F}_l^*,$$

defines an asymptotically good Fermat tower $\mathcal{F}$ over $\mathbb{F}_q$, and its limit satisfies

$$\lambda(\mathcal{F}) \geq \frac{2}{l-2}.$$

Proof. The congruence $r \equiv 0 \bmod 2$ (resp. $l \equiv 0 \bmod 2$; i.e., the characteristic is equal to 2) ensures that $a = -1$ is a $(l-1)$-th power in $\mathbb{F}_q$. The result now follows from Propositions 3.7 and 3.9. □

We now give an example that illustrates the use of Proposition 3.5.

Example 3.12. *Let p be a prime number satisfying*

$$p \equiv 3, 5 \text{ or } 6 \pmod 7,$$

and let $q = p^r$ with $r \geq 1$. Then the equation

$$y^{p+1} = (x+1)^{p+1} - 2$$

defines a Fermat tower $\mathcal{F}$ over $\mathbb{F}_q$. If $r \equiv 0 \bmod 2$, this tower $\mathcal{F}$ is asymptotically good over $\mathbb{F}_q$.

Proof. The polynomials $x^2 + x + 2$ and $x^2 - x + 2$ are both irreducible over $\mathbb{F}_p$. This follows easily from the assumption $p \equiv 3, 5$ or $6 \bmod 7$, using quadratic reciprocity. Choose $\alpha, \beta \in \mathbb{F}_{p^2}$ such that

$$\alpha^2 + \alpha + 2 = \beta^2 - \beta + 2 = 0.$$

The trace (resp. norm) of α in the extension $\mathbb{F}_{p^2}/\mathbb{F}_p$ is then given by $\alpha^p + \alpha$ (resp. α^{p+1}), and since $x^2 + x + 2$ is the minimal polynomial of α over $\mathbb{F}_p$ it follows that $\alpha^p + \alpha = -1$, $\alpha^{p+1} = 2$ and similarly that $\beta^p + \beta = 1$ and $\beta^{p+1} = 2$. We conclude that

$$(\alpha+1)^{p+1} - 2 = \alpha^{p+1} + \alpha^p + \alpha + 1 - 2 = 0, \text{ and}$$

$$(\beta+1)^{p+1} - 2 = \beta^{p+1} + \beta^p + \beta + 1 - 2 = 2 = \alpha^{p+1} = \beta^{p+1}.$$

It now follows from Proposition 3.5 that $\mathcal{F}$ is indeed a Fermat tower. The tower $\mathcal{F}$ is asymptotically good over $\mathbb{F}_{p^2}$ (i.e., for $r = 2$), since $m = p + 1$ is the norm exponent in the extension $\mathbb{F}_{p^2}/\mathbb{F}_p$, as follows from Theorem 3.10. Hence the tower $\mathcal{F}$ is also asymptotically good for any $r \geq 1$ with $r \equiv 0 \bmod 2$. □

Variants of this proof show that the equation $y^{p+1} = (x+1)^{p+1} - 2$ defines a Fermat tower for many other prime numbers p.

Remark 3.13. As the constants $a, b, c \in \mathbb{F}_q^*$ vary, the ramification structures of the Fermat towers $\mathcal{F}$ given by the equations $y^m = a(x+b)^m + c$ may be quite different: If $a \cdot b^m + c = 0$ then the tower is totally ramified, as follows from Proposition 3.4. On the other hand it is easily seen that the tower is not totally ramified in case $a \cdot b^m + c \neq 0$.

4. Towers of quadratic extensions

As we have seen in Theorem 2.24, tame towers $\mathcal{T}$ are particularly interesting if the following two properties hold:

1) The tower $\mathcal{T}$ is of finite ramification type.
2) The tower $\mathcal{T}$ is completely splitting.

Here we will consider those two properties in towers of quadratic extensions; i.e., towers $\mathcal{T}$ over $\mathbb{F}_q$ which are defined recursively by a quadratic equation (see Definition 3.1)

$$y^2 = \varphi(x), \quad \text{with } \varphi(x) \in \mathbb{F}_q(x).$$

We will always assume that the characteristic satisfies $p \geq 3$, and hence towers of quadratic extensions are tame. In this section we will give several explicit examples of towers of quadratic extensions having finite ramification locus, and for some of them we also show that they are completely splitting.

We start with a result which ensures in many cases that an equation of the form $y^2 = \varphi(x)$ defines a tower over $\mathbb{F}_q$. This result will be used in the examples of this section without mentioning it explicitly.

Proposition 4.1. *Suppose that the characteristic satisfies $p \geq 3$. Let $f_1(x)$ and $f_2(x)$ be polynomials over $\mathbb{F}_q$ with $\deg f_1(x) = 1 + \deg f_2(x)$. Then the equation*

$$y^2 = f_1(x)/f_2(x)$$

defines a tower $\mathcal{T} = \mathbb{F}_q(x_0, x_1, x_2, \dots)$ over $\mathbb{F}_q$, where $x_{i+1}^2 = f_1(x_i)/f_2(x_i)$ for all $i \geq 0$. Setting $F_i = \mathbb{F}_q(x_0, \dots, x_i)$ one has that $[F_{i+1} : F_i] = 2$. The place $x_0 = \infty$ is totally ramified in all extensions F_i/F_0.

Proof. Similar to the proof of Proposition 3.4. □

Since we are mainly interested in the construction of asymptotically good towers, we will apply the above Proposition mostly in the case where $\deg f_1(x) = 2$ and $\deg f_2(x) = 1$ (see Remark 3.2).

Next we give a result ensuring completely splitting.

Proposition 4.2. *Let $p \geq 3$ and let $\beta \in \mathbb{F}_q$ be such that $\beta^2 \neq 1$. Consider the tower $\mathcal{T}$ over $\mathbb{F}_q$ which is defined recursively by the equation*

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

Then the two places $x_0 = \pm\beta$ are completely splitting in the tower $\mathcal{T}$.

Proof. The assertion follows immediately from the equations below:

$$\frac{\beta(\beta+\beta^2)}{\beta+1} = \beta^2 = \frac{(-\beta)(-\beta+\beta^2)}{-\beta+1}.$$

□

Notation: It will be convenient to introduce the following notations:
1) For a polynomial $f(x) \in \mathbb{F}_q[x]$, let

$$\mathfrak{z}(f(x)) := \{\alpha \in \bar{\mathbb{F}}_q \mid f(\alpha) = 0\}$$

denote the set of zeros of $f(x)$ in the algebraic closure $\bar{\mathbb{F}}_q$ of $\mathbb{F}_q$.
2) For an irreducible polynomial $h(x) \in \mathbb{F}_q[x]$, we identify the set $\mathfrak{z}(h(x)) \subseteq \bar{\mathbb{F}}_q$ with the place P of the rational function field $F_0 = \mathbb{F}_q(x_0)$ that corresponds to $h(x_0)$. In particular, we have that $\deg P = \deg h(x) = \#\mathfrak{z}(h(x))$.

Next we give an example of an asymptotically good tower of quadratic extensions over the field $\mathbb{F}_9$.

Example 4.3. *Let $p = 3$ and consider the tower $\mathcal{T}$ over $\mathbb{F}_q$ defined recursively by the equation*

$$y^2 = \frac{x(x-1)}{x+1}.$$

This tower is of finite ramification type, and we have that

$$s := \sum_{P \in V_{F_0}(\mathcal{T})} \deg P = 8.$$

The limit $\lambda(\mathcal{T})$ over the field $\mathbb{F}_9$ with 9 elements satisfies $\lambda(\mathcal{T}) \geq 2/3$.

Proof. Suppose we have already shown that $s = 8$. Let $\beta \in \mathbb{F}_9$ be such that $\beta^2 = -1$. It follows from Proposition 4.2 that the places $x_0 = \pm\beta$ are completely splitting in the tower $\mathcal{T}$ over $\mathbb{F}_9$. It then follows from Theorem 2.24 that its limit over $\mathbb{F}_9$ satisfies

$$\lambda(\mathcal{T}) \geq \frac{4}{s-2} = \frac{2}{3}.$$

We show now that $s = 8$ and, in particular, that the tower $\mathcal{T}$ in Example 4.3 is of finite ramification type in characteristic 3. So let $P \in \mathbb{P}_{F_n}$ be a place with $x_n(P)^2 = 1$ that ramifies in F_{n+1}/F_n. If Q denotes the place of F_{n-1} below P and setting $\alpha := x_{n-1}(Q) \in \bar{\mathbb{F}}_q$, we must have:

$$1 = \frac{\alpha(\alpha-1)}{\alpha+1}, \quad \text{hence } \alpha^2 - 2\alpha - 1 = 0.$$

Again, if R denotes the restriction of Q to F_{n-2} and setting $\beta := x_{n-2}(R) \in \bar{\mathbb{F}}_q$, we must have:

$$\alpha^2 = \frac{\beta(\beta-1)}{\beta+1} = 2\alpha + 1, \quad \text{hence } \beta^2 - (2\alpha+2)\beta - (2\alpha+1) = 0.$$

Using that the characteristic is $p = 3$, we see that

$$0 = \beta^2 - (2\alpha+2)\beta - (2\alpha+1) = (\beta - (\alpha+1))^2.$$

Again, if S denotes the restriction of the place R to the field F_{n-3} and setting $\gamma := x_{n-3}(S) \in \bar{\mathbb{F}}_q$, we have:

$$\beta^2 = (\alpha+1)^2 = \frac{\gamma(\gamma-1)}{\gamma+1} = -(2\alpha+1), \quad \text{hence } (\gamma+\alpha)^2 = 0.$$

The computations above show that the F_0-ramification locus of the tower $\mathcal{T}$ is given by

$$V_{F_0}(\mathcal{T}) = \{0, \infty, \pm 1, \pm\alpha, \pm(\alpha+1)\},$$

where $\alpha \in \bar{\mathbb{F}}_q$ is a root of the polynomial $x^2 - 2x - 1$. This finishes the proof that $s = 8$. □

Remark 4.4. i) It can be shown, in Example 4.3, that the limit $\lambda(\mathcal{T})$ is equal to $2/3$ (over $\mathbb{F}_9$), and that $\lambda(\mathcal{T}) = 0$ when q is an odd power of 3.
ii) It seems that if the characteristic is $p \geq 5$, then the tower of Example 4.3 is not of finite ramification type.

In the next example we will change slightly (just a change of sign) the tower of Example 4.3 obtaining a tower of finite ramification type in any characteristic $p \geq 3$.

Example 4.5. *Over a finite field $\mathbb{F}_q$ of characteristic $p \geq 3$, consider the tower $\mathcal{T}$ defined recursively by the equation*

$$y^2 = \frac{x(1-x)}{x+1}.$$

Then this tower is of finite ramification type, and we have

$$s := \sum_{P \in V_{F_0}(\mathcal{T})} \deg P = 10.$$

Proof. Similarly to the proof of Example 4.3 we get in this case:

$$V_{F_0}(\mathcal{T}) = \{0, \infty, \pm 1\} \cup \mathfrak{z}(x^2+1) \cup \mathfrak{z}(x^2 - 2x - 1) \cup \mathfrak{z}(x^2 + 2x - 1).$$

This shows that $s = 10$ and, in particular, that the tower is of finite ramification type in any characteristic $p \geq 3$. □

Remark 4.6. Direct computations show that the tower $\mathcal{T}$ in Example 4.5, considered over the finite field $\mathbb{F}_{81}$, has $t = 8$ rational places of F_0 that are completely splitting in the tower. Theorem 2.24 then gives that the limit $\lambda(\mathcal{T})$ over $\mathbb{F}_{81}$ satisfies

$$\lambda(\mathcal{T}) \geq \frac{2t}{s-2} = 2.$$

It can be shown that equality holds above.

It seems to be hard to decide over which finite fields $\mathbb{F}_q$ the tower of Example 4.5 is completely splitting. A necessary condition is $q \equiv 1 \bmod 4$.

Next we give an example of a tower of finite ramification type in characteristic $p = 5$.

Example 4.7. *For characteristic $p = 5$, the tower $\mathcal{T}$ defined by the equation*

$$y^2 = \frac{3(x^2+3)}{x+1}$$

is of finite ramification type, and one has

$$s := \sum_{P \in V_{F_0}(\mathcal{T})} \deg P = 8.$$

Proof. Similarly to the proof of Example 4.3 one shows that

$$V_F(\mathcal{T}) = \{0, \infty, \pm 1, \pm 2\} \cup \mathfrak{z}(x^2+3).$$

□

It seems to be hard to decide whether the tower in Example 4.7 is completely splitting for some finite fields of characteristic $p = 5$.

Our next example provides a tower over $\mathbb{F}_q$ in characteristic $p = 5$ where both properties (finite ramification type and completely splitting) are easily seen to hold, if the cardinality q of the finite field is a square.

Example 4.8. *In characteristic $p = 5$, consider the tower $\mathcal{T}$ over $\mathbb{F}_q$ defined recursively by the equation*

$$y^2 = \frac{x(x+2)}{x+1}.$$

Then this tower is of finite ramification type, and we have

$$s := \sum_{P \in V_{F_0}(\mathcal{T})} \deg P = 6.$$

Its limit $\lambda(\mathcal{T})$ over the field $\mathbb{F}_{25}$ is $\lambda(\mathcal{T}) = 1$.

Proof. Similar computations as in Example 4.3 show that

$$V_{F_0}(\mathcal{T}) = \{0, \infty, \pm 1, \pm 2\}$$

and hence $s = 6$. It follows from Proposition 4.2 that if there exists an element $\beta \in \mathbb{F}_q$ with $\beta^2 = 2$ (this is the case iff q is an even power of 5), then the places $x_0 = \pm\beta$ are completely splitting in this tower. Denoting by $\lambda(\mathcal{T})$ the limit over $\mathbb{F}_{25}$, it follows from Theorem 2.24 that

$$\lambda(\mathcal{T}) \geq \frac{2 \cdot 2}{s-2} = 1.$$

Direct computations show that we have equality above. □

Example 4.9. *In characteristic $p = 3$, consider the tower $\mathcal{T}$ over $\mathbb{F}_q$ that is defined recursively by the equation*

$$y^2 = \frac{x^2}{x-1}.$$

This tower is of finite ramification type, and we have

$$s := \sum_{P \in V_{F_0}(\mathcal{T})} \deg P = 3.$$

The limit $\lambda(\mathcal{T})$ over the field $\mathbb{F}_9$ with 9 elements is $\lambda(\mathcal{T}) = 2 = \sqrt{9} - 1$, so the tower is asymptotically optimal over $\mathbb{F}_9$.

Proof. It is easily checked that $V_{F_0}(\mathcal{T}) = \{\infty, \pm 1\}$ and that the place $x_0 = 0$ splits completely over $\mathbb{F}_9$ in the tower $\mathcal{T}$. Hence Theorem 2.24 gives that the limit $\lambda(\mathcal{T})$ over $\mathbb{F}_9$ satisfies

$$\lambda(\mathcal{T}) \geq \frac{2t}{s-2} \geq \frac{2}{3-2} = 2 = \sqrt{9} - 1.$$

□

Remark 4.10. Elkies showed in [3, Equation 45] that the modular curves $X_0(3 \cdot 2^n)$ correspond to the tower $\mathcal{T}$ over $\mathbb{F}_{p^2}$ with defining equation

$$y^2 = \frac{x(3+x)}{x-1},$$

for all primes $p \geq 5$. It is easily checked that the ramification locus of this tower $\mathcal{T}$ in any characteristic $p \geq 5$ is given by:

$$V_{F_0}(\mathcal{T}) = \{0, \infty, \pm 1, \pm 3\}.$$

¿From the modular interpretation it follows that the tower is asymptotically optimal over the field $\mathbb{F}_{p^2}$, for any prime number $p \geq 5$ (see [20]).

Note that our Example 4.9 is given in characteristic $p = 3$ by the same defining equation $y^2 = x(3+x)/(x-1)$.

Remark 4.11. One can construct towers of finite ramification type that are specific for certain characteristics p, as was the case in Example 4.3 for $p = 3$, and in Examples 4.7 and 4.8 for $p = 5$. For example if $p = 11$, then the tower $\mathcal{T}$ defined by the equation

$$y^2 = \frac{4(x-2)}{x^2+1}$$

has ramification locus $V_{F_0}(\mathcal{T}) = \{0, \infty, \pm 2, \pm 5\} \cup \mathfrak{z}(x^2+1)$.

In characteristic $p = 13$ if the equation

$$y^2 = \frac{-4(x-3)^2}{x^2+3}$$

defines indeed a tower $\mathcal{T}$, then it has ramification locus $V_{F_0}(\mathcal{T}) = \{0, \infty, \pm 1, \pm 3\} \cup \mathfrak{z}(x^2+3)$.

5. An asymptotically optimal tower

Notation 5.1. Let $\mathbb{F}_q$ be a finite field of characteristic $p \geq 3$. Then we denote by $\mathcal{M}$ the tower over $\mathbb{F}_q$ that is defined recursively by the equation

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

Thus $\mathcal{M}$ is represented by the sequence of function fields $(M_0, M_1, M_2, \dots)$, where $M_n = \mathbb{F}_q(x_0, x_1, \dots, x_n)$ and $x_{i+1}^2 = (x_i^2+1)/2x_i$ holds for each $i \geq 0$.

Note that $\mathcal{M}$ is indeed a tower over $\mathbb{F}_q$, as follows from Proposition 4.1. We now state the main result of this section:

Theorem 5.2. *For all prime numbers $p \geq 3$, the tower $\mathcal{M}$ is asymptotically optimal over the field $\mathbb{F}_{p^2}$ with p^2 elements; i.e., its limit $\lambda(\mathcal{M})$ over $\mathbb{F}_{p^2}$ satisfies*

$$\lambda(\mathcal{M}) = p - 1.$$

The proof of this theorem will be given in several steps.

Proposition 5.3. *The tower $\mathcal{M}$ over $\mathbb{F}_q$ is of finite ramification type. Its ramification locus $V_{M_0}(\mathcal{M})$ over the field $M_0 = \mathbb{F}_q(x_0)$ is given by*

$$V_{M_0}(\mathcal{M}) = \{0, \infty, \pm 1, \pm i\}, \text{ where } i \in \mathbb{F}_{p^2} \text{ satisfies } i^2 = -1.$$

Proof. Let $P \in \mathbb{P}_{M_0}$ and let Q be a place of M_n lying above P. Assume that Q is ramified in the extension M_{n+1}/M_n. ¿From the equation $x_{n+1}^2 = (x_n^2 + 1)/2x_n$ and from the theory of Kummer extensions, it follows that

$$x_n(Q) \in \{0, \infty, \pm i\}.$$

If $x_n(Q) = 0$, then we obtain

$$0 = x_n(Q)^2 = \frac{x_{n-1}(Q)^2 + 1}{2x_{n-1}(Q)}\ , \quad \text{hence } x_{n-1}(Q) = \pm i.$$

If $x_n(Q) = \infty$, then we obtain

$$\infty = \frac{x_{n-1}(Q)^2 + 1}{2x_{n-1}(Q)}\ , \quad \text{hence } x_{n-1}(Q) \in \{0, \infty\}.$$

If $x_n(Q) = \pm i$, then we obtain

$$-1 = x_n(Q)^2 = \frac{x_{n-1}(Q)^2 + 1}{2x_{n-1}(Q)}\ , \quad \text{hence } x_{n-1}(Q) = -1.$$

If $x_{n-1}(Q) = \pm 1$, then we obtain

$$1 = x_{n-1}(Q)^2 = \frac{x_{n-2}(Q)^2 + 1}{2x_{n-2}(Q)}\ , \quad \text{hence } x_{n-2}(Q) = 1.$$

By induction it follows that

$$x_0(P) = x_0(Q) \in \{0, \infty, \pm 1, \pm i\}.$$

Conversely, it can be shown that the places $x_0 = 0$, $x_0 = \infty$, $x_0 = \pm i$ and $x_0 = \pm 1$ are in fact ramified in the tower $\mathcal{M}$. The places $x_0 = 0$, $x_0 = \infty$ and $x_0 = \pm i$ are totally ramified in the tower and the place $x_0 = -1$ is totally ramified starting from the field M_2. The ramification structure of the tower $\mathcal{M}$ above the place $x_0 = 1$ is more complicated. In this case one observes that the places Q of M_4 satisfying $x_3(Q) = 0$ do lie above $x_0 = 1$, and that those places Q are totally ramified in M_n/M_4, for each $n \geq 5$. □

For the description of the set Ω of $\mathbb{F}_{p^2}$-rational places of M_0 that are completely splitting in the tower $\mathcal{M}$, we need the following polynomial $H(X)$ which was introduced by Deuring [1] in order to classify supersingular elliptic curves, see also [12], [14].

Definition 5.4. For a prime number $p \geq 3$ let

$$H(X) := \sum_{j=0}^{(p-1)/2} \binom{\frac{p-1}{2}}{j}^2 \cdot X^j \quad \in \mathbb{F}_p[X],$$

and let

$$\Omega := \{\alpha \in \bar{\mathbb{F}}_p \mid H(\alpha^4) = 0\}.$$

We will need the following properties of the polynomial $H(X)$:

Theorem 5.5.

i) *The polynomial $H(X)$ is a separable polynomial.*

ii) *All roots of the polynomial $H(X)$ are fourth powers in $\mathbb{F}_{p^2}$; equivalently, the set Ω is contained in $\mathbb{F}_{p^2}$. Its cardinality satisfies $\#\Omega = 2(p-1)$.*

Proof. Item i) is well-known, see [1], [18]. Since $H(0) \neq 0$ and $H(X)$ has degree $(p-1)/2$, it follows immediately from item i) that $\#\Omega = 2(p-1)$. The assertion that Ω is contained in the field $\mathbb{F}_{p^2}$ is deeper; it is shown by H. G. Rück in the appendix. □

The next proposition shows that Ω is splitting completely in the tower $\mathcal{M}$.

Proposition 5.6. *Let $\alpha \in \Omega$ and let $\beta \in \bar{\mathbb{F}}_p$ be an element such that $\beta^2 = (\alpha^2+1)/2\alpha$. Then β belongs also to Ω.*

The proof of this proposition will be given below. Let us first show how Theorem 5.2 now follows:

Let $P_\alpha \in \mathbb{P}_{M_0}$ denote the zero of $x_0 - \alpha$, with $\alpha \in \Omega$. By Theorem 5.5, P_α is a $\mathbb{F}_{p^2}$-rational place of M_0. The equation $\beta^2 = (\alpha^2+1)/2\alpha$ has two distinct roots $\beta \in \Omega \subseteq \mathbb{F}_{p^2}$, by Proposition 5.6, hence the place P_α splits completely over $\mathbb{F}_{p^2}$ in the extension M_1/M_0. It follows by induction that P_α splits completely over $\mathbb{F}_{p^2}$ in all extensions M_n/M_0. With notations as in Theorem 2.24 we thus have that

$$t \geq \#\Omega = 2(p-1)$$

and that $s = 6$ (by Proposition 5.3). Therefore the limit $\lambda(\mathcal{M})$ over the field $\mathbb{F}_{p^2}$ satisfies:

$$\lambda(\mathcal{M}) \geq \frac{2t}{2g(M_0)+s-2} \geq \frac{4(p-1)}{6-2} = p-1.$$

By the Drinfeld-Vladut bound one has $\lambda(\mathcal{M}) \leq p-1$, hence equality holds. This finishes the proof of Theorem 5.2. □

We now turn to the proof of Proposition 5.6. So let $\alpha \in \Omega$ and $\beta \in \bar{\mathbb{F}}_p$ be such that $\beta^2 = (\alpha^2+1)/2\alpha$ holds. The assertion of Proposition 5.6 states that $H(\beta^4) = 0$. In other words, we have to show that

$$H(\alpha^4) = 0 \ \Rightarrow \ H\left(\left(\frac{\alpha^2+1}{2\alpha}\right)^2\right) = 0.$$

This implication is an immediate consequence of the following polynomial identity in the polynomial ring $\mathbb{F}_p[X]$:

Theorem 5.7. *The polynomial of Deuring $H(X)$ satisfies*

$$H(X^4) = X^{p-1} \cdot H\left(\left(\frac{X^2+1}{2X}\right)^2\right).$$

Proof. Expanding the right-hand side we obtain

$$
\begin{aligned}
X^{p-1} \cdot H\left(\left(\frac{X^2+1}{2X}\right)^2\right) &= X^{p-1} \cdot \sum_{j=0}^{(p-1)/2} \binom{\frac{p-1}{2}}{j}^2 \cdot \left(\frac{X^2+1}{2X}\right)^{2j} \\
&= \sum_{j=0}^{(p-1)/2} \binom{\frac{p-1}{2}}{j}^2 \cdot \frac{1}{4^j} \cdot (X^2+1)^{2j} \cdot X^{p-1-2j} \\
&= \sum_{k=0}^{p-1} c_k \cdot X^{2k},
\end{aligned}
$$

where the coefficient c_k is given by

$$
c_k = \sum_{j=0}^{(p-1)/2} \binom{\frac{p-1}{2}}{j}^2 \cdot \frac{1}{4^j} \cdot \binom{2j}{k+j-\frac{p-1}{2}}.
$$

Theorem 5.7 will thus follow from the two claims below:

CLAIM 1:

$$
c_k \equiv 0 \bmod p, \quad \text{for } k \text{ odd and } 0 \leq k \leq p-1.
$$

CLAIM 2:

$$
c_k \equiv \binom{(p-1)/2}{k/2}^2 \bmod p, \quad \text{for } k \text{ even and } 0 \leq k \leq p-1.
$$

For each natural number $n \geq 0$ we define

$$
S_n := (-1)^n \cdot \sum_{j=0}^{n} \frac{(-1)^j}{4^j} \cdot \binom{2j}{j}^2 \cdot \binom{n+j}{2j} \in \mathbb{Q}.
$$

Since 4 is prime to the characteristic p, the rational number S_n can be thought of as an element of the field $\mathbb{F}_p$. After some computations one sees that

$$
c_k = S_k \ \text{ (in } \mathbb{F}_p\text{)}, \quad \text{for each } 0 \leq k \leq p-1.
$$

Claim 1 and Claim 2 will then follow from the lemma below. □

Lemma 5.8. *For each natural number n, let $S_n \in \mathbb{Q}$ be as above. Then we have:*

i) $S_n = 0$, *if n is odd.*

ii) $S_n = \frac{1}{4^n} \cdot \binom{n}{n/2}^2$, *if n is even.*

Clearly, Claim 1 follows directly from item i) of the lemma above. Claim 2 follows from item ii) of Lemma 5.8 using the following congruence modulo p (for k even and $0 \leq k \leq p-1$):

$$4^k \cdot \left(\begin{array}{c} (p-1)/2 \\ k/2 \end{array} \right)^2 \equiv \left(\begin{array}{c} k \\ k/2 \end{array} \right)^2 \bmod p.$$

The ideas in the following proof of Lemma 5.8 were communicated to us by Y. Kohayakawa, and we are grateful to him for allowing us to use them here.

Proof of Lemma 5.8. We are going to use the Gaussian hypergeometric function (see [11, Section 5.5]):

$$G(z) := \sum_{n \geq 0} \frac{1}{4^{2n}} \cdot \left(\begin{array}{c} 2n \\ n \end{array} \right)^2 \cdot z^n.$$

This function $G(z)$ satisfies the following differential equation (see [11, Equation 5.108]):

$$z(1-z) \cdot y'' + (1-2z) \cdot y' - \frac{1}{4} \cdot y = 0.$$

¿From this one concludes that both $G(z^2)$ and $\frac{1}{1-z} \cdot G\left(\frac{-4z}{(1-z)^2}\right)$ are solutions for the next differential equation:

$$z(z^2-1) \cdot y'' + (3z^2-1) \cdot y' + z \cdot y = 0.$$

It now follows that the identity below does hold:

$$G(z^2) = \frac{1}{1-z} \cdot G\left(\frac{-4z}{(1-z)^2}\right).$$

Now we come to a key step of the proof of Lemma 5.8 which is the following identity:

$$\sum_{n \geq 0} (-1)^n \cdot S_n \cdot z^n = \frac{1}{1-z} \cdot G\left(\frac{-4z}{(1-z)^2}\right).$$

This identity comes from the fact that the coefficient of z^{n-k} in $\left(\sum_{m=0}^{n} z^m\right)^{2k+1}$ is equal to the binomial coefficient $\left(\begin{array}{c} n+k \\ 2k \end{array} \right)$. Alternatively, this identity also follows from [11, Exercise 5.71].

Putting together the two identities above, we have:

$$\sum_{n \geq 0} (-1)^n \cdot S_n \cdot z^n = \sum_{n \geq 0} \frac{1}{4^{2n}} \cdot \left(\begin{array}{c} 2n \\ n \end{array} \right)^2 \cdot z^{2n}.$$

This finishes the proofs of Lemma 5.8 and Theorem 5.7. □

In the next remark we exhibit relations between three towers over $\mathbb{F}_{p^2}$. The one denoted below by $\mathcal{L}$ corresponds to the modular curves $X_0(2^n)$ as shown by Elkies (see [3, Equations 16 and 17]).

Remark 5.9. We consider the following three towers over $\mathbb{F}_{p^2}$, where the characteristic p satisfies $p \geq 3$:

$$\mathcal{M} = \mathbb{F}_{p^2}(x_0, x_1, x_2, \dots) \text{ with } x_{i+1}^2 = \frac{x_i^2+1}{2x_i}, \text{ for } i \geq 0.$$

$$\mathcal{N} = \mathbb{F}_{p^2}(y_0, y_1, y_2, \dots) \text{ with } y_{i+1}^2 = \frac{(y_i+1)^2}{4y_i}, \text{ for } i \geq 0.$$

$$\mathcal{L} = \mathbb{F}_{q}(z_0, z_1, z_2, \dots) \text{ with } z_{i+1}^2 = \frac{(z_i+3)^2}{8(z_i+1)}, \text{ for } i \geq 0.$$

We now show that $\mathcal{L}$ is a subtower of $\mathcal{N}$ and also that $\mathcal{N}$ is a subtower of $\mathcal{M}$. In fact to see that $\mathcal{N} \subseteq \mathcal{M}$ one considers the following functions of the field $\mathcal{M}$

$$y_n := x_{n+1}^2 = \frac{x_n^2+1}{2x_n}, \quad \text{for each } n \geq 0,$$

and checks that those functions y_n satisfy the recursive equation defining the tower $\mathcal{N}$.

To see that $\mathcal{L} \subseteq \mathcal{N}$ one considers the following functions of the field $\mathcal{N}$

$$z_n := 2y_{n+1}^2 - 1 = \frac{y_n^2+1}{2y_n}, \quad \text{for each } n \geq 0,$$

and checks that those functions z_n satisfy the recursive equation defining the tower $\mathcal{L}$.

Viewing those three towers with the inclusions above, one has that the following holds:

$$[\mathcal{M} : \mathcal{N}] = 2 \text{ and } [\mathcal{N} : \mathcal{L}] = 2.$$

One can also check easily that

$$\mathcal{M} = \mathcal{N}(x_0) \text{ and } \mathcal{N} = \mathcal{L}(y_0).$$

Since the tower $\mathcal{M}$ is asymptotically optimal over $\mathbb{F}_{p^2}$, we conclude that $\mathcal{L}$ and $\mathcal{N}$ are also asymptotically optimal over $\mathbb{F}_{p^2}$, see [7]. The explicit description of the ramification locus and of the set $\Omega(\mathcal{N})$ (resp. $\Omega(\mathcal{L})$) of rational places over $\mathbb{F}_{p^2}$ that are splitting completely is given below:

Tower $\mathcal{N}$: *For the tower $\mathcal{N}$ we have (with $F_0 = \mathbb{F}_{p^2}(y_0)$):*

$$V_{F_0}(\mathcal{N}) = \{0, \infty, \pm 1\} \quad \textit{and } \Omega(\mathcal{N}) = \{\alpha \in \mathbb{F}_{p^2} \mid H(\alpha^2) = 0\}.$$

Tower $\mathcal{L}$: *For the tower $\mathcal{L}$ we have (with $F_0 = \mathbb{F}_{p^2}(z_0)$):*

$$V_{F_0}(\mathcal{L}) = \{\infty, \pm 1\} \quad \textit{and } \Omega(\mathcal{L}) = \{\alpha \in \mathbb{F}_{p^2} \mid H\left(\frac{\alpha+1}{2}\right) = 0\}.$$

The following remark was communicated to us by M. Zieve and H. Roskam.

Remark 5.10. ¿From the inclusion $\mathcal{N} \subseteq \mathcal{M}$ above one can check that we have:

$$\mathbb{F}_{p^2}(x_1, x_2, \ldots, x_n) = \mathbb{F}_{p^2}(y_0, y_1, \ldots, y_n), \quad \text{for each } n \geq 0.$$

Similarly, from the inclusion $\mathcal{L} \subseteq \mathcal{N}$ above one can check that we have:

$$\mathbb{F}_{p^2}(y_1, y_2, \ldots, y_n) = \mathbb{F}_{p^2}(z_0, z_1, \ldots, z_n), \quad \text{for each } n \geq 0.$$

We then have the following isomorphisms of fields

$$\mathbb{F}_{p^2}(x_0, x_1, \ldots, x_{n-2}) \simeq \mathbb{F}_{p^2}(y_0, y_1, \ldots, y_{n-1}) \simeq \mathbb{F}_{p^2}(z_0, z_1, \ldots z_n), \quad \text{for each } n \geq 2.$$

This shows that all three fields above correspond to the modular curve $X_0(2^{n+1})$.

The next remark shifts the emphasis from the fields to the equations defining those fields.

Remark 5.11. A crucial step in our proof of the optimality of the tower $\mathcal{M}$ is the polynomial identity satisfied by the Deuring polynomial $H(X)$:

$$H(X^4) = X^{p-1} \cdot H\left(\left(\frac{X^2+1}{2X}\right)^2\right).$$

Setting $Y := X^2$ (see the inclusion $\mathcal{N} \subseteq \mathcal{M}$) one gets

$$H(Y^2) = Y^{\frac{p-1}{2}} \cdot H\left(\frac{(Y+1)^2}{4Y}\right).$$

This puts in evidence that the explicit description of the set Ω of completely splitting places for the tower $\mathcal{M}$ required the knowledge that the roots of Deuring's polynomial are fourth powers in $\mathbb{F}_{p^2}$, while for the tower $\mathcal{N}$ the knowledge that the roots are squares would be enough.

The Deuring polynomial $H(X)$ is just the reduction (mod p) of the Gaussian hypergeometric series, as follows from the congruence relation just before the proof of Lemma 5.8. Using this fact we obtain the following inversion formula:

$$(1+Y) \cdot Y^{\frac{p-1}{2}} \cdot H\left(\frac{(Y+1)^2}{4Y}\right) = H\left(\frac{4Y}{(Y+1)^2}\right).$$

Remark 5.12. As in Definition 5.4, we denote by Ω the set of all roots of the polynomial $H(X^4)$. For $\alpha \in \Omega$, let $\Omega_0(\alpha) := \{\alpha\}$ and, for $i \geq 0$, let

$$\Omega_{i+1}(\alpha) := \{\beta \mid \beta^2 = \frac{\gamma^2+1}{2\gamma} \text{ for some } \gamma \in \Omega_i(\alpha)\}.$$

By Proposition 5.6 we know that $\Omega_i(\alpha) \subseteq \Omega$ for all $i \geq 0$. Some computer calculations gave us evidence for the question below:

Question: *Is it true that the equality*

$$\Omega = \bigcup_{i \geq 0} \Omega_i(\alpha)$$

holds for each $\alpha \in \Omega$?

A positive answer to this question would mean that starting with any root of

$H(X)$ one gets all the other roots of the Deuring polynomial.

Acknowledgements. We would like to express our gratitude to H. G. Rück and Y. Kohayakawa for their stimulating interest in answering our questions (see Theorem 5.5 and Lemma 5.8) and to N. Medeiros for very helpful discussions and computer calculations. Also to J. F. Voloch, A. Pacheco, M. Zieve and H. Roskam for discussions on the subject of this paper.

Appendix

by Hans-Georg Rück [1]

In this appendix it is proven the following property of the roots of Deuring's polynomial $H(X)$.

Theorem. *Let p be a prime number, $p \geq 3$, and consider the polynomial*

$$H(X) = \sum_{j=0}^{(p-1)/2} \binom{\frac{p-1}{2}}{j}^2 \cdot X^j \in \mathbb{F}_p[X].$$

Then each root of $H(X)$ is a fourth power in $\mathbb{F}_{p^2}$.

Proof. If $p = 3$, then $H(X) = X + 1$, and -1 is a fourth power in $\mathbb{F}_9$. So we may assume that $p \geq 5$.

Let λ be a zero of $H(X)$ in $\bar{\mathbb{F}}_p$. We consider the elliptic curve E_λ given by the equation $y^2 = x(x-1)(x-\lambda)$ over $\bar{\mathbb{F}}_p$. Then E_λ is supersingular (cf. [18] V,4). Since each supersingular elliptic curve can be defined over $\mathbb{F}_{p^2}$ (cf. [1] 10,2), there exists an elliptic curve E'_λ over $\mathbb{F}_{p^2}$ which is (over $\bar{\mathbb{F}}_p$) isomorphic to E_λ.

Furthermore there are three possibilities for the Frobenius endomorphism π' of E'_λ over $\mathbb{F}_{p^2}$ (cf. [22] Theorems 4.1 and 4.2):
i) $\pi' \in \mathbb{Z}$, i.e., $\pi' = \pm p$.
ii) π' satisfies the equation $(\pi')^2 \pm p\pi' + p^2 = 0$, i.e., $\pi' = \rho p$, where ρ is a 6th root of unity. The conductor of the endomorphism ring $\mathrm{End}(E'_\lambda)$ is relatively prime to p. This case occurs only when $p \equiv 2 \bmod 3$.
iii) π' satisfies the equation $(\pi')^2 + p^2 = 0$, i.e., $\pi' = ip$, where i is a 4th root of unity. Again the conductor of $\mathrm{End}(E'_\lambda)$ is relatively prime to p. This case occurs only when $p \equiv 3 \bmod 4$.

We start with case ii): We see that the only possibility for the j-invariant is $j(E'_\lambda) = j(E_\lambda) = 0$. This yields (cf. [18] III,1) that λ satisfies $\lambda^2 - \lambda + 1 = 0$, i.e., λ is a 6th root of unity. Since the order $\#(\mathbb{F}^*_{p^2})$ is divisible by 8, we see that λ is a 4th power in $\mathbb{F}_{p^2}$.

[1] Institut für Experimentelle Mathematik, Ellernstr. 29, 45326 Essen, Germany

In case iii) we get $j(E'_\lambda) = j(E_\lambda) = 12^3$. Then λ is equal to $-1, 2$ or $1/2$ (cf. [18] III,1). Since $\#(\mathbb{F}^*_{p^2})/\#(\mathbb{F}^*_p)$ is divisible by 4 in this case, we see again that λ is a 4th power in $\mathbb{F}_{p^2}$.

It remains to consider the general case i), where $\pi' = \pm p$. Since π' is an odd integer, each 2-division point on E'_λ is fixed by π'. Therefore the elliptic curve E_λ is also defined over $\mathbb{F}_{p^2}$, and hence $\lambda \in \mathbb{F}_{p^2}$. So we can take $E'_\lambda = E_\lambda$ and $\pi' = \pi = \pm p$.

We consider the 2-division point $Q_1 = (0,0)$ on E_λ. Let $Q_2 = (a,b)$ be a point on E_λ with $2 \cdot Q_2 = Q_1$, then $4 \cdot Q_2 = 0$. Since $\pi = \pm p \equiv \pm 1 \bmod 4$, we get $\pi(Q_2) = \pm Q_2$. This means that the first coordinate a of Q_2 is an element of $\mathbb{F}_{p^2}$.

Writing down $2 \cdot Q_2 = Q_1$ explicitly using the addition formulas on E_λ, one gets

$$(a^2 - \lambda)^2 = 0. \tag{1}$$

Hence λ is a square in $\mathbb{F}_{p^2}$.

In the next step we choose a point $Q_3 = (c,d)$ on E_λ with $2 \cdot Q_3 = Q_2$. Here this equation yields explicitly

$$(c-a)^4 + 4c^2(a-1)^2 a = 0. \tag{2}$$

If $p \equiv \pm 1 \bmod 8$, then the 8-division point Q_3 satisfies $\pi(Q_3) = \pm Q_3$. Hence its first coordinate c lies in $\mathbb{F}_{p^2}$, and equation (2) shows that a is a square in $\mathbb{F}_{p^2}$. Hence we get (with (1)) that λ is a 4th power in $\mathbb{F}_{p^2}$.

If $p \equiv \pm 3 \bmod 8$, then $\pi(Q_3) = \pm 3 \cdot Q_3$. Hence c lies in $\mathbb{F}_{p^4}$, and its conjugate c^{p^2} is equal to the first coordinate of the point $3 \cdot Q_3 = Q_1 - Q_3$ which equals λ/c. Then $(C-c)(C-\lambda/c)$ is an irreducible polynomial in $\mathbb{F}_{p^2}[C]$.

The other zeros of the equation (2) are the first coordinates of the points $Q_3 + (1,0)$ and $Q_3 + (\lambda, 0)$, which are equal to $(c-\lambda)/(c-1)$ and $\lambda(c-1)/(c-\lambda)$.

Hence the polynomial (in the variable C) coming from equation (2) factors as

$$(C-a)^4 + 4C^2(a-1)^2 a = (C^2 + eC + \lambda)(C^2 + fC + \lambda), \tag{3}$$

with $e, f \in \mathbb{F}_{p^2}$. Comparing coefficients yields the two equations

$$e + f = -4a \text{ and } ef = 4a^3 - 4a^2 + 4a. \tag{4}$$

¿From (4) we get the quadratic equation (in e)

$$e^2 + 4ae + 4a^3 - 4a^2 + 4a = 0. \tag{5}$$

Since e is a solution of (5) in $\mathbb{F}_{p^2}$, the discriminant $-4(a-1)^2 a$ is a square in $\mathbb{F}_{p^2}$. Hence a is a square and λ is a 4th power in $\mathbb{F}_{p^2}$.

Remark. M. Zieve communicated to us that the theorem above (i.e., all roots of $H(X)$ are fourth powers in $\mathbb{F}_{p^2}$) is a simple consequence of Theorem 5.7 and the fact that all roots of $H(X)$ are in $\mathbb{F}_{p^2}$.

References

[1] *M. Deuring,* Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, Abh. Math. Sem. Hamburg **14** (1941), 197 - 272.

[2] *V. G. Drinfeld, S. G. Vladut,* Number of points of an algebraic curve, Funct. Anal. **17** (1983), 53 - 54.

[3] *N. Elkies,* Explicit modular towers, Proceedings of the 35th Annual Allerton Conference on Communication, Control and Computing, Urbana, IL (1997).

[4] *G. Frey, M. Perret, H. Stichtenoth,* On the different of abelian extensions of global fields, in "Coding Theory and Algebraic Geometry. Proceedings, Luminy, 1991" (H. Stichtenoth and M. A. Tsfasman, Eds.), Lecture Notes in Math. **1518**, 26 - 32. Springer-Verlag, New York, Berlin, 1992.

[5] *A. Garcia, H. Stichtenoth,* Elementary abelian p-extensions of algebraic function fields, Manuscr. Math. **72** (1991), 67 - 79.

[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,* Skew pyramids of function fields are asymptotically bad, in "Coding Theory, Cryptography and Related Topics", Proceedings of a Conference in Guanajuato, 1998 (J. Buchmann et al., Eds.) 111 - 113, Springer-Verlag, Berlin 2000.

[9] *A. Garcia, H. Stichtenoth, M. Thomas,* On towers and composita of towers of function fields over finite fields, Finite Fields and their Appl. **3** (1997), 257 - 274.

[10] *G. van der Geer, M. van der Vlugt,* Tables of curves with many points, www.wins.uva.nl/~geer.

[11] *R. L. Graham, D. E. Knuth, O. Patashnik,* Concrete Mathematics, Addison-Wesley, 1990.

[12] *H. Hasse,* Existenz separabler zyklischer unverzweigter Erweiterungskörper vom Primzahlgrade p über elliptischen Funktionenkörpern der Charakteristik p, J. Reine Angew. Math. **172** (1934), 77 - 85.

[13] *Y. Ihara,* Some remarks on the number of rational points of algebraic curves over finite fields, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28** (1981), 721 - 724.

[14] *C. Moreno,* Algebraic curves over finite fields, Cambridge University Press, Cambridge, 1991.

[15] *H. Niederreiter, C. P. Xing,* Curve sequences with asymptotically many rational points, Contemporary Mathematics **245** (1999), 3 - 14.

[16] *J.-P. Serre,* Sur le nombre des points rationelles d'une courbe algébrique sur une corps fini, C. R. Acad. Sci. Paris **296** (1983), 397 - 402.

[17] *J.-P. Serre,* Rational points on curves over finite fields, Lecture Notes, Harvard University, 1985.

[18] *J. H. Silverman,* The arithmetic of elliptic curves, Graduate Texts in Mathematics No. 106. Springer-Verlag, New York/Berlin, 1986.

[19] *H. Stichtenoth,* Algebraic Function Fields and Codes, Springer Universitext, Berlin/Heidelberg/New York, 1993.

[20] *M. A. Tsfasman, S. G. Vladut and T. Zink,* Modular Curves, Shimura curves and Goppa codes, better than the Varshamov-Gilbert bound, Math. Nachr. **109** (1982), 21 - 28.

[21] *M. A. Tsfasman, S. G. Vladut,* Algebraic-geometric codes, Kluwer Acad. Publ., Dordrecht/Boston/London, 1991.

[22] *W. Waterhouse,* Abelian varieties over finite fields, Ann. Sci. École Norm. Sup. 4,2 (1969), 521 - 560.

[23] *A. Weil,* Sur les courbes algébriques et les variétés qui s'en déduisent, Act. Sc. et Industrielles **1041**. Hermann, Paris, 1948.

Authors' addresses:
A. Garcia, Instituto de Matématica Pura e Aplicada IMPA, 22460-320 Rio de Janeiro RJ, Brazil. e-mail: garcia@impa.br

H. Stichtenoth, Universität GH Essen, FB 6, Mathematik u. Informatik, 45117 Essen, Germany. e-mail: stichtenoth@uni-essen.de