A New Tower Over Cubic Finite Fields

Alp Bassa*, Arnaldo Garcia†‡ and Henning Stichtenoth*

We present a new explicit tower of function fields $(F_n)_{n\geq 0}$ over the finite field with $\ell = q^3$ elements, where the limit of the ratios (number of rational places of F_n)/(genus of F_n) is bigger or equal to $2(q^2-1)/(q+2)$. This tower contains as a subtower the tower which was introduced by Bezerra–Garcia–Stichtenoth (see [3]), and in the particular case $q = 2$ it coincides with the tower of van der Geer–van der Vlugt (see [12]). Many features of the new tower are very similar to those of the optimal wild tower in [8] over the quadratic field $\mathbb{F}_{q^2}$ (whose modularity was shown in [6] by Elkies).

1 Introduction

Let $F/\mathbb{F}_\ell$ be an algebraic function field of one variable whose full constant field is the finite field $\mathbb{F}_\ell$ of cardinality ℓ. We denote by $g(F)$ the genus and by $N(F)$ the number of rational places (i.e., places of degree one) of $F/\mathbb{F}_\ell$. The classical Hasse–Weil Theorem states that $N(F) \leq \ell + 1 + 2g(F)\sqrt{\ell}$.

Ihara [13] was the first to observe that this inequality can be improved substantially if the genus of F is large with respect to ℓ. He introduced the real number

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

where F runs over all function fields over $\mathbb{F}_\ell$. This number $A(\ell)$ is of fundamental importance to the theory of function fields over a finite field, since it gives information about how many rational places a function field $F/\mathbb{F}_\ell$ of large genus can have. While the Hasse–Weil Theorem gives that $A(\ell) \leq 2\sqrt{\ell}$, Ihara showed that $A(\ell) \leq \sqrt{2\ell}$ for any ℓ and that $A(\ell) \geq \sqrt{\ell} - 1$ for ℓ a square. Later Drinfel'd and Vlăduţ [4] showed that

$$A(\ell) \leq \sqrt{\ell} - 1 \quad \text{for any} \quad \ell. \tag{1}$$

*Sabancı University, MDBF, Orhanlı, 34956 Tuzla, İstanbul, Turkey
†Instituto Nacional de Matemática Pura e Aplicada, IMPA, Estrada Dona Castorina 110, 22460-320, Rio de Janeiro, RJ, Brazil
‡A. Garcia was partially supported by PRONEX-FAPERJ and CNPq-Brazil (Proc. 307569/2006-3), and also by Sabancı University, İstanbul

Hence we have the equality $A(\ell) = \sqrt{\ell} - 1$ for ℓ a square (see also [5], [7], [17]).

Much less is known if ℓ is not a square. One knows that for any ℓ (see Serre [15])

$$A(\ell) \geq c \cdot \log \ell, \qquad \text{for some constant } c > 0.$$

For $\ell = p^3$ (p a prime number), the best known lower bound for $A(\ell)$ is due to Zink [18]:

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

Zink obtained this result using degenerations of Shimura modular surfaces. Zink's bound was generalized by Bezerra, Garcia and Stichtenoth [3] who showed that

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

holds for all prime powers q. For more information and references concerning Ihara's quantity $A(\ell)$ we refer to the recent survey article [11].

In order to obtain lower bounds for $A(\ell)$, it is natural to study towers of function fields; i.e., one considers sequences $\mathcal{G} = (G_0, G_1, G_2, \ldots)$ of function fields G_i over $\mathbb{F}_\ell$ with $G_0 \subseteq G_1 \subseteq G_2 \subseteq \ldots$ such that $g(G_i) \to \infty$. It is easy to see that the limit

$$\lambda(\mathcal{G}) := \lim_{i \to \infty} \frac{N(G_i)}{g(G_i)}$$

always exists (see [8]), and it is clear that $0 \leq \lambda(\mathcal{G}) \leq A(\ell)$.

A particularly interesting example is the tower $\mathcal{H} = (H_0, H_1, H_2, \ldots)$ over the field $\mathbb{F}_\ell$ with $\ell = q^2$, which is defined recursively as follows (see [8]): $H_0 = \mathbb{F}_\ell(u_0)$ is the rational function field, and for all $i \geq 0$ one considers the field $H_{i+1} = H_i(u_{i+1})$ with

$$u_{i+1}^q + u_{i+1} = \frac{u_i^q}{u_i^{q-1}+1}. \tag{4}$$

This tower over $\mathbb{F}_{q^2}$ has the limit $\lambda(\mathcal{H}) = q - 1 = \sqrt{\ell} - 1$, and therefore it attains the Drinfel'd–Vlăduţ bound (1). Elkies [6] has shown that $\mathcal{H}$ is in fact a modular tower.

In [3] the following tower $\mathcal{E} = (E_0, E_1, E_2, \ldots)$ over a cubic field $\mathbb{F}_\ell$ with $\ell = q^3$ is considered: again $E_0 = \mathbb{F}_\ell(v_0)$ is the rational function field, and for $i \geq 0$ one considers the field $E_{i+1} = E_i(v_{i+1})$ with

$$\frac{1 - v_{i+1}}{v_{i+1}^q} = \frac{v_i^q + v_i - 1}{v_i}. \tag{5}$$

The limit $\lambda(\mathcal{E})$ satisfies the inequality (thus proving Inequality (3)):

$$\lambda(\mathcal{E}) \geq \frac{2(q^2-1)}{q+2}. \tag{6}$$

The tower $\mathcal{H}$ over the quadratic field $\mathbb{F}_\ell$ with $\ell = q^2$ which is defined by Eqn. (4) has some nice features which allow a rather simple proof of the equality $\lambda(\mathcal{H}) = q - 1$, see [9]. The most important one is that all extensions H_{i+1}/H_i are Galois of degree q, and for all places $Q|P$ with ramification index $e = e(Q|P) > 1$ in H_{i+1}/H_i, the different exponent is $d(Q|P) = 2(e-1)$.

In contrast, the tower $\mathcal{E}$ over the cubic field $\mathbb{F}_\ell$ with $\ell = q^3$ which is defined by Eqn. (5) is much more complicated. Here (for $q \neq 2$) the extensions E_{i+1}/E_i are not even Galois, and there occurs tame and also wild ramification in E_{i+1}/E_i. The determination of the genus of E_n in [3] requires long and rather technical calculations. In [1] these calculations were replaced by a structural argument, thus obtaining a simpler proof of Inequality (6) without the explicit determination of $g(E_n)$. In [14], Ihara provides a construction of an infinite Galois extension, which contains the tower $\mathcal{E}$ and exhibits the splitting places of $\mathcal{E}$ in a more natural way. He also introduces a higher order differential which is invariant under the action of the associated infinite Galois group.

In this paper we present a new tower $\mathcal{F}$ over the cubic field $\mathbb{F}_\ell$ with $\ell = q^3$, whose limit also satisfies the inequality $\lambda(\mathcal{F}) \geq 2(q^2-1)/(q+2)$ and which has nicer properties than the tower given by the recursion in Eqn. (5). This new tower $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ over $\mathbb{F}_\ell$ is defined as follows: $F_0 = \mathbb{F}_\ell(x_0)$ is the rational function field over $\mathbb{F}_\ell$, and for $n \geq 0$ one sets $F_{n+1} = F_n(x_{n+1})$ with

$$(x_{n+1}^q - x_{n+1})^{q-1} + 1 = \frac{-x_n^{q(q-1)}}{(x_n^{q-1} - 1)^{q-1}}. \tag{7}$$

We would like to point out that our proof, that the limit of this new tower also satisfies the inequality $\lambda(\mathcal{F}) \geq 2(q^2-1)/(q+2)$, is much easier, shorter and less computational than the proofs in [3] and [1] for the tower $\mathcal{E}$. Moreover, since we show that $\mathcal{E}$ is a subtower of $\mathcal{F}$ we also get a new and simpler proof of Inequality (6); in fact, it follows from [8] that $\lambda(\mathcal{E}) \geq \lambda(\mathcal{F})$ when $\mathcal{E}$ is a subtower of $\mathcal{F}$.

Another remark is that while for the two towers over $\mathbb{F}_{q^2}$ presented in [7] and [8] the subtower (i.e., the tower $\mathcal{H}$ in [8]) was easier to handle, for the two towers $\mathcal{E}$ and $\mathcal{F}$ over $\mathbb{F}_{q^3}$ the supertower (i.e., the tower $\mathcal{F}$) turns out to be much easier to handle.

Finally we note that the tower $\mathcal{F}$ coincides with the van der Geer–van der Vlugt tower in [12] when $q = 2$, and also that the towers $\mathcal{F}$ and $\mathcal{H}$ have surprising similarities (see Section 8).

This paper is organized as follows: In Sec. 2 we introduce the sequence of function fields $F_0, F_1, F_2, \ldots$ over a field $K \supseteq \mathbb{F}_q$ recursively given by Eqn. (7) and we show in Theorem 2.2 that they define a tower $\mathcal{F}$ over K (i.e., $F_0 \subsetneq F_1 \subsetneq F_2 \subsetneq \ldots$, and K is the full constant field of all fields F_n). In Sec. 3 it is shown that for $K = \mathbb{F}_{q^3}$ there exist $q^3 - q$ rational places of F_0 which split completely in all extensions F_n/F_0, thus providing many rational places of the function fields $F_n/\mathbb{F}_{q^3}$. In Sec. 4 and Sec. 5 we study ramification in the first steps $F_0 \subseteq F_1 \subseteq F_2$ of the tower. We note that the methods in Sec. 4 and Sec. 5 involve just simple calculations about ramification in certain Galois extensions $K(x)/K(w)$ of rational function fields. Section 6 is the core of this paper. The results from Sec. 4 and Sec. 5 are used in Sec. 6 to give an upper bound for the genus of the

n-th function field F_n of the tower (see Thm. 6.5). The main tool here is a variant of Abhyankar's Lemma (see Lemma 6.2) dealing with ramification in composites of certain wildly ramified extensions. Putting together the results from Sec. 3 and Sec. 6 we obtain in Sec. 7 the inequality $\lambda(\mathcal{F}) \geq 2(q^2-1)/(q+2)$ for $K = \mathbb{F}_{q^3}$, which is the main result of the paper. Finally, in Sec. 8 we point out some surprising analogies between the tower $\mathcal{F}$ over $\mathbb{F}_{q^3}$ and the tower $\mathcal{H}$ over $\mathbb{F}_{q^2}$ which is defined by Eqn. (4). We also show that the above-mentioned tower $\mathcal{E}$ is a subtower of $\mathcal{F}$.

NOTATIONS: We consider function fields F/K where K is the full constant field of F. In most cases K will be a finite field or the algebraic closure $\overline{\mathbb{F}}_q$ of a finite field. We denote by $\mathbb{P}(F)$ the set of places of F/K. For $P \in \mathbb{P}(F)$, we will denote by v_P the corresponding discrete valuation of F/K and by $\mathcal{O}_P$ the valuation ring of P. For $z \in \mathcal{O}_P$ we denote by $z(P)$ the residue class of z in $\mathcal{O}_P/P$. We denote by $\deg(P)$ the degree of P. In particular, if P is a place of degree one, then $z(P) \in K$.

For a finite separable extension E of F and a place $Q \in \mathbb{P}(E)$ we will denote by $Q|_F$ the restriction of Q to F. We write $Q|P$ if the place $Q \in \mathbb{P}(E)$ lies over the place $P \in \mathbb{P}(F)$. In this situation, we denote by $e(Q|P)$ and $d(Q|P)$ the ramification index and the different exponent of $Q|P$, respectively. The place $P \in \mathbb{P}(F)$ is said to be totally ramified in E/F if there is a place $Q \in \mathbb{P}(E)$ above P with $e(Q|P) = [E:F]$. It is said to be completely splitting in E/F if there are $n = [E:F]$ distinct places of E above P.

Let E/F be a Galois extension of function fields, let $P \in \mathbb{P}(F)$ and $Q \in \mathbb{P}(E)$ above the place P. We say that $Q|P$ is *weakly ramified* if the second ramification group $G_2(Q|P) = 1$; in other words, if $e(Q|P) = e_0 \cdot e_1$ where $(e_0, p) = 1$ and $e_1 = p^j$ is a power of the characteristic p of F, then $d(Q|P) = (e_0e_1 - 1) + (e_1 - 1)$.

If $F = K(x)$ is a rational function field, we will write $(x = \alpha)$ for the place of F which is the zero of $x - \alpha$ (where $\alpha \in K$), and $(x = \infty)$ for the pole of x in $K(x)/K$.

2 The tower

Let K be a field of characteristic $p > 0$, let q be a power of p and assume that $\mathbb{F}_q \subseteq K$. We study the sequence $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ of function fields F_i/K which is defined recursively as follows: $F_0 = K(x_0)$ is the rational function field, and for $n \geq 0$ let $F_{n+1} = F_n(x_{n+1})$ where x_{n+1} satisfies the equation over F_n below:

$$(x_{n+1}^q - x_{n+1})^{q-1} + 1 = \frac{-x_n^{q(q-1)}}{(x_n^{q-1} - 1)^{q-1}}. \tag{8}$$

Remark 2.1. We set

$$f(T) := (T^q - T)^{q-1} + 1 \in K[T]. \tag{9}$$

Then Eqn. (8) can be written as

$$f(x_{n+1}) = \frac{1}{1 - f(1/x_n)}. \tag{10}$$

We also remark that $f(T) = (T^{q^2} - T)/(T^q - T)$, hence the roots of $f(T)$ are exactly the elements $\beta \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$. This property of the polynomial $f(T)$ will play an important role in Sections 3 and 4.

Theorem 2.2. *Let $\mathcal{F}$ be the sequence of function fields F_n over K which is defined by Eqn. (8). Then $\mathcal{F}$ is a tower over K, and more precisely the following hold:*

(i) The extensions F_{n+1}/F_n are Galois for all $n \geq 0$.

(ii) $[F_1 : F_0] = q(q-1)$ and $[F_{n+1} : F_n] = q$ for all $n \geq 1$.

(iii) K is the full constant field of F_n, for all $n \geq 0$.

The proof of Thm. 2.2 is given in several steps.

Lemma 2.3. *F_{n+1}/F_n is Galois and $[F_{n+1} : F_n]$ divides $q(q-1)$, for all $n \geq 0$.*

Proof. We set

$$u_n := \frac{-x_n^{q(q-1)}}{(x_n^{q-1} - 1)^{q-1}}. \tag{11}$$

Then x_{n+1} is a root of the polynomial $f_n(T) := (T^q - T)^{q-1} + 1 - u_n \in F_n[T]$. The other roots of $f_n(T)$ are the elements $ax_{n+1} + b$ with $a \in \mathbb{F}_q^\times$ and $b \in \mathbb{F}_q$. Therefore F_{n+1} is the splitting field of $f_n(T)$ over F_n and the extension F_{n+1}/F_n is Galois.

Let G_{n+1} be the Galois group of F_{n+1}/F_n. Every element $\sigma \in G_{n+1}$ acts on the function x_{n+1} as $\sigma(x_{n+1}) = a_\sigma x_{n+1} + b_\sigma$, and the map

$$\sigma \mapsto \begin{pmatrix} a_\sigma & 0 \\ b_\sigma & 1 \end{pmatrix}$$

is a monomorphism of G_{n+1} into the group of invertible 2×2-matrices over $\mathbb{F}_q$ of the form $\begin{pmatrix} a & 0 \\ b & 1 \end{pmatrix}$. This group has order $q(q-1)$, and hence $\mathrm{ord}(G_{n+1})$ divides $q(q-1)$. $\square$

Lemma 2.4. *Let $P_0 = (x_0 = \infty)$ be the pole of x_0 in F_0 and let P_n be a place of F_n above P_0. For $i = 1, \ldots, n$ we set $P_i := P_n|_{F_i}$ and $e^{(i)} := e(P_i|P_{i-1})$. Then the place P_i is a pole of x_i. Moreover, $v_{P_i}(x_i)$ divides $(q-1)^i$, and $e^{(i)} \equiv 0 \bmod q$, for $1 \leq i \leq n$.*

Proof. Let $u_i \in F_i$ be defined as in Eqn. (11). We prove the lemma by induction. For the case $i = 1$, we have $v_{P_1}(u_0) = e^{(1)} \cdot v_{P_0}(u_0) = -e^{(1)} \cdot (q-1)$. From the equation $(x_1^q - x_1)^{q-1} + 1 = u_0$, it follows that $v_{P_1}(x_1) < 0$ and therefore

$$v_{P_1}\big((x_1^q - x_1)^{q-1} + 1\big) = q \cdot (q-1) \cdot v_{P_1}(x_1).$$

We conclude that $q \cdot v_{P_1}(x_1) = -e^{(1)}$. To finish this case, notice that $e^{(1)}$ divides the degree $[F_1 : F_0]$, and $[F_1 : F_0]$ divides $q(q-1)$ (by Lemma 2.3). Hence it follows that $v_{P_1}(x_1)$ divides $(q-1)$ and that $e^{(1)} \equiv 0 \bmod q$.

Now we assume that $v_{P_i}(x_i) < 0$ and $v_{P_i}(x_i)$ divides $(q-1)^i$ for some $i \in \{1, \dots, n-1\}$. From Eqn. (11) we obtain $v_{P_i}(u_i) = (q-1) \cdot v_{P_i}(x_i)$, hence

$$v_{P_{i+1}}(u_i) = e^{(i+1)} \cdot (q-1) \cdot v_{P_i}(x_i) < 0.$$

Since $(x_{i+1}^q - x_{i+1})^{q-1} + 1 = u_i$, it follows that P_{i+1} is a pole of x_{i+1} and

$$q(q-1) \cdot v_{P_{i+1}}(x_{i+1}) = e^{(i+1)} \cdot (q-1) \cdot v_{P_i}(x_i).$$

Now we finish as in the case $i = 1$; we conclude that $e^{(i+1)} \equiv 0 \bmod q$ and that $v_{P_{i+1}}(x_{i+1})$ divides $(q-1)^{i+1}$. □

Lemma 2.5. $[F_{n+1} : F_n] \equiv 0 \bmod q$ *for all* $n \geq 0$.

Proof. Follows directly from Lemmas 2.3 and 2.4. □

Lemma 2.6. $[F_1 : F_0] = q(q-1)$*, and* K *is the full constant field of* F_1*.*

Proof. By definition, $F_1 = K(x_0, x_1)$ with

$$(x_1^q - x_1)^{q-1} + 1 = \frac{-x_0^{q(q-1)}}{(x_0^{q-1} - 1)^{q-1}} = u_0. \tag{12}$$

It follows that

$$[K(x_0) : K(u_0)] = [K(x_1) : K(u_0)] = q(q-1). \tag{13}$$

From Eqn. (12) it is obvious that the place $(u_0 = 0)$ of $K(u_0)$ is totally ramified in the extension $K(x_0)/K(u_0)$. The place of $K(x_0)$ above $(u_0 = 0)$ is the place $(x_0 = 0)$, and we have $e((x_0 = 0)|(u_0 = 0)) = q(q-1)$.

However, in the extension $K(x_1)/K(u_0)$ the place $(u_0 = 0)$ is unramified, since the polynomial $(x_1^q - x_1)^{q-1} + 1$ does not have multiple roots. Let Q be a place of $K(x_1)$ lying above $(u_0 = 0)$ and let R be a place of $K(x_0, x_1)$ above Q. It follows from above that $e(R|Q) = q(q-1)$. Therefore $[K(x_0, x_1) : K(x_1)] = q(q-1)$, and K is algebraically closed in $K(x_0, x_1) = F_1$ (as there is a place which is totally ramified in $F_1/K(x_1)$). The assertion $[F_1 : F_0] = q(q-1)$ follows since $[F_1 : F_0] = [F_1 : K(x_1)]$ by Eqn. (13). □

The next lemma shows a striking property of the recursion in Eqn. (8) for $n \geq 1$. It gives a simple Artin-Schreier equation for the extension F_{n+1}/F_n of degree q.

Lemma 2.7. *For each* $n \geq 1$ *there is some* $\mu \in \mathbb{F}_q^\times$ *such that*

$$x_{n+1}^q - x_{n+1} = \mu \cdot \frac{x_{n-1}^q}{(x_{n-1}^{q-1} - 1) \cdot (x_n^{q-1} - 1)}.$$

Proof. By Eqn. (8) we have

$$(x_{n+1}^q - x_{n+1})^{q-1} + 1 = \frac{-x_n^{q(q-1)}}{(x_n^{q-1} - 1)^{q-1}} \quad \text{and} \quad (x_n^q - x_n)^{q-1} + 1 = \frac{-x_{n-1}^{q(q-1)}}{(x_{n-1}^{q-1} - 1)^{q-1}}. \tag{14}$$

Hence we get

$$(x_{n+1}^q - x_{n+1})^{q-1} = \frac{-x_n^{q(q-1)}}{(x_n^{q-1}-1)^{q-1}} - 1 = \frac{-\big((x_n^q - x_n)^{q-1}+1\big)}{(x_n^{q-1}-1)^{q-1}}$$
$$= \frac{x_{n-1}^{q(q-1)}}{(x_{n-1}^{q-1}-1)^{q-1}\cdot(x_n^{q-1}-1)^{q-1}} = \left(\frac{x_{n-1}^q}{(x_{n-1}^{q-1}-1)\cdot(x_n^{q-1}-1)}\right)^{q-1}.$$

□

Proof of Theorem 2.2. Putting together the results of the lemmas above, one gets the assertions of Thm. 2.2. □

3 Splitting places in the tower over $K = \mathbb{F}_\ell$ for $\ell = q^3$

In this section we consider the tower $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ which was introduced in Sec. 2, over the field $K = \mathbb{F}_\ell$ with $\ell = q^3$. We will show that many rational places of the field $F_0 = \mathbb{F}_\ell(x_0)$ split completely in $\mathcal{F}$; i.e., they split completely in all extensions F_n/F_0. This means that the function fields $F_n/\mathbb{F}_\ell$ have "many" rational places. As in Sec. 2, let

$$f(T) = (T^q - T)^{q-1} + 1 \in \mathbb{F}_q[T]. \tag{15}$$

For $q = 2$ we have obviously that $f(T) - c$ is separable for all elements $c \in \overline{\mathbb{F}}_2$.

Lemma 3.1. *Let $c \in \overline{\mathbb{F}}_q$ be an element of the algebraic closure of $\mathbb{F}_q$. Then*

$f(T) - c$ is inseparable if and only if $q \neq 2$ and $c = 1$.

For an element $\beta \in \overline{\mathbb{F}}_q$ we have that $f(\beta) = 1$ if and only if β belongs to $\mathbb{F}_q$.

Proof. Just notice that the derivative of $f(T)$ satisfies $f'(T) = (T^q - T)^{q-2}$. □

Lemma 3.2. *For an element $\beta \in \overline{\mathbb{F}}_q$ we have that $f(\beta) = 0$ if and only if $\beta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$.*

Proof. Just notice that we have (see Rem. 2.1)

$$f(T) = (T^{q^2} - T)/(T^q - T). \tag{16}$$

□

Now we consider the recursive equation for the tower $\mathcal{F}$ (see Eqn. (10)):

$$f(Y) = \frac{1}{1 - f(1/X)}. \tag{17}$$

We will show that if $X = \alpha$ belongs to $\mathbb{F}_{q^3} \setminus \mathbb{F}_q$ then all solutions $Y = \beta \in \overline{\mathbb{F}}_q$ of Eqn. (17) with $X = \alpha$ are such that $\beta \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$. The assertion that $\beta \notin \mathbb{F}_q$ follows directly from Eqn. (17) and the lemmas above.

Using Eqn. (16) we have:

$$\frac{1}{1 - f(T)} = \frac{T - T^q}{T^{q^2} - T^q}. \tag{18}$$

Lemma 3.3. *For an element $\beta \in \overline{\mathbb{F}}_q$ we have that*

$$f(\beta)^q = \frac{1}{1-f(\beta)} \quad \text{if and only if} \quad \beta \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q.$$

Proof. Straightforward using Eqn. (16) and Eqn. (18). □

Eqn. (17) can also be written as below:

$$f(\frac{1}{X}) = 1 - \frac{1}{f(Y)}. \tag{19}$$

Consider now a solution (α, β) of Eqn. (17) with $\alpha \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$. Then $1/\alpha \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$. We have:

$$f(\beta) = \frac{1}{1-f(\frac{1}{\alpha})} = f(\frac{1}{\alpha})^q = 1 - \frac{1}{f(\beta)^q}.$$

In the last two equalities above we have used Lemma 3.3 and Eqn. (19), respectively. Hence we obtained that $f(\beta)^q = 1/(1-f(\beta))$; i.e., $\beta \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$.

We have thus proved the main result of this section:

Theorem 3.4. *Let $\mathcal{F} = (F_0, F_1, \dots)$ be the tower over $\mathbb{F}_{q^3}$ given recursively by Eqn. (17). Then the places $(x_0 = \alpha)$ with $\alpha \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ split completely in all extensions F_n/F_0. In particular the number of $\mathbb{F}_{q^3}$-rational places satisfies:*

$$N(F_n) \geq (q^3 - q) \cdot [F_n : F_0] \quad \text{for all } n \in \mathbb{N}.$$

4 The extensions $K(x)/K(w)$ and $K(x)/K(u)$

Throughout this section, K is a field with $\mathbb{F}_{q^2} \subseteq K$. Let $K(x)/K$ be a rational function field over K. We will consider certain subfields $K(w) \subseteq K(x)$ and $K(u) \subseteq K(x)$ which are related to the recursive definition of the tower $\mathcal{F}$. Detailed information about ramification in $K(x)/K(w)$ and in $K(x)/K(u)$ will enable us to study in Sec. 5 and Sec. 6 the ramification behaviour in the tower $\mathcal{F}$.

As in Sec. 2 we consider the polynomial $f(T) = (T^q - T)^{q-1} + 1 \in K[T]$, and we set

$$w := f(x) = (x^q - x)^{q-1} + 1 \in K(x). \tag{20}$$

Lemma 4.1. *(i) The extension $K(x)/K(w)$ is Galois of degree $q(q-1)$.*

(ii) The place $(w = \infty)$ of $K(w)$ is totally ramified in $K(x)/K(w)$; the place above it is the place $(x = \infty)$. We have $d((x = \infty)|(w = \infty)) = q^2 - 2$; i.e., $(x = \infty)|(w = \infty)$ is weakly ramified.

(iii) Above the place $(w = 1)$ there are the q places $(x = \theta)$ of $K(x)$ with $\theta \in \mathbb{F}_q$, with ramification index $e((x = \theta)|(w = 1)) = q - 1$.

(iv) All other places of $K(w)$ are unramified in $K(x)/K(w)$.

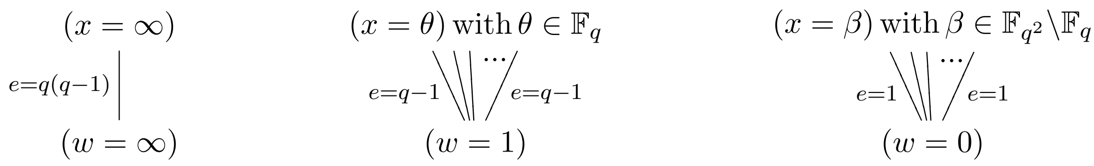

Figure 1: Ramification and splitting in $K(x)/K(w)$.

(v) *The places above $(w=0)$ are exactly the places $(x=\beta)$ with $\beta\in\mathbb{F}_{q^2}\backslash\mathbb{F}_q$.*

Proof. i) One checks easily that $K(w)$ is the fixed field of the following group H of automorphisms of $K(x)/K$:

$$H := \{\sigma\in \mathrm{Aut}(K(x)/K)\mid \sigma(x)=ax+b, a\in\mathbb{F}_q^\times, b\in\mathbb{F}_q\}.$$

ii) It is clear from Eqn. (20) that $(x=\infty)$ is the only place of $K(x)$ lying above $(w=\infty)$, and that the ramification index is $e((x=\infty)|(w=\infty))=q(q-1)$. Since $K(x)/K(w)$ is Galois, it follows from ramification theory (cf. [16, Sec. III.8]) that $d((x=\infty)|(w=\infty))\ge (q(q-1)-1)+(q-1)=q^2-2$. We will show below that equality holds; i.e., that $(x=\infty)|(w=\infty)$ is weakly ramified.

iii) This assertion is obvious from the equation $w-1=(x^q-x)^{q-1}$.

iv) It follows from above that the degree of the different $\mathrm{Diff}(K(x)/K(w))$ satisfies

$$\begin{aligned}\deg\ \mathrm{Diff}(K(x)/K(w)) &\ge d((x=\infty)|(w=\infty))+\sum_{\theta\in\mathbb{F}_q} d((x=\theta)|(w=1))\\ &\ge (q^2-2)+q(q-2)=2(q^2-q-1).\end{aligned}$$

On the other hand, by Hurwitz genus formula for $K(x)/K(w)$ we have

$$\deg\ \mathrm{Diff}(K(x)/K(w)) = -2+2[K(x):K(w)] = 2(q^2-q-1).$$

Now the assertions iv) and ii) follow immediately.

v) Observing that (see Eqn. (16)) $w=f(x)=(x^{q^2}-x)/(x^q-x)$, we see that the places above $(w=0)$ are exactly the places $(x=\beta)$ with $\beta\in\mathbb{F}_{q^2}\backslash\mathbb{F}_q$. □

Next we consider the subfield $K(u)\subseteq K(x)$ where u is defined by

$$u := \frac{-x^{q(q-1)}}{(x^{q-1}-1)^{q-1}}. \tag{21}$$

Lemma 4.2. *(i) The extension $K(x)/K(u)$ is Galois of degree $q(q-1)$.*

(ii) The place $(u=0)$ of $K(u)$ is totally ramified in $K(x)/K(u)$; the place above it is the place $(x=0)$. We have $d((x=0)|(u=0))=q^2-2$; i.e., $(x=0)|(u=0)$ is weakly ramified.

(iii) *Above the place* $(u=\infty)$ *lie exactly* q *places* P *of* $K(x)$*; namely the places* $(x=\infty)$ *and* $(x=\alpha)$ *with* $\alpha \in \mathbb{F}_q^\times$*. We have* $e(P|(u=\infty)) = q-1$*.*

(iv) *No other place of* $K(u)$ *is ramified in* $K(x)$*.*

(v) *The places above* $(u=1)$ *are exactly the places* $(x=\beta)$ *with* $\beta \in \mathbb{F}_{q^2}\backslash\mathbb{F}_q$*.*

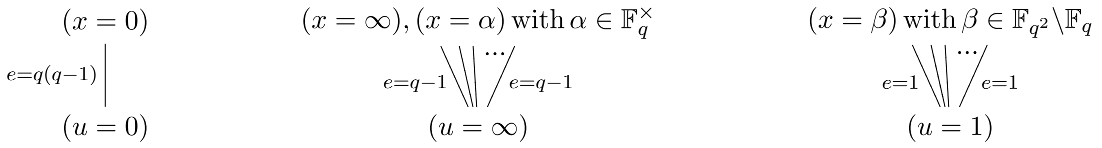

Figure 2: Ramification and splitting in $K(x)/K(u)$.

Proof. Note that $u = 1/(1-f(1/x))$ by Rem. 2.1 and therefore $f(1/x) = (u-1)/u$. The result follows directly from Lemma 4.1 with the change of variables

$$x \mapsto 1/x \quad \text{and} \quad w \mapsto (u-1)/u.$$

□

5 The fields F_1 and F_2

In this section we assume again that $\mathbb{F}_{q^2} \subseteq K$. We want to study ramification in the first two steps of the tower $\mathcal{F}$ over K. So we consider the fields $F_0 = K(x_0)$, $F_1 = K(x_0, x_1)$ and $F_2 = K(x_0, x_1, x_2)$ where

$$(x_1^q - x_1)^{q-1} + 1 = \frac{-x_0^{q(q-1)}}{(x_0^{q-1}-1)^{q-1}} \quad \text{and} \quad (x_2^q - x_2)^{q-1} + 1 = \frac{-x_1^{q(q-1)}}{(x_1^{q-1}-1)^{q-1}}. \tag{22}$$

Lemma 5.1. *The extensions* $F_1/K(x_0)$ *and* $F_1/K(x_1)$ *are both Galois of degree* $q(q-1)$*.*

Proof. We proved the assertion for $F_1/K(x_0)$ in Thm. 2.2. As in Eqn. (11) we set

$$u_0 := \frac{-x_0^{q(q-1)}}{(x_0^{q-1}-1)^{q-1}}.$$

The field F_1 is the compositum of $K(x_0)$ and $K(x_1)$ over $K(u_0)$ as in Figure 3. By Lemma 4.2 the extension $K(x_0)/K(u_0)$ is Galois, hence $F_1/K(x_1)$ is Galois as well.

□

Lemma 5.2. *Let* $\Omega := \mathbb{F}_{q^2} \cup \{\infty\}$*.*

(i) *For a place* $P \in \mathbb{P}(F_1)$ *the following are equivalent:*

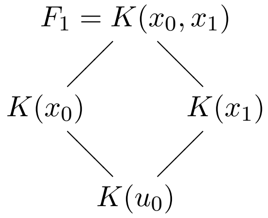

Figure 3: The extension $F_1/K(u_0)$

a) $P|_{K(x_0)} = (x_0 = \omega)$ *for some* $\omega \in \Omega$.

b) $P|_{K(x_1)} = (x_1 = \omega')$ *for some* $\omega' \in \Omega$.

(ii) If a place $Q \in \mathbb{P}(F_1)$ *does not lie above a place* $(x_0 = \omega)$ *with* $\omega \in \Omega$ *then* Q *is unramified over* $K(x_0)$ *and over* $K(x_1)$.

(iii) The ramification indices of the places $(x_0 = \omega)$ *and* $(x_1 = \omega')$ *with* $\omega, \omega' \in \Omega$ *in the extensions* $F_1/K(x_0)$ *and* $F_1/K(x_1)$ *are as depicted in Figure 4. All places of* F_1 *are weakly ramified over* $K(x_0)$ *and over* $K(x_1)$.

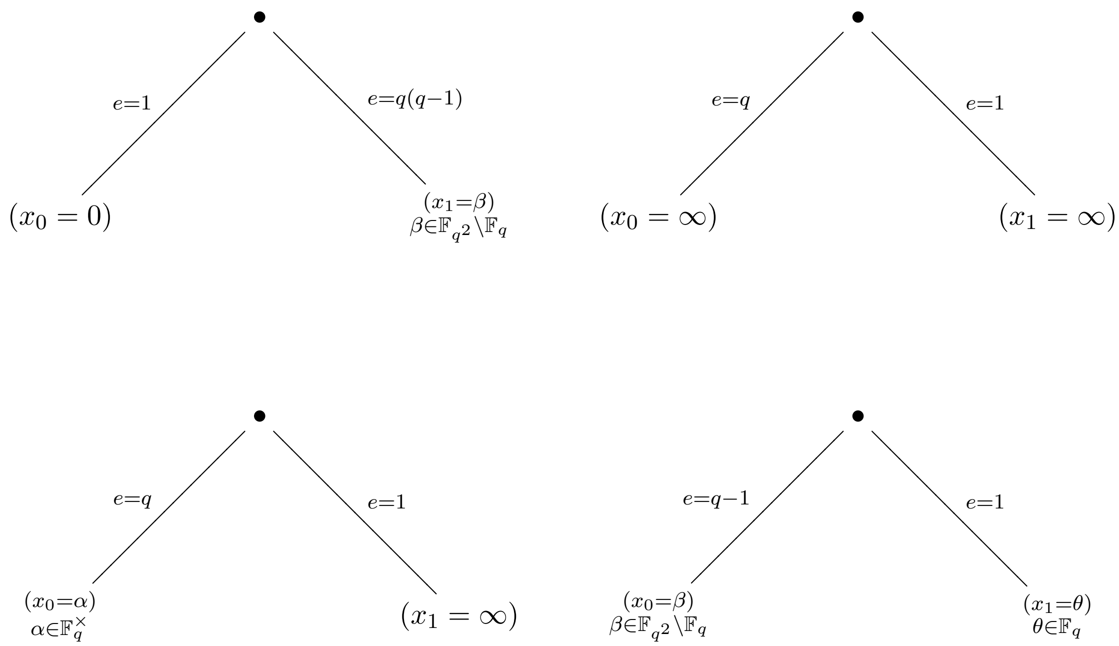

Figure 4: Ramification in $F_1/K(x_0)$ and in $F_1/K(x_1)$.

Proof. According to the notations in Sec. 4 we write $u_0 := -x_0^{q(q-1)}/(x_0^{q-1} - 1)^{q-1}$ and $w_1 := (x_1^q - x_1)^{q-1} + 1$. Hence $u_0 = w_1$ by Eqn. (22). We consider the diagram of fields in Figure 3 where all extensions are Galois of degree $q(q-1)$. We have

$$\begin{aligned} & P|_{K(x_0)} = (x_0 = \omega) \text{ for some } \omega \in \Omega \\ \Leftrightarrow\ & P|_{K(u_0)} \in \{(u_0 = 0), (u_0 = 1), (u_0 = \infty)\} \text{ (by Lemma 4.2)} \\ \Leftrightarrow\ & P|_{K(x_1)} = (x_1 = \omega') \text{ for some } \omega' \in \Omega \text{ (by Lemma 4.1).} \end{aligned}$$

By Lemma 4.1 and Lemma 4.2 we know that only the places $(u_0 = 0)$, $(u_0 = 1)$ and $(u_0 = \infty)$ are ramified in $K(x_0)/K(u_0)$ or in $K(x_1)/K(u_0)$. We will consider here only the case $(u_0 = \infty)$; the other two cases are similar (even easier). Denote by Q a place of F_1 above $(u_0 = \infty)$. The situation is depicted in Figure 5. It follows

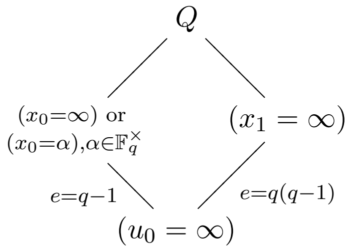

Figure 5: Ramification in $F_1/K(u_0)$

from Abhyankar's Lemma (see [16, Prop. III.8.9]) that Q is unramified over $K(x_1)$ and that the ramification index of Q over $K(x_0)$ is $e = q$. Since $(x_1 = \infty)|(u_0 = \infty)$ is weakly ramified by Lemma 4.1, it follows from the transitivity of different exponents in $F_1 \supseteq K(x_0) \supseteq K(u_0)$ that Q is weakly ramified over $K(x_0)$. □

Lemma 5.3. *The extensions $F_2/K(x_0, x_1)$ and $F_2/K(x_1, x_2)$ are Galois extensions of degree q. All places that are ramified in $F_2/K(x_0, x_1)$ or in $F_2/K(x_1, x_2)$ are totally and weakly ramified.*

Proof. The field F_2 is the compositum of $K(x_0, x_1)$ and $K(x_1, x_2)$ over $K(x_1)$. Since the extensions $K(x_0, x_1)/K(x_1)$ and $K(x_1, x_2)/K(x_1)$ are Galois by Lemma 5.1, it is clear that $F_2/K(x_0, x_1)$ and $F_2/K(x_1, x_2)$ are Galois. The assertion about the degrees follows from Lemma 2.7. Now we consider a place $Q \in \mathbb{P}(F_2)$ which is ramified in $F_2/K(x_1, x_2)$. Then the place $P := Q|_{K(x_0,x_1)}$ is ramified over $K(x_1)$ and therefore $Q|_{K(x_1)} = (x_1 = \beta)$ with some $\beta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, by Lemma 5.2. So we have the situation depicted in Figure 6, where R denotes the restriction of Q to $K(x_1, x_2)$.

As in the proof of Lemma 5.2, we use Abhyankar's lemma to get that $e(Q|R) = q$, and the transitivity of different exponents to get that $d(Q|R) = 2 \cdot (q-1)$.

Now if Q is a place of F_2 which is ramified over F_1, then one also concludes (and it is simpler) that it is totally and weakly ramified over F_1. □

Remark 5.4. It is clear that all statements in this section remain valid when the fields $K(x_0)$, $K(x_0, x_1)$ and $K(x_0, x_1, x_2)$ are replaced by the fields $K(x_n)$, $K(x_n, x_{n+1})$ and $K(x_n, x_{n+1}, x_{n+2})$, respectively.

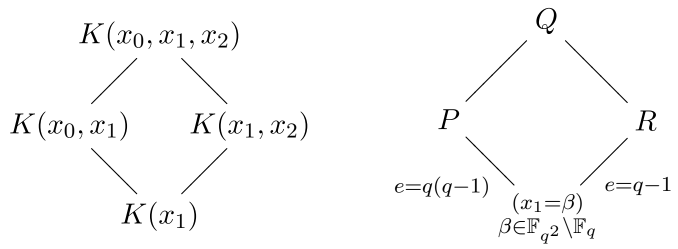

Figure 6:

6 The genus of F_n

In order to estimate the limit $\lambda(\mathcal{F})$ of the tower $\mathcal{F}$ over $\mathbb{F}_{q^3}$ we need an upper bound for the genus of the n-th function field F_n; therefore one has to study ramification in the extension F_n/F_0. Without changing the ramification behaviour (i.e., ramification index and different exponent) and the genus, we can extend the constant field such that it contains $\mathbb{F}_{q^2}$. So we assume in this section that $\mathbb{F}_{q^2} \subseteq K$ and denote $\mathrm{char}(K) = p$.

A place $P \in \mathbb{P}(F_0)$ is said to be ramified in the tower $\mathcal{F}$ if P is ramified in F_m/F_0 for some $m \geq 1$, and the ramification locus $V(\mathcal{F}/F_0)$ is defined as

$$V(\mathcal{F}/F_0) := \{P \in \mathbb{P}(F_0) \mid P \text{ is ramified in } \mathcal{F}\}.$$

Lemma 6.1. *The ramification locus of $\mathcal{F}$ over F_0 satisfies*

$$V(\mathcal{F}/F_0) \subseteq \{(x_0 = \omega) \mid \omega \in \mathbb{F}_{q^2} \text{ or } \omega = \infty\}.$$

Proof. Assume that a place $Q \in \mathbb{P}(F_n)$ is ramified in F_{n+1}/F_n. Then the restriction $Q|_{K(x_n)}$ ramifies in the extension $K(x_n, x_{n+1})/K(x_n)$. We conclude from Lemma 5.2 ii) that $Q|_{K(x_n)} = (x_n = \omega')$ with $\omega' \in \mathbb{F}_{q^2} \cup \{\infty\}$. By induction it follows from Lemma 5.2 i) that $Q|_{F_0} = (x_0 = \omega)$ with $\omega \in \mathbb{F}_{q^2} \cup \{\infty\}$. This proves the lemma. We remark that in fact $V(\mathcal{F}/F_0) = \{(x_0 = \omega) \mid \omega \in \mathbb{F}_{q^2} \text{ or } \omega = \infty\}$ but we do not need this here. $\square$

In the proof of Lemma 6.3 below, the following result is crucial:

Lemma 6.2. *Consider an extension E/F of function fields over K such that $E = E_1 \cdot E_2$ is the composite field of two intermediate fields $F \subseteq E_i \subseteq E$, $i = 1, 2$ and the extensions E_1/F and E_2/F are Galois p-extensions. Let Q be a place of E, and let $Q_i := Q|_{E_i}$ and $P := Q|_F$ be the restrictions of Q. Suppose that $Q_1|P$ and $Q_2|P$ are weakly ramified. Then $Q|Q_1$ and $Q|Q_2$ are also weakly ramified.*

Proof. See [10, Prop. 1.10] and also [9, Lemma 1]. $\square$

A Galois extension E/F is *weakly ramified* if all places are weakly ramified in E/F.

Lemma 6.3. *Let $n \geq 1$. Then the extension F_{n+1}/F_n is weakly ramified.*

Proof. For $0 \le i \le j \le n+1$ we define the subfield $E_{i,j} \subseteq F_{n+1}$ by

$$E_{i,j} := K(x_i, x_{i+1}, \dots, x_j).$$

The extensions $E_{i,i+2}/E_{i,i+1}$ and $E_{i,i+2}/E_{i+1,i+2}$ are weakly ramified Galois p-extensions by Lemma 5.3 (see Figure 7). By induction it follows for all $j \ge i+2$ that $E_{i,j}/E_{i,j-1}$ and $E_{i,j}/E_{i+1,j}$ are weakly ramified Galois p-extensions (using Lemma 6.2). Since $F_n = E_{0,n}$ and $F_{n+1} = E_{0,n+1}$, the assertion of Lemma 6.3 follows. □

Lemma 6.4. *Let E_1/F be a Galois extension of function fields over K and let E/E_1 be a finite and separable extension. Let Q be a place of the field E and denote by P_1 and P the restrictions of Q to E_1 and F, respectively. Suppose that we have:*

(i) $e(Q|P_1)$ is a power of $p = char(K)$ and $d(Q|P_1) = 2\,e(Q|P_1) - 2$.

(ii) The place P_1 is weakly ramified over P.

Then the different exponent $d(Q|P)$ satisfies

$$d(Q|P) = (e_0e_1 - 1) + (e_1 - 1) < e(Q|P) \cdot \Big(1 + \frac{1}{e_0}\Big),$$

where $e(Q|P) = e_0e_1$ with $(p, e_0) = 1$ and e_1 is a p-power.

Proof. Straightforward, using transitivity of different exponents. □

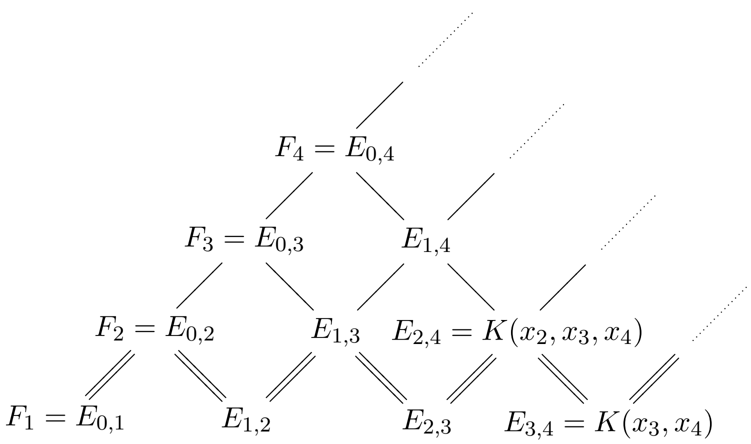

Figure 7: Double lines denote weakly ramified Galois p-extensions

Theorem 6.5. *The genus of the n-th function field of the tower $\mathcal{F} = (F_0, F_1, F_2, \dots)$ defined by Eqn. (8), satisfies*

$$g(F_n) \le \frac{q^2 + 2q}{2} \cdot [F_n : F_0].$$

Proof. Let $n \geq 1$. First we observe that for a place $Q \in \mathbb{P}(F_n)$ and the restriction $P_1 := Q|_{F_1}$ of Q to F_1 we have that

$$e(Q|P_1) \text{ is a } p\text{-power and } d(Q|P_1) = 2e(Q|P_1) - 2.$$

This follows from Lemma 6.3 and repeated applications of Lemma 6.4.

Now we consider the places $P \in \mathbb{P}(F_0)$ which are in the ramification locus $V(\mathcal{F}/F_0)$. According to item (iii) of Lemma 5.2 we distinguish 2 cases:

Case 1: $P = (x_0 = \theta)$ with $\theta \in \mathbb{F}_q$ or $P = (x_0 = \infty)$.

By Lemma 5.2 and Lemma 6.4 we obtain

$$\sum_{\substack{Q \in \mathbb{P}(F_n) \\ Q|P}} d(Q|P) \cdot \deg Q < \sum_{\substack{Q \in \mathbb{P}(F_n) \\ Q|P}} 2e(Q|P) \cdot \deg Q = 2[F_n : F_0]. \tag{23}$$

Case 2: $P = (x_0 = \beta)$ with $\beta \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$.

In this case, Lemma 5.2 and Lemma 6.4 yield

$$\sum_{\substack{Q \in \mathbb{P}(F_n) \\ Q|P}} d(Q|P) \cdot \deg Q < \sum_{\substack{Q \in \mathbb{P}(F_n) \\ Q|P}} \Big(1 + \frac{1}{q-1}\Big) e(Q|P) \cdot \deg Q = \frac{q}{q-1}[F_n : F_0]. \tag{24}$$

There are $q+1$ places $P \in \mathbb{P}(F_0)$ as in Case 1, and $q^2 - q$ places as in Case 2. By Hurwitz genus formula for the extension F_n/F_0 we obtain

$$\begin{aligned} 2g(F_n) &\leq -2[F_n : F_0] + (q+1) \cdot 2[F_n : F_0] + (q^2 - q) \cdot \frac{q}{q-1}[F_n : F_0] \\ &= (q^2 + 2q)[F_n : F_0]. \end{aligned}$$

□

7 The limit of the tower over $K = \mathbb{F}_\ell$ with $\ell = q^3$

Putting together the results of the previous sections we obtain our main result:

Theorem 7.1. *Let $K = \mathbb{F}_\ell$ with $\ell = q^3$, and let $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ be the tower over K which is recursively defined by $F_0 = K(x_0)$ and $F_{n+1} = F_n(x_{n+1})$, where*

$$(x_{n+1}^q - x_{n+1})^{q-1} + 1 = \frac{-x_n^{q(q-1)}}{(x_n^{q-1} - 1)^{q-1}} \quad \textit{for all} \quad n \geq 0.$$

Then the limit $\lambda(\mathcal{F}) = \lim_{n\to\infty} N(F_n)/g(F_n)$ satisfies

$$\lambda(\mathcal{F}) \geq 2(q^2 - 1)/(q + 2).$$

Proof. By Thm. 3.4 and Thm. 6.5 we have

$$N(F_n) \geq (q^3 - q) \cdot [F_n : F_0] \quad \text{and} \quad g(F_n) \leq \frac{q^2 + 2q}{2} \cdot [F_n : F_0].$$

Hence

$$\frac{N(F_n)}{g(F_n)} \geq \frac{(q^3 - q) \cdot 2}{q^2 + 2q} = \frac{2(q^2 - 1)}{q + 2} \quad \text{for all } n \geq 0.$$

□

8 Remarks

We finish this paper with a few remarks.

Remark 8.1. Our tower $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ over $K = \mathbb{F}_{q^3}$ bears remarkable analogy to the tower $\mathcal{H} = (H_0, H_1, H_2, \ldots)$ over the quadratic field $K = \mathbb{F}_{q^2}$ which is defined recursively by the equation

$$u_{i+1}^q + u_{i+1} = \frac{u_i^q}{u_i^{q-1} + 1}$$

and which attains the Drinfel'd–Vlăduţ bound (1). The analogies between $\mathcal{H}$ and $\mathcal{F}$ become even more evident if we substitute $u_i = \xi y_i$ with $\xi^{q-1} = -1$; then the above equation becomes $y_{i+1}^q - y_{i+1} = -y_i^q/(y_i^{q-1} - 1)$. We now compare some features of the towers $\mathcal{F}$ over $\mathbb{F}_{q^3}$ and $\mathcal{H}$ over $\mathbb{F}_{q^2}$, see [8].

1) The tower $\mathcal{H} = (H_0, H_1, H_2, \ldots)$ is defined recursively over the field $K = \mathbb{F}_{q^2}$ by $H_0 = K(y_0)$ and $H_{i+1} = H_i(y_{i+1})$, where

$$y_{i+1}^q - y_{i+1} = \frac{-y_i^q}{y_i^{q-1} - 1} \quad \text{for all } i \geq 0. \tag{25}$$

2) Setting $h(T) := T^q - T$, Eqn. (25) can be written as

$$h(y_{i+1}) = \frac{1}{h(1/y_i)}. \tag{26}$$

3) The extensions H_{i+1}/H_i (for $i \geq 0$) are weakly ramified Galois extensions of degree $[H_{i+1} : H_i] = q$.

4) The ramification locus of $\mathcal{H}$ over H_0 is

$$V(\mathcal{H}/H_0) = \{(y_0 = \omega) \mid \omega \in \mathbb{F}_q \cup \{\infty\}\}.$$

5) The places $(y_0 = \alpha)$ with $\alpha \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$ are completely splitting in the extensions H_n/H_0, for all $n \geq 0$.

The analogous properties of the tower $\mathcal{F}$ are:

1*) The tower $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ is defined recursively over the field $K = \mathbb{F}_{q^3}$ by $F_0 = K(x_0)$ and $F_{i+1} = F_i(x_{i+1})$, where

$$(x_{i+1}^q - x_{i+1})^{q-1} + 1 = \frac{-x_i^{q(q-1)}}{(x_i^{q-1} - 1)^{q-1}} \quad \text{for all } i \geq 0. \tag{27}$$

2*) Setting $f(T) := (T^q - T)^{q-1} + 1$, Eqn. (27) can be written as

$$f(x_{i+1}) = \frac{1}{1 - f(1/x_i)}. \tag{28}$$

3*) The extensions F_{i+1}/F_i (for $i \geq 1$) are weakly ramified Galois extensions of degree $[F_{i+1} : F_i] = q$.

4*) The ramification locus of $\mathcal{F}$ over F_0 is

$$V(\mathcal{F}/F_0) = \{(x_0 = \omega) \mid \omega \in \mathbb{F}_{q^2} \cup \{\infty\}\}.$$

5*) The places $(x_0 = \alpha)$ with $\alpha \in \mathbb{F}_{q^3} \backslash \mathbb{F}_q$ are completely splitting in the extensions F_n/F_0, for all $n \geq 0$.

We also note that the polynomials $h(T)$ and $f(T)$ in Eqn. (26) and Eqn. (28) are defined in a very similar manner:

6) The polynomial $h(T) \in \mathbb{F}_q[T]$ generates the fixed field of $K(T)$ under the group of automorphisms

$$G = \{\sigma : K(T) \to K(T) \bigm| \sigma(T) = T + b \text{ with } b \in \mathbb{F}_q\}.$$

6*) The polynomial $f(T) \in \mathbb{F}_q[T]$ generates the fixed field of $K(T)$ under the group of automorphisms

$$G^* = \{\sigma : K(T) \to K(T) \bigm| \sigma(T) = aT + b \text{ with } a \in \mathbb{F}_q^\times \text{ and } b \in \mathbb{F}_q\}.$$

Another interesting observation is that the generators x_i of the tower $\mathcal{F}$ satisfy

$$x_{i+2}^q - x_{i+2} = \frac{-x_i^q}{(x_i^{q-1} - 1)(x_{i+1}^{q-1} - 1)} \tag{29}$$

for all $i \geq 0$ (with an appropriate choice of the roots x_{i+1}, x_{i+2} of Eqn. (27); see Lemma 2.7). Compare with Eqn. (25).

Remark 8.2. The first explicit tower over a field with cubic cardinality $\ell = q^3$ which attains the Zink bound (Inequality (2)) was found by van der Geer–van der Vlugt [12]. It is a tower over the field $\mathbb{F}_{p^3}$ with $p = 2$, recursively defined by the equation

$$x_{i+1}^2 + x_{i+1} = x_i + 1 + \frac{1}{x_i}. \tag{30}$$

This is the special case $q = 2$ of Eqn. (27) (after the change of variables $x_i \to x_i + 1$).

Remark 8.3. Again we consider the tower $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ over $K = \mathbb{F}_{q^3}$. We set

$$v_i := -\frac{1}{x_i^{q-1} - 1} \quad \text{for all} \quad i \geq 0. \tag{31}$$

It follows by straightforward calculations from Eqn. (27) that

$$\frac{1 - v_{i+1}}{v_{i+1}^q} = \frac{v_i^q + v_i - 1}{v_i}, \quad \text{for all } i \geq 0. \tag{32}$$

This means that $\mathcal{F}$ contains as a subtower the tower $\mathcal{E} = (E_0, E_1, E_2, \ldots)$ (see [3]) with $E_0 = K(v_0)$ and $E_{i+1} = E_i(v_{i+1})$, where v_{i+1} satisfies Eqn. (32) over E_i. Since the limit of a subtower is at least as big as the limit of the tower itself (see [8]), we obtain that

$$\lambda(\mathcal{E}) \geq \lambda(\mathcal{F}) \geq \frac{2(q^2-1)}{q+2}.$$

This gives another (in fact, much simpler) proof of the main result of [3].

Here is another striking analogy between $\mathcal{F}$ and $\mathcal{H}$; again we consider the tower $\mathcal{H} = (H_0, H_1, H_2, \ldots)$ over $K = \mathbb{F}_{q^2}$ given recursively by

$$u_{i+1}^q + u_{i+1} = \frac{u_i^q}{u_i^{q-1} + 1}. \tag{33}$$

Performing the analogous change of variables as in Eqn. (31); i.e., setting

$$w_i := -\frac{1}{u_i^{q-1} + 1} \quad \text{for all } i \geq 0,$$

it follows by straightforward calculations from Eqn. (33) that

$$\frac{w_{i+1} + 1}{w_{i+1}^q} = \frac{w_i^q + 1}{w_i}, \quad \text{for all } i \geq 0. \tag{34}$$

The subtower $\mathcal{G}$ of $\mathcal{H}$ given recursively by Eqn. (34) was studied in [2].

Remark 8.4. We end up this paper with a closer look on the relations between the towers $\mathcal{F}$ and $\mathcal{E}$ given by Eqns. (27) and (32), respectively. One can show that F_1/E_1 is a Galois extension of degree $(q-1)^2$ with group $\mathbb{F}_q^\times \times \mathbb{F}_q^\times$; in fact the automorphisms of $F_1 = \mathbb{F}_{q^3}(x_0, x_1)$ over the subfield $E_1 = \mathbb{F}_{q^3}(v_0, v_1)$ are given by:

$$x_0 \mapsto a x_0 \text{ and } x_1 \mapsto b x_1, \text{ with } a, b \in \mathbb{F}_q^\times.$$

Moreover the n-th field F_n of the tower $\mathcal{F}$ is the compositum with F_1 of the n-th field E_n of the tower $\mathcal{E}$; i.e., we have

$$F_n = E_n \cdot F_1, \quad \text{for all } n \geq 1.$$

The assertions above follow from Eqns. (31) and (29). We note however that for $q \neq 2$ the towers $\mathcal{F}$ and $\mathcal{E}$ are not K-isomorphic; i.e., there is no K-isomorphism

$$\sigma : \bigcup_{i=0}^{\infty} F_i \longrightarrow \bigcup_{j=0}^{\infty} E_j \ .$$

In order to prove this we assume that such an isomorphism σ exists. Then we find integers $n \geq 2$ and $s \geq 2$ such that

$$\sigma(F_1) \subseteq E_n \subseteq E_{n+1} \subseteq \sigma(F_s) \ .$$

In the extension $\sigma(F_s)/\sigma(F_1)$ there occurs only wild ramification by Theorem 2.2, but in the extension E_{n+1}/E_n there is also some tame ramification with ramification index $e = q - 1$, cf. [3], p.177, Fig.1.

Acknowledgment

We would like to thank Y. Ihara for his interest in and helpful discussions about splitting places in the tower $\mathcal{E}$, cf. [14].

References

[1] A. Bassa, H. Stichtenoth, *A simplified proof for the limit of a tower over a cubic finite field*, J. Number Theory **123**, 2007, 154-169.

[2] J. Bezerra, A. Garcia, *A tower with non-Galois steps which attains the Drinfeld-Vladut bound*, J. Number Theory **106**, 2004, 142–154.

[3] J. Bezerra, A. Garcia, H. Stichtenoth, *An explicit tower of function fields over cubic finite fields and Zink's lower bound*, J. Reine Angew. Math. **589**, 2005, 159-199.

[4] V. G. Drinfel'd, S. G. Vlăduţ, *The number of points of an algebraic curve*, Func. Anal. **17**, 1983, 53-54.

[5] N. Elkies, *Explicit modular towers*, Proceedings of the 35th Annual Allerton Conference on Communication, Control and Computing (eds. T. Basar et al.) Urbana IL, 1997, 23-32.

[6] N. Elkies, *Explicit towers of Drinfeld modular curves*, European Congress of Math. (Barcelona, 2000) Vol. II, 189–198, Progr. Math., **202**, Birkhäuser, Basel, 2001.

[7] A. Garcia, H. Stichtenoth, *A tower of Artin–Schreier extensions of function fields attaining the Drinfeld-Vladut bound*, Inventiones Math. **121**, 1995, 211-222.

[8] A. Garcia, H. Stichtenoth, *On the asymptotic behaviour of some towers of functions fields over finite fields*, J. Number Theory **61**, 1996, 248-273.

[9] A. Garcia, H. Stichtenoth, *Some Artin-Schreier towers are easy*, Mosc. Math. J. **5**, 2005, 767-774.

[10] A. Garcia, H. Stichtenoth, *On the Galois closure of towers*, Recent Trends in Coding Theory and its Applications (W. Li, ed.), to appear.

[11] A. Garcia, H. Stichtenoth, *Explicit towers of function fields over finite fields*, Topics in geometry, coding theory and cryptography, 1-58, Algebr. Appl., **6**, Springer, Dordrecht, 2007.

[12] G. van der Geer, M. van der Vlugt, *An asymptotically good tower of curves over the field with eight elements*, Bull. London Math. Soc. **34**, 2002, 291-300.

[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] Y. Ihara, *Some Remarks on the BGS Tower over Finite Cubic Fields*, Proceedings of the conference "Arithmetic Geometry, Related Area and Applications" held at Chuo University, April 2006, 127-131.

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

[16] H. Stichtenoth, *Algebraic function fields and codes*, Springer Verlag, Berlin, 1993.

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

[18] T. Zink, *Degeneration of Shimura surfaces and a problem in coding theory*, in Fundamentals of Computation Theory (L. Budach, ed.), Lecture Notes in Computer Science, Vol. **199**, Springer Verlag, Berlin, 1985, 503-511.