A NEW TOWER OVER CUBIC FINITE FIELDS

ALP BASSA, ARNALDO GARCIA, AND HENNING STICHTENOTH

Abstract. 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, and in the particular case \(q = 2\) it coincides with the tower of van der Geer–van der Vlugt. Many features of the new tower are very similar to those of the optimal wild tower in an earlier work by the second and the third author over the quadratic field \(F_{q^2}\) (whose modularity was shown by Elkies).


Key words and phrases. Towers of function fields, genus, rational places, limits of towers, Zink’s bound, cubic finite fields, Artin–Schreier extensions.

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 \(\ell\). 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 [11] was the first to observe that this inequality can be improved substantially if the genus of \(F\) is large with respect to \(\ell\). 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 \(\ell\) and that \(A(\ell) \geq \sqrt{\ell} - 1\) for \(\ell\) a square. Later Drinfeld and
Vlăduţ [17] showed that
\[ A(\ell) \leq \sqrt{\ell} - 1 \quad \text{for any } \ell. \]  
(1)

Hence we have the equality \( A(\ell) = \sqrt{\ell} - 1 \) for \( \ell \) a square (see also [4], [6], [15]).

Much less is known if \( \ell \) is not a square. One knows that for any \( \ell \) (see Serre [13])
\[ A(\ell) \geq c \cdot \log \ell, \quad \text{for some constant } c > 0. \]

For \( \ell = p^3 \) (\( p \) a prime number), the best known lower bound for \( A(\ell) \) is due to Zink [18]:
\[ A(p^3) \geq \frac{2(p^2 - 1)}{p + 2}. \]  
(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
\[ A(q^3) \geq \frac{2(q^2 - 1)}{q + 2} \]  
(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 [9].

In order to obtain lower bounds for \( A(\ell) \), it is natural to study towers of function fields; i.e., one considers sequences \( G = (G_0, G_1, G_2, \ldots) \) of function fields \( G_i \) over \( \mathbb{F}_\ell \) with \( G_0 \subseteq G_1 \subseteq G_2 \subseteq \ldots \) such that \( g(G_i) \rightarrow \infty \). It is easy to see that the limit
\[ \lambda(G) := \lim_{i \rightarrow \infty} \frac{N(G_i)}{g(G_i)} \]
always exists (see [7]), and it is clear that \( 0 \leq \lambda(G) \leq A(\ell) \).

A particularly interesting example is the tower \( H = (H_0, H_1, H_2, \ldots) \) over the field \( \mathbb{F}_\ell \) with \( \ell = q^2 \), which is defined recursively as follows (see [7]): \( H_0 = \mathbb{F}_\ell(u_0) \) is the rational function field, and for all \( i \geq 0 \) one considers the field \( H_{i+1} = H_i(u_{i+1}) \) with
\[ u_{i+1} = \frac{u_i^q + u_i - 1}{u_i^{q-1} + 1}. \]  
(4)

This tower over \( \mathbb{F}_{q^2} \) has the limit \( \lambda(H) = q - 1 = \sqrt{\ell} - 1 \), and therefore it attains the Drinfeld–Vlăduţ bound (1). Elkies [5] has shown that \( H \) is in fact a modular tower.

In [3] the following tower \( E = (E_0, E_1, E_2, \ldots) \) over a cubic field \( \mathbb{F}_\ell \) with \( \ell = q^3 \) is considered: again \( E_0 = \mathbb{F}_\ell(u_0) \) is the rational function field, and for \( i \geq 0 \) one considers the field \( E_{i+1} = E_i(u_{i+1}) \) with
\[ \frac{1 - v_{i+1}}{v_{i+1}} = \frac{v_i^q + v_i - 1}{v_i}. \]  
(5)

The limit \( \lambda(E) \) satisfies the inequality (thus proving inequality (3)):
\[ \lambda(E) \geq \frac{2(q^2 - 1)}{q + 2}. \]  
(6)

The tower \( H \) over the quadratic field \( \mathbb{F}_\ell \) with \( \ell = q^2 \) which is defined by equation (4) has some nice features which allow a rather simple proof of the equality
λ(ℋ) = q − 1, see [8]. 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 $ℰ$ over the cubic field $ℚ_ℓ$ with $ℓ = q^3$ which is defined by
equation (5) is much more complicated. Here (for $q ≠ 2$) 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 [12], Ihara provides a construction of an infinite Galois extension, which
contains the tower $ℰ$ and exhibits the splitting places of $ℰ$ 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 $ℱ$ over the cubic field $ℚ_ℓ$ with $ℓ = q^3$,
whose limit also satisfies the inequality $λ(ℱ) ≥ 2(q^2 − 1)/(q + 2)$ and which has
good properties than the tower given by the recursion in (5). This new tower
$ℱ = (F_0, F_1, F_2, . . . )$ over $ℚ_ℓ$ is defined as follows: $F_0 = ℚ_ℓ(x_0)$ is the rational
function field over $ℚ_ℓ$, and for $n ≥ 0$ one sets $F_{n+1} = F_n(x_{n+1})$ with

\[ (x_{n+1}^q − x_{n+1})^{q−1} + 1 = \frac{−x_n^{q(q−1)}}{(x_n^{q−1} − 1)^{q−1}}. \]  

(7)

We would like to point out that our proof, that the limit of this new tower also
satisfies the inequality $λ(ℱ) ≥ 2(q^2 − 1)/(q + 2)$, is much easier, shorter and less
computational than the proofs in [3] and [1] for the tower $ℰ$. Moreover, since we
show that $ℰ$ is a subtower of $ℱ$ we also get a new and simpler proof of inequality (6);
in fact, it follows from [7] that $λ(ℰ) ≥ λ(ℱ)$ when $ℰ$ is a subtower of $ℱ$.

Another remark is that while for the two towers over $ℚ_{q^2}$ presented in [6] and [7]
the subtower (i.e., the tower $ℋ$ in [7]) was easier to handle, for the two towers $ℰ$
and $ℱ$ over $ℚ_{q^3}$ the supertower (i.e., the tower $ℱ$) turns out to be much easier to
handle.

Finally we note that the tower $ℱ$ coincides with the van der Geer–van der Vlugt
tower in [16] when $q = 2$, and also that the towers $ℱ$ and $ℋ$ have surprising
similarities (see Section 8).

This paper is organized as follows: In Section 2 we introduce the sequence of
function fields $F_0, F_1, F_2, . . .$ over a field $K ⊇ ℙ_q$ recursively given by (7) and we
show in Theorem 2.2 that they define a tower $ℱ$ over $K$ (i.e., $F_0 ⊆ F_1 ⊆ F_2 ⊆ . . .$, and
$K$ is the full constant field of all fields $F_n$). In Section 3 it is shown that
for $K = ℙ_{q^3}$ 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
$F_n/ℙ_{q^3}$. In Sections 4 and 5 we study ramification in the first steps $F_0 ⊆ F_1 ⊆ F_2$
of the tower. We note that the methods in Sections 4 and 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 Sections 4 and 5
are used in Section 6 to give an upper bound for the genus of the $n$-th function field
$F_n$ of the tower (see Theorem 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 Sections 3 and 6 we obtain in Section 7 the inequality $\lambda(F) \geq 2(q^2 - 1)/(q + 2)$ for $K = \mathbb{F}_{q^2}$, which is the main result of the paper. Finally, in Section 8 we point out some surprising analogies between the tower $\mathcal{F}$ over $\mathbb{F}_{q^2}$ and the tower $\mathcal{H}$ over $\mathbb{F}_{q^2}$ which is defined by (4). We also show that the above-mentioned tower $\mathcal{E}$ is a subtower of $\mathcal{F}$.

**Notation.** 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 $O_P$ the valuation ring of $P$. For $z \in O_P$ we denote by $z(P)$ the residue class of $z$ in $O_P/P$. 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 $d(Q|P) = (e_0 e_1 - 1) + (e_1 - 1)$.

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:

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

(8)

**Remark 2.1.** We set

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

(9)

Then equation (8) can be written as

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

(10)

We also remark that $f(T) = (T^{q^2} - T)/(T^q - T)$, hence the roots of $f(T)$ are exactly the elements $\beta \in \mathbb{F}_{q^2}\setminus\mathbb{F}_q$. This property of the polynomial $f(T)$ will play an important role in Sections 3 and 4.
Theorem 2.2. Let $F$ be the sequence of function fields $F_n$ over $K$ which is defined by (8). Then $F$ 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 Theorem 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

$$u_n := \frac{-x_n^{q(q-1)}}{(x_n^{q-1} - 1)^{q-1}}.$$  \hspace{1cm} (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 $a \in \mathbb{F}_q^*$ 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 $2 \times 2$-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 $\text{ord}(G_{n+1})$ divides $q(q - 1)$.

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 $e^{(i)} \equiv 0 \mod q$, for $1 \leq i \leq n$.

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

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

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 $e^{(1)} \equiv 0 \mod q$.

Now we assume that $v_{P_i}(x_i) < 0$ and $v_{P_i}(x_i)$ divides $(q - 1)^i$ for some $i \in \{1, \ldots, n - 1\}$. From (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 $e^{(i+1)} \equiv 0 \mod q$ and that $v_{P_{i+1}}(x_{i+1})$ divides $(q - 1)^{i+1}$. \qed
Lemma 2.5. \([F_{n+1} : F_n] \equiv 0 \mod q \) for all \(n \geq 0\).

Proof. Follows directly from Lemmas 2.3 and 2.4. \(\square\)

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

\[(x_1^q - x_1)^q - 1 = \frac{-x_0^{q(q-1)}}{(x_0^{q-1} - 1)^{q-1}} = u_0. \quad (12)\]

It follows that

\([K(x_0) : K(u_0)] = [K(x_1) : K(u_0)] = q(q - 1). \quad (13)\]

From (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 virtue of (13). \(\square\)

The next lemma shows a striking property of the recursion in equation (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

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

Proof. By (8) we have

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

Hence we get

\[(x_{n+1}^q - x_{n+1})^{q-1} = \frac{-x_n^{q(q-1)}}{(x_n^{q-1} - 1)^{q-1}} - 1 = \frac{-(x_n^q - x_n)^{q-1} + 1}{(x_n^{q-1} - 1)^{q-1}}\]

\[= \frac{x_n^{q(q-1)}}{(x_n^{q-1} - 1)^{q-1} \cdot (x_n^{q-1} - 1)^{q-1}} = \left(\frac{x_n^{q(q-1)}}{(x_n^{q-1} - 1)^{q-1} \cdot (x_n^{q-1} - 1)}\right)^{q-1}. \quad \square\]

Proof of Theorem 2.2. Putting together the results of the lemmas above, one gets the assertions of Theorem 2.2. \(\square\)
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 Section 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 Section 2, let

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

(15)

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

**Lemma 3.1.** Let $c \in \mathbb{F}_q$ 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 $\beta \in \mathbb{F}_q$ we have that $f(\beta) = 1$ if and only if $\beta$ 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 $\beta \in \mathbb{F}_q$ 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)

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

(16)

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

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

(17)

We will show that if $X = \alpha$ belongs to $\mathbb{F}_{q^3} \setminus \mathbb{F}_q$ then all solutions $Y = \beta \in \mathbb{F}_q$ of equation (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 (17) and the lemmas above.

Using (16) we have:

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

(18)

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

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

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

Equation (17) can also be written as below:

$$f\left(\frac{1}{X}\right) = 1 - \frac{1}{f(Y)}. $$

(19)

Consider now a solution $(\alpha, \beta)$ of (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:

$$f(\beta) = \frac{1}{1 - f\left(\frac{1}{\alpha}\right)} = f\left(\frac{1}{\alpha}\right)^q = 1 - \frac{1}{f(\beta)^q}. $$
In the last two equalities above we have used Lemma 3.3 and (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 \( \mathcal{F} = (F_0, F_1, \ldots) \) be the tower over \( \mathbb{F}_{q^3} \) given recursively by (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 Sections 5 and 6 the ramification behaviour in the tower \( \mathcal{F} \).

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

\[
w := f(x) = (x^q - x)^{q - 1} + 1 \in K(x).
\]

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

(ii) The place \((w = \infty)\) of \( K(x)/K(w) \); 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 \( K(x)/K(w) \).

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

\[
\begin{array}{c|ccc}
\text{place} & (x = \infty) & (x = \theta) & (x = \beta) \\
\hline
\text{ramification index} & e = q(q-1) & e = q-1 & e = q-1 \\
\text{value} & (w = \infty) & (w = 1) & (w = 0)
\end{array}
\]

**Figure 1.** Ramification and splitting in \( K(x)/K(w) \)

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

\[
H := \{ \sigma \in \text{Aut}(K(x)/K) \mid \sigma(x) = ax + b, a \in \mathbb{F}_{q^2}, b \in \mathbb{F}_q \}.
\]

(ii) It is clear from (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. [14, Section III.8]) that \( d((x = \infty)|(w = \infty)) \geq (q(q - 1) - 1) + (q - 1) = q^2 - 2 \). 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 $\text{Diff}(K(x)/K(w))$ satisfies
\[
\deg \text{Diff}(K(x)/K(w)) \geq d((x = \infty)|(w = \infty)) + \sum_{\theta \in \mathbb{F}_q} d((x = \theta)|(w = 1)) \geq (q^2 - 2) + q(q - 2) = 2(q^2 - q - 1).
\]
On the other hand, by Hurwitz genus formula for $K(x)/K(w)$ we have
\[
\deg \text{Diff}(K(x)/K(w)) = -2 + 2[K(x):K(w)] = 2(q^2 - q - 1).
\]
Now the assertions (iv) and (ii) follow immediately.

(v) Observing that (see (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 $\beta \in \mathbb{F}_{q^2}\setminus\mathbb{F}_q$.

Next we consider the subfield $K(u) \subseteq K(x)$ where $u$ is defined by
\[
u := \frac{-x^{q(q-1)}}{(x^{q-1} - 1)^{q-1}}.
\]

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 $\beta \in \mathbb{F}_{q^2}\setminus\mathbb{F}_q$.

\[
\begin{array}{ccc}
(x = 0) & (x = \infty), (x = \alpha) \text{ with } \alpha \in \mathbb{F}_q^\times & (x = \beta) \text{ with } \beta \in \mathbb{F}_{q^2}\setminus\mathbb{F}_q \\
\downarrow e=q(q-1) & \downarrow e=q-1 & \downarrow e=q-1 \\
(u = 0) & (u = \infty) & (u = 1)
\end{array}
\]

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
\[
(x_1^q - x_1)^{q-1} + 1 = \frac{-x_0^{q(q-1)}}{(x_0^{q-1} - 1)^{q-1}} \quad \text{and} \quad (x_2^q - x_2)^{q-1} + 1 = \frac{-x_1^{q(q-1)}}{(x_1^{q-1} - 1)^{q-1}}.
\]
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 Theorem 2.2. As in (11) we set

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

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:

(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 $K(x_1)$.

\begin{figure}[h]
\centering
\begin{tikzpicture}
\node (a) at (0,0) {$F_1 = K(x_0, x_1)$};
\node (b) at (0,-1) {$K(x_0)$};
\node (c) at (1,-1) {$K(x_1)$};
\node (d) at (0,-2) {$K(u_0)$};
\draw (a) -- (b);
\draw (a) -- (c);
\draw (b) -- (d);
\draw (c) -- (d);
\end{tikzpicture}
\caption{The extension $F_1/K(u_0)$}
\end{figure}

\begin{figure}[h]
\centering
\begin{tikzpicture}
\node (a) at (0,0) {$e=1$};
\node (b) at (0,-1) {$e=q(q-1)$};
\node (c) at (1,0) {$e=q$};
\node (d) at (1,-1) {$e=1$};
\node (e) at (-1,0) {$(x_0 = 0)$};
\node (f) at (-1,-1) {$(x_1 = \beta)$};
\node (g) at (0,-0.5) {$\beta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$};
\node (h) at (1,0) {$(x_0 = \infty)$};
\node (i) at (1,-1) {$(x_1 = \infty)$};
\draw (e) -- (f);
\draw (f) -- (g);
\draw (g) -- (h);
\draw (h) -- (i);
\end{tikzpicture}
\caption{Ramification in $F_1/K(x_0)$ and in $F_1/K(x_1)$}
\end{figure}
Proof. According to the notations in Section 4 we write \( u_0 := -x_0^{q(q-1)}/(x_0^{q-1} - 1)^q \) and \( w_1 := (x_1^q - x_1)^{q-1} + 1 \). Hence \( u_0 = w_1 \) by (22). We consider the diagram of fields in Figure 3 where all extensions are Galois of degree \( q(q-1) \). We have

\[
P|_{K(x_0)} = (x_0 = \omega) \text{ for some } \omega \in \Omega
\]

\[
\Leftrightarrow P|_{K(u_0)} \in \{(u_0 = 0), (u_0 = 1), (u_0 = \infty)\} \text{ (by Lemma 4.2)}
\]

\[
\Leftrightarrow P|_{K(x_1)} = (x_1 = \omega') \text{ for some } \omega' \in \Omega \text{ (by Lemma 4.1)}.
\]

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 from Abhyankar’s lemma (see [14, 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 \( F_1 \). \( \square \)
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.

6. The Genus of \(F_n\)

In order to estimate the limit \(\lambda(F)\) of the tower \(F\) over \(\mathbb{F}_{q^n}\) 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 \(\mathbb{F}_{q^n}\). So we assume in this section that \(\mathbb{F}_{q^n} \subseteq K\) and denote \(\text{char}(K) = p\).

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

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

Lemma 6.1. The ramification locus of \(F\) over \(F_0\) satisfies

\[
V(F/F_0) \subseteq \{ (x_0 = \omega) \mid \omega \in \mathbb{F}_{q^n} \text{ or } \omega = \infty \}.
\]

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 \(\omega' \in \mathbb{F}_{q^n} \cup \{\infty\}\). By induction it follows from Lemma 5.2 (i) that \(Q|_{F_0} = (x_0 = \omega)\) with \(\omega \in \mathbb{F}_{q^n} \cup \{\infty\}\). This proves the lemma. We remark that in fact \(V(F/F_0) = \{ (x_0 = \omega) \mid \omega \in \mathbb{F}_{q^n} \text{ or } \omega = \infty \}\) but we do not need this here.

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 \(Q_i|P\) 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 [8, Lemma 1].
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 $0 \leq i \leq j \leq n + 1$ we define the subfield $E_{i,j} \subseteq F_{n+1}$ by

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

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 $j \geq i + 2$ 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 $p = \text{char}(K)$ and $d(Q|P_1) = 2e(Q|P_1) - 2$.

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

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

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

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. □

**Theorem 6.5.** The genus of the $n$-th function field of the tower $F = (F_0, F_1, \ldots)$ defined by (8), satisfies

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

![Figure 7. Double lines denote weakly ramified Galois $p$-extensions](image)
Proof. Let \( n \geq 1 \). First we observe that for a place \( Q \in \mathcal{P}(F_n) \) and the restriction \( P_1 := Q|F_1 \) of \( Q \) to \( F_1 \) we have that
\[
e(Q|P_1) \quad \text{is a } p\text{-power and } d(Q|P_1) = 2e(Q|P_1) - 2.
\]
This follows from Lemma 6.3 and repeated applications of Lemma 6.4.

Now we consider the places \( P \in \mathcal{P}(F_0) \) which are in the ramification locus \( V(F/F_0) \). 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
\[
\sum_{Q \in \mathcal{P}(F_n)} d(Q|P) \cdot \deg Q < \sum_{Q \in \mathcal{P}(F_n)} 2e(Q|P) \cdot \deg Q = 2[F_n : F_0].
\]
(23)

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

In this case, Lemma 5.2 and Lemma 6.4 yield
\[
\sum_{Q \in \mathcal{P}(F_n)} d(Q|P) \cdot \deg Q < \sum_{Q \in \mathcal{P}(F_n)} \left(1 + \frac{1}{q-1}\right) e(Q|P) \cdot \deg Q = \frac{q}{q-1}[F_n : F_0].
\]
(24)

There are \( q+1 \) places \( P \in \mathcal{P}(F_0) \) 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
\[
2g(F_n) \leq -2[F_n : F_0] + (q+1) \cdot 2[F_n : F_0] + (q^2-q) \cdot \frac{q}{q-1}[F_n : F_0] = (q^2+2q)[F_n : F_0].
\]

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

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 Theorems 3.4 and 6.5 we have
\[
N(F_n) \geq (q^3 - q) \cdot [F_n : F_0] \quad \text{and} \quad g(F_n) \leq \frac{q^2+2q}{2}[F_n : F_0].
\]
Hence
\[
\frac{N(F_n)}{g(F_n)} \geq \frac{(q^3-q) \cdot 2}{q^2+2q} = \frac{2(q^2-1)}{q+2} \quad \text{for all } n \geq 0.
\]

\[
\square
\]
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 Drinfeld–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 [7].

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

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

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

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

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

$$V(\mathcal{H}/H_0) = \{ (y_0 = \omega) \mid \omega \in \mathbb{F}_q \cup \{\infty\} \}. \quad (27)$$

5. The places $(y_0 = \alpha)$ with $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ 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

$$(x_{i+1}^q - x_i)^{q-1} + 1 = \frac{-x_i^{q(q-1)}}{(x_i^{q-1} - 1)^{q-1}} \quad \text{for all } i \geq 0. \quad (28)$$

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

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

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

$$V(\mathcal{F}/F_0) = \{ (x_0 = \omega) \mid \omega \in \mathbb{F}_{q^3} \cup \{\infty\} \}. \quad (29)$$

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

W e also note that the polynomials \( h(T) \) and \( f(T) \) in (26) and (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

\[
G = \{ \sigma: K(T) \to K(T) \mid \sigma(T) = T + b \text{ with } b \in \mathbb{F}_q \}.
\]

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

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

Another interesting observation is that the generators \( x_i \) of the tower \( \mathbb{F} \) satisfy

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

for all \( i \geq 0 \) (with an appropriate choice of the roots \( x_{i+1}, x_{i+2} \) of equation (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 [16]. It is a tower over the field \( \mathbb{F}_p^3 \) with \( p = 2 \), recursively defined by the equation

\[
x_{i+1}^q + x_{i+1} = x_{i+1} + 1 + \frac{1}{x_i}.
\]

This is the special case \( q = 2 \) of (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

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

It follows by straightforward calculations from (27) that

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

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 equation (32) over \( E_i \). Since the limit of a subtower is at least as big as the limit of the tower itself (see [7]), 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

\[
u_{i+1}^q + u_{i+1} = \frac{u_i^q}{u_i^{q-1} + 1}.
\]

\[
\ldots
\]
Performing the analogous change of variables as in (31); i.e., setting
\[ w_i := -\frac{1}{u^{q^i-1} + 1} \text{ for all } i \geq 0, \]
it follows by straightforward calculations from (33) that
\[ \frac{w_{i+1} + 1}{w_i^q} = \frac{w_i^q + 1}{w_1} \text{ for all } i \geq 0. \] (34)

The subtower \( \mathcal{G} \) of \( \mathcal{H} \) given recursively by (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 equations (27) and (32), respectively. One can show that \( F_1/E_1 \) is a Galois extension of degree \((q - 1)^2\) with group \( \mathbb{F}_q^* \times \mathbb{F}_q^* \); 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:
\[ x_0 \mapsto ax_0 \text{ and } x_1 \mapsto bx_1, \]
with \( a, b \in \mathbb{F}_q^* \).
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
\[ F_n = E_n \cdot F_1, \text{ for all } n \geq 1. \]
The assertions above follow from (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 \( \sigma \) 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. [12].

References


E-mail address: alpbassa@sabanciuniv.edu

E-mail address: garcia@impa.br

E-mail address: henning@sabanciuniv.edu