AN EXPLICIT TOWER OF FUNCTION FIELDS OVER CUBIC FINITE FIELDS AND ZINK'S LOWER BOUND

JUSCELINO BEZERRA[1], ARNALDO GARCIA[1], HENNING STICHTENOTH[2]

[1] Instituto de Matemática Pura e Aplicada-IMPA
Estrada Dona Castorina 110,
22460-320, Rio de Janeiro RJ,
Brazil

[2] Universität Duisburg-Essen,
FB 6 Mathematik, 45117 Essen,
Germany

Summary: For a function field $F/\mathbb{F}_\ell$ over a finite field of cardinality ℓ, denote by $g(F)$ (resp. $N(F)$) the genus (resp. the number of rational places) of $F/\mathbb{F}_\ell$. In this paper we present an explicit tower of function fields $F_1 \subseteq F_2 \subseteq F_3 \subseteq ...$ over $\mathbb{F}_\ell$ for $\ell = q^3$, such that $\lim_{r\to\infty} N(F_r)/g(F_r) \geq 2(q^2-1)/(q+2)$.

0. Introduction

Let $F/\mathbb{F}_\ell$ be an algebraic function field of one variable, whose full constant field is the finite field of cardinality ℓ. By Weil's theorem, the number $N = N(F)$ of places of degree one of $F/\mathbb{F}_\ell$ is bounded by $N \leq \ell + 1 + 2g\sqrt{\ell}$, where $g = g(F)$ denotes the genus of F. This upper bound is sharp in the sense that there are examples of function fields with $N = \ell + 1 + 2g\sqrt{\ell}$ (if ℓ is a square). However, if the genus of F is large with respect to the size of the constant field, Weil's bound can be improved considerably. This was first observed by Ihara, see [11]. Setting $N_\ell(g) := \max_F\{N(F)\}$, where F runs over all function fields over $\mathbb{F}_\ell$ with $g(F) = g$, and $A(\ell) := \limsup_{g\to\infty} N_\ell(g)/g$, we have the Drinfeld-Vladut bound (see [3])

$$A(\ell) \leq \sqrt{\ell} - 1. \tag{0.1}$$

If $\ell = q^2$ is a square, then inequality (0.1) is in fact an equality. In order to show this, one produces a sequence of function fields $(F_n)_{n\geq 1}$ over $\mathbb{F}_{q^2}$ such that $g(F_n) \to \infty$ and

The first and second authors were partially supported by CNPq-PRONEX # 662408/1996-3 (Brazil), and this work was also partially supported by Sabanci University (Turkey).

$\lim_{n\to\infty} N(F_n)/g(F_n) = q-1$. Ihara [11] and Tsfasman, Vladut and Zink [18] were the first to prove this, by showing that certain modular curves have sufficiently many rational points over $\mathbb{F}_{q^2}$. Garcia and Stichtenoth [6] (see also [5]) gave an explicit and more elementary construction of such a sequence by introducing a tower of function fields $F_1 \subseteq F_2 \subseteq F_3 \subseteq \ldots$ over $\mathbb{F}_{q^2}$ as follows: Let $F_1 = \mathbb{F}_{q^2}(x_1)$ be the rational function field, and for all $i \geq 1$ let $F_{i+1} = F_i(x_{i+1})$ with

$$x_{i+1}^q \cdot x_i^{q-1} + x_{i+1} - x_i^q = 0. \tag{0.2}$$

In the tower given by Eq. (0.2) the genus of the field F_n is $g(F_n) \approx q^{n-1}(q+1)$, and the number of rational places over $\mathbb{F}_{q^2}$ is $N(F_n) \approx q^{n-1}(q^2-1)$, hence $\lim_{n\to\infty} N(F_n)/g(F_n) = q-1$ (for two sequences A_n and B_n, the notation $A_n \approx B_n$ means that $\lim_{n\to\infty} A_n/B_n = 1$). Other explicit towers over $\mathbb{F}_{q^2}$ attaining the Drinfeld-Vladut bound were found subsequently (see [2], [4], [7], [8], [9], [12] and [19]).

In case ℓ is not a square the situation is different. It seems that in this case modular curves do not have enough rational points over $\mathbb{F}_\ell$ in order to produce a sequence of function fields over $\mathbb{F}_\ell$ with $\lim_{n\to\infty} N(F_n)/g(F_n) > 0$. Using classfield theory (in particular the Golod-Şafarevic theorem), Serre (see [14] and [15]) proved the existence of towers $(F_n)_{n\geq 1}$ over $\mathbb{F}_\ell$ such that $\lim_{n\to\infty} N(F_n)/g(F_n) \geq c \cdot \log \ell$ (with a constant $c > 0$, independent of ℓ), hence

$$A(\ell) \geq c \cdot \log \ell > 0 \quad \text{for all } \ell. \tag{0.3}$$

The exact value of $A(\ell)$, however, is not known if ℓ is a non-square. Good lower bounds for $A(\ell)$ were obtained through refinements of Serre's classfield tower method (see [1], [13] and [17]).

In the case $\ell = p^3$ (p a prime number) the best known lower bound is

$$A(p^3) \geq \frac{2(p^2-1)}{p+2}. \tag{0.4}$$

This was shown by Zink [20] using degenerations of Shimura modular surfaces. The method of classfield towers and Zink's approach do not lead to an explicit description of the corresponding function fields. As a mathematical challenge, and also for various applications, e.g. in coding theory and cryptography (see [13] and [16]), it is therefore desirable to construct sequences of function fields $(F_n)_{n\geq 1}$ over $\mathbb{F}_\ell$ explicitly such that $\lim_{n\to\infty} N(F_n)/g(F_n)$ is positive (or even better, a large number).

No explicit sequences with a positive limit are known when ℓ is a prime number. For $\ell = p^t$ with $t > 1$, the tower $F_1 \subseteq F_2 \subseteq F_3 \subseteq \ldots$ over $\mathbb{F}_\ell$ defined recursively by $F_1 = \mathbb{F}_\ell(x_1)$

and $F_{i+1} = F_i(x_{i+1})$ with the relation

$$x_{i+1}^m + (x_i + 1)^m - 1 = 0, \quad \text{where } \ m = (\ell - 1)/(p - 1), \tag{0.5}$$

provides an example with $\lim_{n\to\infty} N(F_n)/g(F_n) \geq 2/(\ell - 2) > 0$, see [9]. However, for $\ell > 4$ the number $2/(\ell - 2)$ is far from the Drinfeld-Vladut bound (0.1).

Recently, van der Geer and van der Vlugt [10] found an explicit tower over the field with 8 elements with a "good" limit. This tower is given recursively by $F_1 = \mathbb{F}_8(x_1)$ and $F_{i+1} = F_i(x_{i+1})$, where

$$x_{i+1}^2 + x_{i+1} = x_i + 1 + 1/x_i. \tag{0.6}$$

For this tower over the finite field $\mathbb{F}_8$ the limit is $\lim_{n\to\infty} N(F_n)/g(F_n) = 3/2$, which is equal to $2(p^2 - 1)/(p + 2)$ for $p = 2$; hence it attains Zink's lower bound (0.4).

It is the aim of this paper to present a new explicit tower $\mathcal{F}$ of function fields over $\mathbb{F}_\ell$ with $\ell = q^3$, for any prime power q. The tower $\mathcal{F}$ is defined recursively by $F_1 = \mathbb{F}_\ell(x_1)$ and, for $i \geq 1$, $F_{i+1} = F_i(x_{i+1})$, where the function x_{i+1} satisfies the following equation over the function field F_i:

$$\frac{1 - x_{i+1}}{x_{i+1}^q} = \frac{x_i^q + x_i - 1}{x_i}. \tag{0.7}$$

The main result is (see Thm.3.3).

Main Theorem. *Let $\ell = q^3$ and let the tower $\mathcal{F} := (F_1 \subseteq F_2 \subseteq F_3 \subseteq ...)$ of function fields $F_i/\mathbb{F}_\ell$ be defined as in (0.7). Then*

$$\lim_{n\to\infty} N(F_n)/g(F_n) \geq \frac{2(q^2 - 1)}{q + 2}.$$

The exact value of the genus $g(F_r)$ is given in Thm.2.9. In the special case of a prime number $p = q$, this Main Theorem provides a new and more elementary proof of Zink's lower bound (0.4) for $A(p^3)$. In Remark 3.7 we point out that the Main Theorem leads to an improvement on the Gilbert-Varshamov bound about the asymptotic behaviour of the parameters of linear codes over $\mathbb{F}_{q^3}$, for all prime powers $q \geq 7$.

The tower in [2] and the van der Geer-van der Vlugt tower [10] provided the inspiration for Equation (0.7). In fact, the tower in [10] is a special case of the tower in (0.7): the substitution $x_i \to 1/x_i$, for all i, transforms Eq.(0.7) into Eq.(0.6) if $q = 2$. But one should note that the cases $q = 2$ and $q > 2$ differ considerably. In the first case (the van der Geer-van der Vlugt tower), all extensions F_{i+1}/F_i are Artin-Schreier extensions of degree 2. For $q > 2$, the extensions F_{i+1}/F_i are of degree q but they are not even Galois. This fact makes the genus calculation more difficult.

The paper is organized as follows: In Section 1 we fix notations and put together some results from the theory of algebraic function fields which will be used later. In Section 2 we study the ramified places in the extensions F_r/F_1 of the tower given by Eq.(0.7), and we determine the genus of F_r for all $r \geq 1$ (see Thm.2.9). It turns out that wild and (for $q > 2$) also tame ramification occur, and that some of the wildly ramified places have a surprising ramification behaviour (see Prop.2.7). The analysis of these places is crucial for the genus calculation. We postpone this analysis to Section 4, as it is very technical. In Section 3 we investigate rational places over $\mathbb{F}_{q^3}$ of the function fields F_r of the tower given by Eq.(0.7). In particular we show that some rational places of the field F_1 split completely in all extensions F_r/F_1 (see Thm.3.2). In conjunction with the genus of F_r, this fact yields the Main Theorem. In Section 5 we present a variation $\mathcal{B}$ of the tower $\mathcal{F}$ above having the same limit over $\mathbb{F}_{q^3}$. The new feature of the tower $\mathcal{B}$ is that it alternates Kummer and Artin-Schreier extensions.

1. Preliminaries

Our general reference for the theory of algebraic function fields is the book [16]. Specifically we will use the following notations:

$\mathbb{F}_\ell$	- the finite field of cardinality ℓ,
$\bar{\mathbb{F}}_\ell$	- an algebraic closure of $\mathbb{F}_\ell$,
K	- any field (in most cases, $K = \mathbb{F}_\ell$ or $\bar{\mathbb{F}}_\ell$),
$F, E, H...$	- algebraic function fields of one variable over K,
$g(F)$	- the genus of F/K,
$\mathbb{P}(F)$	- the set of places of F/K,
$(x = \gamma)$	- the place of the rational function field $K(x)$ which is a zero of $x - \gamma$ (for $\gamma \in K$), resp. the pole of x (for $\gamma = \infty$),
v_P	- the normalized discrete valuation of F/K associated with the place $P \in \mathbb{P}(F)$,
$N(F)$	- the number of rational places (= places of degree one) of F/K, in case $K = \mathbb{F}_\ell$.

Let E/F be a finite separable extension of function fields over K, let $P \in \mathbb{P}(F)$ and let $Q \in \mathbb{P}(E)$ be a place lying over P. Then we write $Q|P$ or $P = Q|_F$ and we denote

$e(Q\|P)$	- the ramification index of $Q\|P$,
$d(Q\|P)$	- the different exponent of $Q\|P$.

A tower of function fields over a field K is an infinite sequence $\mathcal{F} = (F_i)_{i \geq 1}$ of function fields F_i/K with the following properties:

i) $F_1 \underset{\neq}{\subsetneq} F_2 \underset{\neq}{\subsetneq} F_3 \underset{\neq}{\subsetneq} \ldots$,

ii) all extensions F_{i+1}/F_i are separable,

iii) $g(F_i) > 1$ for some i.

It follows from the Hurwitz genus formula that $g(F_n) \to \infty$ for $n \to \infty$. We note that K should be the full constant field of F_i for all i; i.e., the field K should be algebraically closed in F_i for all i.

For the convenience of the reader we recall a few results about ramification in extensions of function fields.

Lemma 1.1. *Let $E = F(y)$ be a finite separable extension of algebraic function fields over K, and let $\varphi(T) \in F[T]$ be the irreducible monic polynomial of the function y over the field F. Let $P \in \mathbb{P}(F)$ be a place of F/K.*

i) *Suppose that y is integral at P (i.e. $v_P(c) \geq 0$ for all coefficients c of $\varphi(T)$), and that $v_Q(\varphi'(y)) = 0$ for all $Q \in \mathbb{P}(E)$ with $Q|P$. Then the place P is unramified in E/F.*

ii) *If $Q|P$ is totally ramified (i.e. $e(Q|P) = [E : F]$) and if y is a prime element at the place Q, then*

$$d(Q|P) = v_Q(\varphi'(y)).$$

Proof. [16], Ch.III.5. □

Another result which will be used frequently in Sections 2 and 4 is a special case of Abhyankar's lemma (plus the transitivity of different exponents).

Lemma 1.2. *Let E/F be a separable extension of function fields over K, and let F_1, F_2 be intermediate fields $F \subset F_i \subset E$ such that $E = F_1 \cdot F_2$ is the composite field of F_1 and F_2. Let $Q \in \mathbb{P}(E)$ and denote $P := Q|_F$ and $P_i := Q|_{F_i}$ for $i = 1, 2$. Suppose that the ramification indices $e_i = e(P_i|P)$ (for $i = 1, 2$) are relatively prime and that e_1 is relatively prime to the characteristic of K. Then*

i) *$e(Q|P_2) = e_1$ and $e(Q|P_1) = e_2$.*

ii) *$d(Q|P_1) = e_1 \cdot d(P_2|P) - (e_1 - 1)(e_2 - 1)$.*

In particular, $d(Q|P_1) = d(P_2|P)$ if $e_1 = 1$.

Proof. From Abhyankar's lemma (see [16], Ch.III.8) it follows immediately that we have $e(Q|P_1) = e_2$ and $e(Q|P_2) = e_1$, and hence $Q|P_2$ is tame. By the transitivity of different exponents (see [16], Ch.III.4) we obtain

$$d(Q|P) = d(Q|P_1) + e(Q|P_1) \cdot d(P_1|P) = d(Q|P_1) + e_2(e_1 - 1),$$

and also

$$d(Q|P) = d(Q|P_2) + e(Q|P_2) \cdot d(P_2|P) = (e_1 - 1) + e_1 \cdot d(P_2|P).$$

Hence

$$d(Q|P_1) = e_1 \cdot d(P_2|P) + (e_1 - 1) - e_2(e_1 - 1).$$

□

As we pointed out in the introduction we want to investigate the tower of function fields $F_1 \subseteq F_2 \subseteq F_3 \subseteq ...$ over $K = \mathbb{F}_\ell$ ($\ell = q^3$), resp. over $K = \bar{\mathbb{F}}_\ell$, where $F_{i+1} = F_i(x_{i+1})$ with the relation

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

We put together some properties of the corresponding "basic function field":

Proposition 1.3. *Let $K = \bar{\mathbb{F}}_\ell$ and consider the function field $F = K(x, y)$ with defining equation*

$$\frac{1 - y}{y^q} = \frac{x^q + x - 1}{x}. \tag{1.1}$$

Then the following holds:

i) $[F : K(x)] = [F : K(y)] = q$.

ii) *The place $(x = 0)$ of $K(x)/K$ is totally ramified in $F/K(x)$; i.e., there is exactly one place $P_0 \in \mathbb{P}(F)$ with $P_0|(x = 0)$. We have $e(P_0|(x = 0)) = q$ and $d(P_0|(x = 0)) = q$.*

iii) *The place $(x = \infty)$ is totally ramified in the extension $F/K(x)$; i.e., there is exactly one place $P_\infty \in \mathbb{P}(F)$ with $P_\infty|(x = \infty)$. We have that $e(P_\infty|(x = \infty)) = q$ and that $d(P_\infty|(x = \infty)) = 2q - 2$.*

iv) *Let $R := \{\alpha \in K \ ; \ \alpha^q + \alpha = 1\}$. Then for $\alpha \in R$, the place $(x = \alpha)$ of $K(x)$ has exactly two places P_α and $Q_\alpha \in \mathbb{P}(F)$ above it. We have that $e(P_\alpha|(x = \alpha)) = 1$ and that $e(Q_\alpha|(x = \alpha)) = q - 1$.*

v) *All other places of $K(x)$ are unramified in $F/K(x)$.*

vi) *For any $\alpha \in R$, there is a unique place $S_\alpha \in \mathbb{P}(F)$ above the place $(y = \alpha)$ of $K(y)$, and this place is a common zero of $x - 1$ and $y - \alpha$.*

vii) *The principal divisors in the function field F of the functions $x, x - 1, x - \alpha$ and of $y, y - 1, y - \alpha$ (for $\alpha \in R$) are as follows:*

$(x) = qP_0 - qP_\infty$,

$(x-1) = \sum_{\alpha \in R} S_\alpha - qP_\infty$,

$(x-\alpha) = P_\alpha + (q-1)Q_\alpha - qP_\infty$,

$(y) = P_0 + (q-1)P_\infty - \sum_{\beta \in R} Q_\beta$,

$(y-1) = \sum_{\alpha \in R} P_\alpha - \sum_{\beta \in R} Q_\beta$,

$(y-\alpha) = qS_\alpha - \sum_{\beta \in R} Q_\beta$.

Proof. We only show the assertions concerning the different exponents in items ii) and iii), and we leave the rest to the reader.

ii) Let $P_0 \in \mathbb{P}(F)$ be a zero of x in F. Then it follows from Eq.(1.1) that $v_{P_0}(x) = q$ and $v_{P_0}(y) = 1$; i.e., the function y is a prime element at P_0. The minimal polynomial of y over $K(x)$ is

$$\sigma(T) = T^q + \frac{x}{x^q + x - 1} \cdot T - \frac{x}{x^q + x - 1}$$

and hence $d(P_0|(x_0 = 0)) = v_{P_0}(\sigma'(y)) = v_{P_0}(x/(x^q + x - 1)) = q$, by Lemma 1.1.

iii) Now we consider a pole P_∞ of x in F. Again from Eq.(1.1) we obtain that $v_{P_\infty}(x) = -q$ and $v_{P_\infty}(y) = q - 1$, so the function $t := (xy)^{-1}$ is a prime element for P_∞. Its irreducible polynomial over $K(x)$ is

$$\tau(T) = T^q - \frac{1}{x} \cdot T^{q-1} - \frac{x^q + x - 1}{x^{q+1}},$$

and hence $d(P_\infty|(x = \infty)) = v_{P_\infty}(\tau'(t)) = v_{P_\infty}(x^{-1} \cdot t^{q-2}) = q + (q-2) = 2q - 2$. □

As an easy consequence we obtain from Prop.1.3 that (for $q > 2$) both extensions $F/K(x)$ and $F/K(y)$ are non-Galois. This follows from the ramification behaviour of the places $(x = \alpha)$ in $F/K(x)$, resp. the place $(y = 0)$ in $F/K(y)$.

2. Ramification and genus

First we introduce some additional notation (valid throughout this section.)

$K = \bar{\mathbb{F}}_q$ is an algebraic closure of $\mathbb{F}_q$ and $R = \{\alpha \in K \ ; \ \alpha^q + \alpha = 1\}$.

$\mathcal{F} = (F_1, F_2, F_3, ...)$ is the sequence of function fields over K, where $F_1 = K(x_1)$ is the rational function field and, for all $i \geq 1$, $F_{i+1} = F_i(x_{i+1})$ with

$$\frac{1 - x_{i+1}}{x_{i+1}^q} = \frac{x_i^q + x_i - 1}{x_i}. \tag{2.1}$$

For a place $Q \in \mathbb{P}(F_r)$, we set

$$Q_j := Q|_{F_j} \ \text{ for } j = 1, \ldots, r$$

and we write, for $\gamma \in K \cup \{\infty\}$,

$$x_j = \gamma \;\text{ at } Q \quad \text{if} \qquad Q|(x_j = \gamma).$$

Lemma 2.1. *For all $r \geq 1$ the following holds:*

i) $[F_r : F_1] = q^{r-1}$.

ii) *The place $(x_1 = 0)$ of F_1/K has a unique extension $Q \in \mathbb{P}(F_r)$. This place Q is also a zero of the function x_r, and we have $e(Q|(x_1 = 0)) = q^{r-1}$ and $e(Q|(x_r = 0)) = 1$.*

Proof. Since Eq.(2.1) is an equation of degree q in the variable x_{i+1}, it is clear that $[F_{j+1} : F_j] \leq q$ for all $j \geq 1$, and therefore $[F_r : F_1] \leq q^{r-1}$.
Now let $Q \in \mathbb{P}(F_r)$ be a zero of x_1 in F_r. It is sufficient to show that Q is a zero of x_r, and that $e(Q|(x_1 = 0)) = q^{r-1}$ and $e(Q|(x_r = 0)) = 1$. The case $r = 1$ is trivial, and we assume that our assertion is true for some r. We choose a place $Q' \in \mathbb{P}(F_{r+1})$ with $Q'|Q$ and set $Q_1 := Q'|_{K(x_r, x_{r+1})}$. By Prop.1.3 we conclude that Q_1 is a zero of x_{r+1} with $e(Q_1|(x_r = 0)) = q$ and $e(Q_1|(x_{r+1} = 0)) = 1$. It follows that $e(Q'|(x_{r+1} = 0)) = 1$ and $e(Q'|Q) = e(Q_1|(x_r = 0)) = q$, by Abhyankar's lemma. Hence $e(Q'|(x_1 = 0)) = q^{r-1} \cdot q = q^r$. □

We will show later (see Thm.2.9) that $g(F_3) > 1$, and therefore we have:

Corollary 2.2. *The sequence $\mathcal{F} = (F_i)_{i \geq 1}$ which is defined recursively by Eq.(2.1) is a tower of function fields over K and, for all $j \geq 1$, we have $[F_{j+1} : F_j] = q$.*

The main goal in this section is to determine the genus $g(F_r)$ for all $r \geq 1$; hence we must study the ramification behaviour of places in the tower $\mathcal{F}$. Our next lemma follows immediately from Prop.1.3 vii).

Lemma 2.3. *Let $r \geq 2$ and consider a place $Q \in \mathbb{P}(F_r)$.*

i) *For $1 \leq j < r$ the following holds at the place Q:*
- *if $x_j = 0$ or $x_j = \infty$ then $x_{j+1} = 0$,*
- *if $x_j = \alpha$ for some $\alpha \in R$ then either $x_{j+1} = \infty$ or $x_{j+1} = 1$,*
- *if $x_j = 1$ then $x_{j+1} = \alpha$ for some $\alpha \in R$.*

ii) *For $2 \leq j \leq r$ we have at the place Q:*
- *if $x_j = 0$ then either $x_{j-1} = 0$ or $x_{j-1} = \infty$,*
- *if $x_j = 1$ or $x_j = \infty$ then $x_{j-1} = \alpha$ for some $\alpha \in R$,*
- *if $x_j = \alpha$ with $\alpha \in R$ then $x_{j-1} = 1$.*

Now we analyze the places $Q \in \mathbb{P}(F_r)$ of the function field F_r which are ramified in the extension F_r/F_1.

Proposition 2.4. *Let $r \geq 2$ and let $Q \in \mathbb{P}(F_r)$ be a place which is ramified in the extension F_r/F_1. Then Q is of one of the following types:*

Type 1: $x_1 = 0$ at Q,
Type 2: $x_1 = \infty$ at Q,
Type 3: $x_s = \infty$ at Q, for some s with $1 < s \leq r$.

Proof. Recall that Q_j denotes the restriction of the place Q to the field $F_j \subseteq F_r$, for $1 \leq j \leq r$. Since $Q|Q_1$ is ramified, there is some $j \leq r-1$ such that $Q_{j+1}|Q_j$ is ramified. Hence the place Q ramifies in the extension $K(x_j, x_{j+1})/K(x_j)$ by Abhyankar's lemma (strictly speaking, the restriction of Q to $K(x_j, x_{j+1})$ ramifies over $K(x_j)$). It follows from Prop.1.3 that $x_{j+1} = 0$ or $x_{j+1} = \infty$ at Q. Now we apply Lemma 2.3 ii) to obtain our assertion. □

The ramification behaviour of each of these 3 types of places of F_r is quite different from each other; we will discuss it in the subsequent propositions.

Proposition 2.5. *(Type 1) There is exactly one place $Q \in \mathbb{P}(F_r)$ which is a zero of x_1, and the following holds:*

i) *$e(Q_j|Q_{j-1}) = q$, $e(Q_j|(x_j = 0)) = 1$ and $d(Q_j|Q_{j-1}) = q$, for $2 \leq j \leq r$.*

ii) *$d(Q|Q_1) = q(q^{r-1} - 1)/(q-1)$.*

Proof. We have already shown in Lemma 2.1 that x_1 has a unique zero Q in F_r, and that Q is a simple zero of x_r. It remains to determine the different exponents of $Q_j|Q_{j-1}$ and of $Q|Q_1$. We set $P_j := Q|_{K(x_{j-1}, x_j)}$ and then $d(P_j|(x_{j-1} = 0)) = q$ by Prop.1.3 ii). Since Q_{j-1} is a simple zero of x_{j-1} by item i), it follows from Lemma 1.2 that $d(Q_j|Q_{j-1}) = d(P_j|(x_{j-1} = 0)) = q$.

Item ii) follows by induction from item i), using the transitivity of different exponents (see [16], Ch.III.4). □

Proposition 2.6. *(Type 2) There is exactly one place $Q \in \mathbb{P}(F_r)$ which is a pole of x_1. This place is a common zero of $x_2, \ldots, x_r$, and we have*

i) *$e(Q_j|Q_{j-1}) = q$, $e(Q_j|(x_j = 0)) = q - 1$ and $d(Q_j|Q_{j-1}) = 2q - 2$, for each index j with $2 \leq j \leq r$.*

ii) *$d(Q|Q_1) = 2(q^{r-1} - 1)$.*

Proof. i) Let $Q \in \mathbb{P}(F_r)$ be a pole of x_1. It follows from Lemma 2.3 i) that Q is a zero of $x_2, \ldots, x_r$, and we prove the remaining assertions by induction over j. The case $j = 2$ follows from Prop.1.3. Now let $2 \leq j \leq r-1$. By induction hypothesis, the place Q_j is a zero of x_j with $e(Q_j|(x_j = 0)) = q - 1$. Let $P_{j+1} = Q|_{K(x_j, x_{j+1})}$. Again by Prop.1.3 we have that $e(P_{j+1}|(x_j = 0)) = q$, $e(P_{j+1}|(x_{j+1} = 0)) = 1$ and $d(P_{j+1}|(x_j = 0)) = q$. By Abhyankar's lemma we conclude that $e(Q_{j+1}|Q_j) = q$ and $e(Q_{j+1}|(x_{j+1} = 0)) = q - 1$, and by Lemma 1.2

we obtain

$$d(Q_{j+1}|Q_j) = (q-1)\cdot q - (q-2)(q-1) = 2q-2.$$

ii) Follows easily from item i) by induction over r. □

The ramification behaviour of places Q of Type 3 (see Prop.2.4) is much more complicated. These places are characterized by the condition $x_s = \infty$ at Q for some s with $1 < s \leq r$. We must distinguish the cases $s \equiv 1 \bmod 2$ and $s \equiv 0 \bmod 2$.

Proposition 2.7. *(Type 3 and s odd). Let $1 < s \leq r$ and $s \equiv 1 \bmod 2$, and let the place $Q \in \mathbb{P}(F_r)$ be a pole of the function x_s. Then we have:*

i) *The place Q_s is ramified in $F_s/K(x_s)$ with ramification index*

$$e(Q_s|(x_s=\infty)) = q^{(s-1)/2}.$$

ii) *The restriction Q_j of the place Q satisfies*

$$e(Q_j|Q_{j-1}) = \begin{cases} 1 & \textit{if } 2 \leq j \leq s-1, \\ q-1 & \textit{if } j = s, \\ q & \textit{if } s < j < 2s \textit{ and } j \equiv 0 \bmod 2, \\ 1 & \textit{if } s < j < 2s \textit{ and } j \equiv 1 \bmod 2, \\ q & \textit{if } j \geq 2s. \end{cases}$$

In all cases where $e(Q_j|Q_{j-1}) = q$, the different exponent is

$$d(Q_j|Q_{j-1}) = 2q-2.$$

iii) *The different exponent of $Q|Q_1$ is*

$$d(Q|Q_1) = \begin{cases} q^{(2r-3s+3)/2} - 2 & \textit{if } s \leq \dfrac{r+1}{2}, \\[2ex] q^{(r-s+3)/2} - 2 & \textit{if } \dfrac{r+1}{2} < s \leq r \textit{ and } r \equiv 0 \bmod 2, \\[2ex] q^{(r-s+2)/2} - 2 & \textit{if } \dfrac{r+1}{2} < s \leq r \textit{ and } r \equiv 1 \bmod 2. \end{cases}$$

iv) *Let $A_{r,s} := \#\{Q \in \mathbb{P}(F_r)\ ;\ Q \textit{ is a pole of } x_s\}$. Then*

$$A_{r,s} = \begin{cases} q^{s-1} & \textit{if } s \leq \dfrac{r+1}{2}, \\[2ex] q^{(r-2)/2} & \textit{if } \dfrac{r+1}{2} < s \leq r \textit{ and } r \equiv 0 \bmod 2, \\[2ex] q^{(r-1)/2} & \textit{if } \dfrac{r+1}{2} < s \leq r \textit{ and } r \equiv 1 \bmod 2. \end{cases}$$

Proof. The proof of items i) and ii) is hard and it is the content of Section 4.

iii) First we consider the case $s \leq \frac{r+1}{2}$, i.e. the case $r \geq 2s-1$. By item ii) and the transitivity of different exponents, the different exponent of $Q_{2s-1}|Q_1$ is

$$d(Q_{2s-1}|Q_1) = q^{(s-1)/2} \cdot (q-2) + (\sum_{i=0}^{(s-3)/2} q^i) \cdot (2q-2) = q^{(s+1)/2} - 2.$$

Again from ii) and the transitivity, we obtain

$$d(Q_r|Q_1) = q^{r-(2s-1)} \cdot d(Q_{2s-1}|Q_1) + (\sum_{i=0}^{r-2s} q^i) \cdot (2q-2)$$

$$= q^{r-(2s-1)+(s+1)/2} - 2 = q^{(2r-3s+3)/2} - 2.$$

In case $\frac{r+1}{2} < s \leq r$ and $r \equiv 0 \bmod 2$, we obtain in a similar manner that

$$d(Q_r|Q_1) = q^{(r-s+1)/2} \cdot (q-2) + (\sum_{i=0}^{(r-s-1)/2} q^i) \cdot (2q-2) = q^{(r-s+3)/2} - 2.$$

In case $\frac{r+1}{2} < s \leq r$ and $r \equiv 1 \bmod 2$, we have

$$d(Q_r|Q_1) = q^{(r-s)/2} \cdot (q-2) + (\sum_{i=0}^{(r-s-2)/2} q^i) \cdot (2q-2) = q^{(r-s+2)/2} - 2.$$

iv) By items i) and ii), all poles $Q \in \mathbb{P}(F_r)$ of the function x_s have the same pole order, namely

$$e(Q|(x_s = \infty)) = \begin{cases} q^{r-s} & \text{if } s \leq \dfrac{r+1}{2}, \\ q^{r/2} & \text{if } \dfrac{r+1}{2} < s \leq r \text{ and } r \equiv 0 \bmod 2, \\ q^{(r-1)/2} & \text{if } \dfrac{r+1}{2} < s \leq r \text{ and } r \equiv 1 \bmod 2. \end{cases}$$

Since $q^{r-1} = [F_r : K(x_s)] = A_{r,s} \cdot e(Q|(x_s = \infty))$, we obtain the desired result. □

Proposition 2.8. *(Type 3 and s even) Let $1 < s \leq r$ and $s \equiv 0 \bmod 2$, and let the place $Q \in \mathbb{P}(F_r)$ be a pole of the function x_s. Then we have:*

i) *The place Q_s has ramification index $e(Q_s|(x_s = \infty)) = q^{(s-2)/2}$ in the extension $F_s/K(x_s)$.*

ii) *The restriction Q_j of the place Q satisfies*

$$e(Q_j|Q_{j-1}) = \begin{cases} 1 & \textit{if } 2 \le j \le s-1, \\ q-1 & \textit{if } j = s, \\ q & \textit{if } s < j \le 2s-2 \textit{ and } j \equiv 1 \bmod 2, \\ 1 & \textit{if } s < j \le 2s-2 \textit{ and } j \equiv 0 \bmod 2, \\ q & \textit{if } j \ge 2s-1. \end{cases}$$

In all cases where $e(Q_j|Q_{j-1}) = q$, the different exponent is

$$d(Q_j|Q_{j-1}) = 2q-2.$$

iii) *The different exponent of $Q|Q_1$ is*

$$d(Q|Q_1) = \begin{cases} q^{(2r-3s+4)/2} - 2 & \textit{if } s \le \dfrac{r+2}{2}, \\ q^{(r-s+2)/2} - 2 & \textit{if } \dfrac{r+2}{2} < s \le r \textit{ and } r \equiv 0 \bmod 2, \\ q^{(r-s+3)/2} - 2 & \textit{if } \dfrac{r+2}{2} < s \le r \textit{ and } r \equiv 1 \bmod 2. \end{cases}$$

iv) *Let $A_{r,s} = \#\{Q \in \mathbb{P}(F_r)\ ;\ Q \text{ is a pole of } x_s\}$. Then*

$$A_{r,s} = \begin{cases} q^{s-1} & \textit{if } s \le \dfrac{r+2}{2}, \\ q^{r/2} & \textit{if } \dfrac{r+2}{2} < s \le r \textit{ and } r \equiv 0 \bmod 2, \\ q^{(r-1)/2} & \textit{if } \dfrac{r+2}{2} < s \le r \textit{ and } r \equiv 1 \bmod 2. \end{cases}$$

Proof. First we assume that $s \ge 4$. Then we know the ramification behaviour of the place Q in the field $K(x_2, \dots, x_s, \dots, x_r)$ from Prop.2.7. Moreover, the place Q_2 is unramified in the extensions $K(x_1, x_2)/K(x_1)$ and $K(x_1, x_2)/K(x_2)$ by Prop.1.3. All assertions of the items i), ii) and iii) in Prop.2.8 follow now by Abhyankar's lemma. In the case $s = 2$ we apply Prop.2.6 instead of Prop.2.7 to the field $K(x_2, \dots, x_r)$. Item iv) is proved similarly as in Prop.2.7. □

Theorem 2.9. *Let $\mathcal{F} = (F_1, F_2, F_3, ...)$ be the tower over $K = \bar{\mathbb{F}}_q$ defined by Eq.(2.1). Then the genus $g(F_r)$ satisfies*

$$\lim_{r\to\infty} \frac{g(F_r)}{q^r} = \frac{q+2}{2(q-1)}.$$

More precisely we have:

i) *For* $r \equiv 0 \bmod 4$,

$$g(F_r) = \frac{1}{2(q-1)}(q^{r+1} + 2q^r - 2q^{(r+2)/2} - 2q^{r/2} + q) \; - \; \frac{r}{4} \cdot q^{(r-2)/2} \cdot (q+1).$$

ii) *For* $r \equiv 2 \bmod 4$,

$$g(F_r) = \frac{1}{2(q-1)}(q^{r+1} + 2q^r - 4q^{(r+2)/2} + q) \; - \; \frac{r-2}{4} \cdot q^{(r-2)/2} \cdot (q+1).$$

iii) *For* $r \equiv 1 \bmod 2$,

$$g(F_r) = \frac{1}{2(q-1)}(q^{r+1} + 2q^r - q^{(r+3)/2} - 3q^{(r+1)/2} + q) \; - \; \frac{r-1}{2} \cdot q^{(r-1)/2}.$$

Proof. We will only consider the case $r \equiv 0 \bmod 4$; the other cases are similar and we leave them to the reader.

For $2 \leq s \leq r$ we choose a place $Q^{(s)} \in \mathbb{P}(F_r)$ which is a pole of x_s, and we denote by

$$d_s := d(Q^{(s)}|Q_1^{(s)})$$

the different exponent of $Q^{(s)}$ over $Q_1^{(s)} := Q^{(s)}|_{F_1}$. As in Prop.2.7 and 2.8, we let $A_{r,s}$ denote the number of poles of x_s in F_r. Applying Prop.2.4, 2.5 and 2.6, we see that the degree of the different of the extension F_r/F_1 is

$$\deg \text{ Diff } (F_r/F_1) = \frac{q^r - q}{q-1} \; + \; 2(q^{r-1} - 1) \; + \; \sum_{s=2}^{r} d_s \cdot A_{r,s}. \tag{2.2}$$

According to Prop.2.7 and 2.8 we split the sum $\sum d_s \cdot A_{r,s}$ into four pieces as follows:

$$D_r^{(j)} := \sum_{s \in M_j} d_s \cdot A_{r,s} \quad \text{for} \quad j = 1, 2, 3 \quad \text{and} \quad 4,$$

where the set M_j is defined as

$$M_1 := \quad \{s \in \mathbb{N}\,; s \equiv 1 \bmod 2 \quad \text{and} \quad 3 \leq s \leq (r+1)/2\},$$

$$M_2 := \quad \{s \in \mathbb{N}\,; s \equiv 1 \bmod 2 \quad \text{and} \quad (r+1)/2 < s \leq r\},$$

$$M_3 := \quad \{s \in \mathbb{N}\,; s \equiv 0 \bmod 2 \quad \text{and} \quad 2 \leq s \leq (r+2)/2\},$$

$$M_4 := \quad \{s \in \mathbb{N}\,; s \equiv 0 \bmod 2 \quad \text{and} \quad (r+2)/2 < s \leq r\}.$$

Since $r \equiv 0 \bmod 4$, we have that

$$\begin{aligned}
M_1 = &\ \{s \in \mathbb{N}\,; s = 1+2i \ \text{ for some } \ i \ \text{ with } \ 1 \le i < r/4\},\\
M_2 = &\ \{s \in \mathbb{N}\,; s = (r+4i-2)/2 \ \text{ for some } \ i \ \text{ with } \ 1 \le i \le r/4\},\\
M_3 = &\ \{s \in \mathbb{N}\,; s = 2i \ \text{ for some } \ i \ \text{ with } \ 1 \le i \le r/4\},\\
M_4 = &\ \{s \in \mathbb{N}\,; s = (r+4i)/2 \ \text{ for some } \ i \ \text{ with } \ 1 \le i \le r/4\}.
\end{aligned}$$

From Prop.2.7 and 2.8 we have

$$\begin{aligned}
D_r^{(1)} = &\ \textstyle\sum_{i=1}^{(r-4)/4}(q^{r-3i}-2)\cdot q^{2i} \ = \ \dfrac{1}{q-1}(q^r - q^{(3r+4)/4}) \ - \ \dfrac{2q^2}{q^2-1}(q^{(r-4)/2}-1),\\
D_r^{(2)} = &\ \textstyle\sum_{i=1}^{r/4}(q^{(r/4)+2-i}-2)\cdot q^{(r-2)/2} \ = \ \dfrac{1}{q-1}(q^{(3r+4)/4} - q^{(r+2)/2}) \ - \ \dfrac{r}{2}\cdot q^{(r-2)/2},\\
D_r^{(3)} = &\ \textstyle\sum_{i=1}^{r/4}(q^{r+2-3i}-2)\cdot q^{2i-1} \ = \ \dfrac{1}{q-1}(q^{r+1} - q^{(3r+4)/4}) \ - \ \dfrac{2q}{q^2-1}(q^{r/2}-1),\\
D_r^{(4)} = &\ \textstyle\sum_{i=1}^{r/4}(q^{(r/4)+1-i}-2)\cdot q^{r/2} \ = \ \dfrac{1}{q-1}(q^{(3r+4)/4} - q^{(r+2)/2}) \ - \ \dfrac{r}{2}\cdot q^{r/2}.
\end{aligned}$$

Now it follows from Eq.(2.2) that

$$\text{deg Diff } (F_r/F_1) = 2(q^{r-1}-1) + \frac{q^r-q}{q-1} + D_r^{(1)} + D_r^{(2)} + D_r^{(3)} + D_r^{(4)}$$

$$= 2(q^{r-1}-1) + \frac{1}{q-1}(q^{r+1} + 2q^r - 2q^{(r+2)/2} - q)$$

$$- \ \frac{2q}{q^2-1}(q+1)(q^{(r-2)/2}-1) - \frac{r}{2}\cdot q^{(r-2)/2}\cdot(q+1)$$

$$= 2(q^{r-1}-1) + \frac{1}{q-1}(q^{r+1} + 2q^r - 2q^{(r+2)/2} - 2q^{r/2} + q) - \frac{r}{2}\cdot q^{(r-2)/2}\cdot(q+1).$$

The Hurwitz genus formula gives

$$2g(F_r) - 2 = -2q^{r-1} + \text{deg Diff } (F_r/F_1),$$

and hence

$$2g(F_r) = \frac{1}{q-1}(q^{r+1} + 2q^r - 2q^{(r+2)/2} - 2q^{r/2} + q) - \frac{r}{2}\cdot q^{(r-2)/2}\cdot(q+1).$$

□

3. Rational places and the limit of the tower

In this section we study the tower $\mathcal{F}$ as a tower of function fields over the finite field $\mathbb{F}_\ell$ of cardinality $\ell = q^3$. So we have the following situation:

$\mathcal{F} = (F_1, F_2, F_3, ...)$ is the tower of function fields over $\mathbb{F}_\ell$ with $\ell = q^3$, where $F_1 = \mathbb{F}_\ell(x_1)$ is the rational function field and $F_{i+1} = F_i(x_{i+1})$ with

$$\frac{1 - x_{i+1}}{x_{i+1}^q} = \frac{x_i^q + x_i - 1}{x_i}. \tag{3.1}$$

Note that $[F_{i+1} : F_i] = q$ and that $\mathbb{F}_\ell$ is the full constant field of F_i for all $i \geq 1$ (as follows from Cor.2.2). Moreover, since the genus of a function field over $\mathbb{F}_\ell$ does not change in the constant field extension with $K = \bar{\mathbb{F}}_\ell$, the formulas for the genus $g(F_r)$ given in Thm.2.9 also hold for the tower $\mathcal{F}$ considered over $\mathbb{F}_\ell$. Our main goal here is to show that certain rational places of $F_1 = \mathbb{F}_\ell(x_1)$ split completely in the tower $\mathcal{F}$; i.e., they split completely in F_r/F_1 for all $r \geq 1$. This will provide many rational places of $F_r/\mathbb{F}_\ell$ and, in conjunction with Thm.2.9, this will prove our main result which is Thm.3.3.

For abbreviation we introduce the rational functions

$$a(T) := \frac{1-T}{T^q} \quad \text{and} \quad b(T) := \frac{T^q + T - 1}{T}.$$

We consider the sets

$$S := \{\gamma \in \bar{\mathbb{F}}_\ell \ ; \ \gamma^{q+1} = \gamma - 1\} \quad \text{and} \quad \Omega := \{\omega \in \bar{\mathbb{F}}_\ell \ ; \ a(\omega) \in S\}. \tag{3.2}$$

Proposition 3.1. *i) We have $\Omega \subseteq \mathbb{F}_\ell$ and $\#\Omega = q(q+1)$.*

ii) Let $\omega \in \Omega$. Then the equation $a(\eta) = b(\omega)$ has exactly q roots η in $\bar{\mathbb{F}}_\ell$ and all these roots belong to the set Ω.

We postpone the proof of Prop.3.1 to the end of this section, and we draw first some consequences of it.

Theorem 3.2. *Let $\mathcal{F} = (F_1, F_2, F_3, ...)$ be the tower of function fields over $\mathbb{F}_\ell$ with $\ell = q^3$ which is defined recursively by Eq.(3.1) and let $\omega \in \Omega$. Then the place $(x_1 = \omega)$ splits completely in all extensions F_r/F_1. Therefore the number of rational places of $F_r/\mathbb{F}_\ell$ satisfies*

$$N(F_r) \geq [F_r : F_1] \cdot \#\Omega = q^r(q+1).$$

Proof. We claim that:

Claim i): The place $(x_1 = \omega)$ has exactly q^{r-1} distinct extensions $Q \in \mathbb{P}(F_r)$.

Claim ii): For any such place Q there is some $\omega' \in \Omega$ such that Q is a zero of the function $x_r - \omega'$.

It is clear that the assertions of Thm.3.2 follow from Claim i). We prove both claims by induction on r. The case $r = 1$ is trivial, and we assume that Claim i) and Claim ii) are both true for some $r \geq 1$. Let $Q \in \mathbb{P}(F_r)$ be one of the places lying above $(x_1 = \omega)$, then by induction the place Q is a zero of $x_r - \omega'$ with $\omega' \in \Omega$. The function x_{r+1} satisfies the equation $a(x_{r+1}) = b(x_r)$. To any solution η of the equation $a(\eta) = b(\omega')$ corresponds a place $Q' \in \mathbb{P}(F_{r+1})$ with $Q'|Q$ such that Q' is a zero of $x_{r+1} - \eta$. By Prop.3.1, the equation $a(\eta) = b(\omega')$ has exactly q distinct roots $\eta \in \Omega$, and hence the claims i) and ii) also hold for $r + 1$. □

For any tower $\mathcal{T} = (T_1, T_2, T_3, ...)$ of function fields over a finite field, the limit

$$\lambda(\mathcal{T}) := \lim_{r \to \infty} \frac{N(T_r)}{g(T_r)}$$

exists, see [7]. An immediate consequence of Thm.2.9 and Thm.3.2 is now:

Theorem 3.3. *Let $\mathcal{F} = (F_1, F_2, F_3, ...)$ be the tower of function fields over $\mathbb{F}_\ell$ (with $\ell = q^3$), which is defined recursively by Eq.(3.1). Then its limit satisfies*

$$\lambda(\mathcal{F}) = \lim_{r \to \infty} \frac{N(F_r)}{g(F_r)} \geq \frac{2(q^2 - 1)}{q + 2}.$$

For the real number $A(q^3)$ (see definition in the introduction) we obtain:

Corollary 3.4. *(Generalization of Zink's lower bound) For any prime power q, we have*

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

Now we prove Prop.3.1. For this we need the following two lemmas:

Lemma 3.5. *Let the sets S and Ω be as defined in (3.2). Then:*

i) *$\#S = q + 1$ and $\#\Omega = q(q + 1)$.*

ii) *If $\gamma \in S$ then $\gamma^{q^2+q+1} = -1$. In particular, the set S is contained in $\mathbb{F}_\ell$.*

iii) *The set Ω is contained in $\mathbb{F}_\ell$.*

Proof. i) By definition, the set S consists of the zeros in the algebraic closure $\bar{\mathbb{F}}_\ell$ of the polynomial $f(T) = T^{q+1} - T + 1$. Since $f(T)$ is clearly separable, we get that $\#S = q + 1$. Similarly, the set Ω consists of the zeros of $h_\gamma(T) := T^q + \gamma^{-1}T - \gamma^{-1}$, for all elements $\gamma \in S$. These polynomials are clearly separable, hence $\#\Omega = q(q + 1)$.

ii) If $\gamma^{q+1} = \gamma - 1$, then $\gamma^{q^2+q} = \gamma^q - 1$. Multiplying the last equality by γ we then get that

$\gamma^{q^2+q+1} = \gamma^{q+1} - \gamma = -1$. Note that q^2+q+1 is the norm exponent in $\mathbb{F}_\ell/\mathbb{F}_q$ and hence the set S is contained in $\mathbb{F}_\ell$.

iii) Let $\omega \in \Omega$. Then $a(\omega) = \gamma$ for some $\gamma \in S$; i.e., we have $1-\omega = \gamma\omega^q$. Using item ii), it then follows that

$$\begin{aligned}\omega^{q^3} &= -\gamma^{q^2+q+1}\cdot\omega^{q^3} = -\gamma^{q+1}(\gamma\omega^q)^{q^2} = -\gamma^{q+1}(1-\omega)^{q^2} = -\gamma^{q+1} + \gamma^{q+1}\cdot\omega^{q^2}\\ &= -\gamma^{q+1} + \gamma\cdot(\gamma\omega^q)^q = -\gamma^{q+1} + \gamma(1-\omega)^q = -\gamma^{q+1} + \gamma - \gamma\omega^q\\ &= -\gamma^{q+1} + \gamma - (1-\omega) = (-\gamma^{q+1} + \gamma - 1) + \omega = \omega,\end{aligned}$$

and hence the set Ω is contained in $\mathbb{F}_\ell$. □

Lemma 3.6. *If $\omega \in \Omega$ then $b(\omega) \in S$.*

Proof. Let $\omega \in \Omega$. Then there is some $\gamma \in S$ with $\gamma\omega^q = 1-\omega$. Hence

$$b(\omega) = \frac{\omega^q + \omega - 1}{\omega} = \frac{\omega^q - \gamma\omega^q}{\omega} = \omega^{q-1}(1-\gamma) =: \beta,$$

and we have to show that $\beta \in S$. We have

$$\begin{aligned}&\gamma\omega(\beta^{q+1} - \beta + 1) = \gamma\omega((1-\gamma)^{q+1}\cdot\omega^{q^2-1} - (1-\gamma)\omega^{q-1} + 1)\\ &= \gamma(1-\gamma-\gamma^q+\gamma^{q+1})\omega^{q^2} - \gamma(1-\gamma)\omega^q + \gamma\omega\\ &= -\gamma^{q+1}\cdot\omega^{q^2} - (1-\gamma)\gamma\omega^q + \gamma\omega\\ &= -\gamma(\gamma\omega^q)^q - (1-\gamma)(1-\omega) + \gamma\omega\\ &= -\gamma(1-\omega)^q - 1 + \gamma + \omega\\ &= \gamma\omega^q - 1 + \omega = 0.\end{aligned}$$

Hence $\beta^{q+1} = \beta - 1$ and $\beta \in S$. □

Now we turn to the proof of Prop.3.1.

Proof of Proposition 3.1 i) This item was already shown in Lemma 3.5.

ii) Let $\Lambda := \{\omega \in \bar{\mathbb{F}}_\ell \ ; \ b(\omega) \in S\}$. Since $\deg(b) = q$, the cardinality of the set Λ satisfies $\#\Lambda \leq q\cdot\#S = q(q+1)$. By Lemma 3.6 we know that $\Omega \subseteq \Delta$ and, since $\#\Omega = q(q+1)$ by Lemma 3.5, we conclude that $\Omega = \Delta$. This completes the proof of Prop.3.1. □

The following remark was pointed out to us by C. P. Xing:

Remark 3.7. (cf. [20]). It is well-known that good lower bounds for the quantity $A(\ell)$ provide lower bounds for the function $\alpha_\ell(\delta)$ which plays a prominent role in coding theory. For the definition of $\alpha_\ell(\delta)$ we refer to [13], Sec.6.2 or [16], Ch.VII.2. The Gilbert-Varshamov bound states that

$$\alpha_\ell(\delta) \geq 1 - H_\ell(\delta) \quad \text{for all} \quad \delta \in [1, (\ell-1)/\ell], \tag{3.3}$$

where $H_\ell(\delta)$ denotes the ℓ-ary entropy function. The following bound which is based on algebraic-geometric codes was first proved by Tsfasman, Vladut and Zink (see [18])

$$\alpha_\ell(\delta) \geq 1 - \delta - A^{-1} \text{ for any } A \in \mathbb{R} \text{ with } 0 < A \leq A(\ell). \tag{3.4}$$

For $\ell = q^3$ we can choose $A = 2(q^2-1)/(q+2)$ by Cor.3.4, and evaluating the bounds (3.3) and (3.4) above at $\delta_0 := (\ell-1)/(2\ell-1)$ we find easily that

$$1 - \delta_0 - \frac{q+2}{2(q^2-1)} > 1 - H_{q^3}(\delta_0) \text{ for all } q \geq 7.$$

Therefore the Tsfasman-Vladut-Zink bound improves on the Gilbert-Varshamov bound in a non-empty open interval containing δ_0, for all $\ell = q^3$ with $q \geq 7$.

4. Ramified places of type 3

In this section we will prove the items i) and ii) of Proposition 2.7 and thus complete the genus calculations (see Thm.2.9) for the tower $\mathcal{F} = (F_i)_{i\geq 1}$ given by Eq.(0.7). Recall that the extensions F_{i+1}/F_i are given by $F_{i+1} = F_i(x_{i+1})$ where

$$\frac{1 - x_{i+1}}{x_{i+1}^q} = \frac{x_i^q + x_i - 1}{x_i}.$$

This means that x_{i+1} is a root of the polynomial

$$\frac{x_i^q + x_i - 1}{x_i} \cdot T^q + T - 1 \in F_i[T],$$

and hence we are led to study polynomials of the form $aT^q + bT + c$ with coefficients a, b, c in a function field F.

Lemma 4.1. *Let E/H be a separable extension of function fields over a field K of characteristic $p > 0$. Assume that $[E : H] = m \equiv 0 \bmod p$, and let $\mu \in E$ be such that $E = H(\mu)$. Suppose that μ satisfies an equation*

$$a\mu^m + b\mu + c = 0$$

with $a, b, c \in H$, and let $P \in \mathbb{P}(H)$ be a place of H such that $v_P(a) = v_P(b) = 0$. Then the following holds:

i) *If $v_P(c) \geq 0$ then P is unramified in E/H.*

ii) *If $v_P(c) = -1$ then P is totally ramified in E/H, and the function μ^{-1} is a prime element for the place $Q \in \mathbb{P}(E)$ which lies over P. Moreover, the different exponent of $Q|P$ is equal to $d(Q|P) = 2m - 2$.*

Proof. By assumption, the polynomial

$$\psi(T) = T^m + \frac{a}{b} \cdot T + \frac{c}{a} \in H[T]$$

is the minimal polynomial of μ over the field H.

i) In this case, $v_P(b/a) = 0$ and $v_P(c/a) \geq 0$, hence μ is integral over the valuation ring of P, and for all $Q \in \mathbb{P}(E)$ with $Q|P$ we have $v_Q(\psi'(\mu)) = v_Q(b/a) = 0$. It follows by Lemma 1.1 i) that the place P is unramified in E/H.

ii) Let Q be a place of E lying over P. Then $v_Q(a) = v_Q(b) = 0$ and $v_Q(c) = -e$, with $e = e(Q|P)$. From the equation $a\mu^m + b\mu + c = 0$ we conclude that $v_Q(\mu) < 0$, hence $v_Q(a\mu^m) = m \cdot v_Q(\mu) < v_Q(\mu) = v_Q(b\mu)$. Then $m \cdot v_Q(\mu) = v_Q(c) = -e$. Since $e \leq [E : H] = m$, this implies that $e = m$ and $v_Q(\mu) = -1$, and so the function μ^{-1} is a prime element for Q. The minimal polynomial of μ^{-1} over H is

$$\rho(T) = T^m + \frac{b}{c} \cdot T^{m-1} + \frac{a}{c}$$

and by Lemma 1.1 ii) we obtain

$$\begin{aligned} d(Q|P) &= v_Q(\rho'(\mu^{-1})) = v_Q((b/c) \cdot (\mu^{-1})^{m-2}) \\ &= v_Q(b) - v_Q(c) + (m-2) = 2m - 2. \end{aligned}$$

□

From here on we assume all notations from Section 2. In particular, $K = \bar{\mathbb{F}}_q$ is an algebraic closure of $\mathbb{F}_q$, and the tower $\mathcal{F} = (F_1, F_2, F_3, ...)$ over K is recursively defined by $F_1 = K(x_1)$ and, for $i \geq 1$, $F_{i+1} = F_i(x_{i+1})$, with

$$\frac{1 - x_{i+1}}{x_{i+1}^q} = \frac{x_i^q + x_i - 1}{x_i}. \tag{0.7}$$

We need to investigate the ramification behaviour of places of "Type 3, for s odd". This means (see Prop.2.4) that we consider a place $Q \in \mathbb{P}(F_r)$ which is a pole of the function x_s for some odd $s \in \{3, \ldots, r\}$. Since we will describe the ramification behaviour of such places in all extensions F_n/F_1, we can assume that $r \geq 2s$; so we have

$$s = 2t + 1 \quad \text{with} \quad t \geq 1, \quad \text{and} \quad r \geq 4t + 2.$$

Since $x_s = \infty$ at Q, it follows from Lemma 2.3 that the following holds at the place Q:

$$x_j = \begin{cases} 0 & \text{for } \; j \geq 2t+2, \\ \infty & \text{for } \; j = 2t+1, \\ 1 & \text{for } \; j = 2t+1-2i, \quad 1 \leq i \leq t, \\ \beta_i & \text{for } \; j = 2t+2-2i, \quad 1 \leq i \leq t, \end{cases} \tag{4.1}$$

with certain elements $\beta_i \in R = \{\alpha \in K\ ;\ \alpha^q + \alpha = 1\}$, for $i = 1, \dots , t$.

Let E/F be an extension of function fields such that $F \subseteq E \subseteq F_r$. We say that the place Q has ramification index e in E/F if the place $Q|_E \in \mathbb{P}(E)$ has ramification index e over the place $Q|_F$. From Proposition 1.3 we can read off the ramification index e of Q in some subextensions of F_r:

$$e = \begin{cases} 1 & \text{in } K(x_i, x_{i+1})/K(x_{i+1}) & \text{for } i \geq 2t+2, \\ q & \text{in } K(x_i, x_{i+1})/K(x_i) & \text{for } i \geq 2t+1, \\ q-1 & \text{in } K(x_i, x_{i+1})/K(x_{i+1}) & \text{for } i = 2t+1, \\ 1 & \text{in } K(x_i, x_{i+1})/K(x_{i+1}) & \text{for } i = 2, 4, \dots , 2t, \\ q & \text{in } K(x_i, x_{i+1})/K(x_{i+1}) & \text{for } i = 1, 3, \dots , 2t-1, \\ q-1 & \text{in } K(x_i, x_{i+1})/K(x_i) & \text{for } i = 2t, \\ 1 & \text{in } K(x_i, x_{i+1})/K(x_i) & \text{for } 1 \leq i \leq 2t-1. \end{cases} \tag{4.2}$$

For $t = 2$ this pattern is shown in Figure 1:

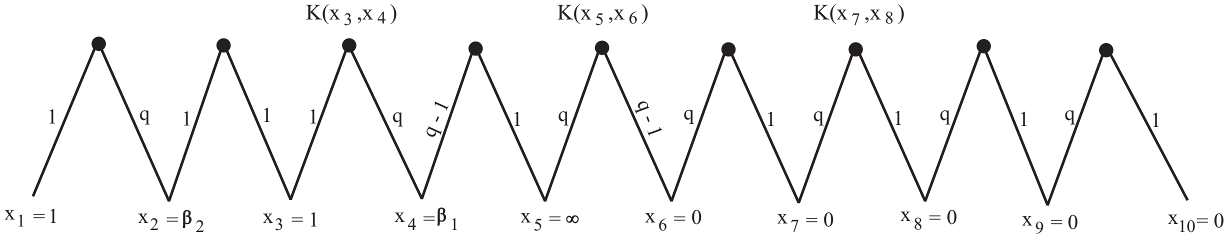

Figure 1 (for t = 2)

By Abhyankar's lemma (see Lemma 1.2) we conclude from (4.2) that the ramification index of the place Q satisfies also

$$e = \begin{cases} 1 & \text{in } F_j/F_{j-1} & \text{for } j = 2, \dots , 2t, \\ q-1 & \text{in } F_j/F_{j-1} & \text{for } j = 2t+1, \\ q^t & \text{in } F_{2t+1}/K(x_{2t+1}). \end{cases}$$

This proves the item i) and part of the item ii) in Prop.2.7. Unfortunately, Abhyankar's lemma does not apply for $j \geq s+1 = 2t+2$, see Fig. 2.

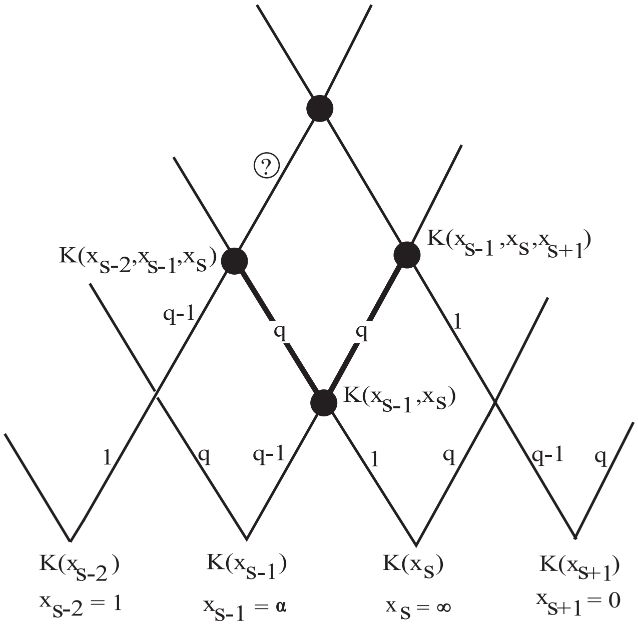

Figure 2

It will be convenient to change the generators x_i of the fields $K(x_i)$ slightly, according to the place Q. We set

$$X_i := \begin{cases} x_{2t+1-i} - 1 & \text{for } \ 1 \leq i \leq 2t, \ \ i \equiv 0 \bmod 2, \\ x_{2t+1-i} - \beta_{(i+1)/2} & \text{for } \ 1 \leq i \leq 2t, \ \ i \equiv 1 \bmod 2, \end{cases}$$

$$Y := \ x_{2t+1}^{-1}$$

$$Z_i := \ x_{2t+1+i} \ \text{ for all } \ i \geq 1.$$

It is then obvious by (4.1) that the place Q is a common zero of the functions $X_1, \ldots, X_{2t}$, $Y, Z_1, Z_2, \ldots$. We can rewrite Eq.(0.7) in terms of the functions X_i, Y, Z_i as follows:

$$\frac{X_i^q + X_i}{X_i^q + \beta_{(i+1)/2}^q} = \frac{-X_{i+1}^q}{X_{i+1} + 1} \quad \text{for } \ i \equiv 1 \bmod 2, \tag{4.3}$$

$$\frac{-X_i}{X_i^q + 1} = \frac{X_{i+1}^q + X_{i+1}}{X_{i+1} + \beta_{(i+2)/2}} \quad \text{for } \ i \equiv 0 \bmod 2, \tag{4.4}$$

$$Y^q - Y^{q-1} - 1 = \frac{X_1^q - \beta_1}{X_1 + \beta_1}, \tag{4.5}$$

$$\frac{Z_1 - 1}{Z_1^q} = \frac{Y^q - Y^{q-1} - 1}{Y^{q-1}}, \tag{4.6}$$

$$\frac{1-Z_{i+1}}{Z_{i+1}^q} = \frac{Z_i^q + Z_i - 1}{Z_i} \quad \text{for} \quad i \geq 1. \tag{4.7}$$

The following subfields of F_r will play a crucial role for the determination of the ramification behaviour of the place Q. We set for $1 \leq j \leq i \leq t$ (see Fig. 3):

$$H_{i,j} := K(X_1, X_2, \ldots , X_{2i}, Y, Z_1, \ldots , Z_{2j-2}),$$

$$E_{i,j} := H_{i,j}(Z_{2j-1})$$

$$L_j := E_{j,j}(Z_{2j}).$$

Moreover we set

$$P_{i,j} := Q|_{H_{i,j}} \quad \text{and} \quad Q_{i,j} := Q|_{E_{i,j}}.$$

The next theorem is the key result leading to the genus formulas in Thm.2.9. The assertions of Thm.4.2 correspond to the encircled ramification indices in Fig.3.

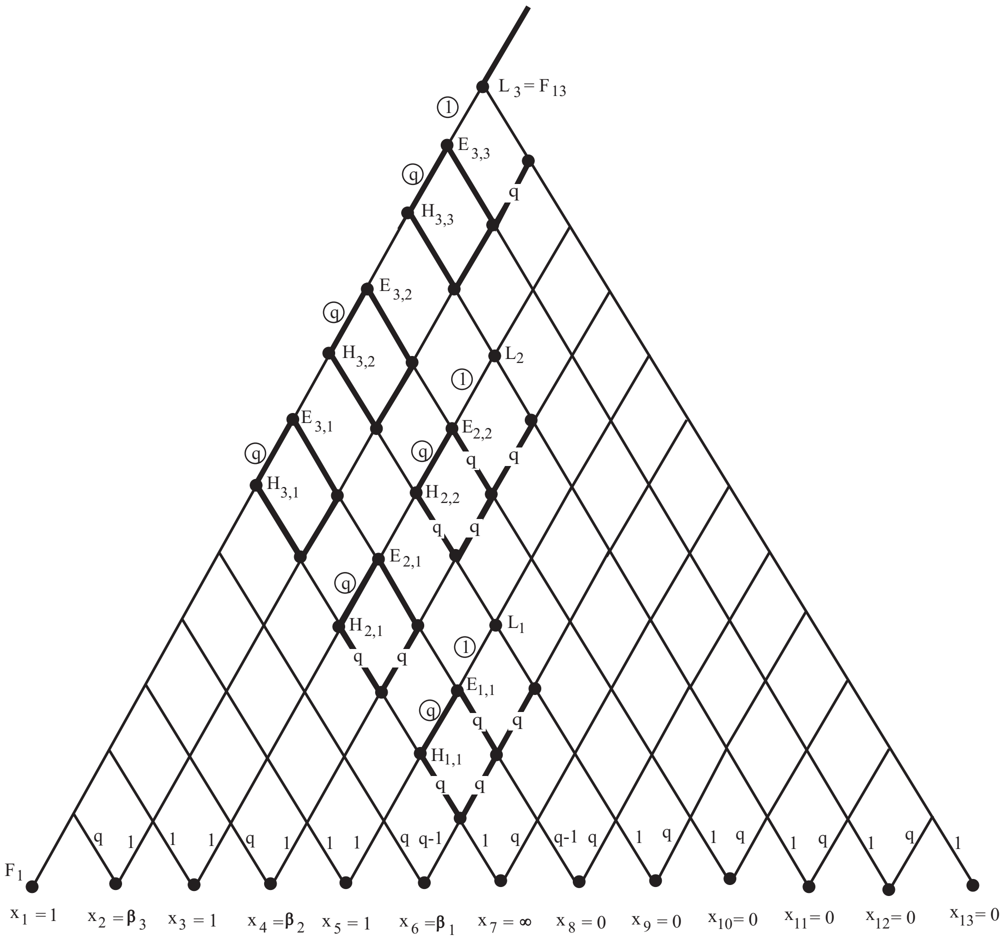

Figure 3 (for t=3)

Theorem 4.2. *Let $1 \leq j \leq i \leq t$. Then the place Q is totally ramified in the extension $E_{i,j}/H_{i,j}$ and it is unramified in the extension $L_j/E_{j,j}$. Moreover, the different exponent of $Q_{i,j}|P_{i,j}$ is*

$$d(Q_{i,j}|P_{i,j}) = 2q - 2.$$

As a consequence of Thm.4.2 we have then

Corollary 4.3. *The restriction $Q_j = Q|_{F_j}$ of the place Q satisfies*

i) $e(Q_j|Q_{j-1}) = 1$ *if* $2t + 1 < j < 4t + 2$ *and* $j \equiv 1 \bmod 2$.

ii) $e(Q_j|Q_{j-1}) = q$ *and* $d(Q_j|Q_{j-1}) = 2q - 2$*, if* $2t + 1 < j < 4t + 2$ *and* $j \equiv 0 \bmod 2$.

iii) $e(Q_j|Q_{j-1}) = q$ *and* $d(Q_j|Q_{j-1}) = 2q - 2$ *if* $j \geq 4t + 2$.

Note that Cor.4.3 includes all the missing assertions of Prop.2.7, and hence completes the proof of the Main Theorem.

Proof of Cor.4.3 i) First we consider the case $j = 4t + 1$. Then $F_j = L_t$ and $F_{j-1} = E_{t,t}$, and Q is unramified in $L_t/E_{t,t}$ by Thm.4.2.
Next let $2t + 1 < j < 4t + 1$ and $j \equiv 1 \bmod 2$. Then $F_j = H_{t,k+1}$ and $F_{j-1} = E_{t,k}$ for some k with $1 \leq k \leq t - 1$ (see Fig.3). Observe that $H_{t,k+1} \supseteq E_{t,k} \supseteq E_{k,k}$ and $H_{t,k+1} \supseteq L_k \supseteq E_{k,k}$, and that $H_{t,k+1}$ is the composite field of $E_{t,k}$ and L_k. By Thm.4.2, the place Q is unramified in the extension $L_k/E_{k,k}$, and therefore Q is unramified in the extension $H_{t,k+1}/E_{t,k}$ by Lemma 1.2.

ii) Now let $2t + 1 < j < 4t + 2$ and $j \equiv 0 \bmod 2$. Then there is some k with $1 \leq k \leq t$ such that $F_j = E_{t,k}$ and $F_{j-1} = H_{t,k}$, and all assertions of item ii) follow immediately from Thm.4.2.

iii) For $j-1 \geq 4t+1$, the ramification index of Q in the extension $F_{j-1}/K(x_{j-1})$ is $e = q-1$, by Thm.4.2 (see Fig.3). The place Q is totally ramified in the extension $K(x_{j-1}, x_j)/K(x_{j-1})$, with different exponent $d = q$ (see Prop.1.3 ii)). Using Lemma 1.2 we conclude that $e(Q_j|Q_{j-1}) = q$ and moreover $d(Q_j|Q_{j-1}) = (q - 1) \cdot q - (q - 2)(q - 1) = 2q - 2$. □

It remains to prove Thm.4.2. This proof will be divided into two propositions which treat the cases $j = 1$ and $j > 1$, respectively. In both cases, the main idea is to apply Lemma 4.1. Unfortunately, the "obvious" generator of the corresponding field extension $E_{i,j}/H_{i,j}$ (resp. $L_j/E_{j,j}$) does not meet the assumptions of Lemma 4.1. Therefore we must first perform "pole order reductions", analogous to Hasse's pole order reductions for Artin-Schreier equations (see [16], Ch.III.7).

The following notation will be very useful. For a function field F/K, a place $P \in \mathbb{P}(F)$, elements $z_1, z_2 \in F$ and an integer $n \in \mathbb{Z}$ we write

$$z_1 = z_2 + \mathcal{O}(n) \ \text{ at } \ P, \quad \text{ if } v_P(z_1 - z_2) \geq n.$$

In particular, we write $z = \mathcal{O}(0)$ at P meaning that z is holomorphic at the place P. Recall that $P_{i,j}$ (resp. $Q_{i,j}$) denotes the restriction of the place $Q \in \mathbb{P}(F_r)$ to the field $H_{i,j}$ (resp. $E_{i,j}$), for $1 \leq j \leq i \leq t$.

Figure 4 below helps to understand the statements in Prop.4.4 and 4.5.

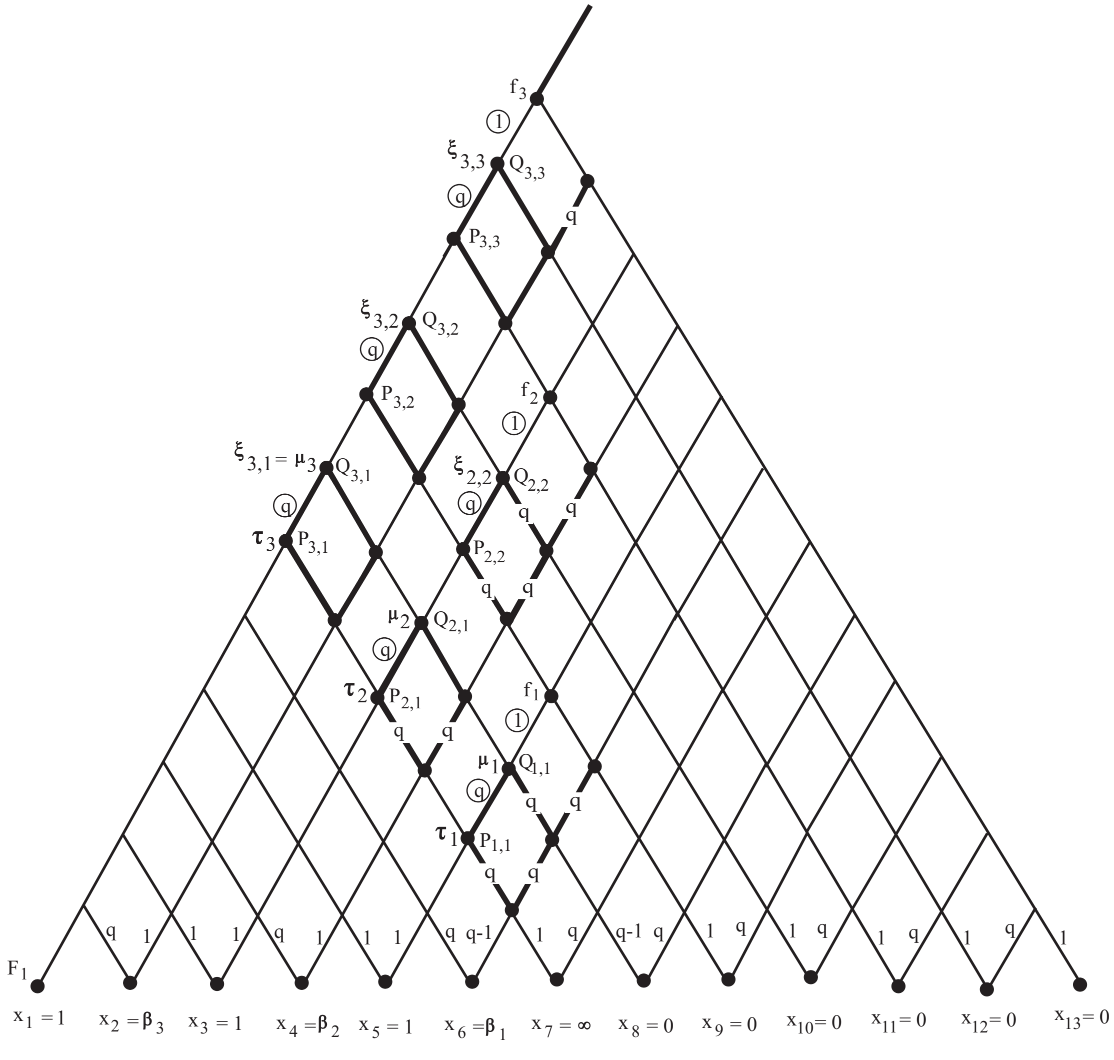

Figure 4 (for t=3)

Proposition 4.4. *(The case $j=1$.) For $1 \le i \le t$ we consider the functions*

$$\tau_i := Y^{-1} \cdot \textstyle\prod_{k=1}^{i} X_{2k} \in H_{i,1} \quad \textit{and}$$

$$\mu_i := Y^{-1} Z_1 + \textstyle\sum_{k=1}^{i} (-1)^k A_k \beta_k \tau_k \in E_{i,1} \quad \textit{with} \quad A_k := \textstyle\prod_{m=1}^{k} \beta_m^{-q}.$$

Then the following holds:

i) $v_{P_{i,1}}(Y) = q^i$,

$$v_{P_{i,1}}(X_k) = \begin{cases} q^{(2i-k+1)/2} \cdot (q-1) & \textit{for} \;\; 1 \le k \le 2i, \;\; k \equiv 1 \bmod 2, \\ q^{(2i-k)/2} \cdot (q-1) & \textit{for} \;\; 1 \le k \le 2i, \;\; k \equiv 0 \bmod 2, \end{cases}$$

$v_{P_{i,1}}(\tau_i) = -1$, *i.e. the function τ_i^{-1} is a local parameter at the place $P_{i,1}$.*

ii) $E_{i,1} = H_{i,1}(\mu_i)$, *and the minimal polynomial of μ_i over $H_{i,1}$ has the form*

$$\varphi(T) = T^q - \frac{X_1 + \beta_1}{X_1^q - \beta_1} \cdot T + (-1)^{i+1} A_i \tau_i - h,$$

for some function $h \in H_{i,1}$ which is holomorphic at the place $P_{i,1}$.

iii) *The place $P_{i,1}$ is totally ramified in the extension $E_{i,1}/H_{i,1}$ and the function μ_i^{-1} is a local parameter at $Q_{i,1}$. The different exponent of $Q_{i,1}$ is*

$$d(Q_{i,1} | P_{i,1}) = 2q - 2.$$

iv) *For $2 \le i \le t$ one has*

$$\tau_{i-1} = A_i^{q-1} \cdot \tau_i^q - \tau_i + \mathcal{O}(0) \quad \textit{at} \quad P_{i,1}.$$

v) *For $2 \le i \le t$ one has*

$$\mu_{i-1} = \beta_i^q \cdot \mu_i - \beta_i \cdot \mu_i^q + \mathcal{O}(0) \quad \textit{at} \quad Q_{i,1}.$$

vi) *Let $f_1 := Z_2 \cdot \mu_1^q + c_1 \cdot \mu_1 \in L_1$ with $c_1 = \beta_1^{q-1}$. Then $L_1 = E_{1,1}(f_1)$ and*

$$(Z_1^q + Z_1 - 1) \cdot f_1^q + (Z_1 \cdot \mu_1^{q(q-1)}) \cdot f_1 + h_1 = 0,$$

for some $h_1 \in E_{1,1}$ which is holomorphic at the place $Q_{1,1}$.

vii) *The place Q is unramified in the extension $L_1/E_{1,1}$.*

Proof. The item i) follows easily from (4.2) and Abhyankar's Lemma, cf. Fig.3. We will first prove ii) and iii) in the case $i = 1$. Eq.(4.6) can be written as

$$\left(\frac{Z_1}{Y}\right)^q = \frac{Z_1 - 1}{Y(Y^q - Y^{q-1} - 1)}$$

and by Eq.(4.5) this gives

$$\left(\frac{Z_1}{Y}\right)^q - \frac{X_1+\beta_1}{X_1^q-\beta_1}\cdot\frac{Z_1}{Y} + \frac{X_1+\beta_1}{X_1^q-\beta_1}\cdot\frac{1}{Y} = 0. \tag{4.8}$$

Observe that $E_{1,1} = H_{1,1}(w)$ with $w = Z_1/Y$, and that Eq.(4.8) is an equation for w over $H_{1,1}$ of the form $aw^q + bw + c = 0$ as in Lemma 4.1, with $v_{P_{1,1}}(a) = v_{P_{1,1}}(b) = 0$. However Lemma 4.1 cannot be applied directly since $v_{P_{1,1}}(c) = -q$. We then replace the generating element Z_1/Y of the field extension $E_{1,1}/H_{1,1}$ by the element

$$\mu_1 = \frac{Z_1}{Y} - A_1\beta_1\tau_1.$$

It follows from Eq.(4.8) that μ_1 is a zero of the polynomial

$$\varphi(T) = T^q - \frac{X_1+\beta_1}{X_1^q-\beta_1}\cdot T + g_1 \tag{4.9}$$

with

$$g_1 = A_1^q\beta_1^q\tau_1^q - A_1\beta_1\tau_1\cdot\frac{X_1+\beta_1}{X_1^q-\beta_1} + \frac{X_1+\beta_1}{X_1^q-\beta_1}\cdot\frac{1}{Y} \in H_{1,1}.$$

Note that $\beta_1 \in \mathbb{F}_{q^2}$ since $\beta_1^q + \beta_1 = 1$. Therefore we have $A_1 = \beta_1^{-q} \in \mathbb{F}_{q^2}$ and $A_1^q\beta_1^q = \beta_1^{q-1}$. Using $\tau_1 = X_2/Y$ and Eq.(4.3) we obtain

$$\begin{aligned} g_1 &= \beta_1^{q-1}\cdot\tau_1^q - \frac{X_1+\beta_1}{X_1^q-\beta_1}\cdot\frac{\tau_1}{\beta_1^{q-1}} + \frac{X_1+\beta_1}{X_1^q-\beta_1}\cdot\frac{1}{Y} \\ &= \frac{1}{Y}\left(\beta_1^{q-1}\cdot\frac{X_2^q}{Y^{q-1}} - \frac{X_1+\beta_1}{X_1^q-\beta_1}\cdot\frac{X_2}{\beta_1^{q-1}} + \frac{X_1+\beta_1}{X_1^q-\beta_1}\right). \end{aligned}$$

From Eq.(4.3) and (4.5) we have

$$\frac{X_2^q}{Y^{q-1}} = \frac{X_2^q(1-Y)}{Y^{q-1}-Y^q} = \frac{(1-Y)(X_2+1)}{(X_1+\beta_1)^{q-1}} \tag{4.10}$$

and hence

$$\begin{aligned} g_1 &= \frac{1}{Y}\left(\frac{\beta_1^{q-1}(1-Y)}{(X_1+\beta_1)^{q-1}}\cdot(X_2+1) - \frac{X_1+\beta_1}{X_1^q-\beta_1}\cdot\frac{X_2}{\beta_1^{q-1}} + \frac{X_1+\beta_1}{X_1^q-\beta_1}\right) \\ &= \frac{1}{Y}\left((1+\mathcal{O}(q))\cdot(X_2+1) + (1+\mathcal{O}(q))\cdot\frac{X_2}{\beta_1^{q-1}} - 1 + \mathcal{O}(q)\right) \\ &= \frac{1}{Y}\left(X_2 + \frac{X_2}{\beta_1^{q-1}} + \mathcal{O}(q)\right) \\ &= \frac{X_2}{Y}\cdot\frac{1}{\beta_1^q} + \mathcal{O}(0) = A_1\tau_1 + \mathcal{O}(0) \ \text{ at the place } \ P_{1,1}. \end{aligned} \tag{4.11}$$

We have used here that $v_{P_{1,1}}(Y) = q$ and $v_{P_{1,1}}(X_1) \geq q$. Thus we have proved ii) in the case $i = 1$. The assertions of iii) (for $i = 1$) follow now immediately from Lemma 4.1 (observe that the place $P_{1,1}$ is a zero of X_1 and $v_{P_{1,1}}(\tau_1) = -1$ by i), so Lemma 4.1 applies).

Now we show the item vi). By Eq.(4.7) we have

$$(Z_1^q + Z_1 - 1) \cdot Z_2^q + Z_1 \cdot Z_2 - Z_1 = 0,$$

hence

$$(Z_1^q + Z_1 - 1) \cdot f_1^q + (Z_1 \mu_1^{q(q-1)}) \cdot f_1 - (\mu_1^{q^2} + c_1 \mu_1^{q^2-q+1}) \cdot Z_1 + c_1^q \mu_1^q + \tilde{h}_1 = 0,$$

with some function $\tilde{h}_1 \in E_{1,1}$ which is holomorphic at the place $Q_{1,1}$. So we have to prove that the function

$$(\mu_1^{q^2} + c_1 \mu_1^{q^2-q+1}) \cdot Z_1 - c_1^q \mu_1^q \tag{4.12}$$

is holomorphic at $Q_{1,1}$. It follows from (4.9) and (4.11) that

$$\tau_1 = -\beta_1^q(\mu_1^q + \mu_1) + \mathcal{O}(0) \quad \text{at} \quad Q_{1,1},$$

and hence

$$\begin{aligned} Z_1/Y \quad &= \mu_1 + A_1\beta_1\tau_1 = \mu_1 + \beta_1\beta_1^{-q}\tau_1 \\ &= \mu_1 - \beta_1(\mu_1^q + \mu_1) + \mathcal{O}(0) \\ &= -\beta_1\mu_1^q + (1 - \beta_1)\mu_1 + \mathcal{O}(0) \\ &= -\beta_1\mu_1^q + \beta_1^q\mu_1 + \mathcal{O}(0) \quad \text{at} \quad Q_{1,1}. \end{aligned} \tag{4.13}$$

Eq.(4.5) and (4.6) give

$$\frac{Z_1^q}{Y^q} \cdot \frac{Y}{Z_1 - 1} = (X_1 + \beta_1) \cdot \left(\frac{-1}{\beta_1}\right) + \mathcal{O}(q^2(q-1)) \quad \text{at} \quad Q_{1,1},$$

and therefore

$$\frac{Z_1^q}{Y^q} = - \, \frac{Z_1}{Y} + \frac{1}{Y} + \mathcal{O}(q^2(q-2)) \quad \text{at} \quad Q_{1,1}. \tag{4.14}$$

We conclude from (4.13) and (4.14) that

$$\frac{1}{Y} = -\beta_1^q \cdot \mu_1^{q^2} \cdot (1 - \mu_1^{-q^2+1} + \mathcal{O}(q^2)),$$

hence

$$Y = -\beta_1^{-q} \cdot \mu_1^{-q^2} \cdot (1 + \mu_1^{-q^2+1} + \mathcal{O}(q^2))$$

and

$$Z_1 = \frac{Z_1}{Y} \cdot Y = (\beta_1^{q-1})^q \cdot \mu_1^{-q^2+q} - \mu_1^{-q^2+1} + \mathcal{O}(q^2) \ \text{ at } \ Q_{1,1}.$$

Since $c_1 = \beta_1^{q-1}$ we obtain

$$(\mu_1^{q^2} + c_1\mu_1^{q^2-q+1}) \cdot Z_1 - c_1^q\mu_1^q = \mathcal{O}(0) \quad \text{at} \quad Q_{1,1}.$$

This completes the proof of the item vi), cf. (4.12). The assertion in vii) follows now from vi) and Lemma 4.1.

Our next aim is to prove the items iv) and v) of Prop.4.4 in the case $i = 2$. By definition of the function τ_j we have $\tau_2 = X_4 \cdot \tau_1$ and hence

$$\tau_1 = \tau_2^q \cdot \frac{1}{\tau_2^{q-1} \cdot X_4}.$$

From Eq.(4.3), (4.4) and (4.5) we obtain

$$\begin{aligned}\frac{1}{\tau_2^{q-1} \cdot X_4} &= \frac{Y^{q-1}}{X_2^q} \cdot \frac{X_2}{X_4^q} = \frac{(X_3+\beta_2)^{q-1} \cdot (X_1+\beta_1)^{q-1} \cdot (1+X_2)^{q-1}}{(1-Y)(1+X_4)} \\ &= (\beta_1\beta_2)^{q-1} \cdot (1 - X_4) + \mathcal{O}(q) \\ &= A_2^{q-1} \cdot (1 - X_4) + \mathcal{O}(q) \quad \text{at} \quad P_{2,1}.\end{aligned}$$

We have used above that $P_{2,1}$ is a zero of X_1, X_2, X_3 and Y of order $\geq q$, and it is a zero of X_4 of order $(q-1)$. Since the function τ_2^{-1} is a prime element at $P_{2,1}$, it follows that

$$\begin{aligned}\tau_1 &= \tau_2^q \cdot A_2^{q-1} \cdot (1 - X_4) + \mathcal{O}(0) \\ &= A_2^{q-1} \cdot \tau_2^q - \tau_2 A_2^{q-1} \cdot \tau_2^{q-1} \cdot X_4 + \mathcal{O}(0) \\ &= A_2^{q-1} \cdot \tau_2^q - \tau_2 + \mathcal{O}(0) \quad \text{at} \quad P_{2,1}.\end{aligned}$$

This is the assertion in iv) for $i = 2$.

By (4.9) and (4.11),

$$\mu_1^q - \frac{X_1+\beta_1}{X_1^q - \beta_1} \cdot \mu_1 + A_1\tau_1 = \mathcal{O}(0) \quad \text{at} \quad P_{1,1},$$

so

$$\mu_1^q - \frac{X_1+\beta_1}{X_1^q - \beta_1} \cdot \mu_1 + \frac{1}{\beta_1^q} \cdot (A_2^{q-1}\tau_2^q - \tau_2) = \mathcal{O}(0) \quad \text{at} \quad P_{2,1}.$$

Therefore

$$(\mu_1 + A_2\beta_2\tau_2)^q - \frac{X_1+\beta_1}{X_1^q - \beta_1} \cdot (\mu_1 + A_2\beta_2\tau_2) + \frac{X_1+\beta_1}{X_1^q - \beta_1} \cdot A_2\beta_2\tau_2 - \frac{1}{\beta_1^q} \cdot \tau_2 = \mathcal{O}(0)$$

and by the definition of the function μ_2,

$$\mu_2^q - \frac{X_1 + \beta_1}{X_1^q - \beta_1} \cdot \mu_2 - A_2\tau_2 = \mathcal{O}(0) \quad \text{at} \quad P_{2,1}. \tag{4.15}$$

By Lemma 4.1, the place $P_{2,1}$ is totally ramified in the extension $E_{2,1}/H_{2,1}$ and the function μ_2^{-1} is a prime element of the place $Q_{2,1} = Q|_{E_{2,1}}$. Moreover we conclude from (4.15) that

$$\mu_2^q + \mu_2 - A_2\tau_2 = \mathcal{O}(0) \quad \text{at} \quad Q_{2,1}.$$

Since $\mu_2 = \mu_1 + A_2\beta_2\tau_2$, this implies

$$\begin{aligned} \mu_1 \quad &= \mu_2 - \beta_2 A_2\tau_2 = \mu_2 - \beta_2(\mu_2^q + \mu_2) + \mathcal{O}(0) \\ &= -\beta_2\mu_2^q + \beta_2^q\mu_2 + \mathcal{O}(0) \quad \text{at the place} \quad Q_{2,1}. \end{aligned}$$

Hereby we have proved the item v) in the case $i = 2$. Note that we have also proved the items ii) and iii) of Prop.4.4 in the case $i = 2$, by (4.15).

Now we proceed by induction. Let $2 \leq i < t$ and suppose that the assertions ii) - v) of Prop.4.4 hold for $2 \leq k \leq i$. We want to show that they hold also for $k = i+1$. By induction hypothesis we have

$$\tau_i = X_{2i} \cdot \tau_{i-1} = X_{2i} \cdot A_i^{q-1} \cdot \tau_i^q + \mathcal{O}(0) \quad \text{at} \quad P_{i,1}$$

and hence

$$\tau_i = A_i^{q-1} \cdot \frac{X_{2i}}{X_{2(i+1)}^q} \cdot \tau_{i+1}^q + \mathcal{O}(0) \quad \text{at} \quad P_{i+1,1}.$$

By Eq.(4.3) and (4.4), the following identity holds:

$$\frac{X_{2i}}{X_{2(i+1)}^q} = \frac{(X_{2i}^q + 1)(X_{2i+1} + \beta_{i+1})^q}{(X_{2i+1} + \beta_{i+1})(X_{2(i+1)} + 1)}. \tag{4.16}$$

So

$$\frac{X_{2i}}{X_{2(i+1)}^q} = \beta_{i+1}^{q-1} \cdot (1 - X_{2(i+1)}) + \mathcal{O}(q) \quad \text{at} \quad P_{i+1,1}$$

and consequently

$$\begin{aligned} \tau_i \quad &= A_i^{q-1} \cdot \beta_{i+1}^{q-1} \cdot (1 - X_{2(i+1)})\tau_{i+1}^q + \mathcal{O}(0) \\ &= A_{i+1}^{q-1} \cdot \tau_{i+1}^q - A_{i+1}^{q-1} \cdot (X_{2(i+1)}\tau_{i+1}^{q-1}) \cdot \tau_{i+1} + \mathcal{O}(0) \quad \text{at} \quad P_{i+1,1}. \end{aligned} \tag{4.17}$$

Now we observe that

$$X_{2(i+1)} \cdot \tau_{i+1}^{q-1} = A_{i+1}^{1-q} + \mathcal{O}(1) \quad \text{at} \quad P_{i+1,1},$$

which follows easily by induction (using (4.10) and (4.16)), and hence (4.17) yields

$$\tau_i = A_{i+1}^{q-1} \cdot \tau_{i+1}^q - \tau_{i+1} + \mathcal{O}(0) \quad \text{at} \quad P_{i+1,1}. \tag{4.18}$$

This is assertion iv) of Prop.4.4.

The induction hypothesis for item ii) says that

$$\mu_i^q - \frac{X_1+\beta_1}{X_1^q-\beta_1}\cdot \mu_i + (-1)^{i+1}A_i\tau_i = \mathcal{O}(0) \quad \text{at} \quad P_{i,1}.$$

By (4.18) we obtain then

$$\mu_i^q - \frac{X_1+\beta_1}{X_1^q-\beta_1}\cdot \mu_i + (-1)^{i+1}A_i(A_{i+1}^{q-1}\cdot \tau_{i+1}^q - \tau_{i+1}) = \mathcal{O}(0) \ \text{ at } \ P_{i+1,1}.$$

Therefore

$$\left(\mu_i + (-1)^{i+1}A_i\cdot(\frac{1}{\beta_{i+1}})^{q-1}\tau_{i+1}\right)^q - \frac{X_1+\beta_1}{X_1^q-\beta_1}\cdot\left(\mu_i + (-1)^{i+1}A_i\cdot(\frac{1}{\beta_{i+1}})^{q-1}\cdot\tau_{i+1}\right)$$

$$+\frac{X_1+\beta_1}{X_1^q-\beta_1}\cdot(-1)^{i+1}A_i\cdot(\frac{1}{\beta_{i+1}})^{q-1}\cdot\tau_{i+1} + (-1)^iA_i\tau_{i+1} = \mathcal{O}(0) \ \text{ at } \ P_{i+1,1}.$$

This implies that

$$(\mu_i + (-1)^{i+1}A_{i+1}\beta_{i+1}\tau_{i+1})^q - \frac{X_1+\beta_1}{X_1^q-\beta_1}\cdot(\mu_i + (-1)^{i+1}A_{i+1}\beta_{i+1}\tau_{i+1})$$

$$+(-1)^{i+2}A_{i+1}\tau_{i+1} = \mathcal{O}(0) \quad \text{at} \quad P_{i+1,1}$$

i.e.,

$$\mu_{i+1}^q - \frac{X_1+\beta_1}{X_1^q-\beta_1}\cdot\mu_{i+1} + (-1)^{i+2}A_{i+1}\tau_{i+1} = h' \tag{4.19}$$

with $h' \in H_{i+1,1}$ holomorphic at $P_{i+1,1}$. This is assertion ii) for $k = i+1$, and now the item iii) follows from Lemma 4.1. Finally, from the definition of μ_j,

$$\mu_{i+1} = \mu_i + (-1)^{i+1}A_{i+1}\beta_{i+1}\tau_{i+1}$$

and then it follows from (4.19) that

$$\begin{aligned}\mu_i &= \mu_{i+1} + (-1)^{i+2}\beta_{i+1}A_{i+1}\tau_{i+1}\\ &= \mu_{i+1} - \beta_{i+1}\left(\mu_{i+1}^q - \frac{X_1+\beta_1}{X_1^q-\beta_1}\cdot\mu_{i+1}\right) + \mathcal{O}(0)\\ &= -\beta_{i+1}\mu_{i+1}^q + \beta_{i+1}^q\mu_{i+1} + \mathcal{O}(0) \ \text{ at } \ Q_{i+1,1}.\end{aligned}$$

This finishes the proof of Prop.4.4. □

In the following proposition we will investigate the case $j \geq 2$. We keep all notations as above. In particular we have a place $Q \in \mathbb{P}(F_r)$ of Type 3 and consider the fields $H_{i,j}, E_{i,j}$ and L_j and the places $Q_{i,j}$ and $P_{i,j}$, for $1 \leq j \leq i \leq t$. As before, we set $c_1 = \beta_1^{q-1}$.

Proposition 4.5. *(The case $j \geq 2$.) Define $\xi_{i,1} := \mu_i \in E_{i,1}$ as in Prop.4.4, and for $2 \leq j \leq i \leq t$ define the function $\xi_{i,j} \in E_{i,j}$ by*

$$\xi_{i,j} := \begin{cases} Z_{2j-i} \cdot \xi_{j-1,j-1} + c_1^q \cdot \beta_2^q \cdot \xi_{j,j-1} & \text{if } i = j, \\ \\ \xi_{i-1,j} + (\beta_{i-j+1} \cdot \beta_{i-j+2}^q / \beta_1^q) \cdot \xi_{i,j-1} & \text{if } i > j. \end{cases}$$

Then the following holds, for $2 \leq j \leq i \leq t$:

i) $v_{P_{i,j}}(Y) = q^{j-1} \cdot q^i$,

$$v_{P_{i,j}}(Z_k) = q^{j-1} \cdot q^{i-k} \cdot (q-1) \quad \text{for } 1 \leq k \leq 2(j-1),$$

$$v_{P_{i,j}}(X_k) = \begin{cases} q^{j-1} \cdot q^{(2i-k+1)/2} \cdot (q-1) & \text{for } 1 \leq k \leq 2i, \quad k \equiv 1 \bmod 2, \\ q^{j-1} \cdot q^{(2i-k)/2} \cdot (q-1) & \text{for } 1 \leq k \leq 2i, \quad k \equiv 0 \bmod 2. \end{cases}$$

ii) *$E_{i,j} = H_{i,j}(\xi_{i,j})$, and the function $\xi_{i,j}$ satisfies an equation of the form*

$$(Z_{2j-2}^q + Z_{2j-2} - 1) \cdot \xi_{i,j}^q + (Z_{2j-2} \cdot \xi_{j-1,j-1}^{q-1}) \cdot \xi_{i,j} + \frac{\beta_{i-j+2}^q}{\beta_1} \cdot c_1^{j-2} \cdot \xi_{i,j-1} = h,$$

with some function $h \in H_{i,j}$ which is holomorphic at $P_{i,j}$.

iii) *The place $Q_{i,j}$ is totally ramified over $P_{i,j}$, the function $\xi_{i,j}^{-1}$ is a local parameter at $Q_{i,j}$, and the different exponent is*

$$d(Q_{i,j}|P_{i,j}) = 2q - 2.$$

iv) *If $i + 1 \leq t$ then there exists a function $h \in E_{i+1,j}$ which is holomorphic at the place $Q_{i+1,j}$ such that*

$$\xi_{i,j} = \beta_{i-j+2}^q \cdot \xi_{i+1,j} - \frac{\beta_{i-j+2}}{c_1^{j-1}} \cdot \xi_{i+1,j}^q + h.$$

v) *Let $f_j := Z_{2j} \cdot \xi_{j,j}^q + c_1^j \cdot \xi_{j,j} \in L_j$. Then $L_j = E_{j,j}(f_j)$, and the function f_j satisfies an equation of the form*

$$(Z_{2j-1}^q + Z_{2j-1} - 1) \cdot f_j^q + (Z_{2j-1} \cdot \xi_{j,j}^{q(q-1)}) \cdot f_j - h = 0,$$

with some function $h \in E_{j,j}$ which is holomorphic at the place $Q_{j,j}$.

vi) *The place $Q_{j,j}$ is unramified in the extension $L_j/E_{j,j}$.*

Proof. We first consider the case $j = 2$. Item i) follows then (for all $2 \leq i \leq t$) immediately from Prop.4.4 and Abhyankar's Lemma, see Fig.3. We prove the remaining assertions (for $j = 2$) by induction over i. By Prop.4.4 vi), the function $f_1 = Z_2\mu_1^q + c_1\mu_1$ is holomorphic at the place $P_{2,2}$; i.e.

$$Z_2\mu_1^q = -c_1\mu_1 + \mathcal{O}(0) \text{ at } P_{2,2}.$$

Eq.(4,7) for $i = 2$ gives

$$(Z_2^q + Z_2 - 1) \cdot Z_3^q + Z_2 Z_3 - Z_2 = 0.$$

We multiply this equation by μ_1^q and obtain

$$(Z_2^q + Z_2 - 1) \cdot (Z_3\mu_1)^q + Z_2\mu_1^{q-1} \cdot (Z_3\mu_1) - Z_2\mu_1^q = 0,$$

hence

$$(Z_2^q + Z_2 - 1) \cdot (Z_3\mu_1)^q + Z_2\mu_1^{q-1} \cdot (Z_3\mu_1) + c_1\mu_1 = \mathcal{O}(0) \quad \text{at} \quad P_{2,2}.$$

Observing that the place $Q_{2,1}$ lies below $P_{2,2}$ and using Prop.4.4 v), we get

$$(Z_2^q + Z_2 - 1) \cdot (Z_3\mu_1)^q + Z_2\mu_1^{q-1} \cdot (Z_3\mu_1) - c_1\beta_2\mu_2^q + c_1\beta_2^q\mu_2 = \mathcal{O}(0) \quad \text{at} \quad P_{2,2}.$$

Since $(Z_2^q + Z_2) \cdot \mu_2^q$ is holomorphic at $P_{2,2}$, it follows that

$$\begin{aligned}(Z_2^q + Z_2 - 1) \cdot (Z_3\mu_1 + c_1^q\beta_2^q\mu_2)^q + Z_2\mu_1^{q-1} \cdot (Z_3\mu_1 + c_1^q\beta_2^q\mu_2)&\\ - Z_2\mu_1^{q-1} \cdot c_1^q\beta_2^q\mu_2 + c_1\beta_2^q\mu_2 = \mathcal{O}(0) \quad \text{at} \quad P_{2,2}.&\end{aligned}$$

Since $(Z_2\mu_1^{q-1} + c_1) \cdot \mu_1$ is holomorphic at the place $P_{2,2}$ and since $v_{P_{2,2}}(\mu_1) = -q$, we have $Z_2\mu_1^{q-1} = -c_1 + \mathcal{O}(q)$ at $P_{2,2}$ and hence

$$(Z_2^q + Z_2 - 1) \cdot \xi_{2,2}^q + Z_2\mu_1^{q-1} \cdot \xi_{2,2} + \frac{\beta_2^q}{\beta_1} \cdot \mu_2 = \mathcal{O}(0) \quad \text{at} \quad P_{2,2}. \tag{4.20}$$

Since $v_{P_{2,2}}(\mu_2) = -1$, it now follows from Lemma 4.1 that the place $P_{2,2}$ is totally ramified in the extension $E_{2,2}/H_{2,2}$, that the function $\xi_{2,2}^{-1}$ is a prime element at the place $Q_{2,2}$ and that $d(Q_{2,2}|P_{2,2}) = 2q - 2$. Moreover we obtain from (4.20) that

$$\beta_2^q\mu_2 = \beta_1\xi_{2,2}^q + \beta_1 c_1\xi_{2,2} + \mathcal{O}(0) \quad \text{at} \quad Q_{2,2}. \tag{4.21}$$

We know from Prop.4.4v) that

$$\mu_1 = \beta_2^q\mu_2 - (\beta_2^q\mu_2)^q + \mathcal{O}(0) \quad \text{at} \quad Q_{2,2}, \tag{4.22}$$

hence (4.21) yields

$$\mu_1 = -\beta_1^q \cdot \xi_{2,2}^{q^2} + \beta_1^q \cdot \xi_{2,2} + \mathcal{O}(0) = -\beta_1^q \cdot \xi_{2,2}^{q^2}(1 - \xi_{2,2}^{1-q^2} + \mathcal{O}(q^2))$$

and therefore

$$\mu_1^{-1} = -\left(\frac{1}{\beta_1}\right)^q \cdot \xi_{2,2}^{-q^2} \cdot (1 + \xi_{2,2}^{1-q^2} + \mathcal{O}(q^2)) \quad \text{at} \quad Q_{2,2}.$$

From the definition of the function $\xi_{2,2}$ and (4.21), we have

$$Z_3\mu_1 = \beta_1^q\xi_{2,2} - c_1^q\beta_1\xi_{2,2}^q + \mathcal{O}(0) \quad \text{at} \quad Q_{2,2},$$

and then

$$Z_3 = (Z_3\mu_1)\mu_1^{-1} = c_1^{q-1} \cdot \xi_{2,2}^{-(q^2-q)} - \xi_{2,2}^{-(q^2-1)} + \mathcal{O}(q^2) \quad \text{at} \quad Q_{2,2}. \tag{4.23}$$

Eq.(4.7) gives, for $i = 3$,

$$(Z_3^q + Z_3 - 1)(Z_4\xi_{2,2}^q)^q + (Z_3\xi_{2,2}^{q(q-1)})(Z_4\xi_{2,2}^q) - Z_3\xi_{2,2}^{q^2} = 0.$$

Since $(Z_3^q + Z_3) \cdot \xi_{2,2}^q$ is holomorphic at $Q_{2,2}$, this implies

$$\begin{aligned}(Z_3^q + Z_3 - 1)(Z_4\xi_{2,2}^q + c_1^2 \cdot \xi_{2,2})^q + (Z_3\xi_{2,2}^{q(q-1)})(Z_4\xi_{2,2}^q + c_1^2 \cdot \xi_{2,2})& \\ + \; c_1^{2q} \cdot \xi_{2,2}^q - Z_3(c_1^2 \cdot \xi_{2,2}^{q^2-q+1} + \xi_{2,2}^{q^2}) = \mathcal{O}(0) \;\text{ at }\; Q_{2,2}.&\end{aligned} \tag{4.24}$$

By (4.23) we have

$$\begin{aligned} Z_3 \cdot (c_1^2 \cdot \xi_{2,2}^{q^2-q+1} + \xi_{2,2}^{q^2}) &= (c_1^{q-1} \cdot \xi_{2,2}^{-(q^2-q)} - \xi_{2,2}^{-(q^2-1)} + \mathcal{O}(q^2)) \cdot (c_1^2 \cdot \xi_{2,2}^{q^2-q+1} + \xi_{2,2}^{q^2}) \\ &= c_1^{q-1} \cdot \xi_{2,2}^q + \mathcal{O}(0) = (c_1^2 \cdot \xi_{2,2})^q + \mathcal{O}(0) \quad \text{at} \quad Q_{2,2}. \end{aligned}$$

So (4.24) gives an equation for the function f_2 over $E_{2,2}$ as follows:

$$(Z_3^q + Z_3 - 1) \cdot f_2^q + (\xi_{2,2}^{q(q-1)} Z_3) \cdot f_2 - h_1 = 0,$$

with $h_1 \in E_{2,2}$ holomorphic at $Q_{2,2}$. This is assertion v) (for $j = 2$), and item vi) follows from v) and Lemma 4.1. The induction hypothesis over i (for $j = 2$) tells us that

$$(Z_2^q + Z_2 - 1) \cdot \xi_{i,2}^q + Z_2\mu_1^{q-1} \cdot \xi_{i,2} + \frac{\beta_i^q}{\beta_1} \cdot \mu_i = h$$

with $h \in H_{i,2}$ holomorphic at $P_{i,2}$. By Prop.4.4 v) we have

$$\mu_i = \beta_{i+1}^q \cdot \mu_{i+1} - \beta_{i+1} \cdot \mu_{i+1}^q + \mathcal{O}(0) \quad \text{at} \quad P_{i+1,2},$$

therefore

$$(Z_2^q + Z_2 - 1) \cdot \xi_{i,2}^q + Z_2\mu_1^{q-1} \cdot \xi_{i,2} + \frac{\beta_i^q}{\beta_1}(\beta_{i+1}^q\mu_{i+1} - \beta_{i+1}\mu_{i+1}^q) = \mathcal{O}(0) \quad \text{at } P_{i+1,2}.$$

As $(Z_2^q + Z_2) \cdot \mu_{i+1}^q$ is holomorphic at $P_{i+1,2}$, it follows that

$$\begin{aligned}(Z_2^q + Z_2 - 1) \cdot \left(\xi_{i,2} + \frac{\beta_i}{\beta_1^q}\beta_{i+1}^q\mu_{i+1}\right)^q + Z_2\mu_1^{q-1} \cdot \left(\xi_{i,2} + \frac{\beta_i}{\beta_1^q}\beta_{i+1}^q\mu_{i+1}\right)& \\ - Z_2\mu_1^{q-1}\frac{\beta_i}{\beta_1^q}\beta_{i+1}^q\mu_{i+1} + \frac{\beta_i^q}{\beta_1}\beta_{i+1}^q\mu_{i+1} = \mathcal{O}(0) \quad \text{at} \quad P_{i+1,2}.&\end{aligned}$$

Using once again that $Z_2\mu_1^{q-1} = -c_1 + \mathcal{O}(1)$ at $P_{2,2}$, we conclude the proof of item ii) for $j = 2$; i.e.,

$$(Z_2^q + Z_2 - 1) \cdot \xi_{i+1,2}^q + Z_2\mu_1^{q-1} \cdot \xi_{i+1,2} + \frac{\beta_{i+1}^q}{\beta_1} \cdot \mu_{i+1} = \mathcal{O}(0) \;\text{ at }\; P_{i+1,2}. \tag{4.25}$$

Since $P_{i+1,2}$ is a simple pole of the function μ_{i+1}, we apply Lemma 4.1 to Eq.(4.25) and this finishes the proof of item iii) for $j = 2$. It remains to prove the item iv). From Eq.(4.25) it follows that

$$\xi_{i+1,2}^q + c_1 \cdot \xi_{i+1,2} - \frac{\beta_{i+1}^q}{\beta_1} \cdot \mu_{i+1} = \mathcal{O}(0) \quad \text{at} \quad Q_{i+1,2}. \tag{4.26}$$

Using the definition of the function $\xi_{i+1,2}$, Eq.(4.26) yields assertion iv) of Prop.4.5 for $j = 2$; i.e.

$$\xi_{i,2} = \beta_i^q \cdot \xi_{i+1,2} - \frac{\beta_i}{c_1} \cdot \xi_{i+1,2}^q + \mathcal{O}(0) \;\; \text{at} \;\; Q_{i+1,2}.$$

The proof of Prop.4.5 in the case $j = 2$ is thus finished.

Suppose now that all statements of Prop.4.5 hold for some j with $2 \leq j < t$. We want to show that they also hold for $j + 1$.

Assertion i) (for $j + 1$) follows from the induction hypothesis (i.e., from items iii) and vi) for j). It also follows from the induction hypothesis that the function $f_j = Z_{2j} \cdot \xi_{j,j}^q + c_1^j \cdot \xi_{j,j}$ is holomorphic at the place $P_{i,j+1}$ for $i \geq j + 1$, and that

$$\xi_{i,j} = \beta_{i-j+2}^q \cdot \xi_{i+1,j} - \frac{\beta_{i-j+2}}{c_1^{j-1}} \cdot \xi_{i+1,j}^q + \mathcal{O}(0) \;\; \text{at} \;\; P_{i+1,j+1}.$$

This means that, for $i \geq j$, we have

$$Z_{2j} \cdot \xi_{j,j}^q = -\, c_1^j \cdot \xi_{j,j} + h \tag{4.27}$$

and

$$\xi_{i,j} = \beta_{i-j+2}^q \cdot \xi_{i+1,j} - \frac{\beta_{i-j+2}}{c_1^{j-1}} \cdot \xi_{i+1,j}^q + h' \tag{4.28}$$

with $h, h' \in H_{i+1,j+1}$ holomorphic at $P_{i+1,j+1}$. From Eq.(4.7) with $i = 2j$ and Eq.(4.27) we find

$$(Z_{2j}^q + Z_{2j} - 1) \cdot (Z_{2j+1} \cdot \xi_{j,j})^q + Z_{2j} \cdot \xi_{j,j}^{q-1} \cdot (Z_{2j+1} \cdot \xi_{j,j}) + c_i^j \cdot \xi_{j,j} = \mathcal{O}(0) \quad \text{at} \quad P_{j+1,j+1}.$$

Now Eq.(4.28), for $i = j$, implies

$$\begin{aligned}(Z_{2j}^q + Z_{2j} - 1) \cdot (Z_{2j+1} \cdot \xi_{j,j})^q + Z_{2j}\xi_{j,j}^{q-1} \cdot (Z_{2j+1} \cdot \xi_{j,j})& \\ + c_1^j \cdot \beta_2^q \cdot \xi_{j+1,j} - c_1\beta_2 \cdot \xi_{j+1,j}^q = \mathcal{O}(0) \quad \text{at} \quad P_{j+1,j+1}&.\end{aligned}$$

Observing that the place $P_{j+1,j+1}$ is a simple pole of the function $\xi_{j+1,j}$, that the function $(Z_{2j}^q + Z_{2j}) \cdot \xi_{j+1,j}^q$ is holomorphic and that $Z_{2j} \cdot \xi_{j,j}^{q-1} = -\, c_1^j + \mathcal{O}(1)$ at the place $P_{j+1,j+1}$, we obtain

$$\begin{aligned}(Z_{2j}^q + Z_{2j} - 1) \cdot (Z_{2j+1} \cdot \xi_{j,j} + c_1^q \cdot \beta_2^q \cdot \xi_{j+1,j})^q + Z_{2j} \cdot \xi_{j,j}^{q-1} \cdot (Z_{2j+1} \cdot \xi_{j,j} + c_1^q \cdot \beta_2^q \cdot \xi_{j+1,j})& \\ + c_1^j \cdot \beta_2^q \cdot \xi_{j+1,j} + c_1^j \cdot c_1^q \cdot \beta_2^q \cdot \xi_{j+1,j} = \mathcal{O}(0) \quad \text{at} \quad P_{j+1,j+1}&.\end{aligned}$$

Thus at the place $P_{j+1,j+1}$ we have

$$(Z_{2j}^q + Z_{2j} - 1) \cdot \xi_{j+1,j+1}^q + (Z_{2j} \cdot \xi_{j,j}^{q-1}) \cdot \xi_{j+1,j+1} + \frac{\beta_2^q}{\beta_1} \cdot c_1^{j-1} \cdot \xi_{j+1,j} = \mathcal{O}(0). \tag{4.29}$$

By induction over i we show then that

$$(Z_{2j}^q + Z_{2j} - 1) \cdot \xi_{i,j+1}^q + (Z_{2j} \cdot \xi_{j,j}^{q-1}) \cdot \xi_{i,j+1} + \frac{\beta_{i-j+1}^q}{\beta_1} \cdot c_1^{j-1} \cdot \xi_{i,j} = \tilde{h} \tag{4.30}$$

with $\tilde{h} \in H_{i,j+1}$ holomorphic at $P_{i,j+1}$, for $j+1 \leq i \leq t$. In fact, (4.29) gives (4.30) for $i = j+1$. Assuming (4.30) for i and using (4.28), we obtain

$$\begin{aligned}(Z_{2j}^q + Z_{2j} - 1) \cdot \xi_{i,j+1}^q &+ (Z_{2j}\xi_{j,j}^{q-1}) \cdot \xi_{i,j+1} \\ &+ \frac{\beta_{i-j+1}^q}{\beta_1} \cdot c_1^{j-1} \left(\beta_{i-j+2}^q \cdot \xi_{i+1,j} - \frac{\beta_{i-j+2}}{c_1^{j-1}} \cdot \xi_{i+1,j}^q \right) = h'\end{aligned} \tag{4.31}$$

with $h' \in H_{i+1,j+1}$ holomorphic at $P_{i+1,j+1}$. Since $P_{i+1,j+1}$ is a simple pole of $\xi_{i+1,j}$, since the function $(Z_{2j}^q + Z_{2j}) \cdot \xi_{i+1,j}^q$ is holomorphic and since $Z_{2j} \cdot \xi_{j,j}^{q-1} = -c_1^j + \mathcal{O}(1)$ at $P_{i+1,j+1}$, we obtain from (4.31) and the definition of the function $\xi_{i+1,j+1}$ that

$$(Z_{2j}^q + Z_{2j} - 1) \cdot \xi_{i+1,j+1}^q + (Z_{2j}\xi_{j,j}^{q-1}) \cdot \xi_{i+1,j+1} + \frac{\beta_{(i+1)-j+1}^q}{\beta_1} \cdot c_1^{j-1} \cdot \xi_{i+1,j} = \mathcal{O}(0)$$

at $P_{i+1,j+1}$. We have thus proved (4.30) for all i with $j+1 \leq i \leq t$, and hence Prop.4.5 ii) holds for $j+1$. It is then clear that also the assertion iii) holds for $j+1$, by Lemma 4.1.

Next we prove item iv) for $j+1$. By Prop.4.5 iii) and observing that $\xi_{i+1,j}$ has a simple pole at $P_{i+1,j+1}$ we see that the function

$$\xi_{i+1,j+1}^q + c_1^j \cdot \xi_{i+1,j+1} - \frac{\beta_{i-j+2}^q}{\beta_1} \cdot c_1^{j-1} \cdot \xi_{i+1,j} \tag{4.32}$$

is holomorphic at $Q_{i+1,j+1}$. Note that (4.32) in case $j+1 = 2$ is just (4.26). So, as in case $j+1 = 2$, we obtain assertion iv) from (4.32) and from the definition of the function $\xi_{i+2,j+1}$; i.e., we have

$$\xi_{i+1,j+1} = \beta_{i-j+2}^q \cdot \xi_{i+2,j+1} - \frac{\beta_{i-j+2}}{c_1^j} \cdot \xi_{i+2,j+1}^q + h,$$

with h holomorphic at the place $Q_{i+2,j+1}$.

In order to simplify notation we set $\eta_i := \xi_{i,i}$. From Prop.4.5 iii) it follows that $\eta_{j+1}^{-1} = \xi_{j+1,j+1}^{-1}$ is a local parameter at the place $Q_{j+1,j+1}$, and by (4.32) we have

$$\eta_{j+1}^q + c_1^j \cdot \eta_{j+1} - \frac{\beta_2^q}{\beta_1} \cdot c_1^{j-1} \cdot \xi_{j+1,j} = \mathcal{O}(0) \quad \text{at} \quad Q_{j+1,j+1}. \tag{4.33}$$

Note that (4.33) in case $j+1=2$ is just (4.21). By Prop.4.5 iv) we know that

$$\eta_j = \xi_{j,j} = \beta_2^q \cdot \xi_{j+1,j} - \frac{\beta_2}{c_1^{j-1}} \cdot \xi_{j+1,j}^q + \mathcal{O}(0) \ \text{ at } \ Q_{j+1,j+1}.$$

Hence it follows from (4.33) that

$$\begin{aligned} \eta_j \ &= -\beta_1^q \cdot \eta_{j+1}^{q^2} + \beta_1^q \cdot \eta_{j+1} + \mathcal{O}(0) \\ &= -\beta_1^q \cdot \eta_{j+1}^{q^2} \cdot (1 - \eta_{j+1}^{1-q^2} + \mathcal{O}(q^2)) \quad \text{at } \ Q_{j+1,j+1} \end{aligned}$$

and consequently

$$\eta_j^{-1} = -\frac{1}{\beta_1^q} \cdot \eta_{j+1}^{-q^2} \cdot (1 + \eta_{j+1}^{1-q^2} + \mathcal{O}(q^2)) \quad \text{at } \ Q_{j+1,j+1}.$$

Since $Z_{2j+1} \cdot \eta_j = \eta_{j+1} - c_1^q \cdot \beta_2^q \cdot \xi_{j+1,j}$, we obtain from (4.33) that

$$Z_{2j+1} \cdot \eta_j = \eta_{j+1} - c_1^q \cdot \beta_2^q \left(\frac{\beta_1}{\beta_2^q c_1^{j-1}} \cdot \eta_{j+1}^q + \frac{\beta_1^q}{\beta_2^q} \cdot \eta_{j+1} \right) + \mathcal{O}(0) \ \text{ at } \ Q_{j+1,j+1}$$

and hence we have an equation of the form

$$Z_{2j+1} \cdot \eta_j = \beta_1^q \cdot \eta_{j+1} - c_1^q \cdot \frac{\beta_1}{c_1^{j-1}} \cdot \eta_{j+1}^q + h,$$

with h holomorphic at $Q_{j+1,j+1}$. We multiply this equation by η_j^{-1}, and we obtain

$$\begin{aligned} Z_{2j+1} \ &= - \left(\eta_{j+1}^{1-q^2} - \frac{c_1^q}{c_1^j} \cdot \eta_{j+1}^{q-q^2} + \mathcal{O}(q^2) \right) \cdot (1 + \eta_{j+1}^{1-q^2} + \mathcal{O}(q^2)) \\ &= -\eta_{j+1}^{1-q^2} + \frac{c_1^q}{c_1^j} \cdot \eta_{j+1}^{q-q^2} + \mathcal{O}(q^2) \quad \text{at } \ Q_{j+1,j+1}. \end{aligned} \tag{4.34}$$

We have from Eq.(4.7) for $i = 2j+1$, that

$$(Z_{2j+1}^q + Z_{2j+1} - 1) \cdot (Z_{2j+2} \cdot \eta_{j+1}^q)^q + (Z_{2j+1} \cdot \eta_{j+1}^{q(q-1)}) \cdot (Z_{2j+2} \cdot \eta_{j+1}^q) - Z_{2j+1} \cdot \eta_{j+1}^{q^2} = 0.$$

As before (cf. (4.24)) this implies that

$$\begin{aligned} (Z_{2j+1}^q + Z_{2j+1} - 1) \cdot (Z_{2j+2} \cdot \eta_{j+1}^q + c_1^{j+1} \cdot \eta_{j+1})^q + (Z_{2j+1} \cdot \eta_{j+1}^{q(q-1)}) \cdot (Z_{2j+2} \cdot \eta_{j+1}^q + c_1^{j+1} \cdot \eta_{j+1}) \\ + c_1^{(j+1)q} \cdot \eta_{j+1}^q - Z_{2j+1} \cdot (c_1^{j+1} \cdot \eta_{j+1}^{q^2-q+1} + \eta_{j+1}^{q^2}) = \mathcal{O}(0) \ \text{ at } \ Q_{j+1,j+1}. \end{aligned}$$

From (4.34) we then get

$$\begin{aligned} & Z_{2j+1} \cdot (c_1^{j+1} \cdot \eta_{j+1}^{q^2-q+1} + \eta_{j+1}^{q^2}) \\ &= - \left(\eta_{j+1}^{1-q^2} - \frac{c_1^q}{c_1^j} \cdot \eta_{j+1}^{q-q^2} + \mathcal{O}(q^2) \right) \cdot (c_1^{j+1} \cdot \eta_{j+1}^{q^2-q+1} + \eta_{j+1}^{q^2}) \\ &= \frac{c_1^q}{c_1^j} \cdot \eta_{j+1}^q + \mathcal{O}(0) \quad \text{at } \ Q_{j+1,j+1}. \end{aligned}$$

Since $f_{j+1} = Z_{2j+2} \cdot \eta_{j+1}^q + c_1^{j+1} \cdot \eta_{j+1}$, we have thus found an equation

$$(Z_{2j+1}^q + Z_{2j+1} - 1) \cdot f_{j+1}^q + (\eta_{j+1}^{q(q-1)} \cdot Z_{2j+1}) \cdot f_{j+1} = h$$

with a function $h \in E_{j+1,j+1}$ which is holomorphic at the place $Q_{j+1,j+1}$. This proves assertion v) for $j+1$ and, as before, assertion vi) follows from v) and from Lemma 4.1. The proof of Proposition 4.5 and therefore of the Main Theorem is finished. □

5. Making the tower galois

We consider again the tower $\mathcal{F} = (F_1, F_2, F_3, \dots)$ over the field $\mathbb{F}_\ell$ (with $\ell = q^3$) which is defined recursively by $F_1 = \mathbb{F}_\ell(x_1)$ and $F_{n+1} = F_n(x_{n+1})$, where x_{n+1} satisfies the equation

$$\frac{1 - x_{n+1}}{x_{n+1}^q} = \frac{x_n^q + x_n - 1}{x_n}, \qquad \text{for all } n \geq 1. \tag{5.1}$$

As we pointed out before, all extensions F_{n+1}/F_n in this tower $\mathcal{F}$ are of degree q and they are non-Galois in the case $q > 2$. In this section we show that we can enlarge $\mathcal{F}$ to a tower $\mathcal{B}$ over $\mathbb{F}_\ell$ having the same limit as $\mathcal{F}$, and with the additional property that all steps in the tower $\mathcal{B}$ are Galois extensions.

We define the tower $\mathcal{B}$ over the field $\mathbb{F}_\ell = \mathbb{F}_{q^3}$ inductively as follows:

$$\begin{aligned} \mathcal{B} &= (G_1, H_1, G_2, H_2, \dots, G_j, H_j, \dots), \\ G_1 &= \mathbb{F}_\ell(x_1) \quad \text{is the rational function field,} \\ H_1 &= G_1(z_1) \quad \text{with} \quad z_1^{q-1} + (x_1^q + x_1 - 1)/x_1 = 0, \\ G_{n+1} &= H_n(x_{n+1}) \quad \text{with} \quad (x_{n+1} z_n)^q - (x_{n+1} z_n) + z_n = 0, \\ H_{n+1} &= G_{n+1}(z_{n+1}) \quad \text{with} \quad z_{n+1}^{q-1} + (x_{n+1}^q + x_{n+1} - 1)/x_{n+1} = 0, \end{aligned} \tag{5.2}$$

for all $n \geq 1$. The main result of this section is

Theorem 5.1. *The tower $\mathcal{B} = (G_1, H_1, G_2, H_2, \dots)$ over the field $\mathbb{F}_\ell = \mathbb{F}_{q^3}$ as defined in (5.2) has the following properties:*

(i) *For all $n \geq 1$ the extensions H_n/G_n and G_{n+1}/H_n are Galois. The extension H_n/G_n is a Kummer extension of degree $[H_n : G_n] = q - 1$, and G_{n+1}/H_n is an Artin-Schreier extension of degree $[G_{n+1} : H_n] = q$.*

(ii) *The limit $\lambda(\mathcal{B})$ satisfies $\lambda(\mathcal{B}) \geq 2(q^2 - 1)/(q + 2)$.*

Remark 5.2. It follows immediately from (5.2) that the elements $x_n \in G_n$ satisfy the equation

$$(1 - x_{n+1})/x_{n+1}^q = (x_n^q + x_n - 1)/x_n, \qquad \text{for all} \quad n \geq 1.$$

Hence the tower $\mathcal{F}$ given by (5.1) is a subtower of the tower $\mathcal{B}$.

For the proof of Thm 5.1 we need an analogue of the Hurwitz genus formula for towers of function fields, see [9]. For the convenience of the reader we recall this result here. Consider a tower $\mathcal{L} = (L_1, L_2, L_3, \dots)$ of function fields over $\mathbb{F}_\ell$, where L_{n+1}/L_n is separable of degree $[L_{n+1}, L_n] > 1$ for all $n \geq 1$. We define the *relative genus* $\gamma(\mathcal{L}/L_1)$ as

$$\gamma(\mathcal{L}/L_1) := \lim_{n\to\infty} g(L_n)/[L_n : L_1].$$

Moreover we define the *ramification locus* of $\mathcal{L}/L_1$ as

$$V(\mathcal{L}/L_1) := \{P \in \mathbb{P}(L_1) \ ; \ P \text{ is ramified in } L_n/L_1 \text{ for some } n \geq 2\}.$$

If $V(\mathcal{L}/L_1)$ is finite, we define the divisors

$$A_n(\mathcal{L}/L_1) := \sum_{\substack{Q\in\mathbb{P}(L_n)\\ Q\cap L_1\in V(\mathcal{L}/L_1)}} Q, \quad \text{for all} \quad n \geq 2.$$

It is easy to see that the limit

$$\alpha(\mathcal{L}/L_1) := \lim_{n\to\infty} \deg A_n(\mathcal{L}/L_1)/[L_n : L_1]$$

exists. Now we can state the *Hurwitz genus formula* for towers of function fields.

Proposition 5.3. *(see [9], Thm 3.6). Suppose that $\mathcal{L} = (L_1, L_2, L_3, \dots)$ is a tower of function fields over $\mathbb{F}_\ell$. Let L_1^*/L_1 be a finite separable extension such that L_1^* and L_n are linearly disjoint over L_1, and such that $\mathbb{F}_\ell$ is algebraically closed in $L_n^* := L_1^* \cdot L_n$ for all $n \geq 1$. Denote by $\mathcal{L}^* := (L_1^*, L_2^*, L_3^*, \dots)$ the composite tower of $\mathcal{L}$ and L_1^*. Assume that the following conditions hold:*

(i) *The ramification locus $V(\mathcal{L}/L_1)$ is finite, and $\alpha(\mathcal{L}/L_1) = 0$.*
(ii) *All places $P \in V(\mathcal{L}/L_1)$ are tame in the extension L_1^*/L_1.*

Then we have

$$2g(L_1^*) - 2\gamma(\mathcal{L}^*/L_1^*) - 2 = [L_1^* : L_1] \cdot (2g(L_1) - 2\gamma(\mathcal{L}/L_1) - 2) + \delta,$$

with

$$\delta = \sum_{\substack{Q\in\mathbb{P}(L_1^*)\\ Q\cap L_1\in V(\mathcal{L}/L_1)}} d(Q \mid Q \cap L_1) \cdot deg\ Q.$$

Corollary 5.4. *In addition to the assumptions (i) and (ii) in Prop. 5.3 we assume:*

(iii) *All places $P \in \mathbb{P}(L_1)$ which are ramified in the extension L_1^*/L_1 belong to the ramification locus $V(\mathcal{L}/L_1)$.*

Then we have $\gamma(\mathcal{L}^*/L_1^*) = [L_1^* : L_1] \cdot \gamma(\mathcal{L}/L_1)$.

Proof. From assumption (iii) it follows that the number δ in Prop. 5.3 is equal to the different degree of the extension L_1^*/L_1, and hence $2g(L_1^*)-2 = [L_1^* : L_1](2g(L_1)-2)+\delta$. Now the assertion of Cor. 5.4 follows immediately from Prop. 5.3.

□

Proof of Thm. 5.1 As in Secton 3 let us denote $b(T) := (T^q+T-1)/T$. We start with the tower $\mathcal{F} = (F_1, F_2, F_3, \dots)$ which is recursively defined by (5.1), i.e., by the equation $(1-x_{n+1})/x_{n+1}^q = b(x_n)$, and we consider the composite tower $\mathcal{E} = (E_1, E_2, E_3, \dots)$ of the tower $\mathcal{F}$ with the function field $E_1 := F_1(z_1)$, where $z_1^{q-1}+b(x_1) = 0$. Note that $E_n = F_n(z_1)$ and in particular $E_2 = F_2(z_1) = E_1(x_2z_1)$, with the following relation

$$\begin{aligned}(x_2z_1)^q - (x_2z_1) + z_1 &= z_1(x_2^qz_1^{q-1} - x_2 + 1) \\ &= z_1(-x_2^q \cdot b(x_1) - x_2 + 1) = z_1((x_2-1) - x_2 + 1) = 0.\end{aligned} \tag{5.3}$$

By Prop. 2.4 and Lemma 2.3 the ramification locus of $\mathcal{F}/F_1$ is

$$V(\mathcal{F}/F_1) = \{(x_1 = \alpha)\ ;\ \alpha = 0, 1, \infty \text{ or } \alpha^q + \alpha = 1\}.$$

So $V(\mathcal{F}/F_1)$ is finite, and it follows from Prop. 2.5, 2.6, 2.7 and 2.8 that $\alpha(\mathcal{F}/F_1) = 0$. Therefore condition (i) of Prop. 5.3 is satisfied. The condition (ii) of Prop. 5.3 holds trivially since E_1/F_1 is Galois of degree $q-1$. By the theory of Kummer extentions of function fields (see [16], Prop. III.7.3), only the zeroes and the poles of the function $b(x_1) = (x_1^q + x_1 - 1)/x_1$ may ramify in the extension E_1/F_1, and hence also the condition (iii) in Cor. 5.4 holds. Therefore we obtain $\gamma(\mathcal{E}/E_1) = (q-1)\cdot\gamma(\mathcal{F}/F_1)$ from Cor. 5.4. Observing that $\gamma(\mathcal{E}/E_2) = q\cdot\gamma(\mathcal{E}/E_1)$ and that $\gamma(\mathcal{F}/F_1) = q(q+2)/2(q-1)$ by Thm. 2.9, it follows

$$\gamma(\mathcal{E}/E_2) = q^2(q+2)/2. \tag{5.4}$$

Next we show that sufficiently many rational places of E_2 split completely over $\mathbb{F}_{q^3}$ in the tower $\mathcal{E}/E_2$. Let

$$\Omega := \{\omega \in \mathbb{F}_\ell\ ;\ b(\omega)^{q+1} = b(\omega) - 1\},$$

and

$$\Omega(F_1) := \{(x_1 = \omega)\ ;\ \omega \in \Omega\} \subseteq \mathbb{P}(F_1).$$

We know from Prop. 3.1 and Thm 3.2 that $\#\Omega = q(q+1)$ and that all places $P \in \Omega(F_1)$ split completely in the tower $\mathcal{F}/F_1$.

We want to show that the places $P = (x_1 = \omega) \in \Omega(F_1)$ also split completely in the extension E_1/F_1. In fact, since $E_1 = F_1(z_1)$ and $z_1^{q-1} = -b(x_1)$ we have to show that the element $-b(\omega)$ is a $(q-1)$-th power in the finite field $\mathbb{F}_\ell$, and this assertion is equivalent to show that $(-b(\omega))^{q^2+q+1} = 1$. We have by Lemma 3.5

$$(-b(\omega))^{q^2+q+1} = -b(\omega)^{q^2+q+1} = -(-1) = 1$$

and this proves our claim. Since $E_n = E_1 \cdot F_n$ it follows now that the places $P \in \Omega(F_1)$ are also completely splitting in the extensions E_n/F_1, for all $n \geq 1$. Setting

$$\Omega(E_2) := \{P \in \mathbb{P}(E_2)\ ;\ P \cap F_1 \in \Omega(F_1)\}$$

we have shown:

(1) All places $P \in \Omega(E_2)$ are $\mathbb{F}_\ell$-rational, and they split completely in the tower $\mathcal{E}/E_2$.
(2) $\#\Omega(E_2) = [E_2 : F_1] \cdot \#\Omega(F_1) = q^2(q^2-1)$.
(3) The places $P \in \Omega(E_2)$ are exactly the zeroes in the function field E_2 of the functions $x_2 - \omega$, with $\omega \in \Omega$.

From (1) and (2) it follows that the number of $\mathbb{F}_\ell$-rational places of E_n satisfies the inequality $N(E_n) \geq [E_n : E_2] \cdot q^2(q^2-1)$, and then Eq.(5.4) yields

$$\lambda(\mathcal{E}) \geq \frac{\#\Omega(E_2)}{\gamma(\mathcal{E}/E_2)} = \frac{q^2(q^2-1)}{q^2(q+2)/2} = \frac{2(q^2-1)}{q+2}.$$

In the tower $\mathcal{E}/E_2$, the extensions E_{n+1}/E_n are non-Galois for all $n \geq 2$ (in the case $q \neq 2$), and we consider therefore the composite tower $\mathcal{L} = (L_2, L_3, L_4, \dots)$ of the tower $\mathcal{E}$ with the function field $L_2 := E_2(z_2)$ where $z_2^{q-1} + b(x_2) = 0$. As before we see that $L_3 = L_2(x_3z_2)$ with $(x_3z_2)^q - (x_3z_2) + z_2 = 0$, so L_3/L_2 is an Artin-Schreier extension of degree q. The relative genus of $\mathcal{L}/L_3$ is

$$\gamma(\mathcal{L}/L_3) = q(q-1) \cdot \gamma(\mathcal{E}/E_2),$$

and the set

$$\Omega(L_3) := \{P \in \mathbb{P}(L_3)\ ; \mathbb{P} \cap E_2 \in \Omega(E_2)\}$$

has cardinality $q(q-1) \cdot \#\Omega(E_2)$. All places $P \in \Omega(L_3)$ split completely in the tower $\mathcal{L}/L_3$, and we obtain that the limit of the tower $\mathcal{L}$ satisfies $\lambda(\mathcal{L}) \geq 2(q^2-1)/(q+2)$. Continuing this process we now define the tower $\mathcal{M} = (M_3, M_4, M_5, \dots)$ as the composite of the tower $\mathcal{L}/L_3$ with the function field $M_3 = L_3(z_3)$ where $z_3^{q-1} + b(x_3) = 0$, etc.

Setting $G_1 := F_1$, $H_1 := E_1$, $G_2 := E_2$, $H_2 := L_2$, $G_3 := L_3$, $H_3 := M_3$, etc... we see that the tower $\mathcal{B} = (G_1, H_1, G_2, H_2, \dots,)$ is defined as in (5.2). Since the limit of all horizontal towers in Fig. 5 below is bigger than or equal to $2(q^2-1)/(q+2)$, it follows that also the limit of $\mathcal{B}$ satisfies $\lambda(\mathcal{B}) \geq 2(q^2-1)/(q+2)$, and this proves Thm 5.1. □

The following picture summarizes the construction above leading to a tower with alternating Kummer and Artin-Schreier extensions (the bold-face vertical extensions are Kummer extensions of degree $q-1$ and the bold-face horizontal extensions are Artin-Schreier extensions of degree q).

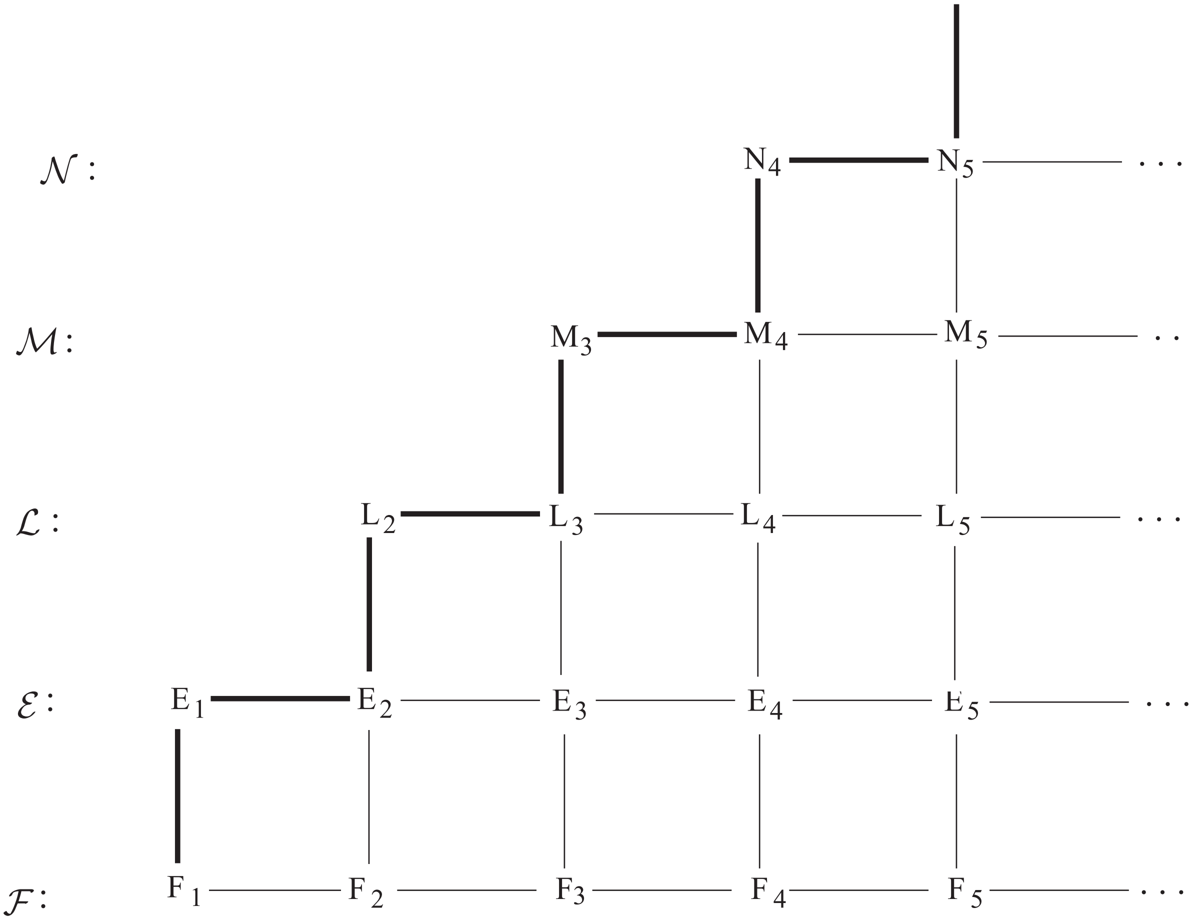

Figure 5

References

[1] B. Angles and C. Maire, *A note on tamely ramified towers of global function fields*, Finite Fields Appl. **8** (2002), 207–215.

[2] J. Bezerra and A. Garcia, *A tower with non-Galois steps which attains the Drinfeld-Vladut bound*, to appear in J. Number Theory.

[3] V.G. Drinfeld and S.G. Vladut, *The number of points of an algebraic curve*, Funktsional. Anal. i Prilozhen. **17** (1983), 68–69. [Funct. Anal. Appl. **17** (1983), 53–54.]

[4] N.D. Elkies, *Explicit modular towers*, in: Proceedings of the Thirty-Fifth [1997] Annual Allerton Conference on Communication, Control and Computing, (T. Basar and A. Vardy, eds.), Univ. of Illinois at Urbana-Champaign, (1998), 23–32.

[5] N.D. Elkies, *Explicit towers of Drinfeld modular curves*, in: European Congress of Mathematics (Barcelona, 2000), Vol. II (C. Casacuberta et all., eds.), Birkhauser, Basel, (2001), 189–198. arXiv:math.NT/0005140 (2000).

[6] A. Garcia and 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 and H. Stichtenoth, *On the asymptotic behavior of some towers of function fields over finite fields*, J. Number Theory **61** (1996), 248–273.

[8] A. Garcia and H. Stichtenoth, *On tame towers over finite fields*, J. Reine Angew. Math. **557** (2003), 53–80.

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

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

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

[12] W.-C.W. Li, H. Maharaj and H. Stichtenoth, *New optimal towers over finite fields*, in: Algorithmic Number Theory [Sydney, 2002] (C. Fieker and D. Kohel, eds.), 372–389.

[13] H. Niederreiter and C. Xing, *Rational points on curves over finite fields: theory and applications*, Cambridge Univ. Press, Cambridge, 2001.

[14] 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; = Euvres [128].

[15] J.-P. Serre, *Rational points on curves over finite fields*, unpublished lecture notes by F.Q. Gouvêa, Harvard University, (1985).

[16] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer Verlag, Berlin, 1993.

[17] A. Temkine, *Hilbert class field towers of function fields over finite fields and lower bounds for $A(q)$*, J. Number Theory **87** (2001), 189–210.

[18] 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.

[19] J. Wulftange, *Zahme Türme algebraischer Funktionenkörper*, Ph.D. thesis (Essen, 2003).

[20] Th. Zink, *Degeneration of Shimura surfaces and a problem in coding theory*, in: Fundamentals of Computation Theory [Cottbus] (L. Budach, ed.), Springer-Verlag, New York, 1985, 503–511.