A PROBLEM OF BEELEN, GARCIA AND STICHTENOTH ON AN ARTIN-SCHREIER TOWER IN CHARACTERISTIC TWO

MARÍA CHARA, HORACIO NAVARRO, AND RICARDO TOLEDANO

Abstract. We study a tower of function fields of Artin-Schreier type over a finite field with 2^s elements. The study of the asymptotic behavior of this tower was left as an open problem by Beelen, García and Stichtenoth in 2006. We prove that this tower is optimal over a finite field with four elements.

1. Introduction

In 2006 P. Beelen, A. Garcia and H. Stichtenoth gave the first steps in [BGS] towards the classification, according to their asymptotic behavior, of recursive towers of function fields over a finite field $\mathbb{F}_q$ with q elements. They focused on recursive towers defined by equations of the form $f(y) = g(x)$, where f and g are suitable rational functions over $\mathbb{F}_q$. Towers defined in this way were called (f, g)-towers over $\mathbb{F}_q$. In particular, they noticed that many (f, g)-towers can be recursively defined by equations of the form $h(y) = A \cdot h(B \cdot x)$ for some polynomial h over $\mathbb{F}_q$ and A, $B \in GL(2, \mathbb{F}_q)$. Here the symbol $A \cdot u$ stands for the usual action of elements of $GL(2, \mathbb{F}_q)$ as fractional transformations, i.e.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot u := \frac{au + b}{cu + d}.$$

This was a key observation that allowed them to obtain classification results in the important cases of recursive towers of Kummer and Artin-Schreier type. As an application of these results, they gave a complete list of all (f, g)-towers of Artin-Schreier type with $\deg f = \deg g = 2$ over the finite field $\mathbb{F}_2$. They checked that all the possible cases were already considered in previous works, except for the following Artin-Schreier tower $\mathcal{H}$ recursively defined by the equation

$$y^2 + y = \frac{x}{x^2 + x + 1}, \qquad (1.1)$$

2010 *Mathematics Subject Classification.* Primary 11R58, 11G20; Secondary 14H05.
Key words and phrases. Function fields, Artin-Schreier extensions, genus, rational places, towers, limit of towers.

over $\mathbb{F}_2$. Nothing else was said about this tower and in fact they posed, as an open problem, to determine when the above equation (1.1) defines an asymptotically good tower over $\mathbb{F}_{2^s}$ with $s \geq 1$. The aim of this work is to prove that equation (1.1) defines an optimal tower over $\mathbb{F}_4$. We will also show that equation (1.1) defines a tower $\mathcal{H}$ of finite genus and positive splitting rate over $\mathbb{F}_{2^s}$ for every even integer $s > 0$. It can be also shown that equation (1.1) defines a tower of finite genus and zero splitting rate when s is odd. Thus equation (1.1) defines an asymptotically bad tower over $\mathbb{F}_{2^s}$ for s odd, but we will not include the details here and the interested reader can find them in [HN17].

The organization of this paper is as follows. In Section 2 we give some basic definitions and we recall some known results. In Section 3 we prove that equation (1.1) defines a tower $\mathcal{H}$ of function fields over $\mathbb{F}_{2^s}$ of finite genus when s is even. Finally, Section 4 is devoted to the study of the splitting rate of $\mathcal{H}$ over $\mathbb{F}_4$ and we prove our main result, namely that the tower $\mathcal{H}$ is optimal over $\mathbb{F}_4$. This section contains the most intricate and interesting part of the paper. After some technical lemmas, we will show that all the rational places in the base step of the tower ramify first and then they start to split completely in the tower. Our detailed study of this behavior, which heavily relies on the explicit construction of what we call Artin-Schreier elements of type 1 and 2 (see Definition 4.3) in each function field of $\mathcal{H}$, allowed us to compute, in Theorem 4.11, the exact number of rational places in each step of the tower $\mathcal{H}$ over $\mathbb{F}_4$.

2. Preliminaries

We give now the basic definitions and concepts of function fields and towers of function fields which will be used in this paper. The standard reference for all of this is [S]. Let k be a perfect field. A function field (of one variable) F over k is a finite algebraic extension F of the rational function field $k(x)$, where x is a transcendental element over k.

Let F be a function field over k. The symbol $\mathbb{P}(F)$ stands for the set of all places of F and $g(F)$ for the genus of F.

Let F' be a finite extension of F and let $Q \in \mathbb{P}(F')$. We will write $Q|P$ when the place Q of F' lies over the place P of F, i.e. $P = Q \cap F$. In this case the symbols $e(Q|P)$ and $d(Q|P)$ denote, as usual, the ramification index and the different exponent of $Q|P$, respectively.

A *tower* $\mathcal{F}$ (of function fields) over k is a sequence $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ of function fields over k such that

(a) $F_i \subsetneq F_{i+1}$ for all $i \geq 0$.
(b) The extension F_{i+1}/F_i is finite and separable, for all $i \geq 1$.
(c) The field k is algebraically closed in F_i, for all $i \geq 0$.
(d) The genus $g(F_i) \to \infty$ as $i \to \infty$.

A tower $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ over k is called *recursive* if there exist a sequence of transcendental elements $\{x_i\}_{i=0}^{\infty}$ over k and a bivariate polynomial $H(X, Y) \in k[X, Y]$ such that $F_0 = k(x_0)$ and

$$F_{i+1} = F_i(x_{i+1}),$$

where $H(x_i, x_{i+1}) = 0$ for all $i \geq 0$. Associated to any recursive tower $\mathcal{F}$ we have its *basic function field* $F = k(x, y)$ where $H(x, y) = 0$ and x is a transcendental element over k.

The *the genus* $\gamma(\mathcal{F})$ of $\mathcal{F}$ over F_0 is defined as

$$\gamma(\mathcal{F}) := \lim_{i\to\infty} \frac{g(F_i)}{[F_i : F_0]} \,.$$

When $k = \mathbb{F}_q$ we denote by $N(F_i)$ the number of rational places (i.e., places of degree one) of F_i and the *splitting rate* $\nu(\mathcal{F})$ of $\mathcal{F}$ over F_0 is defined as

$$\nu(\mathcal{F}) := \lim_{i\to\infty} \frac{N(F_i)}{[F_i : F_0]}.$$

A tower $\mathcal{F}$ over $\mathbb{F}_q$ is called *asymptotically good* if $\nu(\mathcal{F}) > 0$ and $\gamma(\mathcal{F}) < \infty$. Otherwise $\mathcal{F}$ is called *asymptotically bad*. Equivalently, a tower $\mathcal{F}$ is asymptotically good over $\mathbb{F}_q$ if and only if *the limit* of the tower $\mathcal{F}$

$$\lambda(\mathcal{F}) := \lim_{i\to\infty} \frac{N(F_i)}{g(F_i)} = \frac{\nu(\mathcal{F})}{\gamma(\mathcal{F})},$$

is positive.

An straightforward upper bound for the limit of a tower $\mathcal{F}$ over $\mathbb{F}_q$ is given by Ihara's function

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

where $N_q(g)$ is the maximum number of rational places that a function field over $\mathbb{F}_q$ of genus g can have. A result of Drinfeld and Vladut [S, Theorem 7.1.3] establishes that

$$\lambda(\mathcal{F}) \leq A(q) \leq \sqrt{q} - 1.$$

A tower $\mathcal{F}$ over $\mathbb{F}_q$ is called *asymptotically optimal* if $\lambda(\mathcal{F}) = A(q)$. It is well known ([S, Remark 7.1.4 (b)]) that if q is a prime square power then $A(q) = \sqrt{q} - 1$ so that in this case a tower $\mathcal{F}$ over $\mathbb{F}_q$ is asymptotically optimal when $\lambda(\mathcal{F}) = \sqrt{q} - 1$.

In the study of the asymptotic behavior of a tower $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ over $\mathbb{F}_q$, the following sets play an important role: the *ramification locus* $R(\mathcal{F})$ of $\mathcal{F}$, which is the set of places P of F_0 such that P is ramified in F_i for some $i \geq 1$ and the *splitting locus* $Sp(\mathcal{F})$ of $\mathcal{F}$, which is the set of rational places P of F_0 such that P splits completely in F_i for all $i \geq 1$.

Let $B \geq 0$ be a real number and let F'/F be a finite extension of function fields over k. A place P of F is called B-*bounded* in F' if

$$d(Q|P) \leq B \cdot (e(Q|P) - 1),$$

for any place Q of F' lying over P. The extension F'/F is called B-*bounded* if every place of F is B-bounded in F'. A tower $\{F_i\}_{i=0}^{\infty}$ over k is called B-*bounded* if every extension F_i/F_0 is $B-$bounded. In [GS, Proposition 1.5] the following result is proved.

Proposition 2.1. *A B-bounded tower $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ over k with finite ramification locus has finite genus. More precisely, the following bound for the genus of $\mathcal{F}$ holds:*

$$\gamma(F) \leq g(F_0) - 1 + \frac{B}{2} \sum_{P \in \mathcal{R}(\mathcal{F})} \deg P.$$

We immediately see that a tower $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ over $\mathbb{F}_q$ is asymptotically good if the tower is B-bounded, $R(\mathcal{F})$ is a finite set and $Sp(\mathcal{F}) \neq \emptyset$. The next proposition is proved in [S, Proposition 3.9.6].

Proposition 2.2. *Let $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ be a tower over $\mathbb{F}_q$ and let $\mathcal{E} = \{E_i\}_{i=0}^{\infty}$ be the tower over $\mathbb{F}_{q^n}$ where each E_i is the composite of the fields F_i and $\mathbb{F}_{q^n}$. Then $Sp(\mathcal{F}) \subseteq Sp(\mathcal{E}) \cap \mathbb{P}(F_0)$.*

We recall now from [S, Section 7.4] the concept of weakly ramified extensions.

Definition 2.3. *Let F be a function field over k with $Char(k) = p$. A finite field extension E/F is said to be weakly ramified, if the following conditions hold:*

(i) There exist intermediate fields $F = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_n = E$ such that all extensions E_{i+1}/E_i are Galois p-extensions (i.e., $[E_{i+1} : E_i]$ is a power of p), for $i = 0, 1 \ldots, n-1$.

(ii) *For any $P \in \mathbb{P}(F)$ and any $Q \in \mathbb{P}(E)$ lying over P, the different exponent is given by $d(Q|P) = 2(e(Q|P) - 1)$.*

We have (see [S, Remark 7.4.11, Proposition 7.4.13]) the following results:

Proposition 2.4. *Let E/F be an extension of function fields over k such that $[E : F] = p^m$ where $p = char\, F$. Assume that there exist a chain of intermediate fields*

$$F = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_n = E$$

with the property E_{i+1}/E_i is a Galois p-extension for all $i = 0, 1 \ldots, n-1$. Let $P \in \mathbb{P}(F)$ and $Q \in \mathbb{P}(E)$ lying over P and let Q_i be the restriction of Q to E_i for $i = 0, \ldots n-1$. Then the following conditions are equivalent:

(i) *$d(Q|P) = 2(e(Q|P) - 1)$.*
(ii) *$d(Q_{i+1}|Q_i) = 2(e(Q_{i+1}|Q_i) - 1)$ for $i = 0, \ldots, n-1$.*

Notice that if every extension F_i/F_0 of a tower $\{F_i\}_{i=0}^{\infty}$ over k is weakly ramified then the tower is 2-bounded.

Proposition 2.5. *Let E/F be a finite extension of function fields over k and let M and N be intermediate fields of $E \supseteq F$ such that $E = MN$ is the compositum of M and N. If both extensions M/F and N/F are weakly ramified then E/F is weakly ramified.*

Now we can prove the following result which will be useful in the study of the genus of the tower $\mathcal{H}$.

Corollary 2.6. *Let $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ be a recursive tower of function fields over k such that the extension F_{i+1}/F_i is a Galois p-extension for $i \geq 0$. Let $F = k(x, y)$ be the basic function field associated to F and suppose that the extensions $F/k(x)$ and $F/k(y)$ are weakly ramified. Then each extension F_i/F_0 is weakly ramified (in which case we say that $\mathcal{F}$ is weakly ramified tower). Furthermore $\mathcal{F}$ has finite genus if the ramification locus of $\mathcal{F}$ is finite.*

Proof. We have that $F_0 = k(x_0)$ and $F_{i+1} = F_i(x_{i+1})$ for $i \geq 0$ where $\{x_i\}_{i=0}^{\infty}$ is a sequence of transcendental elements over k. By hypothesis, the extensions $F_1/k(x_0)$ and $F_1/k(x_1)$ are weakly ramified. In particular F_1/F_0 is weakly ramified. Now suppose that F_i/F_0 is weakly ramified. Since $F_i = k(x_0, \ldots, x_i)$, the extensions F_i/F_0 and $k(x_1, \ldots, x_i, x_{i+1})/k(x_1)$ are isomorphic over k (by the map sending

$x_j \to x_{j+1}$ for $j = 0, \ldots, i$), hence $k(x_1, \ldots, x_i, x_{i+1})/k(x_1)$ is weakly ramified. Since F_{i+1} is the compositum of the fields $F_1 = k(x_0, x_1)$ and $k(x_1, \ldots, x_i, x_{i+1})$, we have that the extension $F_{i+1}/k(x_1)$ is weakly ramified by Proposition 2.5 and so F_{i+1}/F_i is a weakly ramified extension by Proposition 2.4. This immediately implies that F_{i+1}/F_0 is a weakly ramified extension and this proves the first part. In particular we have that $\mathcal{F}$ is a 2-bounded tower, so the second statement follows directly from Proposition 2.1. □

3. The genus of the tower $\mathcal{H}$ over $\mathbb{F}_{2^s}$ for s even

Let $s > 0$ be an even integer and let $\mathcal{H} = \{F_i\}_{i=0}^{\infty}$ be the sequence of function fields over $k = \mathbb{F}_{2^s}$ recursively defined by (1.1).

In this section we will show that $\mathcal{H}$ is a tower over k of finite genus. Our first task is to prove that equation (1.1) defines a tower over k since this was not established in [BGS]. From now on we will consider $\mathbb{F}_4 := \{0, 1, \alpha, \alpha+1\} \subset \mathbb{F}_{2^s}$ for any s where $\alpha^2 + \alpha + 1 = 0$.

Let x be a transcendental element over k and let us consider the polynomial $\varphi(T) = T^2 + T + x/h(x) \in k(x)[T]$, where $h(x) = x^2 + x + 1 = (x - \alpha)(x - \alpha - 1) \in k[x]$. Let y be a root of $\varphi(T)$. If we denote by P the rational place of $k(x)$ defined by any of the linear factors of $h(x)$, we have

$$\nu_P\left(x/h(x)\right) = -1 \not\equiv 0 \mod 2, \tag{3.1}$$

so that Eisenstein's criterion ([S, Proposition 3.1.15]) implies that $\varphi(T)$ is the minimal polynomial of y over $k(x)$ and also that P is totally ramified in $k(x, y)/k(x)$. Therefore $k(x, y)/k(x)$ is an Artin-Schreier extension of degree 2 and k is the full field of constants of $k(x, y)$.

The next lemma describes the ramification in the basic function field $k(x, y)$ corresponding to the equation (1.1) (see Figure 1). We will use the following notation: the symbol P_a (resp. R_a) denotes the only zero of $x + a$ (resp. $y + a$) in $k(x)$ (resp. $k(y)$) for $a \in k$, while P_∞ (resp. R_∞) denotes the only pole of x in $k(x)$ (resp. y in $k(y)$). Notice that we can write either $x - a$ or $x + a$ because we are in even characteristic.

Lemma 3.1. *Let $F = k(x, y)$ be the basic function field for the equation* (1.1) *and let $\beta \in \{\alpha, \alpha + 1\}$. Then*

(i) The place P_β of $k(x)$ is totally ramified in F and its different exponent is 2*. Moreover, if $Q \in \mathbb{P}(F)$ lies over P_β then $Q \cap k(y) = R_\infty$.*

(ii) The place P_0 of $k(x)$ splits completely in F. Moreover, if $Q \in \mathbb{P}(F)$ lies over P_0, then $Q \cap k(y)$ is either R_0 or R_1.

(iii) The place P_∞ of $k(x)$ splits completely in F. Moreover, if $Q \in \mathbb{P}(F)$ lies over P_∞ then $Q \cap k(y)$ is either R_0 or R_1.

(iv) The place P_1 of $k(x)$ splits completely in F. Moreover, if $Q \in \mathbb{P}(F)$ lies over P_1 then $Q \cap k(y)$ is either R_α or $R_{\alpha+1}$.

(v) The place R_β of $k(y)$ is totally ramified in F and its different exponent is 2.

(vi) If P is a place of $k(x)$ (resp. $k(y)$) different from P_β (resp. R_β) then P is not ramified in F. Therefore the extensions $F/k(x)$ and $F/k(y)$ are weakly ramified.

Proof. If we write $m_{P_\beta} = -\nu_{P_\beta}(x/h(x))$, then $m_{P_\beta} = 1$ from (3.1) and if Q_i is the place of F lying over P_β then $d(Q_i|P_\beta) = (2-1)(m_{P_\beta}+1) = 2$ by the theory of Artin-Schreier extensions ([S, Proposition 3.7.8]). Since Q_i is a pole (of order 2) of y^2+y in F, then Q_i is also a simple pole of y in F so that $Q_i \cap k(y) = R_\infty$ which completes the proof of (i).

The places P_0 and P_∞ of $k(x)$ are zeros of $x/h(x)$ in $k(x)$ so that the reduction $\varphi(T) \mod P_\gamma$ with $\gamma = 0, \infty$ is the polynomial $T(T+1)$. Also the reduction $\varphi(T)$ mod P_1 is the polynomial T^2+T+1. Then Kummer's Theorem ([S, Theorem 3.3.7]) implies that (ii), (iii) and (iv) hold.

Now we prove (v). Let Q_i be a place of F lying over R_β. Then $\nu_{Q_i}(y^2+y+1) = e(Q_i|R_\beta)$. By writing $S_i = Q_i \cap k(x)$ we see from (iii) that $S_i \neq P_\infty$ and since

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

we have

$$2 \geq e(Q_i|R_\beta) = e(Q_i|S_i)\nu_{S_i}((x+1)^2/h(x)) = 2e(Q_i|S_i)\nu_{S_i}((x+1)/h(x)).$$

This implies that $S_i = P_1$, because $h(x)$ is a polynomial, and also that $e(Q_i|R_\beta) = 2$. Thus we have proved that R_β is totally ramified in F and Q_i lies over P_1 in $k(x)$. In particular $\nu_{Q_i}(x+1) = 1$, i.e. $x+1$ is a prime element for Q_i. We also have that

$$(x+1)^2 + (x+1)\left(\frac{y^2+y+1}{y^2+y}\right) + \frac{y^2+y+1}{y^2+y} = 0,$$

so that

$$\phi(T) = T^2 + \left(\frac{y^2+y+1}{y^2+y}\right)T + \frac{y^2+y+1}{y^2+y} \tag{3.2}$$

is the minimal polynomial of $x+1$ over $k(y)$ because it is irreducible over $k(y)$ by Eisenstein criterion ([S, Proposition 3.1.15]) using the place R_β. From [S, Proposition 3.5.12] we have

$$d(Q_i|R_\beta) = \nu_{Q_i}(\phi'(x+1)) = \nu_{Q_i}\left(\frac{y^2+y+1}{y^2+y}\right) = 2,$$

which finishes the proof of (v).

Finally, we prove (vi). From (iii) and the theory of Artin-Schreier extensions we see that the places P_α and $P_{\alpha+1}$ are the only ones ramified in F. Now consider the polynomial $\phi(T)$ given in (3.2), which is the minimal polynomial of $x+1$ over $k(y)$. We have that $k(x+1,y) = F$ and also for any place P of $k(y)$ different from R_γ for $\gamma = 0,1$, the polynomial $\phi(T)$ is integral over $\mathcal{O}_P$, the valuation ring corresponding to P. Let Q be a place of F lying over $P \neq R_\gamma$ with $\gamma \in \{0,1,\alpha,\alpha+1\}$, then by [S, Theorem 3.5.10], we have

$$d(Q|P) \leq \nu_Q(\varphi'(x+1)) = \nu_Q\left(\frac{y^2+y+1}{y^2+y}\right) = e(Q|R_\gamma)\nu_{R_\gamma}\left(\frac{y^2+y+1}{y^2+y}\right) = 0,$$

so that P is unramified in F. Finally if either $P = R_0$ or R_1 and Q is a place of F lying over P, then $\nu_Q(y^2+y) = e(Q|P)$. Let $S = Q \cap k(x)$, then

$$1 \leq e(Q|P) = e(Q|S)\nu_S(x/h(x)),$$

which implies that S is either P_0 or P_∞. By (ii) and (iii) we have that $e(Q|P) = 1$ and we are done. ☐

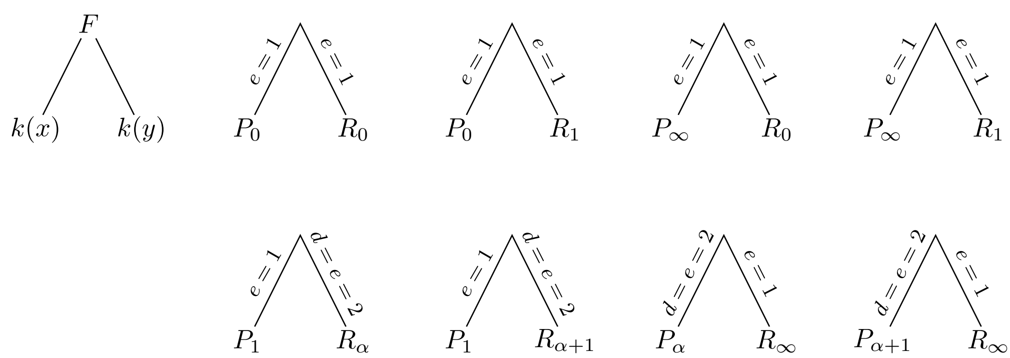

FIGURE 1. Ramification in $F/k(x)$ and $F/k(y)$

Now we prove a key identity for the study of the ramification of certain places in the sequence $\mathcal{H}$ over k.

Lemma 3.2. *Let us consider the equation $y^2 + y = f(x)$ in $k(x, y)$ where $f(x)$ denotes the right hand side of* (1.1)*. Then*

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

Proof.

$$\begin{aligned} f(y) + \left(\frac{y+1}{x+1}\right)^2 + \frac{y+1}{x+1} &= \frac{y}{y^2+y+1} + \left(\frac{y+1}{x+1}\right)^2 + \frac{y+1}{x+1} \\ &= \frac{y}{f(x)+1} + \left(\frac{y+1}{x+1}\right)^2 + \frac{y+1}{x+1} \\ &= y\frac{x^2+x+1}{(x+1)^2} + \left(\frac{y+1}{x+1}\right)^2 + \frac{y}{x+1} + \frac{1}{x+1} \\ &= \frac{y(x^2+1) + yx + y^2 + 1 + y(x+1)}{(x+1)^2} + \frac{1}{x+1} \\ &= \frac{y(x+1)^2}{(x+1)^2} + \frac{yx + y^2 + 1 + y(x+1)}{(x+1)^2} + \frac{1}{x+1} \\ &= y + \frac{1}{x^2+x+1} + \frac{1}{x+1}. \end{aligned}$$

□

Proposition 3.3. *The sequence of function fields $\mathcal{H} = \{F_i\}_{i=0}^{\infty}$ defined by equation* (1.1) *is a tower over k.*

Proof. Let $f(x)$ be the right hand side of (1.1) and let Q_0^i (resp. Q_1^i) be a zero of x_i (resp. $x_i + 1$) in F_i. Let Q_β^i be a zero of $x_i + \beta$ where $\beta \in \{\alpha, \alpha+1\}$. We already know, as established after (3.1), that F_1/F_0 is an extension of degree 2 with k as the full field of constants of F_1 and that Q_β^0 is totally ramified in F_1/F_0.

Now consider the place Q_0^0. Since $T(T+1)$ is the reduction modulo Q_0^0 of $T^2 + T + f(x_0)$, from Kummer's Theorem the place Q_0^0 splits completely in F_1/F_0 into the places Q_0^1 and Q_1^1. On the other hand $T^2 + T + 1$ is the reduction modulo Q_1^0 of $T^2 + T + f(x_0)$. By Kummer's Theorem we have that Q_1^0 splits completely in F_1/F_0 into the places Q_α^1 and $Q_{\alpha+1}^1$. Therefore

$$\nu_{Q_\beta^1}(x_0 + 1) = \nu_{Q_1^0}(x_0 + 1) = 1.$$

By writing $u = \frac{x_1+1}{x_0+1}$, we have from Lemma 3.2 that

$$f(x_1) + u^2 + u = x_1 + \frac{1}{x_0^2 + x_0 + 1} + \frac{1}{x_0 + 1},$$

and since $\nu_{Q^1_\beta}(x_1) = 0$, we readily see that $\nu_{Q^1_\beta}(f(x_1) + u^2 + u) = -1 \not\equiv 0 \mod 2$. The same argument used in the proof of [S, Proposition 3.7.8] shows that Q^1_β is totally ramified in F_2/F_1. Therefore k is the full field of constants of F_2 and F_2/F_1 is an extension of degree 2. From Kummer's Theorem we see now that Q^1_1 splits completely in F_2/F_1 into the places Q^2_α and $Q^2_{\alpha+1}$ because T^2+T+1 is the reduction modulo Q^1_1 of $T^2 + T + f(x_1)$. Since $x_1^2 + x_1 = f(x_0)$ we have that $\nu_{Q^1_1}(x_1 + 1) = 1$ so that $\nu_{Q^2_\beta}(x_1 + 1) = 1$.

Now suppose that F_i/F_{i-1} is a extension of degree 2 such that k is the full field of constants of F_i, the place Q^{i-1}_1 splits completely in F_i/F_{i-1} into the places Q^i_α and $Q^i_{\alpha+1}$ and $\nu_{Q^{i-1}_1}(x_{i-1} + 1) = 1$. Then $\nu_{Q^i_\beta}(x_{i-1} + 1) = 1$ and since $\nu_{Q^i_\beta}(x_i) = 0$, by writing $u = \frac{x_i+1}{x_{i-1}+1}$, we have from Lemma 3.2 that

$$f(x_i) + u^2 + u = x_i + \frac{1}{x^2_{i-1} + x_{i-1} + 1} + \frac{1}{x_{i-1} + 1},$$

and so $\nu_{Q^i_\beta}(f(x_i) + u^2 + u) = -1 \not\equiv 0 \mod 2$. As above this condition implies that Q^i_β is totally ramified in F_{i+1}/F_i. Therefore k is the full field of constants of F_{i+1} and F_{i+1}/F_i is an extension of degree 2. From Kummer's Theorem we see that the place Q^i_1 splits completely in F_{i+1}/F_i into the places Q^{i+1}_α and $Q^{i+1}_{\alpha+1}$ because $T^2 + T + 1$ is the reduction modulo Q^i_1 of $T^2 + T + f(x_i)$. Since $x_i^2 + x_i = f(x_{i-1})$ we have that $\nu_{Q^i_1}(x_i + 1) = 1$ so that $\nu_{Q^{i+1}_\beta}(x_i + 1) = 1$.

We have proved that each extension F_i/F_{i-1} is an extension of degree 2 and that k is the full field of constants of each F_i. It remains to prove that $g(F_i) \to \infty$ as $i \to \infty$ and for this it suffices to check that $g(F_i) > 1$ for some $i \geq 0$. From Lemma 3.1 and Proposition 2.5 we have that F_1/F_0 is a weakly ramified Artin-Schreier extension of degree 2 and just the places Q^0_α and $Q^0_{\alpha+1}$ ramify in F_1 and they are totally ramified. It follows from [S, Proposition 3.7.8] that $g(F_1) = 1$. Again, from Lemma 3.1 and Proposition 2.5, we have that F_2/F_1 is a weakly ramified Artin-Schreier extension of degree 2 and we have proved above that the places Q^1_α and $Q^1_{\alpha+1}$ lying above Q^0_1 are totally ramified in F_2/F_1. From Hurwitz's genus formula [S, Theorem 3.4.13] we conclude that $g(F_2) \geq 3$ and we are done. □

As a direct consequence of the previous results we have:

Proposition 3.4. *The sequence of function fields $\mathcal{H}$ defined by equation* (1.1) *is a tower over k with finite ramification locus $R(\mathcal{H})$. More precisely*

$$R(\mathcal{H}) \subseteq \{P_0, P_1, P_\alpha, P_{\alpha+1}, P_\infty\},$$

with the notation used in Lemma 3.1.

Remark 3.5. *We will prove in the next section (see Remark 4.12) that, in fact, equality holds in Proposition 3.4, i.e.*

$$R(\mathcal{H}) = \{P_0,\, P_1,\, P_\alpha,\, P_{\alpha+1},\, P_\infty\},$$

and also that every place Q in the tower $\mathcal{H}$ lying over a place of $R(\mathcal{H})$ is rational.

Now we can state and prove the main result of this section.

Theorem 3.6. *The tower $\mathcal{H} = \{F_i\}_{i=0}^{\infty}$ is a weakly ramified tower over k and its genus $\gamma(\mathcal{H})$ satisfies the estimate*

$$\gamma(\mathcal{H}) \le 2.$$

Proof. For any set S of places of F_0 let $O_i(S)$ be the set of all places of F_i lying over the places of S. From Lemma 3.1 and Corollary 2.6 we have that $\mathcal{H}$ is a weakly ramified tower over k. Thus Hurwitz's genus formula, Proposition 3.4 and Remark 3.5 give

$$\begin{aligned} 2g(F_i) - 2 &= -2[F_i : F_0] + 2 \sum_{P \in R(\mathcal{H})} \sum_{Q|P} (e(Q|P) - 1) \\ &= -2[F_i : F_0] + 2 \sum_{P \in R(\mathcal{H})} \sum_{Q|P} e(Q|P) - 2|O_i(R(\mathcal{H}))| \\ &= 2[F_i : F_0](|R(\mathcal{H})| - 1) - 2|O_i(R(\mathcal{H}))| \\ &= 8[F_i : F_0] - 2|O_i(R(\mathcal{H}))|. \end{aligned}$$

As a consequence of Theorem 4.11 to be proved later we have the estimate

$$|O_i(R(\mathcal{H}))| \ge 2[F_i : F_0].$$

Therefore

$$\gamma(\mathcal{H}) = \lim_{i\to\infty} \frac{g(F_i) - 1}{[F_i : F_0]} \le 2,$$

as claimed. □

4. The splitting rate of the tower $\mathcal{H}$ over $\mathbb{F}_4$

Throughout this section the symbol Tr denotes the trace map from $\mathbb{F}_4$ to $\mathbb{F}_2$ and recall that $\mathbb{F}_4 := \{0, 1, \alpha, \alpha + 1\}$ where $\alpha^2 + \alpha + 1 = 0$. We will show next that the ramification behavior in the tower $\mathcal{H} = \{F_i\}_{i=0}^{\infty}$ over $\mathbb{F}_4$ of the zeros of x_i and $x_i + 1$ and the poles of x_i in F_i is well understood. However the understanding of the ramification behavior of the zeros of $x_i + \alpha$ and $x_i + \alpha + 1$ in F_i in the tower $\mathcal{H}$ will be achieved in Theorem 4.10 after the proof of some technical results.

Proposition 4.1. *Let F be a function field over $\mathbb{F}_4$ such that $\mathbb{F}_4$ is its full field of constants and let $x \in F \setminus \mathbb{F}_4$ such that $f(x) \neq u^2 + u$ for all $u \in F$ where $f(x)$ is the right hand side of* (1.1)*. Let $F' = F(y)$ where y satisfies* (1.1)*, i.e. $y^2 + y = f(x)$. Then F'/F is an Artin-Schreier extension of degree 2 where any zero P_0 and any pole P_∞ of x in F respectively, split completely in F'/F into a zero Q_0 of y and a zero Q_1 of $y + 1$. Also any zero P_1 of $x + 1$ in F splits completely in F'/F into a zero Q_α of $y+\alpha$ and a zero $Q_{\alpha+1}$ of $y+\alpha+1$ in F' (see Figure 2 below). Moreover*

$$\nu_{Q_i}(y + i) = \nu_{P_0}(x) \qquad \text{and} \qquad \nu_{Q_i}(y + i) = -\nu_{P_\infty}(x),$$

where $i = 0, 1$ and

$$\nu_{Q_\beta}(y + \beta) = 2\nu_{P_1}(x + 1),$$

where $\beta = \alpha$ or $\beta = \alpha + 1$.

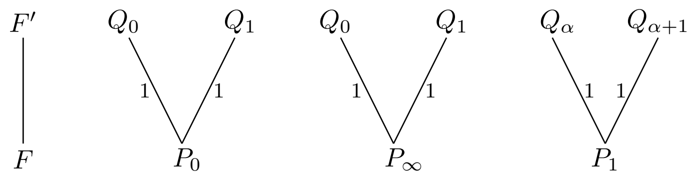

FIGURE 2. Decomposition of some zeros and poles in F'/F

Proof. The first assertion follows from [S, Proposition 3.7.8]. Now consider the polynomial

$$\varphi(T) = T^2 + T + f(x) \in F[T].$$

First notice that each zero or pole P of x in F is a zero of $f(x)$ in F. Then

$$\varphi(T) \mod P = T^2 + T = T(T + 1),$$

so that Kummer's Theorem implies that the first two diagrams of Figure 2 are correct, i.e. there is a zero Q_0 of y in F' and a zero Q_1 of $y + 1$ in F' lying over P. Therefore

$$\nu_{Q_i}(y + i) = \nu_{P_0}(x) \qquad \text{and} \qquad \nu_{Q_i}(y + i) = -\nu_{P_\infty}(x).$$

Let P_1 be a zero of $x+1$ in F. Then $\nu_{P_1}(x+1) > 0$ and $\nu_{P_1}(x) = 0$ so that $\nu_{P_1}(f(x)) = 0$ and the residual class $x(P_1) = 1$. Thus

$$\varphi(T) \mod P_1 = T^2 + T + 1 = (T+\alpha)(T+\alpha+1),$$

and again Kummer's Theorem shows that the last diagram is correct. Now, by rewriting (1.1) as

$$y^2 + y + 1 = \frac{(x+1)^2}{x^2+x+1}, \tag{4.1}$$

we see that if $Q_\beta | P_1$ then $\nu_{Q_\beta}(y+\beta) = 2\nu_{P_1}(x+1)$ as desired. □

Proposition 4.2. *Under the conditions of Proposition 4.1, let us consider a zero P_β of $x+\beta$ in F.*

(i) Suppose that there exists an element $u \in F$ such that

$$\nu_{P_\beta}(f(x) + u^2 + u) = -1,$$

then P_β is totally ramified in F'/F. The only place of F' lying over P_β is a pole Q_∞ of y in F' and

$$\nu_{Q_\infty}(y) = -\nu_{P_\beta}(x+\beta).$$

(ii) Suppose that P_β is rational and that there exists an element $u \in F$ such that

$$\nu_{P_\beta}(f(x) + u^2 + u) \geq 0 \quad \text{and} \quad \mathrm{Tr}((f(x) + u^2 + u)(P_\beta)) = 0.$$

Then P_β splits completely in F'/F into two poles of y in F' and

$$2\nu_{Q_\infty}(y) = -\nu_{P_\beta}(x+\beta)$$

where Q_∞ denotes any of these two poles (see Figure 3 below).

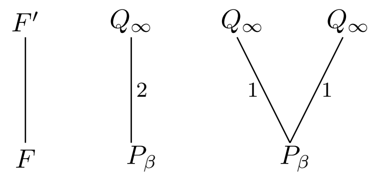

FIGURE 3. The two possible decompositions of P_β

Proof. The first part of (i) is just [S, Proposition 3.7.8]. It is clear from the equation (1.1) defining the extension F'/F that $\nu_{Q_\infty}(y) = -\nu_{P_\beta}(x+\beta)$.

Let us see (ii). From [S, Proposition 3.7.8] and its proof, we have that P_β is unramified in F' and also $F' = F(y+u)$ where

$$\varphi(T) = T^2 + T + f(x) + u^2 + u,$$

is the minimal polynomial of $y+u$ over F. Then the reduction of $\varphi(T)$ modulo P_β splits into linear factors over $\mathbb{F}_4$ because $\mathrm{Tr}((f(x)+u^2+u)(P_\beta)) = 0$ and thus we can conclude, by Kummer's Theorem, that P_β splits completely in F'/F. From equation (1.1) we see at once that $2\nu_{Q_\infty}(y) = -\nu_{P_\beta}(x+\beta)$. □

The construction of elements satisfying (i) or (ii) in the above proposition will be a crucial technical point in our proof of the existence of rational places which split completely in the tower $\mathcal{H}$ over $\mathbb{F}_4$. At this point it is convenient to introduce the following definition:

Definition 4.3. *Let F'/F be an Artin-Schreier extension defined by* (1.1) *as in Proposition 4.1 and let $f(x)$ be the right hand side of* (1.1). *Let P be a place of F. An element $u \in F$ is called an Artin-Schreier element of type 1 for P if*

$$\nu_P(f(x) + u^2 + u) = -m,$$

for some odd positive integer m. Suppose now that P is rational. An element $u \in F$ is called an Artin-Schreier element of type 2 for P if

$$\nu_P(f(x) + u^2 + u) \geq 0 \quad \textit{and} \quad \mathrm{Tr}((f(x) + u^2 + u)(P)) = 0.$$

Remark 4.4. *The arguments given in Proposition 4.2 show that a place P of F is totally ramified in F'/F if there is an Artin-Schreier element of type 1 for P. Furthermore if P is rational then P splits completely in F'/F if there is an Artin-Schreier element of type 2 for P.*

From now on we will use the following notation: let $i \geq 0$. A zero of x_i (resp. $x_i + 1$) in F_i will be denoted as Q_0^i (resp. Q_1^i) and a pole of x_i in F_i will be denoted as Q_∞^i. A zero of $x_i + \beta$ in F_i will be denoted as Q_β^i for $\beta \in \{\alpha, \alpha+1\}$ and this will be the meaning of any symbol of the form Q_γ^i when a Greek letter such as γ is used as a subindex. Also from now on all the considered places lie over Q_1^0 (the only zero of $x_0 + 1$ in the rational function field F_0 of $\mathcal{H}$). We will write in many occasions $P \subset Q$ when a place Q lies over a place P.

We state and prove now some technical results (Lemmas 4.5, 4.6 and 4.7). In all of them we will assume that the following condition holds:

Ramification condition. *Let $k \geq 0$ and consider the function fields $F_k \subset F_{k+1} \subset F_{k+2}$ of the tower $\mathcal{H}$. For the places $Q_1^k \subset Q_\beta^{k+1}$ one and only one of the following conditions hold:*

(R1) either $\nu_{Q_1^k}(x_k+1) = 1$ and Q_β^{k+1} is totally ramified in F_{k+2}/F_{k+1} (so that there is only one pole Q_∞^{k+2} of x_{k+2} in F_{k+2} lying over Q_β^{k+1}), or

(R2) $\nu_{Q_1^k}(x_k+1) = 2$ and Q_β^{k+1} splits completely in F_{k+2}/F_{k+1} (so that there are exactly two poles Q_∞^{k+2} of x_{k+2} in F_{k+2} lying over Q_β^{k+1}).

If (R1) (resp. (R2)) holds, we will say that the sequence $Q_1^k \subset Q_\beta^{k+1} \subset Q_\infty^{k+2}$ satisfies the ramification condition (R1) (resp. (R2)).

Lemma 4.5. *For $k \geq 0$ and $i \geq k+4$ let us consider the subsequence $\{F_j\}_{j=k}^{i-1}$ of the tower $\mathcal{H}$ an also the following sequence of places:*

$$Q_1^k \subset Q_\beta^{k+1} \subset Q_\infty^{k+2} \subset Q_0^{k+3} \subset Q_0^{k+4} \subset \cdots \subset Q_0^{i-1},$$

where we are having only the places Q_0^j for $k+3 \leq j \leq i-1$. Then $e(Q_0^{i-1}|Q_\infty^{k+2}) = 1$ and if we write

$$\delta = x_{k+2} + \frac{x_{k+1}+1}{x_k+1},$$

then

$$(x_{k+2} + (x_{k+1}\delta)^2 + x_{k+1}\delta)(Q_\infty^{k+2}) = \beta \qquad \textit{and} \qquad \nu_{Q_0^{i-1}}(\delta) = \nu_{Q_\infty^{k+2}}(\delta) = -1,$$

for $i \geq k+4$.

Proof. Any of the ramification conditions (R1) or (R2) together with Proposition 4.1 imply that $e(Q_0^{i-1}|Q_\infty^{k+2}) = 1$. Now we prove that $\nu_{Q_0^{i-1}}(\delta) = -1$. Since $x_{k+2}^2 + x_{k+2} = f(x_{k+1})$, by Lemma 3.2 we have that

$$\delta^2 + \delta = x_{k+1} + \frac{1}{x_k^2 + x_k + 1} + \frac{1}{x_k+1}.$$

Notice also that from any of the ramification conditions we have

$$\nu_{Q_\infty^{k+2}}(x_k+1) = e(Q_\infty^{k+2}|Q_\beta^{k+1})\nu_{Q_1^k}(x_k+1) = 2. \tag{4.2}$$

On the other hand, we know that $\nu_{Q_1^k}(x_k^2+x_k+1) = 0$ and $\nu_{Q_\beta^{k+1}}(x_{k+1}) = 0$, thus

$$\nu_{Q_\infty^{k+2}}(x_{k+1}) = \nu_{Q_\infty^{k+2}}\left(\frac{1}{x_k^2+x_k+1}\right) = 0 \tag{4.3}$$

and

$$\nu_{Q_\infty^{k+2}}(\delta^2+\delta) = \nu_{Q_\infty^{k+2}}\left(x_{k+1} + \frac{1}{x_k^2+x_k+1} + \frac{1}{x_k+1}\right) = -2,$$

therefore $\nu_{Q_0^{i-1}}(\delta) = \nu_{Q_\infty^{k+2}}(\delta) = -1$ because $Q_0^{i-1}|Q_\infty^{k+2}$ is not ramified in F_{i-1}/F_{k+2}. In order to prove that

$$(x_{k+2} + (x_{k+1}\delta)^2 + x_{k+1}\delta)(Q_\infty^{k+2}) = \beta$$

we will use an identity which is a consequence of some tedious manipulations, so for the sake of simplicity we will write $x = x_k$, $y = x_{k+1}$ and $z = x_{k+2}$. We have now that $\delta = z + \frac{y+1}{x+1}$ and x, y, z satisfy the following equations:

$$z^2 = z + f(y),$$

$$y^2 f(y) = 1 + y + \frac{1}{y^2+y+1},$$

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

Then, from the above three equalities and (4.1), we have

$$\begin{aligned} z + (y\delta)^2 + y\delta &= z + (z+f(y))y^2 + zy + \frac{y^2(y+1)^2}{(x+1)^2} + \frac{y(y+1)}{(x+1)} \\ &= z(y^2+y+1) + 1 + y + \frac{1}{y^2+y+1} + \frac{y^2(y+1)^2}{(x+1)^2} + \frac{y(y+1)}{(x+1)} \\ &= z(y^2+y+1) + 1 + y + \frac{(y^2+y+1)^2}{(x+1)^2} + \frac{y^2+y+1}{(x+1)} + 1 \\ &= z\frac{(x+1)^2}{x^2+x+1} + y + \frac{(x+1)^2}{(x^2+x+1)^2} + \frac{x+1}{x^2+x+1}. \end{aligned}$$

Therefore

$$\begin{aligned} x_{k+2} + (x_{k+1}\delta)^2 + x_{k+1}\delta = x_{k+2}\frac{(x_k+1)^2}{x_k^2+x_k+1} + x_{k+1} + \frac{(x_k+1)^2}{(x_k^2+x_k+1)^2} + \\ + \frac{x_k+1}{x_k^2+x_k+1}. \end{aligned}$$

We have that $\nu_{Q_\infty^{k+2}}(x_k+1) = 2$ and $\nu_{Q_\infty^{k+2}}(x_{k+1}) = \nu_{Q_\infty^{k+2}}\left(\frac{1}{x_k^2+x_k+1}\right) = 0$ by (4.2) and (4.3), respectively. This implies that $\nu_{Q_\infty^{k+2}}(x_{k+2}) = -2$ because

$$x_{k+2}^2 + x_{k+2} = x_{k+1}\frac{x_k^2+x_k+1}{(x_k+1)^2}.$$

We conclude now that

$$\nu_{Q_\infty^{k+2}}(x_{k+2} + (x_{k+1}\delta)^2 + x_{k+1}\delta) = 0, \tag{4.4}$$

and

$$(x_{k+2} + (x_{k+1}\delta)^2 + x_{k+1}\delta)(Q_\infty^{k+2}) = x_{k+1}(Q_\infty^{k+2}) = x_{k+1}(Q_\beta^{k+1}) = \beta.$$

□

Lemma 4.6. *With the same hypothesis as in Lemma 4.5 we have that for all* $j = k+3, \dots, i-1$

$$\nu_{Q_0^j}\left(\frac{1}{x_j} + x_{k+2}\right) > 0.$$

Proof. For all j we have

$$x_j^2 + x_j = f(x_{j-1}) \qquad \text{and} \qquad \frac{1}{f(x_{j-1})} = \frac{1}{x_{j-1}} + 1 + x_{j-1}$$

then

$$\begin{aligned}\frac{1}{x_j} + x_{k+2} &= \frac{x_j+1}{x_j^2+x_j} + x_{k+2} = \frac{x_j+1}{f(x_{j-1})} + x_{k+2} \\ &= \frac{x_j}{x_{j-1}} + x_j + x_jx_{j-1} + 1 + x_{j-1} + \frac{1}{x_{j-1}} + x_{k+2}.\end{aligned}$$

On the other hand, in the previous proof we showed that Q_∞^{k+2} is a pole of order two of x_{k+2} and $e(Q_0^j|Q_\infty^{k+2}) = 1$, thus by Proposition 4.1 we have

$$\nu_{Q_0^j}(x_j) = \cdots = \nu_{Q_0^{k+3}}(x_{k+3}) = -\nu_{Q_\infty^{k+2}}(x_{k+2}) = 2. \tag{4.5}$$

Now we proceed by induction on j. If $j = k+3$ we have

$$\frac{1}{x_{k+3}} + x_{k+2} = \frac{x_{k+3}}{x_{k+2}} + x_{k+3} + x_{k+3}x_{k+2} + 1 + \frac{1}{x_{k+2}}$$

and $\nu_{Q_0^{k+3}}(x_{k+3}/x_{k+2}) > 0$ by (4.5). Moreover, $\nu_{Q_0^{k+3}}(x_{k+3}x_{k+2}+1) > 0$ because the residual class

$$(x_{k+3}x_{k+2})(Q_0^{k+3}) = ((x_{k+3}+1)(x_{k+3}x_{k+2}))(Q_0^{k+3}) = (x_{k+2}f(x_{k+2}))(Q_\infty^{k+2}) = 1.$$

Thus

$$\nu_{Q_0^{k+3}}\left(\frac{1}{x_{k+3}} + x_{k+2}\right) > 0.$$

Now assume that the result is valid for $j-1 \geq k+3$. From the equation

$$\frac{(x_j+1)x_j}{x_{j-1}} = \frac{1}{x_{j-1}^2 + x_{j-1} + 1}, \tag{4.6}$$

we have the residual class $(\frac{x_j}{x_{j-1}})(Q_0^j) = (\frac{(x_j+1)x_j}{x_{j-1}})(Q_0^j) = 1$ which implies that $\nu_{Q_0^j}(\frac{x_j}{x_{j-1}}+1) > 0$. Furthermore, by inductive hypothesis, the term $1/x_{j-1}+x_{k+2}$ has positive valuation and also the remaining terms of the right hand side of

$$\frac{1}{x_j} + x_{k+2} = \frac{x_j}{x_{j-1}} + 1 + x_j + x_j x_{j-1} + x_{j-1} + \frac{1}{x_{j-1}} + x_{k+2},$$

with respect to Q_0^j. Therefore

$$\nu_{Q_0^j}\left(\frac{1}{x_j} + x_{k+2}\right) > 0.$$

□

Lemma 4.7. *For $k \geq 0$ and $i \geq k+3$ let us consider the subsequence $\{F_j\}_{j=k}^{i+2}$ of the tower $\mathcal{H}$ and the sequence of places*

$$Q_1^k \subset Q_\beta^{k+1} \subset Q_\infty^{k+2} \subset Q_1^{k+3} \subset Q_\theta^{k+4} \subset Q_\infty^{k+5},$$

if $i = k+3$ or the sequence

$$Q_1^k \subset Q_\beta^{k+1} \subset Q_\infty^{k+2} \subset Q_0^{k+3} \subset \cdots \subset Q_0^{i-1} \subset Q_1^i \subset Q_\theta^{i+1} \subset Q_\infty^{i+2},$$

if $i > k+3$, where we are having only the places Q_0^j for $k+3 \leq j \leq i-1$. Then Q_θ^{i+1} splits completely in F_{i+2}/F_{i+1} and the ramification condition (R2) holds for

$$Q_1^i \subset Q_\theta^{i+1} \subset Q_\infty^{i+2}.$$

Proof. In order to prove that Q_θ^{i+1} splits completely in F_{i+2}/F_{i+1} it suffices to find an Artin-Schreier element of type 2 for Q_θ^{i+1}. Let

$$u := \frac{x_{i+1}+1}{x_i+1} + x_{k+1}\delta,$$

where δ is as in Lemma 4.5. From Lemma 3.2 we have

$$\begin{aligned} f(x_{i+1}) + u^2 + u &= x_{i+1} + \frac{1}{x_i^2+x_i+1} + \frac{1}{x_i+1} + (\delta x_{k+1})^2 + \delta x_{k+1} \\ &= x_{i+1} + \frac{1}{x_i^2+x_i+1} + x_i\left(x_{i-1}+1+\frac{1}{x_{i-1}}\right) + (\delta x_{k+1})^2 + \delta x_{k+1} \\ &= x_{i+1} + \frac{1}{x_i^2+x_i+1} + x_i(x_{i-1}+1) + \frac{x_i+1}{x_{i-1}} + \left(\frac{1}{x_{i-1}} + x_{k+2}\right) \\ &\quad + (x_{k+2} + (\delta x_{k+1})^2 + \delta x_{k+1}). \end{aligned}$$

Now we compute the residual class $(f(x_{i+1}) + u^2 + u)(Q_\theta^{i+1})$. It is clear that

$$\left(x_{i+1} + \frac{1}{x_i^2+x_i+1} + x_i(x_{i-1}+1)\right)(Q_\theta^{i+1}) = \theta + 1 + 1 = \theta.$$

For $i > k+3$ we have from (4.5) that Q_0^{i-1} is a zero of order 2 of x_{i-1} and by Proposition 4.1 and equation (1.1) we also have that Q_1^i is a zero of order 2 of x_i+1. The same holds for $i = k+3$, i.e. Q_∞^{k+2} is a zero of order 2 of x_{k+2} and Q_1^{k+3} is a zero of order 2 of $x_{k+3}+1$. Then for $i \geq k+3$ we have that $\nu_{Q_1^i}\left(\frac{x_i+1}{x_{i-1}}\right) = 0$ and so $\frac{x_i+1}{x_{i-1}}(Q_1^i) = 1$. Finally, Lemma 4.6 and Lemma 4.5 imply that

$$\left(\frac{1}{x_{i-1}} + x_{k+2}\right)(Q_\theta^{i+1}) + (x_{k+2} + (\delta x_{k+1})^2 + \delta x_{k+1})(Q_\theta^{i+1}) = \beta,$$

therefore

$$(f(x_{i+1}) + u^2 + u)(Q_\theta^{i+1}) = \theta + 1 + \beta.$$

Since $\theta + 1 + \beta$ is equal to 0 or 1, then

$$\nu_{Q_\theta^{i+1}}(f(x_{i+1}) + u^2 + u) \geq 0 \quad \text{and} \quad \mathrm{Tr}\left((f(x_{i+1}) + u^2 + u)(Q_\theta^{i+1})\right) = 0,$$

so that u is an Artin-Schreier element of type 2 for Q_θ^{i+1}. In particular, the sequence $Q_1^i \subset Q_\theta^{i+1} \subset Q_\infty^{i+2}$ satisfies the ramification condition (R2). □

From Proposition 4.1 we know that the places between Q_∞^{k+2} and Q_1^i for $i > k+2$ are given by a combination of sequences of places of the form

$$Q_1^j \subset Q_\gamma^{j+1} \subset Q_\infty^{j+2} \quad \text{or} \quad Q_0^j \subset \cdots \subset Q_0^{j+l-1} \subset Q_1^{j+l} \subset Q_\eta^{j+l+1} \subset Q_\infty^{j+l+2}.$$

By using Proposition 4.1 and Lemma 4.7 as many times as needed we have

Corollary 4.8. *Suppose that the place Q_1^k is rational. If in the tower $\mathcal{H}$ we have the sequence of places $Q_1^k \subset Q_\beta^{k+1} \subset Q_\infty^{k+2}$ satisfying the ramification condition (R2) and a sequence of places of the form $Q_1^i \subset Q_\theta^{i+1} \subset Q_\infty^{i+2}$ with Q_1^i lying over Q_∞^{k+2} for $i > k+2$, then this sequence also satisfies the ramification condition (R2) and Q_1^k splits completely in F_{i+3}/F_k. In particular the place Q_1^i is rational.*

Proposition 4.9. *Consider the subsequence $\{F_j\}_{j=k}^{k+2}$ of the tower $\mathcal{H}$ and the sequence of places*

$$Q_1^k \subset Q_\beta^{k+1} \subset Q_\infty^{k+2}.$$

If Q_1^k is a simple zero of $x_k + 1$ then $e(Q_\infty^{k+2}|Q_\beta^{k+1}) = 2$, i.e. the above sequence of places satisfies the ramification condition (R1).

Proof. Let $u = \frac{x_{k+1}+1}{x_k+1}$ and let $\delta = x_{k+2} + u$. By Lemma 3.2 we have

$$\delta^2 + \delta = f(x_{k+1}) + u^2 + u = x_{k+1} + \frac{1}{x_k^2 + x_k + 1} + \frac{1}{x_k + 1}.$$

Since Q_1^k is a simple zero of x_k+1 and $e(Q_\beta^{k+1}|Q_1^k)=1$ from Proposition 4.1, we see that Q_β^{k+1} is also a simple zero of x_k+1. Then, by writing $e=e(Q_\infty^{k+2}|Q_\beta^{k+1})$, we have

$$\nu_{Q_\infty^{k+2}}(\delta^2+\delta)=e\,\nu_{Q_\beta^{k+1}}\left(x_{k+1}+\frac{1}{x_k^2+x_k+1}+\frac{1}{x_k+1}\right)=-e,$$

so that $2\nu_{Q_\infty^{k+2}}(\delta)=-e$. Therefore $e=2$ as desired. □

We are finally in a position to state and prove the main results of this work.

Theorem 4.10. *Let $\{F_j\}_{j=k}^{k+2}$ be a subsequence of the tower $\mathcal{H}$ and consider the sequence of places*

$$Q_1^k\subset Q_\beta^{k+1}\subset Q_\infty^{k+2}.$$

Suppose that Q_1^k is a rational place and a simple zero of x_k+1. Then Q_∞^{k+2} splits completely in $\mathcal{H}$.

Proof. From Proposition 4.1 we see that the sequence of places in the tower $\mathcal{H}$ lying above Q_∞^{k+2} is a combination of the following two types of sequences of places (S1) and (S2) respectively:

$$Q_1^j\subset Q_\theta^{j+1}\subset Q_\infty^{j+2},$$

and

$$Q_0^j\subset\cdots\subset Q_0^{j+l-1}\subset Q_1^{j+l}\subset Q_\gamma^{j+l+1}\subset Q_\infty^{j+l+2},$$

for $j\geq k+3$ and $l\geq 4$. From Proposition 4.9 we have that Q_∞^{k+2} is a rational place so that from Proposition 4.1 we see that the place Q_1^{k+3} (resp. Q_1^{k+3+l}) is rational in the case (S1) (resp. (S2)) for $j=k+3$. Then Lemma 4.7 implies that the sequence of type (S1) satisfies the ramification condition (R2) for $j=k+3$ and so does the sequence $Q_1^{j+l}\subset Q_\gamma^{j+l+1}\subset Q_\infty^{j+l+2}$ in the sequence of type (S2) for $j=k+3$ and $l\geq 4$. In the first case Q_∞^{k+2} splits completely in F_{k+5} while in the second one Q_∞^{k+2} splits completely in F_{k+5+l} for $l\geq 4$. Now the conclusion follows immediately from Corollary 4.8. □

Now we compute the exact number of rational places of each $F_l\in\mathcal{H}$ for $l\geq 3$.

Theorem 4.11. *Let $l\geq 3$. The number $N(F_l)$ of rational places of the function field $F_l\in\mathcal{H}$ is*

$$N(F_l)=2^{l+1}+8.$$

Proof. Since Q_1^0 is rational and a simple zero of $x_0+1 \in F_0$, we have two sequences

$$Q_1^0 \subset Q_\alpha^1 \subset Q_\infty^2 \qquad \text{and} \qquad Q_1^0 \subset Q_{\alpha+1}^1 \subset Q_\infty^2,$$

by Proposition 4.1. Moreover each Q_∞^2 splits completely in F_l/F_2 by Theorem 4.11, so we have $2 \cdot 2^{l-2}$ rational places in F_l lying over Q_0^1.

Now we consider the rational place Q_0^0 which is a simple zero of $x_0 \in F_0$. By Proposition 4.1 Q_0^0 splits completely into the places Q_1^1, a simple zero of x_1+1, and Q_0^1, a simple zero of x_1. Thus we have two sequences $Q_0^0 \subset Q_1^1$ and $Q_0^0 \subset Q_0^1$. In the first case we have the sequences

$$Q_1^1 \subset Q_\alpha^2 \subset Q_\infty^3 \qquad \text{and} \qquad Q_1^1 \subset Q_{\alpha+1}^2 \subset Q_\infty^3,$$

and we are in the above same situation because Q_1^1 is rational and a simple zero of $x_1+1 \in F_1$. The same argument we used above shows that we have 2^{l-2} rational places of F_l lying over Q_1^1. Now for $1 \le i \le l-2$ we have the following sequences of places lying over Q_0^0

$$Q_0^0 \subset Q_0^1 \subset \cdots \subset Q_0^{i-1} \subset Q_1^i, \quad \text{and} \quad Q_0^0 \subset Q_0^1 \subset \cdots \subset Q_0^{l-3} \subset Q_0^{l-2}.$$

Each of the first $l-2$ sequences add 2^{l-i-1} rational places to F_l and for the latter we conclude from Proposition 4.1 that there are four additional rational places Q_α^l, $Q_{\alpha+1}^l$, Q_∞^l and Q_∞^l lying over Q_0^{l-2}. Therefore the number of rational places of F_l lying over Q_0^0 is

$$2^{l-2} + 2^{l-3} + \cdots + 2 + 4 = 2^{l-1} + 2.$$

Let us consider now the rational place Q_∞^0, which is a simple pole of x_0. From Proposition 4.1 we see that the rational places of F_l lying above the rational place Q_∞^0 exhibit the same behavior we already saw for Q_0^0. Thus the number of rational places of F_l lying over Q_∞^0 is also $2^{l-1}+2$.

Finally we consider the number of rational places of F_l lying over Q_β^0 with $\beta \in \{\alpha, \alpha+1\}$. Since Q_β^0 is a simple pole of $x_0+\beta$, from Proposition 4.2 (i) with $u=0$, we have that Q_β^0 is totally ramified in F_1/F_0 and the place Q_∞^1 of F_1 over Q_β^0 is a simple pole of x_1. We see that we are in the situation considered for the place Q_∞^0 but starting from F_1. Therefore the number of rational places of F_l lying over Q_β^0 is $2^{l-2}+2$. Putting all together we have that the number $N(F_l)$ of rational places of F_l is exactly

$$N(F_l) = 2^{l-1} + 2 \cdot (2^{l-1}+2) + 2 \cdot (2^{l-2}+2) = 2^{l+1} + 8.$$

□

Remark 4.12. *We see from Proposition 4.9 and the arguments used in the above proof that every rational place of the base step F_0 in the tower $\mathcal{H}$ over $\mathbb{F}_4$ ramifies in the tower and also every place of F_i lying over any rational place of F_0 is also rational . This is exactly what was claimed in Remark 3.5.*

Corollary 4.13. *The tower $\mathcal{H}$ over $\mathbb{F}_4$ is optimal.*

Proof. From Theorem 4.11 we have that $\nu(\mathcal{H}) = 2$ and from Theorem 3.6 we know that $\gamma(\mathcal{H}) \leq 2$, then

$$1 = \sqrt{4} - 1 \geq \lambda(\mathcal{H}) = \frac{\nu(\mathcal{H})}{\gamma(\mathcal{H})} \geq 1,$$

so that $\lambda(\mathcal{H}) = 1$. □

Corollary 4.14. *The tower $\mathcal{H}$ over $\mathbb{F}_{2^s}$ is asymptotically good for s even with limit*

$$\lambda(\mathcal{H}) \geq 1.$$

Acknowledgements. We would like to thank Peter Beelen for his careful and detailed reading which greatly contributed in both aspects presentation and improvements of some important results in this paper, like Theorem 3.6, and for making us note that the optimality of the tower $\mathcal{H}$ over $\mathbb{F}_4$ would follow from our earlier results. This work was partially supported by CONICET and Proyecto CAI+D 2014, Nro. 50420150100090LI - Universidad Nacional del Litoral, Santa Fe, Argentina.

References

[BGS] P. Beelen, A. Garcia, and H. Stichtenoth, *Towards a classification of recursive towers of function fields over finite fields*, Finite Fields Appl., 12(1), (2006), 56–77.

[GS] A. Garcia and H. Stichtenoth, *On the Galois Closure of Towers*, Recent trends in coding theory and its applications, AMS/IP Stud. Adv. Math., 41, Amer. Math. Soc., Providence, RI, (2007), 83-92.

[HN17] H. Navarro Oyola, *Estudio asintótico de torres y subtorres de cuerpos de funciones*. Ph.D. Thesis, Universidad Nacional del Litoral, 2017.

[S] H. Stichtenoth, *Algebraic function fields and codes*, GTM 254, Springer, Berlin, 2nd edition, 2009.

Instituto de Matemática Aplicada del Litoral, Colectora Ruta Nac. N 168, Paraje El Pozo, (3000) Santa Fe - Argentina
E-mail address: mchara@santafe-conicet.gov.ar

Instituto de Matemática Aplicada del Litoral, Colectora Ruta Nac. N 168, Paraje El Pozo, (3000) Santa Fe - Argentina, and

Universidad del Valle, Calle 13 # 100-00, Cali - Colombia
E-mail address: horacio.navarro@correounivalle.edu.co

Departamento de Matemática, Facultad de Ingeniería Química (UNL), Santiago del Estero 2829, (3000) Santa Fe - Argentina
E-mail address: rtoledano@santafe-conicet.gov.ar