On Ramification and Genus of Recursive Towers

Peter Beelen, Arnaldo Garcia and Henning Stichtenoth

Abstract: We introduce the notion of the dual tower of a recursive tower of function fields over a finite field. We relate the ramification set of the tower with the one of the dual tower, for the case of good asymptotic behaviour of the genus.

1 Introduction

The interest on the theory of algebraic curves(or function fields) over finite fields has a long history in mathematics and it was crowned by the famous theorem of A. Weil (see [13]) bounding the number of rational points(or rational places) in terms of the genus and the cardinality of the finite field. This theorem is equivalent to the validity of the Riemann hypothesis for the associated congruence Zeta function. The asymptotic aspect of this theory; i.e., towers of curves(or of function fields) over finite fields, received much attention in recent years after Tfasman-Vladut-Zink showed its application to Coding Theory leading to linear codes better than the Gilbert-Varshamov bound (see [12]).

Throughout this paper we denote by $\mathbb{F}_q$ the finite field with q elements and by $\overline{\mathbb{F}}_q$ the algebraic closure of $\mathbb{F}_q$. Also, we denote by p the characteristic of $\mathbb{F}_q$. A *tower* $\mathcal{F}$ *over* $\mathbb{F}_q$ or an $\mathbb{F}_q$-tower is an infinite sequence $F_1 \subset F_2 \subset \cdots \subset F_n \subset \ldots$ of function fields over $\mathbb{F}_q$, with $\mathbb{F}_q$ algebraically closed in F_n for all n, such that the genus $g(F_n) \to \infty$ as $n \to \infty$. Since for any purely inseparable extension E/F of function fields over $\mathbb{F}_q$ the fields E and F are isomorphic, we can assume that all extensions F_{n+1}/F_n are separable.

We say that a tower $\mathcal{F}$ is *recursively defined by the polynomial* $f(X,Y) \in \mathbb{F}_q[X,Y]$ if there exist elements $x_n \in F_n$ for all $n \geq 1$ such that the following holds: i) $F_1 = \mathbb{F}_q(x_1)$ is the rational function field, and $F_{n+1} = F_n(x_{n+1})$ for all $n \geq 1$. ii) $f(x_n, x_{n+1}) = 0$ and $[F_{n+1} : F_n] = \deg_Y f(X,Y)$ for all $n \geq 1$. If the polynomial $f(X,Y)$ has the special form

$$f(X,Y) = \varphi_0(Y) \cdot \psi_1(X) - \varphi_1(Y) \cdot \psi_0(X)$$

with polynomials $\varphi_0(Y), \varphi_1(Y) \in \mathbb{F}_q[Y]$ and $\psi_0(X), \psi_1(X) \in \mathbb{F}_q[X]$ then we

Keywords: function fields, finite fields, ramification, genus, recursive towers, dual towers.

AMS Subject Classification: 11G20, 14H05, 14G15.

This work was partially done while the authors were visiting Sabanci University (Istanbul, Turkey) in Nov-Dec 2003.

A. Garcia was partially supported by PRONEX # 662408/1996-3(CNPq-Brazil).

also say that the tower $\mathcal{F}$ is recursively given by the equation

$$\frac{\psi_0(X)}{\psi_1(X)} = \frac{\varphi_0(Y)}{\varphi_1(Y)}.$$

If a tower $\mathcal{F}$ can be defined recursively by some polynomial $f(X,Y) \in \mathbb{F}_q[X,Y]$ it is called a *recursive tower*.

We denote by $N(F_n)$ the number of $\mathbb{F}_q$-rational places of F_n and by $g(F_n)$ its genus. Then the following limits exist (see [9]):

$$\nu(\mathcal{F}) := \lim_{n\to\infty} \frac{N(F_n)}{[F_n : F_1]}, \text{ called the } \textit{splitting rate} \text{ of } \mathcal{F}/F_1,$$

and

$$\gamma(\mathcal{F}) := \lim_{n\to\infty} \frac{g(F_n)}{[F_n : F_1]}, \text{ called the } \textit{genus} \text{ of } \mathcal{F}/F_1.$$

The *limit* $\lambda(\mathcal{F})$ of the tower $\mathcal{F}$ over $\mathbb{F}_q$ is then defined as

$$\lambda(\mathcal{F}) := \frac{\nu(\mathcal{F})}{\gamma(\mathcal{F})}.$$

Weil's theorem implies that $\lambda(\mathcal{F}) \leq 2\sqrt{q}$, for any $\mathbb{F}_q$-tower $\mathcal{F}$. It was first observed by Ihara that this upper bound can be significantly improved. Refining Ihara's arguments, Drinfeld and Vladut proved the following upper bound (see [4]):

$$\lambda(\mathcal{F}) \leq \sqrt{q} - 1, \text{ for any } \mathbb{F}_q\text{-tower } \mathcal{F}.$$

An $\mathbb{F}_q$-tower is called *good* if $\lambda(\mathcal{F}) > 0$. Clearly a tower is good if and only if $\nu(\mathcal{F}) > 0$ and $\gamma(\mathcal{F}) < \infty$. We say that the tower has *finite genus* if $\gamma(\mathcal{F}) < \infty$. When dealing with the genus we will often abuse notation and also denote by $\mathcal{F}$ the tower $F_1 \cdot \overline{\mathbb{F}}_q \subset F_2 \cdot \overline{\mathbb{F}}_q \subset \cdots \subset F_n \cdot \overline{\mathbb{F}}_q \subset \ldots$ over the field $\overline{\mathbb{F}}_q$.

Suppose that the tower $\mathcal{F}$ over $\mathbb{F}_q$ can be defined recursively by the polynomial $f(X,Y) \in \mathbb{F}_q[X,Y]$, where $f(X,Y)$ is separable in both variables. It is easy to prove (see [5]) that if $\mathcal{F}$ is a good tower then

$$\deg_X f(X,Y) = \deg_Y f(X,Y).$$

In most cases, especially when wild ramification occurs in the tower, it is not an easy task to decide if the tower has finite genus. The aim of this paper is to present some necessary conditions for finite genus (hence for being a good tower). This will be done in terms of the *dual tower* of $\mathcal{F}$ (see definition in Section 2). The criteria for finite genus of a tower are given in Theorem 3.3 and Theorem 3.6 of Section 3.

2 Preliminaries and Definitions

We denote by $\mathbb{P}(E)$ the set of places of a function field E. If $\mathcal{F}$ is a tower over $\mathbb{F}_q$ we consider the *ramification locus* $V(\mathcal{F})$ which is the subset of $\mathbb{P}(F_1)$ defined by

$$\begin{aligned} V(\mathcal{F}) \quad := \quad & \{P \in \mathbb{P}(F_1)\,;\ \text{for some } n \geq 2 \text{ there exists} \\ & \text{a place } Q \in \mathbb{P}(F_n) \text{ with } Q|P \text{ and } e(Q|P) > 1\}. \end{aligned}$$

The symbol $e(Q|P)$ above denotes the ramification index of a place $Q \in \mathbb{P}(F_n)$ over its restriction P to the first field F_1 of the tower $\mathcal{F}$. The tower $\mathcal{F}$ is called *tame* if all places $P \in V(\mathcal{F})$ are only tamely ramified in all extensions F_n/F_1; i.e., $e(Q|P)$ is not divisible by the characteristic p of $\mathbb{F}_q$ for all $n \geq 2$ and all $Q \in \mathbb{P}(F_n)$ lying above P. Otherwise the tower is said to be *wild*. For tame towers with finite ramification locus $V(\mathcal{F})$ we have $\gamma(\mathcal{F}) < \infty$ (see [8]), but there are examples of wild towers with finite ramification locus and $\gamma(\mathcal{F}) = \infty$ (see Example 3.8).

For any tower $\mathcal{F}$ we also consider the *wild ramification locus* $V_w(\mathcal{F})$ which is the subset of $V(\mathcal{F})$ defined by

$$\begin{aligned} V_w(\mathcal{F}) \quad := \quad & \{P \in \mathbb{P}(F_1)\,;\ \text{for some } n \geq 2 \text{ there exists a place} \\ & Q \in \mathbb{P}(F_n) \text{ with } Q|P \text{ such that } e(Q|P) \text{ is divisible by } p\}. \end{aligned}$$

Suppose that the tower $\mathcal{F} = (F_1, F_2, F_3, \dots)$ is defined recursively by the polynomial $f(X,Y) \in \mathbb{F}_q[X,Y]$. We define its *dual tower* $\mathcal{G} = (G_1, G_2, G_3, \dots)$ as the tower given recursively by the polynomial $f(Y,X)$. We identify the rational function fields $F_1 = \mathbb{F}_q(x_1)$ and $G_1 = \mathbb{F}_q(y_1)$ by setting $x_1 = y_1$, and then we have

$$\begin{aligned} F_n &= \mathbb{F}_q(x_1, \dots, x_n) \text{ with } f(x_i, x_{i+1}) = 0, \text{ and} \\ G_n &= \mathbb{F}_q(y_1, \dots, y_n) \text{ with } f(y_{i+1}, y_i) = 0 \end{aligned} \tag{$*$}$$

for all $n \geq 2$ and $1 \leq i \leq n-1$.

Example 2.1 Let $\mathcal{F}_1$ be the tower in characteristic $p = 2$ given recursively by

$$Y^2 + Y = X + \frac{1}{X} + 1.$$

It was shown in [10] that the limit of this tower over the finite field with eight elements is equal to $3/2$ (see also Theorem 4.10 and Example 5.5 in [1]). Its dual tower $\mathcal{G}_1$ is given recursively by the equation

$$Y + \frac{1}{Y} + 1 = X^2 + X.$$

Changing variables $X = (\tilde{X}+1)/\tilde{X}$ and $Y = (\tilde{Y}+1)/\tilde{Y}$ we get the equality $\tilde{Y}^2 + \tilde{Y} = \tilde{X}^2/(\tilde{X}^2 + \tilde{X} + 1)$, and hence the tower $\mathcal{G}_1$ can also be defined recursively by the equation

$$Y^2 + Y = \frac{X^2}{X^2 + X + 1}.$$

A recursive tower $\mathcal{F}$ and its dual tower $\mathcal{G}$ have the same limit; i.e., we have $\lambda(\mathcal{F}) = \lambda(\mathcal{G})$. In fact if $\mathcal{F} = (F_1, F_2, \ldots)$ and $\mathcal{G} = (G_1, G_2, \ldots)$, the function fields F_n and G_n are isomorphic over $\mathbb{F}_q$: if we present $F_n = \mathbb{F}_q(x_1, \ldots, x_n)$ and $G_n = \mathbb{F}_q(y_1, \ldots, y_n)$ as in $(*)$ above, then the map $x_1 \mapsto y_n$, $x_2 \mapsto y_{n-1}$, $\ldots$, $x_n \mapsto y_1$ gives an isomorphism from F_n onto G_n. In particular the dual tower $\mathcal{G}_1$ in Example 2.1 has limit $\lambda(\mathcal{G}_1) = 3/2$ over the field with 8 elements.

Example 2.2 The tower $\mathcal{F}_2$ over the finite field $\mathbb{F}_q$ with $q = \ell^2$ which is given recursively by the equation

$$Y^\ell + Y = \frac{X^\ell}{X^{\ell-1}+1} \tag{1}$$

attains the Drinfeld-Vladut bound; i.e., its limit over $\mathbb{F}_q$ satisfies $\lambda(\mathcal{F}_2) = \ell - 1$ (see [7]). We show here that $\mathcal{F}_2$ is *self-dual*; i.e., its dual tower $\mathcal{G}_2$ can also be defined recursively by Equation (1). Indeed, Equation (1) can be written as

$$Y^\ell + Y = \left(\left(\frac{1}{X}\right)^\ell + \frac{1}{X}\right)^{-1},$$

and hence the dual tower $\mathcal{G}_2$ is defined by

$$\left(\frac{1}{Y}\right)^\ell + \frac{1}{Y} = \frac{1}{X^\ell + X}.$$

Setting $\tilde{Y} := 1/Y$ and $\tilde{X} := 1/X$ we get the following equation which also defines $\mathcal{G}_2$ recursively:

$$\tilde{Y}^\ell + \tilde{Y} = \frac{1}{\tilde{X}^{-\ell} + \tilde{X}^{-1}} = \frac{\tilde{X}^\ell}{\tilde{X}^{\ell-1}+1}.$$

This shows that the tower $\mathcal{F}_2$ is in fact self-dual.

Let $\mathcal{H} = (H_1, H_2, H_3, \ldots)$ be a tower over $\mathbb{F}_q$ and let $P \in \mathbb{P}(H_1)$ be a place of the first function field H_1 of the tower $\mathcal{H}$. We now give some definitions concerning the ramification in the tower.

Definition 2.3 We define

$$\epsilon(P, \mathcal{H}) := \sup_{n \geq 2}\{e(Q_n|P)\},$$

where Q_n runs over all places of H_n lying over P.

Definition 2.4 Denoting by p the characteristic of $\mathbb{F}_q$, we define

$$\pi(P, \mathcal{H}) := \sup_{n\geq 2\,;\, i \geq 0}\{p^i\,;\, p^i \text{ divides } e(Q_n|P)\},$$

where again Q_n runs over all places of H_n lying over P.

It is clear that the tower $\mathcal{H}$ is tame if and only if $\pi(P, \mathcal{H}) = 1$ for all places $P \in \mathbb{P}(H_1)$. In the next section we will give necessary conditions for finite genus of recursive towers in terms of the concepts introduced in Definition 2.3 and Definition 2.4.

3 Ramification and Finite Genus

We first relate the concept in Definition 2.3 and the finiteness of the genus of recursive towers. For that we need two lemmas:

Lemma 3.1 ([7]) *Let $\mathcal{F} = (F_1, F_2, F_3, \dots)$ be a tower over $\mathbb{F}_q$ and denote by $D_n := \deg \mathrm{Diff}\,(F_{n+1}/F_n)$ the degree of the different of F_{n+1}/F_n, for all $n \geq 1$. Suppose that there exists a sequence $(\rho_1, \rho_2, \rho_3, \dots)$ of positive real numbers satisfying:*

i) $\rho_n \leq D_n$ holds for each $n \geq 1$.

ii) We have $\rho_{n+1} \geq [F_{n+2} : F_{n+1}] \cdot \rho_n$, for all $n \geq 1$.

Then the genus $\gamma(\mathcal{F})$ of the tower is infinite.

Lemma 3.2 ([14]) *Let E_1/F and E_2/F be linearly disjoint function field extensions and denote by $E := E_1 \cdot E_2$ the composite field of E_1 and E_2. Let $P \in \mathbb{P}(F)$ be a place of F and let $Q_1 \in \mathbb{P}(E_1)$ and $Q_2 \in \mathbb{P}(E_2)$ be places above P. Then there exists a place $Q \in \mathbb{P}(E)$ lying above the places Q_1 and Q_2.*

Our first result is:

Theorem 3.3 *Let $\mathcal{F}$ be a recursive tower over $\mathbb{F}_q$, defined by a polynomial $f(X,Y) \in \mathbb{F}_q[X,Y]$ which is separable in both variables. Let $\mathcal{G}$ be the dual tower of $\mathcal{F}$, and let P be a place of the first function field $F_1 = G_1$. If the tower has finite genus $\gamma(\mathcal{F}) < \infty$, then*

$$\epsilon(P, \mathcal{F}) = \epsilon(P, \mathcal{G}).$$

Proof. We can consider $\mathcal{F}$ as a tower over the algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$, since genus and ramification indices do not change in constant field extensions. Hence all places occurring in the proof below will be of degree one. By the remark at the end of Section 1 we also have $\deg_X f(X,Y) = \deg_Y f(X,Y) =: a > 1$ and therefore

$$[F_{n+1} : F_n] = [G_{n+1} : G_n] = a$$

for all $n \geq 1$. We are going to show that $\epsilon(P, \mathcal{F}) > \epsilon(P, \mathcal{G})$ implies that the genus $\gamma(\mathcal{F})$ is infinite. Interchanging $\mathcal{F}$ and $\mathcal{G}$ and observing that $\gamma(\mathcal{F}) = \gamma(\mathcal{G})$, this will prove the theorem.

Suppose then that $\epsilon(P, \mathcal{F}) > \epsilon(P, \mathcal{G})$. In particular we have that $e_1 := \epsilon(P, \mathcal{G})$ is a finite number. By definition of $\epsilon(P, \mathcal{G})$ there is some $n \geq 1$ and a place $Q_1 \in \mathbb{P}(G_n)$ such that

i) $e(Q_1|P) = e_1$.

ii) Q_1 is unramified in G_m/G_n, for all $m \geq n$.

It follows that for all $m \geq n$ there are exactly $[G_m : G_n]$ places of G_m above the place Q_1. Now we fix a field F_{k+1} (with $k \geq 1$) in the tower $\mathcal{F}$ and a place $Q_2 \in \mathbb{P}(F_{k+1})$ lying above P with

$$e_2 := e(Q_2|P) > e_1.$$

The existence of such a place Q_2 follows from the assumption $\epsilon(P, \mathcal{F}) > \epsilon(P, \mathcal{G})$. Let $m \geq n$ and let $H_m := F_{k+1} \cdot G_m$ (resp. $H_n := F_{k+1} \cdot G_n$) be the composite field of F_{k+1} with G_m (resp. with G_n). Consider a place $R_1 \in \mathbb{P}(G_m)$ lying above the place Q_1. Then we have the following picture:

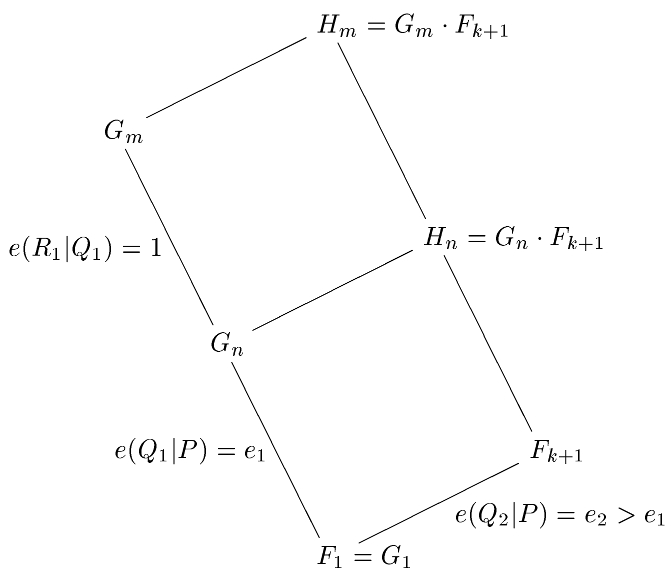

Figure 1.

Note that the field G_m is isomorphic to F_m, and H_m is isomorphic to the field F_{m+k}. Moreover the degree of the field extension H_m/G_m is

$$[H_m : G_m] = a^k$$

with $a = \deg_X f(X, Y)$ as above. Now we fix a place $R_2 \in \mathbb{P}(H_n)$ lying above Q_1 and Q_2 (the existence of R_2 follows from Lemma 3.2). Since $e_2 > e_1$ we have $e(R_2|Q_1) > 1$. Again by Lemma 3.2 there exists a place $S_1 \in \mathbb{P}(H_m)$ above the places R_1 and R_2, and it follows that $e(S_1|R_1) = e(R_2|Q_1) > 1$. We conclude that

$$\deg \mathrm{Diff}\,(H_m/G_m) \geq \#\{R_1 \in \mathbb{P}(G_m)\,;\, R_1|Q_1\} = [G_m : G_n] = a^{m-n},$$

and hence

$$\deg \text{Diff}\,(F_{m+k}/F_m) = \deg \text{Diff}\,(H_m/G_m) \geq a^{m-n}, \text{ for all } m \geq n.$$

Considering the tower $\mathcal{E} = (E_1, E_2, E_3, \dots)$ with

$$E_s := F_{n+(s-1)k}, \text{ for all } s \geq 1,$$

we see that

$$\deg \text{Diff}\,(E_{s+1}/E_s) = \deg \text{Diff}\,(F_{n+sk}/F_{n+(s-1)k}) \geq a^{n+(s-1)k-n} = a^{(s-1)k}.$$

We use the terminology of Lemma 3.1 and set $\rho_s := a^{(s-1)k}$. Then the assumptions of Lemma 3.1 are satisfied, and we conclude that $\gamma(\mathcal{E}) = \infty$, and hence also that $\gamma(\mathcal{F}) = \infty$ (see [8, Lemma 2.6]). □

Corollary 3.4 *Let $\mathcal{F}$ be a recursive tower over $\mathbb{F}_q$, defined by a polynomial $f(X,Y) \in \mathbb{F}_q[X,Y]$ which is separable in both variables, and let $\mathcal{G}$ be the dual tower of $\mathcal{F}$. If $\mathcal{F}$ has finite genus $\gamma(\mathcal{F}) < \infty$, then $\mathcal{F}$ and $\mathcal{G}$ have the same ramification locus:*

$$V(\mathcal{F}) = V(\mathcal{G}).$$

We remark that Corollary 3.4 was already shown by J. Wulftange under the additional hypothesis that the tower $\mathcal{F}$ is tame, see [14, Satz 3.2.1].
We now relate the concept in Definition 2.4 and the finiteness of the genus of recursive towers. We will need Abhyankar's lemma (see [11, Prop.III.8.9]):

Lemma 3.5 *Let E/F be a finite extension of function fields and let E_1, E_2 be intermediate fields $F \subset E_1, E_2 \subset E$ such that $E = E_1 \cdot E_2$ is the composite of E_1 and E_2. Let S_1 be a place of E and denote by R_1, R_2, and Q_1 the restrictions of the place S_1 to the fields E_1, E_2, and F respectively. Suppose that R_1 is tame over F; i.e., the characteristic of F does not divide $e(R_1|Q_1)$. Then we have*

$$e(S_1|Q_1) = \text{lcm}\{e(R_1|Q_1), e(R_2|Q_1)\},$$

where lcm *stands for the least common multiple.*

Theorem 3.6 *Let $\mathcal{F}$ be a recursive tower over $\mathbb{F}_q$, defined by a polynomial $f(X,Y) \in \mathbb{F}_q[X,Y]$ which is separable in both variables. Let $\mathcal{G}$ be the dual tower of $\mathcal{F}$, and let P be a place of the first function field $F_1 = G_1$. If the tower has finite genus $\gamma(\mathcal{F}) < \infty$, then*

$$\pi(P, \mathcal{F}) = \pi(P, \mathcal{G}).$$

Proof. As in the proof of Theorem 3.3 we can consider $\mathcal{F}$ as a tower over the algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$, and we can also assume that the equality of degrees $[F_{n+1} : F_n] = [G_{n+1} : G_n] = a > 1$ holds for all $n \geq 1$. We are going to show that the assumption $\pi(P, \mathcal{F}) > \pi(P, \mathcal{G})$ implies that the genus $\gamma(\mathcal{F})$ is infinite.

The assumption $\pi(P,\mathcal{F}) > \pi(P,\mathcal{G})$ gives in particular that $\pi(P,\mathcal{G})$ is a finite number. We then fix $n \in \mathbb{N}$ and a place $Q_1 \in \mathbb{P}(G_n)$ such that Q_1 lies above P and $\pi(P,\mathcal{G})$ divides $e(Q_1|P)$. We also fix $k \in \mathbb{N}$ and a place $Q_2 \in \mathbb{P}(F_{k+1})$ lying above P such that $p \cdot \pi(P,\mathcal{G})$ divides $e(Q_2|P)$ (where p denotes the characteristic of $\mathbb{F}_q$). Such a place Q_2 exists, since $\pi(P,\mathcal{F}) > \pi(P,\mathcal{G})$. As in the proof of Theorem 3.3 we define $H_m := G_m \cdot F_{k+1}$ for all $m \geq n$. Using Lemma 3.2 we fix a place $R_2 \in \mathbb{P}(H_n)$ lying above Q_1 and Q_2. Since the power of p appearing in $e(Q_2|P)$ is strictly larger than the one in $e(Q_1|P)$ we conclude that R_2 is wild; i.e., p divides $e(R_2|Q_1)$.

Now let $m \geq n$. For any place $R_1 \in \mathbb{P}(G_m)$ lying above Q_1 we choose a place $S_1 \in \mathbb{P}(H_m)$ lying above R_1 and R_2 (using Lemma 3.2 again). Then we have the following picture:

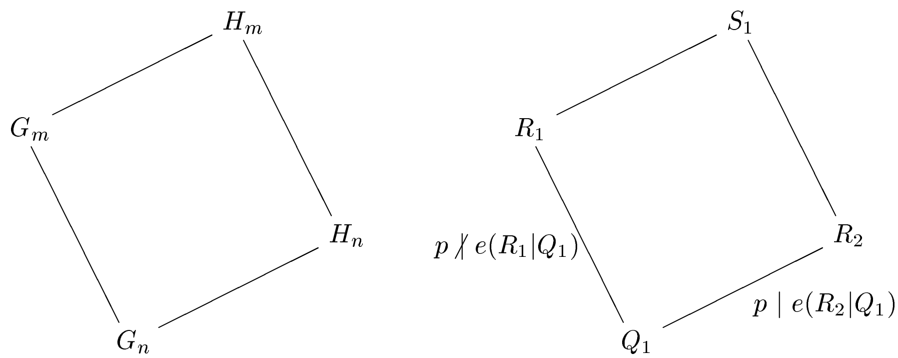

Figure 2.

Given a separable extension E/F of function fields and two places $P_1 \in \mathbb{P}(F)$, $P_2 \in \mathbb{P}(E)$ with $P_2|P_1$, we denote by $d(P_2|P_1)$ the different exponent of $P_2|P_1$. From the transitivity of the different exponents (see [11, Cor.III.4.11]) we obtain in our situation (see Figure 2):

$$\begin{aligned} d(S_1|Q_1) &= d(S_1|R_1) + e(S_1|R_1) \cdot d(R_1|Q_1) \\ &= d(S_1|R_1) + e(S_1|R_1)(e(R_1|Q_1) - 1), \end{aligned}$$

and also

$$\begin{aligned} d(S_1|Q_1) &= d(S_1|R_2) + e(S_1|R_2) \cdot d(R_2|Q_1) \\ &= e(S_1|R_2) - 1 + e(S_1|R_2) \cdot d(R_2|Q_1). \end{aligned}$$

Here we have used that $R_1|Q_1$ and hence also $S_1|R_2$ are tame. For simplicity we set $e_1 := e(R_1|Q_1)$ and $e_2 := e(R_2|Q_1)$. We also set $D := \gcd(e_1, e_2)$. By Lemma 3.5 we know that $e(S_1|R_2) = e_1/D$ and $e(S_1|R_1) = e_2/D$, and since $R_2|Q_1$ is wild we also have $d(R_2|Q_1) \geq e_2$ (see [11, Theor.III.5.1]). It follows from the expressions involving different exponents above that

$$d(S_1|R_1) + e(S_1|R_1) \cdot (e_1 - 1) = e(S_1|R_2) - 1 + e(S_1|R_2) \cdot d(R_2|Q_1),$$

hence

$$\begin{aligned} e_2 \cdot d(S_1|R_1) &\geq D \cdot d(S_1|R_1) = e_1 - D + e_1 \cdot d(R_2|Q_1) - e_2(e_1 - 1) \\ &\geq e_1 - D + e_1 e_2 - e_2(e_1 - 1) = e_1 + e_2 - D \geq e_1. \end{aligned}$$

We have shown that for any place $R_1 \in \mathbb{P}(G_m)$ lying above Q_1 the different exponent of $S_1|R_1$ satisfies

$$d(S_1|R_1) \geq \frac{1}{e_2} \cdot e(R_1|Q_1),$$

where the number e_2 is independent of the place S_1. It now follows that

$$\deg \mathrm{Diff}\,(H_m|G_m) \geq \sum_{\substack{R_1 \in \mathbb{P}(G_m) \\ R_1|Q_1}} d(S_1|R_1) \geq \frac{1}{e_2} \sum_{\substack{R_1 \in \mathbb{P}(G_m) \\ R_1|Q_1}} e(R_1|Q_1) = \frac{1}{e_2} \cdot [G_m : G_n],$$

and we finish the proof of Theorem 3.6 as in Theorem 3.3. □

Corollary 3.7 *Let $\mathcal{F}$ be a recursive tower over $\mathbb{F}_q$, defined by a polynomial $f(X, Y) \in \mathbb{F}_q[X, Y]$ which is separable in both variables, and let $\mathcal{G}$ be the dual tower of $\mathcal{F}$. If $\mathcal{F}$ has finite genus $\gamma(\mathcal{F}) < \infty$, then $\mathcal{F}$ and $\mathcal{G}$ have the same wild ramification locus:*

$$V_w(\mathcal{F}) = V_w(\mathcal{G}).$$

We apply this corollary in the next example, which is a generalization of an example given in [2]:

Example 3.8 Let ℓ be a prime power and consider the tower $\mathcal{F}_3$ over $\mathbb{F}_q$ with $q = \ell^p$ (where $p = \mathrm{char}(\mathbb{F}_q)$) which is given recursively by the equation

$$Y^\ell - Y = \frac{(X+1)(X^{\ell-1} - 1)}{X^{\ell-1}}.$$

In the particular case $\ell = p = 2$ this tower attains the Drinfeld-Vladut bound over $\mathbb{F}_4$; i.e., in this particular case its limit is $\lambda(\mathcal{F}_3) = 1 = \sqrt{4} - 1$. Indeed, after the substitutions $X = \tilde{X} + 1$ and $Y = \tilde{Y} + 1$ we get

$$\tilde{Y}^2 + \tilde{Y} = \frac{\tilde{X}^2}{\tilde{X} + 1},$$

and this defines the tower $\mathcal{F}_2$ over $\mathbb{F}_4$ in Example 2.2.

From the defining equation for the tower $\mathcal{F}_3$ one sees that $X^\ell = X + 1$ implies that $Y^\ell = Y + 1$. Hence the set $\Omega = \{\alpha\,;\,\alpha^\ell = \alpha + 1\}$ splits completely in the tower $\mathcal{F}_3$ over $\mathbb{F}_q$ (it is easy to verify that $\Omega \subset \mathbb{F}_q$). Therefore the splitting rate satisfies $\nu(\mathcal{F}_3) > 0$. Moreover we have $V(\mathcal{F}_3) = \mathbb{F}_\ell \cup \{\infty\}$, and it seems worthwhile to investigate the limit of the tower $\mathcal{F}_3$ more closely.

There is only tame ramification in the extensions $\mathbb{F}_q(x_n, x_{n+1})/\mathbb{F}_q(x_{n+1})$ for $p \neq 2$, as follows from the defining equation of the tower. Hence we have

$$V_w(\mathcal{F}_3) \neq \emptyset \text{ and } V_w(\mathcal{G}_3) = \emptyset,$$

denoting by $\mathcal{G}_3$ the dual tower of $\mathcal{F}_3$. We conclude from Corollary 3.7 that $\gamma(\mathcal{F}_3) = \infty$ and therefore $\lambda(\mathcal{F}_3) = 0$. Hence the tower $\mathcal{F}_3$ is bad in characteristic $p \neq 2$.

For $p = 2$ both towers $\mathcal{F}_3$ and $\mathcal{G}_3$ are wild. However, we believe that also in the case $2 = p < \ell$ the genus of $\mathcal{F}_3$ is infinite. If this is really the case, it would be nice to have a criterion similar to the one in Theorem 3.6 that would imply easily that $\gamma(\mathcal{F}_3) = \infty$. One should look for a criterion involving $\pi(P, \mathcal{F})$ and $\pi(P, \mathcal{G})$ even in the case where both of them are infinite.

References

[1] P. Beelen, A. Garcia and H. Stichtenoth, On towers of function fields over finite fields, preprint available at www.preprint.impa.br/indexEngl.html.

[2] P. Beelen, A. Garcia and H. Stichtenoth, On towers of function fields of Artin-Schreier type, to appear in Bulletin Braz. Math. Soc.

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

[4] 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].

[5] A. Garcia and H. Stichtenoth, *Skew pyramids of function fields are asymptotically bad*, Coding Theory, Cryptography and Related Areas, J. Buchmann, T. Høholdt, H. Stichtenoth, H. Tapia-Recillas (eds.), Springer Verlag, 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 behaviour 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 function fields over the field with eight elements*, Bull. London Math. Soc. **34** (2002), 291-300.

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

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

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

[14] J. Wulftange, *Zahme Türme algebraischer Funktionenkörper*, Ph.D. Thesis, University of Essen, 2003.

Authors' addresses:

Peter Beelen, Fachbereich Mathematik, Universität Duisburg-Essen, 45117 Essen, Germany. e-mail: peter.beelen@uni-essen.de.

Arnaldo Garcia, Instituto de Matemática Pura e Aplicada IMPA, Estrada Dona Castorina 110, 22460-320, Rio de Janeiro RJ, Brazil. e-mail: garcia@impa.br

Henning Stichtenoth, Fachbereich Mathematik, Universität Duisburg-Essen, 45117 Essen, Germany. e-mail: stichtenoth@uni-essen.de