Séminaires & Congrès
11, 2005, p. 1–20

ON TOWERS OF FUNCTION FIELDS OVER FINITE FIELDS

by

Peter Beelen, Arnaldo Garcia & Henning Stichtenoth

Abstract. — The topic of this paper is the construction of good recursive towers of function fields over finite fields. We give an exposition of a number of known results and illustrate the theory by several examples.

***Résumé* (Tours des corps de fonctions sur des corps finis).** — Le sujet de cet article est la construction de tours de corps de fonctions sur des corps finis qui sont définies récursivement. Nous donnons un exposé des quelques résultats connus en illustrant la théorie avec plusieurs exemples.

1. Introduction

The study of solutions of polynomial equations over finite fields has a long history in mathematics, going back to C.F. Gauss. In case these polynomials define a one-dimensional object (*i.e.*, they define a curve or equivalently an algebraic function field), we have the famous result of A. Weil (see [**16**]) bounding the number of such solutions having all coordinates in the finite field. This bound is given in terms of the cardinality of the finite field and the genus of the curve, and it is equivalent to the validity of the Riemann Hypothesis for the associated Congruence Zeta Function. When the genus is large with respect to the cardinality of the finite field, Ihara (see [**14**]) noticed that Weil's bound cannot be reached. This observation led to the consideration of towers of function fields over a fixed finite field.

The interest on towers was enhanced after Tsfasman-Vladut-Zink showed (using towers and a construction of linear codes from function fields due to Goppa) the existence of sequences of codes with limit parameters (transmission rate and relative distance) above the so-called Gilbert-Varshamov bound (see [**15**]).

2000 ***Mathematics Subject Classification.*** — 14H05, 14G05, 11G20.
Key words and phrases. — Towers of function fields, finite fields, good towers, graphs.

In this paper we present several topics in the theory of towers of function fields over finite fields. We will omit most proofs, since these are already given in other papers by the authors. We will give references to these papers when necessary.

After starting with basic definitions and first properties of towers of function fields over finite fields, we study the limit of a tower and give several examples in order to illustrate the concept of towers. In Section 3 we present two interesting new examples of asymptotically good towers, one of them over the field of cardinality q^2, the other over the field of cardinality q^3. In the last two sections we use methods from graph theory to investigate the splitting behaviour of places in a recursive tower. We obtain a functional equation which gives in many cases further insight in completely splitting places.

2. The limit of a tower

In this section we discuss some properties of towers of function fields over finite fields, and we also give some examples. Let $\mathbb{F}_q$ be the finite field with q elements. A *function field F over $\mathbb{F}_q$* is a finitely generated field extension $F/\mathbb{F}_q$ of trans-cendence degree one, with $\mathbb{F}_q$ algebraically closed in the field F. We denote by $g(F)$ the genus of the function field F. A *tower* $\mathcal{F}$ over $\mathbb{F}_q$ is an infinite sequence $\mathcal{F} = (F_1 \subset F_2 \subset F_3 \subset \cdots)$ of function field extensions F_{n+1}/F_n for all $n \in \mathbb{N}$, satisfying:

a) Each extension F_{n+1}/F_n is finite and separable.

b) We have $g(F_n) \to \infty$ as $n \to \infty$.

Let $N(F_i)$ denote the number of rational places of $F_i/\mathbb{F}_q$. We are interested in the *limit* $\lambda(\mathcal{F})$ of a tower $\mathcal{F}$ over $\mathbb{F}_q$, *i.e.*, by definition

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

It is an easy consequence of Hurwitz's genus formula that the limit above exists (see [**9**]). Towers are specially interesting if they have many rational places with respect to the genera; we then say that the tower $\mathcal{F}$ is *good over* $\mathbb{F}_q$ if its limit $\lambda(\mathcal{F})$ satisfies $\lambda(\mathcal{F}) > 0$, otherwise $\mathcal{F}$ is said to be *bad.* It is a non-trivial problem to find such good towers over finite fields, since in most cases it happens that either $g(F_i)$ increases too fast or $N(F_i)$ does not grow fast enough. We therefore divide the study of the limit $\lambda(\mathcal{F})$ into two limits:

(1) The *genus* $\gamma(\mathcal{F})$ *of* $\mathcal{F}$ *over* F_1

$$\gamma(\mathcal{F}) := \lim_{i\to\infty} \frac{g(F_i)}{[F_i : F_1]}.$$

(2) The *splitting rate* $\nu(\mathcal{F})$ *of* $\mathcal{F}$ *over* F_1

$$\nu(\mathcal{F}) := \lim_{i\to\infty} \frac{N(F_i)}{[F_i : F_1]}.$$

The two limits above do exist (see [**12**]) and we clearly have:

$$0 < \gamma(\mathcal{F}) \leqslant \infty, \quad 0 \leqslant \nu(\mathcal{F}) \leqslant N(F_1), \quad \text{and} \quad \lambda(\mathcal{F}) = \frac{\nu(\mathcal{F})}{\gamma(\mathcal{F})}.$$

In particular, the tower $\mathcal{F}$ is good over $\mathbb{F}_q$ if and only if $\nu(\mathcal{F}) > 0$ and $\gamma(\mathcal{F}) < \infty$.

Let F be a function field over $\mathbb{F}_q$ and let P be a rational place of F over $\mathbb{F}_q$; *i.e.*, the degree of the place P satisfies $\deg P = 1$. We say that the place P *splits completely in the finite extension* E/F if there are $[E : F]$ places of E above the place P. Let $\mathcal{F} = (F_1 \subset F_2 \subset F_3 \subset \cdots)$ be a tower over $\mathbb{F}_q$ and let P be a rational place of the first field F_1 in the tower $\mathcal{F}$. We say that the place P *splits completely in the tower* if the place P splits completely in the extension F_{n+1}/F_1 for all $n \in \mathbb{N}$. We denote

$$t(\mathcal{F}/F_1) = t(\mathcal{F}) := \#\{P \text{ a rational place of } F_1 \ ; \ P \text{ splits completely in } \mathcal{F}\}.$$

We clearly have $\nu(\mathcal{F}) \geqslant t(\mathcal{F})$, for any tower $\mathcal{F}$. Hence if the tower is *completely splitting* (*i.e.*, if we have $t(\mathcal{F}) > 0$) then $\nu(\mathcal{F}) > 0$. Let us also denote by $\mathcal{F}$ the limit field of the tower; *i.e.*, let

$$\mathcal{F} := \bigcup_{n \in \mathbb{N}} F_n.$$

Complete splitting is a reasonable condition; we have a partial converse of the statement above (see [**11**]). If for some value of $n \in \mathbb{N}$ the field extension $\mathcal{F}/F_n$ is Galois, then the condition $\nu(\mathcal{F}) > 0$ implies that the tower is completely splitting over F_n (*i.e.*, $\nu(\mathcal{F}) > 0$ implies that $t(\mathcal{F}/F_n) > 0$).

Next we consider the genus $\gamma(\mathcal{F})$ of the tower $\mathcal{F}$ over the first field F_1. It is useful to observe that the genus $\gamma(\mathcal{F})$ does not change under constant field extensions, so we can replace the function fields $F_i/\mathbb{F}_q$ by the function fields $\overline{F}_i/\overline{\mathbb{F}}_q := (F_i \cdot \overline{\mathbb{F}}_q)/\overline{\mathbb{F}}_q$, where $\overline{\mathbb{F}}_q$ denotes the algebraic closure of the finite field $\mathbb{F}_q$. We clearly have $[F_{n+1} : F_n] = [\overline{F}_{n+1} : \overline{F}_n]$, for each $n \in \mathbb{N}$. A place P of $\overline{F}_1 = F_1 \cdot \overline{\mathbb{F}}_q$ is ramified in $\overline{F}_{n+1}$ if there exist fewer than $[F_{n+1} : F_1]$ places of $\overline{F}_{n+1}$ above the place P. We then define the *ramification locus of* $\mathcal{F}$ *over* $\overline{F}_1$ by

$$V(\mathcal{F}) := \{P \text{ place of } \overline{F}_1 \ ; \ P \text{ ramifies in } \overline{F}_{n+1} \text{ for some } n \in \mathbb{N}\}.$$

Let E/F be a separable extension of function fields over the algebraic closure $\overline{\mathbb{F}}_q$. Let P be a place of the field F and let $Q_1, Q_2, \ldots, Q_r$ be all places of E above P. There are natural numbers $e(Q_i|P)$ called *ramification indices* of Q_i over P, for all $1 \leqslant i \leqslant r$, and the following fundamental equality holds:

$$\sum_{i=1}^{r} e(Q_i|P) = [E : F].$$

The place P is called *tame in* E/F if the characteristic p does not divide $e(Q_i|P)$, for all $1 \leqslant i \leqslant r$. Otherwise P is called *wild*. The extension E/F is called *tame* if all places P of the field F are tame places. We call a tower $\mathcal{F}$ over $\mathbb{F}_q$ a *tame tower* if the extensions $\overline{F}_{n+1}/\overline{F}_1$ are tame extensions, for all $n \in \mathbb{N}$.

Here is a simple sufficient criterion for the finiteness of the genus $\gamma(\mathcal{F})$ of a tower (see [**11**]): if the tower $\mathcal{F}$ is a tame tower with a finite ramification locus (*i.e.*, $\#V(\mathcal{F}) < \infty$), then it has a finite genus $\gamma(\mathcal{F}) < \infty$.

The statement above is false in general when $\mathcal{F}$ is a *wild tower*; *i.e.*, when the tower $\mathcal{F}$ is not tame. Before giving some examples $\mathcal{F}$ of tame and wild towers, and before discussing the splitting rate $\nu(\mathcal{F})$ and the genus $\gamma(\mathcal{F})$ in these examples, we introduce the concept of recursive towers. We say that a tower $\mathcal{F}$ is *recursively given by a polynomial* $f(X,Y) \in \mathbb{F}_q[X,Y]$, if $F_1 = \mathbb{F}_q(x_1)$ is the rational function field and, for each $n \in \mathbb{N}$, the field F_{n+1} is defined by

$$F_{n+1} := F_n(x_{n+1}), \text{ with } f(x_n, x_{n+1}) = 0.$$

Further we demand that $[F_{n+1} : F_n] = \deg_Y f(X,Y)$ for all $n \in \mathbb{N}$. The polynomial $f(X,Y)$ should have balanced degrees; *i.e.*, $\deg_X f(X,Y) = \deg_Y f(X,Y)$. Otherwise the limit $\lambda(\mathcal{F})$ of the tower is equal to zero (see [**10**]).

An upper bound for the limit $\lambda(\mathcal{F})$ of a tower $\mathcal{F}$ over the finite field $\mathbb{F}_q$ is the following bound due to Drinfeld-Vladut (see [**7**]):

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

We now give some examples of towers:

Example 2.1 **(**see [**12**]**).** — Consider the tower $\mathcal{F}$ over $\mathbb{F}_4$ given recursively by the polynomial

$$f(X,Y) = Y^3 + (X+1)^3 + 1 \in \mathbb{F}_4[X,Y].$$

This is a tame tower with $\#V(\mathcal{F}) = 4$ and $t(\mathcal{F}) = 1$ (the place at infinity of $F_1 = \mathbb{F}_4(x_1)$ splits completely). Its limit satisfies

$$\lambda(\mathcal{F}) = 1 = \sqrt{4} - 1;$$

i.e., it attains the Drinfeld-Vladut bound.

Example 2.2 **(**see [**9**]**).** — Consider the tower $\mathcal{F}$ over $\mathbb{F}_{q^2}$, defined recursively by

$$f(X,Y) = (X^{q-1}+1)(Y^q + Y) - X^q \in \mathbb{F}_{q^2}[X,Y].$$

This is a wild tower $\mathcal{F}$ satisfying

$$\nu(\mathcal{F}) = q^2 - q \text{ and } \gamma(\mathcal{F}) = q.$$

In particular it attains the Drinfeld-Vladut bound; *i.e.*,

$$\lambda(\mathcal{F}) = q - 1.$$

For wild towers it is in general very hard to decide if the genus $\gamma(\mathcal{F})$ is finite or not. This is the case in Example 2.2 where to show that $\gamma(\mathcal{F}) = q$ involves long and technical computations.

For simplicity we say for example that the tower over $\mathbb{F}_{q^2}$ in Example 2.2 is given by the equation

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

Example 2.3 **(see [2, 3])**. — Consider the tower $\mathcal{F}$ over $\mathbb{F}_q$ with $q = p^p$ (p an odd prime number) defined by the following equation

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

The tower $\mathcal{F}$ is wild, and its ramification locus $V(\mathcal{F})$ is a finite set. Also $t(\mathcal{F}) \geqslant p$ (the places of $F_1 = \mathbb{F}_q(x_1)$ which are the zeros of the polynomial $x_1^p - x_1 - 1$ are completely splitting in the tower $\mathcal{F}$). Nevertheless we have $\lambda(\mathcal{F}) = 0$ for $p \geqslant 3$.

If one considers the tower in Example 2.3 in the case $p = 2$, one can show that it is the same tower as in Example 2.2 with $q = 2$. In fact just consider the substitutions $X \mapsto X + 1$ and $Y \mapsto Y + 1$.

Example 2.4 **(see [11])**. — Consider the tower $\mathcal{F}$ over $\mathbb{F}_q$, with $q = p^2$ and p an odd prime number, defined recursively by the equation

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

It is easy to see that $\mathcal{F}$ is a tame tower with $\gamma(\mathcal{F}) = 2$. The hard part here is to show that $\nu(\mathcal{F}) = 2(p-1)$. From this we conclude that $\mathcal{F}$ attains the Drinfeld-Vladut bound over the finite field $\mathbb{F}_{p^2}$; *i.e.*, we conclude

$$\lambda(\mathcal{F}) = p - 1.$$

The proof that $\nu(\mathcal{F}) = 2(p-1)$ involves the investigation of $\mathbb{F}_q$-rationality of the roots of Deuring's polynomial

$$H(t) := \sum_{j=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{j}^2 t^j \in \mathbb{F}_p[t].$$

The roots of $H(t)$ parametrize supersingular elliptic curves in Legendre's normal form.

Now we consider some specific classes of polynomials $f(X, Y) \in \mathbb{F}_q[X, Y]$ which lead to good towers over $\mathbb{F}_q$ in many cases. A tower over $\mathbb{F}_q$ is a *Kummer tower* if it can be defined recursively by an equation as below

$$Y^m = f(X), \text{ with } f(X) \in \mathbb{F}_q(X) \text{ and } (m, q) = 1.$$

If m divides $(q-1)$, each step F_{n+1}/F_n in a Kummer tower is cyclic of degree m. Example 2.4 above is a Kummer tower. A more specific class of towers consists of *towers of Fermat type* which are given by

$$Y^m = a(X+b)^m + c, \text{ with } a, b, c \in \mathbb{F}_q.$$

The equation above defines a tower if and only if $abc \neq 0$ (see [**17**]). The difficulty here is to show that the equation remains irreducible in each step F_{n+1}/F_n in the tower. In case $ab^m + c = 0$, this is easily seen, since the place $x_1 = 0$ of $F_1 = \mathbb{F}_q(x_1)$ is totally ramified in the tower. In case $ab^m + c \neq 0$, no place ramifies totally throughout the tower and the proof that the equation remains irreducible in each step, is more involved.

Even this simple looking class of towers of Fermat type presents examples with quite interesting behaviour. Example 2.1 belongs to this class and it attains the Drinfeld-Vladut bound over $\mathbb{F}_4$. We now give other examples in this class:

Example 2.5 (see [**12**]). — Consider the tower $\mathcal{F}$ over $\mathbb{F}_9$ defined by the equation

$$Y^2 = -(X+1)^2 + 1.$$

We have $\#V(\mathcal{F}) = 3$ and $t(\mathcal{F}) = 1$, since the place at infinity of $F_1 = \mathbb{F}_9(x_1)$ splits completely in this tower. We also have

$$\lambda(\mathcal{F}) = 2 = \sqrt{9} - 1;$$

i.e., this tower attains the Drinfeld-Vladut bound.

Example 2.6. — Consider the tower $\mathcal{F}$ over the prime field $\mathbb{F}_3$ defined by the equation

$$Y^2 = (X+1)^2 - 1.$$

In this tower the place at infinity of $F_1 = \mathbb{F}_3(x_1)$ splits completely and one can check that the ramification locus $V(\mathcal{F})$ is infinite. It is not likely, but if it turns out that this tower has a finite genus $\gamma(\mathcal{F})$, then this would be the first example of an explicit good tower over a prime field.

Another interesting class of recursive towers is the class of *towers of Artin-Schreier type*. These towers can be given by an equation

$$\varphi(Y) = \psi(X),$$

where $\varphi(Y) \in \mathbb{F}_q[Y]$ is an additive separable polynomial and where $\psi(X) \in \mathbb{F}_q(X)$ is a rational function. If the additive polynomial $\varphi(Y)$ has all its roots in the finite field $\mathbb{F}_q$, then each step F_{n+1}/F_n is an elementary abelian p-extension with $[F_{n+1} : F_n] = \deg \varphi(Y)$. Ramification in this class of towers is always wild. Examples 2.2 and 2.3 give towers belonging to this class. Another very interesting example is the following:

Example 2.7 (see [**13**]). — Consider the tower $\mathcal{F}$ over $\mathbb{F}_8$ defined recursively by

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

We have $t(\mathcal{F}) = 6$, since the places corresponding to $x_1 = \alpha$ with $\alpha \in \mathbb{F}_8 \backslash \mathbb{F}_2$ are completely splitting in the tower. The hard thing here is to prove that $\gamma(\mathcal{F}) = 4$ and hence

$$\lambda(\mathcal{F}) \geqslant \frac{t(\mathcal{F})}{\gamma(\mathcal{F})} = \frac{3}{2}.$$

T. Zink proved in [**18**], using degenerations of Shimura modular surfaces, that there is a sequence of function fields $(F_1, F_2, F_3, \dots)$ over a field of cardinality p^3 (with p any prime number) such that

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

For $p = 2$, this lower bound is $2(p^2-1)/(p+2) = 3/2$. The tower $\mathcal{F}/\mathbb{F}_8$ in Example 2.7 is the first explicit example of a tower which attains Zink's lower bound above.

It is then natural to look for towers $\mathcal{F}$ of Artin-Schreier type, given by $\varphi(Y) = \psi(X)$ as above, satisfying $\lambda(\mathcal{F}) > 0$. For a fixed additive polynomial $\varphi(Y) \in \mathbb{F}_q[Y]$ with all roots in $\mathbb{F}_q$, there are however just a few possibilities for the rational functions $\psi(X) \in \mathbb{F}_q(X)$ which may lead to good towers over the finite field $\mathbb{F}_q$ (see [**2**]). To illustrate this assertion, consider a recursive tower $\mathcal{F}$ over $\mathbb{F}_q$ given by an equation

$$Y^p + \alpha Y = \psi(X), \text{ with } \alpha \in \mathbb{F}_q^* \text{ and } \psi(X) \in \mathbb{F}_q(X).$$

If the tower $\mathcal{F}$ is a good tower (*i.e.*, if $\lambda(\mathcal{F}) > 0$), then we just have 3 possibilities for the rational function $\psi(X) \in \mathbb{F}_q(X)$:

(1) $\psi(X) = a + (X+b)^p/f(X)$, with $a, b \in \mathbb{F}_q$ and $f(X)$ a polynomial with $\deg f \leqslant p$.
(2) $\psi(X) = f(X)/(X+b)^p$, with $b \in \mathbb{F}_q$ and $f(X)$ a polynomial with $\deg f \leqslant p$.
(3) $\psi(X) = a + 1/f(X)$, with $a \in \mathbb{F}_q$ and $f(X)$ a polynomial with $\deg f = p$.

We believe that case (3) above can be discarded; *i.e.*, case (3) would always lead to $\lambda(\mathcal{F}) = 0$. The examples already given here (see Examples 2.2 and 2.7) belong to case (1). The tower given in Example 2.3 satisfies $\lambda(\mathcal{F}) = 0$, since its rational function

$$\psi(X) = \frac{(X+1)(X^{p-1}+1)}{X^{p-1}}$$

does not belong to any of the three cases above for $p \neq 2$. In characteristic $p = 2$ it belongs to case (1) with $a = 0$, $b = 1$, and $f(X) = X$. A natural problem here is the determination of the polynomials $f(X)$ with $\deg f(X) \leqslant p$ leading to a finite genus $\gamma(\mathcal{F}) < \infty$ and even better leading to $\lambda(\mathcal{F}) > 0$.

We finish this section with two conjectures:

Conjecture 1. — *Let $\mathcal{F}$ be a recursive tower over a finite field. If $\nu(\mathcal{F}) > 0$, then $t(\mathcal{F}) > 0$.*

In other words, Conjecture 1 says that recursive towers with a positive splitting rate are completely splitting. A refinement of Conjecture 1 would be that the equality $\nu(\mathcal{F}) = t(\mathcal{F})$ always holds for any recursive tower $\mathcal{F}$ over a finite field.

Conjecture 2. — *Let $\mathcal{F}$ be a recursive tower over a finite field. If $\gamma(\mathcal{F}) < \infty$, then $\#V(\mathcal{F}) < \infty$.*

In other words, Conjecture 2 says that recursive towers with a finite genus have a finite ramification locus.

Both Conjecture 1 and Conjecture 2 are false without the hypothesis that the tower $\mathcal{F}$ is a recursive tower (see [**8**]). We will give a partial answer to Conjecture 1 in Section 4 below.

3. Two new non-Galois towers

The aim of this section is to present two new towers, one over finite fields $\mathbb{F}_{q^2}$ with square cardinality and the other over finite fields $\mathbb{F}_{q^3}$ with cubic cardinality. The new feature of these two towers of function fields is that each step F_{n+1}/F_n is non-Galois for $q \neq 2$. Even more, for any $n \geqslant 2$ and any intermediate field $F_1 \subsetneq E \subset F_n$ the extension E/F_1 is non-Galois.

Example 3.1 **(see [5])**. — Consider the tower $\mathcal{F}$ over $\mathbb{F}_{q^2}$ defined recursively by the equation

$$\frac{Y-1}{Y^q} = \frac{X^q-1}{X}.$$

It is easily seen that $t(\mathcal{F}) = q$, since the places of $F_1 = \mathbb{F}_{q^2}(x_1)$ which are zeros of $x_1^q + x_1 - 1$ are completely splitting in the tower $\mathcal{F}$ over $\mathbb{F}_{q^2}$. The hard part here is to show that $\gamma(\mathcal{F}) = q/(q-1)$. Hence we conclude

$$\lambda(\mathcal{F}) \geqslant \frac{t(\mathcal{F})}{\gamma(\mathcal{F})} = q-1;$$

i.e., the tower $\mathcal{F}$ attains the Drinfeld-Vladut bound over $\mathbb{F}_{q^2}$. This fact can also be seen from the fact that our new tower $\mathcal{F}$ is a subtower of the tower in Example 2.2. Indeed denoting by $\mathcal{E}$ the tower over $\mathbb{F}_{q^2}$ defined recursively by

$$W^q + W = \frac{V^q}{V^{q-1}+1},$$

and setting

$$X := \frac{1}{V^{q-1}+1} \quad \text{and} \quad Y := \frac{1}{W^{q-1}+1},$$

one checks easily that these functions X and Y satisfy the equation defining the tower $\mathcal{F}$; *i.e.*,

$$\frac{Y-1}{Y^q} = \frac{X^q-1}{X}.$$

Being a subtower, we have (see [**9**])

$$\lambda(\mathcal{F}) \geqslant \lambda(\mathcal{E}) = q-1, \text{ and hence } \lambda(\mathcal{F}) = q-1.$$

One can also go the other way around; *i.e.*, knowing that $\lambda(\mathcal{F}) = q-1$, one can deduce that $\lambda(\mathcal{E}) = q-1$. In order to do this we will need the concept of a composite tower. Let $\mathcal{F} = (F_1 \subset F_2 \subset \cdots \subset F_n \subset \cdots)$ be a tower and let E_1/F_1 be a tame function field extension which is linearly disjoint from F_{n+1} over F_1 for all $n \in \mathbb{N}$. Let $\mathcal{E}$ denote the *composite tower*; *i.e.*, the tower $\mathcal{E} = (E_1 \subset E_2 \subset E_3 \subset \cdots)$ where the field E_n is the compositum $E_n := E_1 \cdot F_n$, for all $n \in \mathbb{N}$. Under certain hypotheses (see [**12**]) one has the following genus formula:

$$2g(E_1) - 2\gamma(\mathcal{E}) - 2 = [E_1 : F_1](2g(F_1) - 2\gamma(\mathcal{F}) - 2) + \delta,$$

where $\gamma(\mathcal{E})$ is the genus over E_1 of the tower $\mathcal{E}$, where $\gamma(\mathcal{F})$ is the genus over F_1 of the tower $\mathcal{F}$, and where δ is the degree of the part of the different $\operatorname{Diff}(E_1/F_1)$ supported above the ramification locus $V(\mathcal{F})$ of the tower $\mathcal{F}$. If one assumes furthermore that the whole of the different $\operatorname{Diff}(E_1/F_1)$ is supported at places of E_1 lying above places of F_1 belonging to $V(\mathcal{F})$, then we have

$$\delta = \deg \operatorname{Diff}(E_1/F_1)$$

in the above genus formula. In this situation, from the classical Hurwitz genus formula, we conclude:

$$\gamma(\mathcal{E}) = [E_1 : F_1]\gamma(\mathcal{F}).$$

We now return to the towers $\mathcal{E}$ and $\mathcal{F}$ as in Example 3.1. One checks easily that the tower $\mathcal{E}$ is the composite tower of $\mathcal{F}$ with the extension $E_1 = F_1(v_1)$, where

$$v_1^{q-1} = \frac{1-x_1}{x_1}.$$

From the discussion above we then conclude that

$$\gamma(\mathcal{E}) = [E_1 : F_1]\gamma(\mathcal{F}) = (q-1) \cdot \frac{q}{q-1} = q.$$

Also one sees easily that $t(\mathcal{E}) = q^2 - q$, since the places of $E_1 = \mathbb{F}_{q^2}(v_1)$ corresponding to the elements of $\mathbb{F}_{q^2} \backslash \mathbb{F}_q$ are completely splitting in the tower $\mathcal{E}$ over $\mathbb{F}_{q^2}$. Hence

$$\lambda(\mathcal{E}) \geqslant \frac{t(\mathcal{E})}{\gamma(\mathcal{E})} = \frac{q^2-q}{q} = q-1.$$

Example 3.2 **(**see [**6**]**).** — Consider the tower $\mathcal{F}$ over $\mathbb{F}_{q^3}$, with q any prime power, defined recursively by the equation

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

Let

$$A := \{\alpha \in \overline{\mathbb{F}}_q \ ; \ \alpha^{q+1} = \alpha - 1\}$$

and let

$$\Omega = \Big\{\omega \in \overline{\mathbb{F}}_q \ ; \ \frac{\omega^q + \omega - 1}{\omega} = \alpha, \text{ for some } \alpha \in A\Big\}.$$

One checks easily that

$$\#\Omega = q(q+1) \quad \text{and} \quad \Omega \subset \mathbb{F}_{q^3},$$

and also that $t(\mathcal{F}) \geqslant q(q+1)$ since the places of $F_1 = \mathbb{F}_{q^3}(x_1)$ which are zeros of $(x_1 - \omega)$, for $\omega \in \Omega$, are completely splitting in the tower $\mathcal{F}$ over $\mathbb{F}_{q^3}$. Much harder here is to show that the genus $\gamma(\mathcal{F})$ is given by

$$\gamma(\mathcal{F}) = \frac{q}{q-1} \cdot \frac{q+2}{2}.$$

The limit $\lambda(\mathcal{F})$ then satisfies:

$$\lambda(\mathcal{F}) \geqslant \frac{t(\mathcal{F})}{\gamma(\mathcal{F})} = \frac{q(q+1)}{\frac{q}{q-1} \cdot \frac{q+2}{2}} = \frac{2(q^2-1)}{q+2}.$$

In fact we will show in Section 5 below that the limit of the tower $\mathcal{F}$ is equal to $\lambda(\mathcal{F}) = 2(q^2-1)/(q+2)$. This tower $\mathcal{F}$ over $\mathbb{F}_{q^3}$ gives in particular a generalization of a theorem of T. Zink (see [**18**]) for non-prime values of q (see also Example 2.7).

4. Graphs and recursive towers

Suppose we are given a tower $\mathcal{F}$ of function fields recursively given by the polynomial $f(X,Y)$. Throughout this and the following section we will assume that $\deg_X f(X,Y) = \deg_Y f(X,Y)$, which is not a real restriction according to the remark before Example 2.1. In this section we will associate to an absolutely irreducible polynomial $f(X,Y) \in \mathbb{F}_q[X,Y]$ a combinatorial object, a graph, that will be useful in the description of the places of the function fields in the tower $\mathcal{F}$. In particular the behaviour of completely splitting places will be clearer in many cases. For proofs of the results in Sections 4 and 5 we refer to [**1**].

We first give some standard facts and notations concerning graphs. For more information about graphs see for example [**4**]. We define a *directed graph* Γ to be a triple (V, A, e), where

i) V is a set of elements called *vertices*,
ii) A is a set of elements called *arcs*, and
iii) $e : A \to V \times V$ is a map.

Observe that in the literature a directed graph is sometimes defined as a tuple (V, A), with A a subset of $V \times V$. We will not use that definition here, since we want to allow multiple arcs from one vertex to another. For $a \in A$ write $e(a) = (v, w)$. We say that the arc a connects v with w, and that it starts at v and it ends in w. Note that the map e need not be injective, allowing the possibility of multiple arcs. With slight abuse of notation we say that (v, w) occurs as an arc in Γ if there exists an $a \in A$ such that $e(a) = (v, w)$.

If it is possible to write V as a disjoint union of non-empty sets V_1 and V_2 such that no arcs exist connecting a vertex in V_1 to a vertex in V_2 or vice versa, then we call the graph *decomposable*. The induced graphs with vertex sets V_1 and V_2 are called *components* of Γ. Any directed graph can be divided into indecomposable components.

Assume for the moment that the sets V and A are finite. We define the *in-degree* $\deg_{\mathrm{in}} v$ (resp. *out-degree* $\deg_{\mathrm{out}} v$) of a vertex v of the graph Γ to be the number of arcs of Γ ending in (resp. starting at) v. Given an ordering $v_1, v_2, \ldots, v_k$ of the vertex set, we define the *adjacency matrix* $M = (m_{ij})$ of the graph $\Gamma = (V, A, e)$ to be the $k \times k$ matrix given by:

$$m_{ij} := \text{ the number of arcs } a \in A \text{ with } e(a) = (v_i, v_j).$$

Any other ordering of the vertex set gives a matrix that differs from M only by a conjugation with a permutation matrix. We have the following elementary lemma connecting in- and out-degrees with the adjacency matrix.

Lemma 4.1. — *Let $\Gamma = (V, A, e)$ be a directed graph with $\#V = n < \infty$. Let M be the adjacency matrix of Γ with respect to some ordering $v_1, v_2, \ldots, v_k$ of the vertices. Then for all $1 \leqslant i \leqslant k$ we have*

$$\deg_{\mathrm{out}} v_i = \sum_{j=1}^{k} m_{ij} \quad \textit{and} \quad \deg_{\mathrm{in}} v_i = \sum_{j=1}^{k} m_{ji}.$$

Now we come to the definition of the graphs we will use in connection to the theory of recursive towers. Let $f(X,Y) \in \mathbb{F}_q[X,Y]$ be an absolutely irreducible polynomial. We denote by $\overline{\mathbb{F}}_q$ the algebraic closure of $\mathbb{F}_q$ and by $\mathbb{F}$ a field satisfying $\mathbb{F}_q \subset \mathbb{F} \subset \overline{\mathbb{F}}_q$. Denote by $\mathbb{F}(x,y)$ the function field defined by $f(x,y) = 0$ and let $g \in \mathbb{F}(x,y)$ be a function and R an $\mathbb{F}$-rational place of $\mathbb{F}(x,y)$. If the function g does not have a pole at the place R, we denote as usual by $g(R)$ the *evaluation* of g in R (i.e. the unique element α of $\mathbb{F}$ such that $g \equiv \alpha \pmod{R}$). If the function g has a pole at the place R we define $g(R) := \infty$.

Definition 4.2. — We define the graph

$$\Gamma(f, \mathbb{F}) := (V, A, e)$$

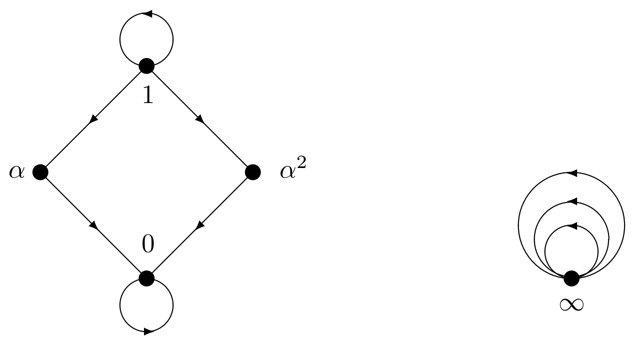
as follows:

$$\begin{aligned} V &:= \mathbb{F} \cup \{\infty\}, \\ A &:= \mathbb{P}_{\mathbb{F}}(\mathbb{F}(x,y)), \text{ and} \\ e(R) &= (x(R), y(R)), \text{ for } R \in \mathbb{P}_{\mathbb{F}}(\mathbb{F}(x,y)). \end{aligned}$$

Here $\mathbb{P}_{\mathbb{F}}(\mathbb{F}(x,y))$ denotes the set of $\mathbb{F}$-rational places of the function field $\mathbb{F}(x,y)$. Of course the sets V and A in the above definition depend on $\mathbb{F}$ and on $f(X,Y)$. If we want to make this explicit we will write $V(f,\mathbb{F})$ (resp. $A(f,\mathbb{F})$) instead of V (resp. A). Note that the number of arcs of the graph $\Gamma(f,\mathbb{F})$ is by definition the same as the number of $\mathbb{F}$-rational places of the function field $\mathbb{F}(x,y)$, while the number of vertices equals the number of $\mathbb{F}$-rational places of the rational function field $\mathbb{F}(x)$.

For α and β in $\mathbb{F}$, the tuple (α, β) occurs as an arc in the graph $\Gamma(f,\mathbb{F})$ only if $f(\alpha,\beta) = 0$. The converse implication need not be true, as can be seen by taking for example $f(X,Y)=X^3+X^2+XY+Y^2$ over the field $\mathbb{F}_2$. In this case $f(0,0)=0$, but there does not exist an arc in the graph $\Gamma(f,\mathbb{F}_2)$ connecting 0 to 0. Such an arc only appears if we extend the constant field to $\mathbb{F}_4$. The reason for this behaviour is that $(0,0)$ is a singular point of the curve defined by $f(X,Y)=0$. If $\mathbb{F}=\overline{\mathbb{F}}_q$, we have $f(\alpha,\beta)=0$ if and only if there exists a place $R\in\mathbb{P}_{\mathbb{F}}(\mathbb{F}(x,y))$ such that $(x(R),y(R))=(\alpha,\beta)$. If the curve given by $f(X,Y)=0$ is nonsingular, then this provides a bijection between arcs of $\Gamma(f,\mathbb{F})$ and places $R\in\mathbb{P}_{\mathbb{F}}(\mathbb{F}(x,y))$.

Example 4.3. — In this example we consider the absolutely irreducible polynomial $Y^3+(X+1)^3+1\in\mathbb{F}_4[X,Y]$ (see also Example 2.1). We write $\mathbb{F}_4=\mathbb{F}_2(\alpha)$, with $\alpha^2=\alpha+1$. After some calculations we find that the graph $\Gamma(f,\mathbb{F}_4)$ looks as follows:



Using the ordering $1,\alpha,\alpha^2,0,\infty$ of the vertices, we find that the adjacency matrix M of $\Gamma(f,\mathbb{F}_4)$ is given by:

$$M=\begin{pmatrix}1&1&1&0&0\\0&0&0&1&0\\0&0&0&1&0\\0&0&0&1&0\\0&0&0&0&3\end{pmatrix}.$$

We define a *path of length* n in a graph $\Gamma=(V,A,e)$ to be a sequence of arcs $a_1,a_2,\dots,a_n$ such that for all $1\leqslant i\leqslant n-1$ the second coordinate of $e(a_i)$ is equal to the first coordinate of $e(a_{i+1})$. Corresponding to such a path, we have the *sequence of visited vertices* $v_1,v_2,\dots,v_{n+1}$; *i.e.*, $e(a_i)=(v_i,v_{i+1})$. We also say that $a_1,a_2,\dots,a_n$ is a path from vertex v_1 to vertex v_{n+1}.

Now we consider a path $a_1,a_2,\dots,a_n$ of length n in the graph $\Gamma(f,\mathbb{F})$ considered above. An arc a_i in this graph is by definition an $\mathbb{F}$-rational place of the function field $\mathbb{F}(x,y)$ (where $f(x,y)=0$). The fact that $a_1,a_2,\dots,a_n$ is a path in this graph implies that $y(a_i)=x(a_{i+1})$ for $1\leqslant i\leqslant n-1$. Therefore we have for the sequence of visited vertices $v_1,v_2,\dots,v_{n+1}$:

$$f(v_i,v_{i+1})=0,\ \text{for } 1\leqslant i\leqslant n,$$

where we do allow the possibility that v_j is infinity for some values of j. In this sense a path in the graph $\Gamma(f,\mathbb{F})$ gives rise to a solution over $\mathbb{F}$ of the above system of equations. Note that different paths may yield the same solution and that, conversely, any solution with coefficients in $\overline{\mathbb{F}}_q \cup \{\infty\}$ can be found by considering an appropriate path in the graph $\Gamma(f,\overline{\mathbb{F}}_q)$.

Now we return to a tower $\mathcal{F}$ over $\mathbb{F}_q$ recursively defined by a polynomial $f(X,Y) \in \mathbb{F}_q[X,Y]$. The function field F_n can be described as $\mathbb{F}_q(x_1, x_2, \ldots, x_n)$ with the relations $f(x_i, x_{i+1}) = 0$, for $1 \leqslant i \leqslant n-1$. An $\mathbb{F}_q$-rational place P of the function field F_n therefore gives rise to a path of length $n-1$ in the graph $\Gamma(f,\mathbb{F}_q)$. The corresponding sequence of visited vertices is $x_1(P), \ldots, x_n(P)$. The number of paths of length $n-1$ in the graph therefore gives some information on the number of $\mathbb{F}_q$-rational places of the function field F_n. We will now give some facts about paths in graphs. The following lemma is well-known in graph theory (see [**4**]).

Lemma 4.4. — *Let $\Gamma = (V, A, e)$ be a directed graph and suppose that the sets A and V are finite. Let M be the adjacency matrix of Γ for some ordering of the vertices. Then the number of paths from vertex v_i to vertex v_j of length n is equal to the ij-th element of the matrix M^n.*

It is also well-known that given a square matrix M with entries in $\mathbb{C}$, the growth of the entries of the matrix M^n depends on the largest eigenvalue of M. Therefore we define

$$\sigma(M) := \max\{|\lambda| \ ; \ \lambda \in \mathbb{C} \text{ is an eigenvalue of } M\}.$$

This number is also called the *spectral radius* of the matrix M. We have the following lemma.

Lemma 4.5. — *Let M be a square matrix with entries in $\mathbb{C}$ and denote by $m_{ij}(n)$ the ij-th entry of the matrix M^n. Then for any $\varepsilon > 0$ we have*

$$\lim_{n\to\infty} \frac{|m_{ij}(n)|}{(\sigma(M)+\varepsilon)^n} = 0.$$

The above lemma follows for example quite easily using the Jordan normal form of a matrix. If M is the adjacency matrix of a graph Γ with finite vertex set and with finite arc set, and M' the adjacency matrix of the graph corresponding to a different choice of the ordering of the vertex set, we have $\sigma(M) = \sigma(M')$. Therefore it makes sense to speak of $\sigma(\Gamma)$, the *spectral radius of the graph* Γ. We have the following proposition:

Proposition 4.6. — *Let Γ be a graph with finite arc and vertex set. Then for any $\varepsilon > 0$ we have:*

$$\lim_{n\to\infty} \frac{\#\{\textit{paths in } \Gamma \textit{ of length } n\}}{(\sigma(\Gamma)+\varepsilon)^n} = 0.$$

We can sharpen the above proposition for the graphs $\Gamma(f,\mathbb{F})$, since for any vertex v of such a graph we have $\deg_{\mathrm{out}} v \leqslant \deg_Y f(X,Y)$ and $\deg_{\mathrm{in}} v \leqslant \deg_X f(X,Y)$. Recall that we always assume $\deg_X f(X,Y) = \deg_Y f(X,Y)$. For graphs with this property we have the following proposition:

Proposition 4.7. — *Let $\Gamma = (V, A, e)$ be an indecomposable directed graph with finitely many vertices and arcs. Suppose that there exists a natural number m such that all out-degrees are less than or equal to m. Then we have*

$$\sigma(\Gamma) \leqslant m.$$

If $\sigma(\Gamma) = m$ and all in- and out-degrees are bounded from above by m, then all in- and out-degrees are equal to m.

The two propositions above imply the following corollary.

Corollary 4.8. — *Let $f(X,Y) \in \mathbb{F}_q[X,Y]$ be an absolutely irreducible polynomial such that $m := \deg_X f(X,Y) = \deg_Y f(X,Y)$. Then we have*

$$\lim_{n\to\infty} \frac{\#\{\text{paths of length } n \text{ in } \Gamma(f,\mathbb{F}_q)\}}{m^n} > 0$$

if and only if there exists an indecomposable component Δ of $\Gamma(f,\mathbb{F}_q)$ whose vertices all have in- and out-degree equal to m.

A graph Δ as in the corollary above has the property that it is a finite indecomposable component of the graph $\Gamma(f,\overline{\mathbb{F}}_q)$, since the number of arcs that occur in Δ is the maximal possible number.

Using the above results, we can prove a partial answer to Conjecture 1 (see end of Section 2). We need some preliminaries. Consider a tower $\mathcal{F}$ recursively defined over the field $\mathbb{F}_q$ by the polynomial $f(X,Y)$. We can extend the constant field to $\overline{\mathbb{F}}_q$. After doing so we can interpret the ramification locus $V(\mathcal{F})$ as a subset of $\overline{\mathbb{F}}_q \cup \{\infty\}$, hence as a subset of the vertex set of the graph $\Gamma(f,\overline{\mathbb{F}}_q)$. In the same way we can interpret the ramification locus $V(\mathcal{G})$ of the dual tower $\mathcal{G}$ given by the polynomial $f(Y,X)$ (also see [**3**]), as a subset of the vertex set of the graph $\Gamma(f,\overline{\mathbb{F}}_q)$.

We denote by $W(\mathcal{F})$ the vertex set of the smallest component Δ of $\Gamma(f,\overline{\mathbb{F}}_q)$ whose vertex set contains $V(\mathcal{F}) \cup V(\mathcal{G})$. In other words: any indecomposable component of the graph Δ has at least one element of $V(\mathcal{F})$ or $V(\mathcal{G})$ among its vertices. The set $W(\mathcal{F}) \subset \overline{\mathbb{F}}_q \cup \{\infty\}$ can be interpreted as a set of places of the function field $\overline{\mathbb{F}}_q(x_1)$. One associates to $\alpha \in W(\mathcal{F})$ the place that is the unique zero of the function $x_1 - \alpha$ if $\alpha \neq \infty$ and the unique pole of x_1 if $\alpha = \infty$. It is easy to see that the set of places we have obtained in this way can be reinterpreted as a set of (possibly non-rational) places of the function field $F_1 = \mathbb{F}_q(x_1)$. Hence we may view $W(\mathcal{F})$ as a set of places of F_1.

Definition 4.9. — Let $\mathcal{F}$ be a tower over the field $\mathbb{F}_q$, then we define

$$\rho(\mathcal{F}) := \lim_{n\to\infty} \frac{\#\{\mathbb{F}_q\text{-rational places } P \text{ of } F_n \text{ above } W(\mathcal{F})\}}{[F_n : F_1]}.$$

Using these concepts we obtain a partial answer to Conjecture 1:

Theorem 4.10. — *Let $\mathcal{F} = (F_1, F_2, \dots)$ be a tower over $\mathbb{F}_q$ recursively given by a polynomial $f(X,Y)$. Suppose that $\rho(\mathcal{F}) = 0$. Then $t(\mathcal{F}) = \nu(\mathcal{F})$.*

Proof. — As usual we define $m := \deg_X f = \deg_Y f$. Further we denote by $\overline{\mathcal{F}} = (\overline{F}_1, \overline{F}_2, \dots)$ the tower of function fields obtained from $\mathcal{F}$ by extending the constant field of the tower to $\overline{\mathbb{F}}_q$. We first consider the graph $\Gamma(f, \overline{\mathbb{F}}_q)$. Recall that vertices of this graph are elements of $\overline{\mathbb{F}}_q \cup \{\infty\}$ and that arcs in this graph are places of the function field $\overline{\mathbb{F}}_q(x,y)$ where $f(x,y) = 0$. Also recall that any place of the function field $\overline{F}_{n+1}$ gives rise to a path of length n, namely the path $P \cap \overline{\mathbb{F}}_q(x_1,x_2), P \cap \overline{\mathbb{F}}_q(x_2,x_3), \dots, P \cap \overline{\mathbb{F}}_q(x_n,x_{n+1})$. We implicitly assume the relations $f(x_i, x_{i+1}) = 0$ for all $1 \leqslant i \leqslant n$. Conversely given a path $a_1, \dots, a_n$ of length n in the graph $\Gamma(f, \overline{\mathbb{F}}_q)$ we can construct at least one place P of $\overline{F}_{n+1}$ such that $P \cap \overline{\mathbb{F}}_q(x_i, x_{i+1}) = a_i$ for all $1 \leqslant i \leqslant n$ (this follows for example inductively from [**17**, Lemma 2.1.3]).

Now suppose we work in a component Δ of $\Gamma(f, \overline{\mathbb{F}}_q)$ such that any vertex v of Δ has in- and out-degree m. A necessary and sufficient condition for this property is that the vertex set of Δ is disjoint from the set $W(\overline{\mathcal{F}})$. Clearly the number of paths of length n starting in a vertex α is m^n. Conversely, the number of places of $\overline{F}_{n+1}$ lying above the place P_1 of $\overline{F}_1$ defined by $x_1 = \alpha$ is also m^n. We see that paths of length n in Δ correspond bijectively to places P of $\overline{F}_{n+1}$ such that $x_1(P)$ is a vertex of Δ. Moreover one can show that such a place P is $\mathbb{F}_q$-rational if and only if its corresponding path in Δ is defined over $\mathbb{F}_q$ (*i.e.*, all arcs $P \cap \overline{\mathbb{F}}_q(x_i, x_{i+1})$ are $\mathbb{F}_q$-rational). This means that there is a bijective correspondence between $\mathbb{F}_q$-rational places P of F_{n+1} such that $x_1(P)$ is a vertex of Δ and paths of length n in the graph $\Delta \cap \Gamma(f, \mathbb{F}_q)$ (*i.e.*, the subgraph of Δ consisting of all vertices and arcs of Δ defined over $\mathbb{F}_q$).

We are now ready to prove the theorem. By the above observations, we can count the number of $\mathbb{F}_q$-rational places of F_{n+1} not lying above $W(\mathcal{F})$ by counting suitable paths of length n in the graph $\Gamma(f, \mathbb{F}_q)$. On the other hand, since we assumed $\rho(\mathcal{F}) = 0$, the amount of $\mathbb{F}_q$-rational places lying above $W(\mathcal{F})$ do not contribute to $\nu(\mathcal{F})$ asymptotically. If $\nu(\mathcal{F}) = 0$, there is nothing to prove. Hence from now on we suppose that $\nu(\mathcal{F}) > 0$. By Corollary 4.8, we conclude that $\nu(\mathcal{F}) > 0$ if and only if there exists a component of $\Gamma(f, \mathbb{F}_q)$ with all in- and out-degrees equal to m. More precisely, writing Δ for the maximal component of $\Gamma(f, \mathbb{F}_q)$ with the property that any vertex of Δ has in- and out-degree equal to m, we have $\nu(\mathcal{F}) = \#$ vertices of Δ.

But it is then clear that any place P_1 of the function field F_1 with $x_1(P)$ a vertex of Δ is completely splitting, *i.e.*, we have $\nu(\mathcal{F}) = t(\mathcal{F})$. □

5. The functional equation

From now on we assume that the recursive tower $\mathcal{F}$ over $\mathbb{F}_q$ can be defined by an equation of the form:

$$\varphi(Y) = \psi(X), \text{ with } \varphi(t) \text{ and } \psi(t) \in \mathbb{F}_q(t) \text{ rational functions.}$$

We still assume that the equation is balanced; *i.e.*, $\deg \varphi(t) = \deg \psi(t)$. This condition can now also be expressed as:

$$[\mathbb{F}_q(t) : \mathbb{F}_q(\varphi(t))] = [\mathbb{F}_q(t) : \mathbb{F}_q(\psi(t))].$$

We will reformulate the results of the previous section for this special case. We write

$$\varphi(t) = \frac{\varphi_1(t)}{\varphi_2(t)}, \text{ with } \varphi_1(t) \text{ and } \varphi_2(t) \in \mathbb{F}_q[t] \text{ relatively prime polynomials.}$$

Similarly we write

$$\psi(t) = \frac{\psi_1(t)}{\psi_2(t)}, \text{ with } \psi_1(t) \text{ and } \psi_2(t) \in \mathbb{F}_q[t] \text{ relatively prime polynomials.}$$

We saw in Section 4 that finite components of the graph $\Gamma(f, \overline{\mathbb{F}}_q)$ are interesting, particularly when all in- and out-degrees are maximal. We have the following lemma.

Lemma 5.1. — *Let $f(X,Y) = \psi_2(X)\varphi_1(Y) - \psi_1(X)\varphi_2(Y) \in \mathbb{F}_q[X,Y]$ be an absolutely irreducible polynomial such that $\deg_X f(X,Y) = \deg_Y f(X,Y) =: m$. Let Δ be a component of the graph $\Gamma(f, \mathbb{F}_q)$ and suppose that any vertex of Δ has in- and out-degree equal to m. Then there exists a homogeneous polynomial $H(t,s) \in \mathbb{F}_q[t,s]$ and a non-zero constant c such that the following functional equation is satisfied:*

$$H(\varphi_1(T), \varphi_2(T)) = c \cdot H(\psi_1(T), \psi_2(T)).$$

More specifically, writing S for the vertex set of Δ and setting $\varphi(t) := \varphi_1(t)/\varphi_2(t)$, one can choose

$$H(t,s) := \prod_{\alpha \in S} (t - \varphi(\alpha)s),$$

with the convention that $(t - \infty s) := s$.

We call a homogeneous polynomial $H(t,s)$ satisfying the equation in the above lemma, a *solution of the functional equation for $\varphi(t)$ and $\psi(t)$*.

Now suppose we are given a tower $\mathcal{F}$ over $\mathbb{F}_q$ defined by the equation $\varphi(Y) = \psi(X)$ as above and write $f(X,Y) = \psi_2(X)\varphi_1(Y) - \psi_1(X)\varphi_2(Y)$. The significance of components Δ of the graph $\Gamma(f, \mathbb{F}_q)$ satisfying the assumptions of Lemma 5.1 has also become apparent in the proof of Theorem 4.10; in fact, if one can find such a component, then $t(\mathcal{F}) > 0$ (and hence $\nu(\mathcal{F}) > 0$). More general, suppose that there exists a finite component Δ of the graph $\Gamma(f, \overline{\mathbb{F}}_q)$ such that any vertex has maximal in- and out-degree. Denote by $\mathbb{F}$ the smallest extension of $\mathbb{F}_q$ over which all vertices and arcs of Δ are defined, and denote by $\mathcal{F}'$ the tower of function fields obtained from $\mathcal{F}$ by extending the constant field to $\mathbb{F}$. Then we have $t(\mathcal{F}') > 0$.

We have seen that if a tower over $\mathbb{F}_q$ recursively defined by $f(X,Y) = 0$, satisfies $\rho(\mathcal{F}) = 0$ and $\nu(\mathcal{F}) > 0$, then the graph $\Gamma(f, \mathbb{F}_q)$ will have a finite component with maximal in- and out-degrees. If the polynomial $f(X,Y)$ has the special form as in Lemma 5.1, we will find a solution of the functional equation. We will now give some examples.

Example 5.2. — Consider, as in Example 2.2, the tower $\mathcal{F}$ over $\mathbb{F}_{q^2}$ defined recursively by the equation

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

and define $f(X,Y) := (X^{q-1}+1)(Y^q+Y) - X^q$. One can check that the graph $\Gamma(f, \overline{\mathbb{F}}_{q^2})$ has a finite component satisfying the conditions of Lemma 5.1 with vertex set $S = \{\alpha \in \mathbb{F}_{q^2}\ ;\ \alpha^q + \alpha \neq 0\}$. In this case the polynomial $H(t,s)$ mentioned in Lemma 5.1 is

$$\prod_{\alpha \in S} (t - (\alpha^q + \alpha)s) = \left(t^{q-1} - s^{q-1}\right)^q.$$

In this case one can check Lemma 5.1 directly by showing

$$(T^q + T)^{q-1} - 1 = (T^q)^{q-1} - (T^{q-1}+1)^{q-1},$$

i.e., we can also choose $t^{q-1} - s^{q-1}$ as a solution.

In general if a homogeneous polynomial $H(t,s)$ is a solution of the functional equation mentioned in Lemma 5.1 for certain $\varphi(t)$ and $\psi(t)$, and one can write $H(t,s) = H_1(t,s)^a$, then $H_1(t,s)$ is also a solution of the functional equation for the same rational functions. There are other, similar properties. For example, if $H_1(t,s)$ and $H_2(t,s)$ are two solutions of the functional equation for $\varphi(t)$ and $\psi(t)$, then their product is also a solution. Conversely, if $H_1(t,s)$ and $H_2(t,s)$ are solutions and $H_1(t,s)$ is a multiple of $H_2(t,s)$, then $H_1(t,s)/H_2(t,s)$ is also a solution. Finally note that trivially a constant polynomial is always a solution.

We give another example to illustrate that the solutions predicted by Lemma 5.1 can be highly non-trivial.

Example 5.3. — We now return to the tower $\mathcal{F}$ defined over $\mathbb{F}_{p^2}$ mentioned in Example 2.4. In this case we have

$$\varphi(t) = t^2 \text{ and } \psi(t) = \frac{t^2+1}{2t}.$$

It is not hard to check that $\rho(\mathcal{F}) = 0$ for this tower. Since we know that $\nu(\mathcal{F}) > 0$, this means that there exists a solution of the functional equation for $\varphi(t)$ and $\psi(t)$.

This solution involves Deuring's polynomial $H(t)$. A non-trivial result in [**11**] is the following equality:

$$H(T^4) \equiv T^{p-1} H\Big(\Big(\frac{T^2+1}{2T}\Big)^2\Big) \pmod p.$$

We can interpret this equation as a solution to the functional equation for t^2 and $(t^2+1)/2t$. Indeed, define $H_1(t,s) \equiv s^{p-1} H(t^2/s^2) \pmod p$. Then $H_1(t,s) \in \mathbb{F}_p[t,s]$ is a homogeneous polynomial of total degree $p-1$. The above equation immediately implies

$$H_1(T^2, 1) = H_1(T^2+1, 2T),$$

and indeed there exists a non-trivial solution of the functional equation for t^2 and $(t^2+1)/2t$.

The point of formulating matters in terms of a functional equation, is that one can sometimes prove a uniqueness result. We illustrate this with the following proposition.

Proposition 5.4. — *Let $\varphi(t) \in \mathbb{F}_q[t]$ be a monic polynomial of degree m and $\psi(t) \in \mathbb{F}_q(t)$ be a rational function such that*

$$\psi(t) = \frac{\psi_1(t)}{\psi_2(t)},$$

with $\psi_1(t), \psi_2(t) \in \mathbb{F}_q[t]$ relatively prime polynomials satisfying

1) *the polynomial $\psi_1(t)$ is monic and $\deg \psi_1(t) = m$,*
2) $0 < \deg \psi_2(t) < m$.

Then there exists a homogeneous polynomial $H(t,s) \in \mathbb{F}_q[t,s]$ such that for any solution $H_1(t,s) \in \overline{\mathbb{F}}_q[t,s]$ of the functional equation for $\varphi(t)$ and $\psi(t)$ there exist $a \in \overline{\mathbb{F}}_q$ and $n \in \mathbb{N}$ with $H_1(t,s) = a \cdot H(t,s)^n$.

In other words the above proposition states that there exists essentially only one solution of the functional equation for $\varphi(t)$ and $\psi(t)$ if the assumptions of Proposition 5.4 hold. We give an example to illustrate the use of Proposition 5.4.

Example 5.5. — We consider again the tower $\mathcal{F}$ over $\mathbb{F}_{q^3}$ in Example 3.2 given by the equation

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

We have seen that for this tower we have

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

We will show that equality holds.

Using results in [**6**] one can show that $\rho(\mathcal{F}) = 0$ for this tower. As we have seen in Theorem 4.10 this implies $t(\mathcal{F}) = \nu(\mathcal{F})$. Moreover, we have seen that the completely splitting places in the tower $\mathcal{F}$ are described by solutions of the functional equation for $\varphi(t) := (1-t)/t^q$ and $\psi(t) := (t^q+t-1)/t$. If we could show as in Proposition 5.4 that essentially only one solution $H(t,s)$ exists, we would be done. All possible completely splitting places P_ω of F_1 (*i.e.*, P_ω is defined as the zero of $x_1-\omega$) would then be given by $H(\omega^q+\omega-1,\omega)=0$. As it is, we cannot apply the proposition directly. However, we can rewrite the defining equation of the tower $\mathcal{F}$. Define $V:=1/X$ and $W:=1/Y$. From the defining equation of the tower we obtain

$$W^q-W^{q-1}=\frac{V^q-V^{q-1}-1}{-V^{q-1}}.$$

Hence we can apply Proposition 5.4 with

$$\varphi(t)=t^q-t^{q-1}\quad\text{and}\quad\psi(t)=(t^q-t^{q-1}-1)/(-t^{q-1}).$$

We find that for these $\varphi(t)$ and $\psi(t)$ there is essentially only one solution of the functional equation. One can check that this solution can be chosen to be $H(t,s)=t^{q+1}-t\cdot s^q+s^{q+1}$. In particular we conclude

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

As another illustration of the use of Proposition 5.4, we discuss the following problem stated in [**11**].

Given $\alpha\in\mathbb{F}_{p^2}$ such that $H(\alpha^4)=0$, with $H(t)$ Deuring's polynomial in characteristic p. It is proved in [**11**] that all roots of $H(t^4)$ lie in $\mathbb{F}_{p^2}$. We have remarked in Examples 2.4 and 5.3 that any $\beta\in\mathbb{F}_{p^2}$ such that $\beta^2=(\alpha^2+1)/2\alpha$ is again a root of the polynomial $H(t^4)$. Of course, we can obtain more roots of $H(t^4)$ by iterating this procedure. A natural question is to ask if in this way one can obtain all roots of $H(t^4)$. For convenience, we define $f(X,Y):=2XY^2-(X^2+1)$ and $\Gamma:=\Gamma(f,\overline{\mathbb{F}}_{p^2})$ for the remainder of this section.

Reformulated in graph theoretical means, this question is equivalent to: What vertices of the graph Γ can we reach with paths in Γ starting at the vertex α?

We know (see Example 5.3 and the remarks preceding Example 5.2) that the graph Γ has a component Δ with vertex set $\{\beta\in\mathbb{F}_{p^2}\ ;\ H(\beta^4)=0\}$ and that any vertex of Δ has in- and out-degree 2. Hence by Lemma 5.1 , any indecomposable component of Δ gives a solution of the functional equation for t^2 and $(t^2+1)/2t$. However, by Proposition 5.4, there exists essentially only one solution, which implies that Δ is indecomposable. In general one can show that in an indecomposable graph with all in- and out-degrees equal to a number m, one can reach any vertex with paths starting in a certain fixed vertex. Hence the answer to the above question is affirmative.

References

[1] P. Beelen – Graphs and recursively defined towers of function fields, *J. Number Theory* **108** (2004), p. 217–240.

[2] P. Beelen, A. Garcia & H. Stichtenoth – On towers of function fields of Artin-Schreier type, *Bulletin Braz. Math. Soc. (N.S.)* **35** (2004), p. 151–164.

[3] ______, On ramification and genus of recursive towers, *Portugal. Math.* (to appear).

[4] C. Berge – *Graphs*, 2nd ed., North-Holland, Amsterdam, 1985.

[5] J. Bezerra & A. Garcia – A tower with non-Galois steps which attains the Drinfeld-Vladut bound, *J. Number Theory* **106** (2004), p. 142–54.

[6] J. Bezerra, A. Garcia & H. Stichtenoth – An explicit tower of function fields over cubic finite fields and Zink's lower bound for $A(q^3)$, *J. reine angew. Math.* (to appear).

[7] V.G. Drinfeld & S.G. Vladut – The number of points of an algebraic curve, *Func. Anal.* **17** (1983), p. 53–54.

[8] I.M. Duursma, B. Poonen & M. Zieve – Everywhere ramified towers of global function fields, in *International Conference on Finite Fields and Applications, 2003* (G.L. Mullen, A. Poli & H. Stichtenoth, eds.), Lecture Notes in Computer Science, vol. 2948, Springer, 2004, p. 148–153.

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

[10] ______, Skew pyramids of function fields are asymptotically bad, in *Coding Theory, Cryptography and Related Areas* (J. Buchmann, T. Høholdt, H. Stichtenoth & H. Tapia-Recillas, eds.), 2000, p. 111–113.

[11] ______, On tame towers over finite fields, *J. reine angew. Math.* **557** (2003), p. 53–80.

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

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

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

[15] 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), p. 21–28.

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

[17] J. Wulftange – Zahme Türme algebraischer Funktionenkörper, Ph.D. Thesis, Universität Essen, Essen, 2002.

[18] T. Zink – Degeneration of Shimura surfaces and a problem in coding theory, in *Fundamentals of Computation Theory*, Lecture Notes in Computer Science, vol. 199, Springer, Berlin, 1985, p. 503–511.

P. Beelen, Fachbereich Mathematik, Universität Duisburg-Essen, 45117 Essen, Germany • Current address: Department of Mathematics, Technical University of Denmark, Matematiktorvet, Building 303, DK-2800 Kongens Lyngby, Denmark • *E-mail :* `P.Beelen@mat.dtu.dk`

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

H. Stichtenoth, Fachbereich Mathematik, Universität Duisburg-Essen, 45117 Essen, Germany *E-mail :* `stichtenoth@uni-essen.de` • Sabanci University, MDBF, Orhanli, Tuzla, 34956 Istanbul, Turkey • *E-mail :* `henning@sabanciuniv.edu`