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

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