Explicit Constructions of Towers of Function Fields with Many Rational Places

Henning Stichtenoth

Abstract. We discuss several examples of function field towers $F_0 \subseteq F_1 \subseteq F_2 \subseteq \dots$ over a finite field $\mathbb{F}_l$, for which the limit (number of rational places of F_n)/(genus of F_n) is positive.

1. Introduction

We consider algebraic function fields (of one variable) $F/\mathbb{F}_l$ whose constant field is the finite field $\mathbb{F}_l$ of cardinality l. By $g(F)$ (resp. $N(F)$) we denote the genus (resp. the number of rational places, i.e. places of degree one) of $F/\mathbb{F}_l$. A tower of function fields over $\mathbb{F}_l$ is a sequence

$$\mathcal{F} = (F_0, F_1, F_2, \dots)$$

of function fields $F_i/\mathbb{F}_l$ with the following properties:

i) $F_0 \subseteq F_1 \subseteq F_2 \subseteq \dots$
ii) For each $n \geq 0$, the extension F_{n+1}/F_n is separable of degree $[F_{n+1} : F_n] > 1$.
iii) $g(F_j) \geq 2$, for some $j \geq 0$.

It is easily seen that $g(F_n) \to \infty$ for $n \to \infty$, and that the limit

$$\lambda(\mathcal{F}) := \lim_{n\to\infty} N(F_n)/g(F_n)$$

exists [5]. The Drinfeld-Vladut bound [1] gives an upper bound for $\lambda(\mathcal{F})$,

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

A tower $\mathcal{F}$ is said to be asymptotically good if $\lambda(\mathcal{F}) > 0$; it is asymptotically optimal if it attains the Drinfeld-Vladut bound $\lambda(\mathcal{F}) = \sqrt{l} - 1$. These notions are motivated by applications to coding theory: asymptotically good towers of function fields yield asymptotically good sequences of (algebraic geometric) codes over $\mathbb{F}_l$, see [9, 10].

In general, it is hard to find asymptotically good towers of function fields. A famous result of Ihara [7] and Tsfasman, Vladut and Zink states that certain (reductions of) modular towers are asymptotically optimal, for $l = q^2$ being a square.

As a consequence, there exist sequences of codes having excellent error-correcting properties: they improve the so-called Gilbert-Varshamov bound [10].

Another approach how to construct asymptotically good towers is the method of class field towers which was introduced by Serre [8]. Class field towers are, however, not explicit, and modular towers require deep results from algebraic geometry.

It is therefore desirable to give a more elementary construction of asymptotically good towers of function fields. In the following I will present some joint results with A. García.

2. The Method

We begin with some simple observations on the asymptotic behaviour of a tower of function fields.

Proposition 2.1. *A tower $\mathcal{F} = (F_0, F_1, F_2, \dots)$ of function fields $F_i/\mathbb{F}_l$ is asymptotically good if and only if there exists constants $c_1, c_2 > 0$ such that*

$$g(F_n) \le c_1 \cdot [F_n : F_0], \quad \text{and} \tag{A}$$

$$N(F_n) \ge c_2 \cdot [F_n : F_0] \tag{B}$$

hold for all $n \ge 0$.

Proof. Obviously conditions (A) and (B) imply that $\mathcal{F}$ is asymptotically good. Conversely we assume now that $\mathcal{F}$ is asymptotically good. For $n \ge j \ge 0$, the Hurwitz genus formula yields a relation between the genera $g(F_n)$ and $g(F_j)$

$$g(F_n) - 1 = [F_n : F_j] \cdot (g(F_j) - 1) + \frac{1}{2} \deg(\mathrm{Diff}(F_n/F_j)) \\ \ge [F_n : F_j] \cdot (g(F_j) - 1),$$

where $\mathrm{Diff}(F_n/F_j)$ denotes the different divisor of F_n/F_j. On the other hand, we have the trivial estimate

$$N(F_n) \le [F_n : F_0] \cdot N(F_0).$$

Conditions (A) and (B) follow easily from these two inequalities. □

The simplest way to ensure condition (B) is a follows:

Lemma 2.2. *Suppose that $\mathcal{S}$ is a non-empty set of rational places of F_0 such that any $P \in \mathcal{S}$ splits completely in all extensions F_n/F_0. Then*

$$N(F_n) \ge \#(\mathcal{S}) \cdot [F_n : F_0].$$

Condition (A) is more delicate: we need to know the behaviour of the degree $\deg(\mathrm{Diff}(F_n/F_0))$ of the different divisor of F_n/F_0. The following notion is useful: A place P of F_0 is said to be unramified in $\mathcal{F}$ if P is unramified in all extensions F_n/F_0; otherwise P is called ramified in $\mathcal{F}$. The set

$$V(\mathcal{F}) = \{P \mid P \text{ is a place of } F_0 \text{ which is ramified in } \mathcal{F}\}$$

is called the ramification locus of $\mathcal{F}$. For a place P of F_0 and a place Q_n of F_n lying above P, let $d(Q_n \mid P)$ be the different exponent of Q_n over P, and let

$$d_n(P) := \sum_{Q_n|P} d(Q_n \mid P) \cdot \deg Q_n.$$

Then we have

$$\deg(\mathrm{Diff}(F_n/F_0)) = \sum_{P \in V(\mathcal{F})} d_n(P).$$

Lemma 2.3. *Assume that the ramification locus $V(\mathcal{F})$ is finite, and that there exists a constant $c_3 \geq 0$ such that*

$$d_n(P) \leq c_3 \cdot [F_n : F_0] \tag{A$_1$}$$

for all $P \in V(\mathcal{F})$ and all $n \geq 0$. Then condition (A) *holds.*

Proof. This follows immediately from the Hurwitz genus formula. □

From here on we will consider towers $\mathcal{F} = (F_0, F_1, F_2, \dots)$ over $\mathbb{F}_l$ of the following specific form: There are two rational functions $f(Z), h(Z) \in \mathbb{F}_l(Z)$ of the same degree

$$\deg f(Z) = \deg h(Z) = m,$$

such that $F_n = \mathbb{F}_l(x_0, x_1, \dots, x_n)$ with

$$h(x_{n+1}) = f(x_n) \quad \text{and} \quad [F_{n+1} : F_n] = m \tag{$*$}$$

for all $n \geq 0$ (as usual, the degree of a rational function $f(Z) = f_0(Z)/f_1(Z)$ with relatively prime polynomials $f_0(Z), f_1(Z) \in \mathbb{F}_l[Z]$ is defined as $\deg f(Z) = \max\{\deg f_0(Z), \deg f_1(Z)\}$). Note that $F_0 = \mathbb{F}_l(x_0)$ is a rational function field, and $[F_n : F_0] = m^n$ for all $n \geq 0$.

We need a criterion whether the ramification locus of this tower is finite. Since ramification does not change in constant field extensions, we may replace $\mathbb{F}_l$ by its algebraic closure $\bar{\mathbb{F}}$ and the fields F_n by $\bar{F}_n := F_n \cdot \bar{\mathbb{F}}$, and we consider the tower $\bar{\mathcal{F}} = (\bar{F}_0, \bar{F}_1, \bar{F}_2, \dots)$ of function fields over $\bar{\mathbb{F}}$. For $\gamma \in \bar{\mathbb{F}} \cup \{\infty\}$ we denote by "$x_i = \gamma$" the unique place of the rational function field $\bar{\mathbb{F}}(x_i)$ which is a zero of $x_i - \gamma$ (resp. the pole of x_i if $\gamma = \infty$). Let

$$R_0 := \{\gamma \in \bar{\mathbb{F}} \cup \{\infty\} \mid x_0 = \gamma \text{ ramifies in } \bar{F}_1/\bar{F}_0\}.$$

This is a finite set since $\bar{F}_1/\bar{F}_0$ is separable.

Lemma 2.4. *Notations as above. Assume in addition that $R \subseteq \bar{\mathbb{F}} \cup \{\infty\}$ is a finite set which contains R_0 and has the following property:*

$$\gamma \in R \Rightarrow \textit{all roots of the equation } f(Z) = h(\gamma) \textit{ are in } R. \tag{A$_2$}$$

Then all places $x_0 = \alpha$ with $\alpha \notin R$ are unramified in $\bar{\mathcal{F}}$. In particular the ramification locus $V(\bar{\mathcal{F}})$ and, a forteriori, the ramification locus $V(\mathcal{F})$ are finite.

Proof. Suppose that $x_0 = \gamma \in \bar{\mathbb{F}} \cup \{\infty\}$ is ramified in $\bar{\mathcal{F}}$. Then there is some $n \geq 0$ and a place Q_n of $\bar{F}_n$ lying above $x_0 = \gamma$ which ramifies in the extension $\bar{F}_{n+1}/\bar{F}_n$. The restriction of Q_n to $\bar{\mathbb{F}}(x_n)$ is of the form $x_n = \alpha$ with $\alpha \in \bar{\mathbb{F}} \cup \{\infty\}$. Since Q_n ramifies in $\bar{F}_{n+1}/\bar{F}_n$, the place $x_n = \alpha$ ramifies in the extension $\bar{\mathbb{F}}(x_n, x_{n+1})/\bar{\mathbb{F}}(x_n)$, hence $\alpha \in R_0$. By condition (A_2) we conclude that $\gamma \in R$. □

We summarize: For a tower $\mathcal{F}$ as defined in $(*)$, the two conditions (A_1) and (A_2) imply condition (A).

3. Examples

In this section we describe some examples of towers of the form $(*)$ explicitly.

3.1. Tame towers

We say that a tower $\mathcal{F} = (F_0, F_1, F_2, \dots)$ over $\mathbb{F}_l$ is tame if for all $n \geq 0$ and all places Q_n of F_n, the ramification index $e(Q_n)$ in F_n/F_0 is relatively prime to the characteristic of $\mathbb{F}_l$. This implies that

$$d_n(P) \leq [F_n : F_0] \cdot \deg P$$

for all places P of F_0, i.e. condition (A_1) holds in tame towers.

Example 3.1. (See [6]) *Let $l = p^e$ with $e \geq 2$ and $m = (l-1)/(p-1)$. Consider the tower $\mathcal{F} = (F_0, F_1, F_2, \dots)$ with $F_n = \mathbb{F}_l(x_0, \dots, x_n)$ and*

$$x_{i+1}^m = 1 - (1 + x_i)^m \quad \textit{for} \quad 0 \leq i \leq n-1,$$

i.e. the functions $f(Z)$ resp. $h(Z)$ in $(*)$ are here

$$f(Z) = 1 - (1+Z)^m,\ h(Z) = Z^m.$$

This is a tame tower, and it is easily seen that the place $x_0 = \infty$ splits completely in $\mathcal{F}$. Condition (A_2) from Lemma 2.4 holds for $R := \mathbb{F}_l$, and we obtain

$$\lambda(\mathcal{F}) \geq \frac{2}{l-2} > 0.$$

For $l = 4$ the tower is optimal, i.e. $\lambda(\mathcal{F}) = \sqrt{l} - 1$.

Example 3.2. (See [6]) *Let $l = q^2 > 4$ be a square and $F_n = \mathbb{F}_l(x_0, \dots, x_n)$ with*

$$x_{i+1}^{q-1} = 1 - (1 + x_i)^{q-1} \quad \textit{for} \quad 0 \leq i \leq n-1.$$

Here again the pole of x_0 splits completely, and we can take $R := \mathbb{F}_q$ in this case. It follows that

$$\lambda(\mathcal{F}) \geq \frac{2}{q-2} > 0.$$

The tower is optimal for $l = 9$.

3.2. Wild towers

If some ramification index in the tower is divisible by the characteristic of $\mathbb{F}_l$, the tower $\mathcal{F}$ is said to be wild. In this case one does not have an obvious bound (A_1) for the different degrees.

Example 3.3. (See [5]) *Let $l = q^2$ be a square and $F_n = \mathbb{F}_l(x_0, \ldots, x_n)$ with*

$$x_{i+1}^q + x_{i+1} = \frac{x_i^q}{x_i^{q-1} + 1} \quad \text{for} \quad 0 \le i \le n-1,$$

i.e. $f(Z) = Z^q/(Z^{q-1}+1)$ and $h(Z) = Z^q + Z$. Condition (A_2) holds for $R = \{\gamma \in \mathbb{F}_l \mid \gamma^q + \gamma = 0\} \cup \{\infty\}$ (this is easily checked), and condition (A_1) holds with $c_3 = 2$ (this is non-trivial). All places $x_0 = \alpha$ with $\alpha \in \mathbb{F}_l \setminus R$ split completely in this tower, and we conclude that

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

Hence the tower is optimal: it attains the Drinfeld-Vladut bound $\sqrt{l} - 1$.

Example 3.4. (See [4]) *This example is similar to example 3.3. Again let $l = q^2$ be a square. Define $F_n = \mathbb{F}_l(x_0, \ldots, x_n)$ by*

$$x_{i+1}^q x_i^{q-1} + x_{i+1} = x_i^q \quad \text{for} \quad 0 \le i \le n-1.$$

Although this is not precisely of the form ($*$), one can determine ramification and rational places in an analogous manner. One obtains that $\lambda(\mathcal{F}) = q-1$, i.e. this tower is also optimal. It can be shown that example 3.3 is in fact a subtower of example 3.4 (see [5]).

For more information about the examples of this section see N. Elkies' paper [2] in this volume.

References

[1] V. G. Drinfeld and S. G. Vladut, *Number of points of an algebraic curve,* Functional Anal. Appl., **17** (1983), 53–54.

[2] N. Elkies, *Explicit towers of drinfeld modular curves*, this volume.

[3] G. van der Geer, *Curves over finite fields and codes*, this volume.

[4] A. García and H. Stichtenoth, *A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound,* Invent. Math., **121** (1995), 211–222.

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

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

[7] 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), 721–724.

[8] J. P. Serre, *Rational points on curves over finite fields,* Lecture Notes, Harvard University, 1985.

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

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

FB 6,
Mathematik und Informatik,
Universität GH Essen,
45117 Essen, Germany
E-mail address: stichtenoth@uni-essen.de