On tame towers of function fields and the Drinfeld-Vladut bound

Arnaldo Garcia

IMPA

Estrada Dona Catorina, 110 - Jardim Botanico

22.460–320, Rio de Janeiro-RJ

Brazil

1 Introduction

The interest on the set of solutions of algebraic equations with coefficients in a finite field $\mathbb{F}_q$ with q elements has a long history in mathematics. It is already present with the language of higher congruences in the work of Euler, Lagrange, Gauss, etc. (for the case in which q is a prime number). Nowadays we use the language of function fields over finite fields (and their rational places) or the language of curves over finite fields (and their rational points). In his thesis E. Artin [A] introduced a Zeta Function for the function field E of a hyperelliptic curve defined over a finite field $\mathbb{F}_q$ (in analogy with the one introduced by Dedekind for number fields) and, by assuming the validity of Riemann's hypothesis for this Zeta Function, he made a conjecture bounding the number of rational places $N(E)$ in terms of the cardinality q of the finite field and the genus $g(E)$ of the function field E. Artin's conjecture was

then proved by H. Hasse in the case $g(E) = 1$, and widely generalized by A. Weil that proved it for all function fields over $\mathbb{F}_q$ (not only for the ones coming from hyperelliptic curves). More recently Y. Ihara noticed that the bound for $N(E)$ in Weil's theorem could be improved if the genus $g(E)$ is large with respect to q, and he introduced a function $A(q)$ measuring the asymptotic behaviour of $\frac{N(E)}{g(E)}$ as $g(E) \to \infty$, when E varies over the function fields over $\mathbb{F}_q$. Using Shimura modular curves, Y. Ihara proved the inequality $A(q^2) \geq q - 1$, for any q. Soon after that (elaborating on ideas of Y. Ihara) V. Drinfeld and S. Vladut established the upper bound:

$$A(q) \leq \sqrt{q} - 1, \text{ for any } q.$$

Hence we have that $A(q^2) = q - 1$, for any q. For $q = p$ a prime number the equality $A(p^2) = p - 1$ was settled independently by M. Tsfasman, S. Vladut and T. Zink using elliptic modular curves and moreover, using Goppa's construction of linear codes from algebraic curves over finite fields, they were able to show the existence of sequences of codes with increasing length having limit parameters (transmission rate and relative distance) above the so-called asymptotic Gilbert-Varshamov bound, which caused a sensation among the coding theorists. This renewed the interest on explicit equations for modular curves, which have attracted interest at least since the classical works of F. Klein. The main objective here is to present a tame tower of function fields over $\mathbb{F}_{p^2}$ (p a prime number) with explicit and simple equations that attains the Drinfeld-Vladut upper bound, and also give an explicit description of its set of rational places over $\mathbb{F}_{p^2}$. Such a description is done in terms of Deuring's polynomial whose roots give the supersingular elliptic curves in Legendre's form. This was obtained in a joint work with H. Stichtenoth having an appendix by H.-G. Rück (see [GS3]). The modular

provenance of this tower is due to M. Zieve by comparison with an explicit modular tower worked out by N. Elkies.

2 Preliminaries

We denote by $\mathbb{F}_q(X)$ the rational function field (i.e., the field of fractions of the polynomial ring $\mathbb{F}_q[X]$ in one variable over the finite field $\mathbb{F}_q$). By a *function field E over $\mathbb{F}_q$* we mean a finite separable field extension E of $\mathbb{F}_q(X)$ such that $\mathbb{F}_q$ is algebraically closed in the field E. The following is a celebrated theorem of A. Weil:

THEOREM ([W]). *Let E be a function field over $\mathbb{F}_q$ and denote by $N(E)$ its number of $\mathbb{F}_q$-rational places, then*

$$N(E) \leq q + 1 + 2\sqrt{q} \cdot g(E),$$

where $g(E)$ denotes the genus of E. The theorem above was first proved by H. Hasse [H] in the case $g(E) = 1$. Function fields attaining the upper bound in this theorem are called *maximal* and for a survey on this topic we refer to [Ga] (see also [Ge]). Ihara [I] noticed that if $2g(E) > \sqrt{q}(\sqrt{q} - 1)$ then Weil's upper bound cannot be attained. To analyze the asymptotic behaviour of $N(E)$ as $g(E) \to \infty$ (for function fields E over a fixed finite field $\mathbb{F}_q$) he introduced:

$$N_q(g) = \max\{N(E) \mid g(E) = g\}$$

and

$$A(q) = \limsup_{g \to \infty} N_q(g)/g.$$

Using class field methods Serre [S] showed in particular that one has:

$$A(q) > 0, \quad \text{for any} \quad q.$$

The best known upper bound for the function $A(q)$ is due to Drinfeld-Vladut ([DV]):

$$A(q) \leq \sqrt{q} - 1, \quad \text{for any} \quad q.$$

When the cardinality of the finite field is a square the Drinfeld-Vladut bound is attained; i.e., $A(q^2) = q - 1$ holds for any q (see [I] and [TVZ]).

DEFINITION: A *tower over* $\mathbb{F}_q$ is an infinite sequence of function fields over $\mathbb{F}_q$

$$E_1 \subsetneqq E_2 \subsetneqq E_3 \subsetneqq \cdots \subsetneqq E_n \subsetneqq E_{n+1} \subsetneqq \ldots$$

such that: a) Each field extension $E_{n+1}|E_n$ is finite and separable. b) We have $g(E_n) \to \infty$ as $n \to \infty$.

Denoting by ξ a tower over $\mathbb{F}_q$ as above, one has that the following limit exists (see [GS2])

$$\lambda(\xi) = \lim_{n \to \infty} N(E_n)/g(E_n).$$

Of course one has

$$0 \leq \lambda(\xi) \leq A(q) \leq \sqrt{q} - 1.$$

The tower ξ is called *good* when $\lambda(\xi) > 0$ and *optimal* when $\lambda(\xi) = \sqrt{q} - 1$. The first explicit optimal tower (i.e., given by explicit equations and with an explicit description of its set of rational places) appeared in [GS1] and its Drinfeld modularity was proven by N. Elkies (see [E2]). In this first explicit optimal tower all ramifications in the tower are wild.

DEFINITON: A tower ξ over $\mathbb{F}_q$ is said to be *tame* when all ramifications in the tower are tame. For example, if each extension $E_{n+1}|E_n$ is Galois with extension degree $[E_{n+1} : E_n]$ not divisible by the characteristic p of the finite field $\mathbb{F}_q$, then ξ is a tame tower over $\mathbb{F}_q$. For a tame tower ξ over $\mathbb{F}_q$ we define:

$$S(\xi) = \{P \text{ place of } E_1 \mid P \text{ ramifies in } E_n, \text{ for some } n\}$$

and

$T(\xi) = \{P \text{ place of } E_1 \mid \text{ deg } P = 1 \text{ and } P \text{ splits completely in } E_n, \text{ for all } n\}$.

Tame towers ξ over $\mathbb{F}_q$ are especially interesting when they satisfy: a) The ramification set $S(\xi)$ is finite. b) The set of completely splitting places $T(\xi)$ is non-empty. Tame towers ξ over $\mathbb{F}_q$ satisfying a) and b) above are interesting since we have (see [GST])

$$\lambda(\xi) \geq \frac{2t}{2g(E_1) + s - 2},$$

where t denotes the cardinality of $T(\xi)$ and where s is defined by

$$s = \sum_{P \in S(\xi)} degP.$$

3 Some good and some optimal tame towers

All tame towers ξ over $\mathbb{F}_q$ that we consider here are such that each of the extensions $E_{n+1}|E_n$ is a Kummer extension. Moreover they are *recursive towers* in the sense of the following definition.

DEFINITON: Let $m > 1$ be a divisor of $(q-1)$ and let $\varphi(X) \in \mathbb{F}_q(X)$ be a rational function of degree m. Then we say that the tower ξ over $\mathbb{F}_q$ is *defined recursively by the equation*

$$Y^m = \varphi(X),$$

if one has that $[E_{n+1} : E_n] = m$ (for each $n \geq 1$) and moreover $E_1 = \mathbb{F}_q(X_1)$ and $E_{n+1} = E_n(X_{n+1})$ with

$$X_{n+1}^m = \varphi(X_n), \quad \text{for each} \quad n \geq 1.$$

EXAMPLE 1. Let $\mathbb{F}_q$ be a non-prime finite field of characteristc p (i.e., $q > p$) and let

$$m = q - 1/p - 1.$$

Let ξ_0 denote the tower over $\mathbb{F}_q$ defined recursively by the equation (see [GST]):

$$Y^m = \varphi(X), \quad \text{with} \quad \varphi(X) = 1 - (X+1)^m.$$

One can easily see that

$$S(\xi_0) = \mathbb{F}_q \quad \text{and} \quad t = \#T(\xi_0) = 1.$$

In fact, the only completely splitting place of degree 1 is the place at infinity of $E_1 = \mathbb{F}_q(X_1)$ and the ramified places of E_1 are the ones corresponding to $(X_1 - \alpha)$, with α running thru the elements of $\mathbb{F}_q$. We then conclude that

$$\lambda(\xi_0) \geq \frac{2t}{2g(E_1) + s - 2} = \frac{2}{q-2} > 0.$$

In particular this gives a simple proof of a result due to Serre:

$$A(q) > 0, \text{ for any non-prime } q.$$

Unfortunately we were not able to find an explicit recursive tower over $\mathbb{F}_p$ showing that $A(p) > 0$. Recently it was remarked by Lenstra (see [L]) that our more general construction (see [GST, Theorem 2.2]) does not apply to prime fields.

EXAMPLE 2. This is the main point of this paper. We consider now three recursive towers over $\mathbb{F}_{p^2}$, where p is an odd prime number (see [GS3] and [E1]):

The tower ξ_1 *Given recursively by the equation*

$$Y^2 = \varphi_1(X), \text{ with } \varphi_1(X) = \frac{(X+3)^2}{8(X+1)}.$$

The tower ξ_2 *Given recursively by the equation*

$$Y^2 = \varphi_2(X), \text{ with } \varphi_2(X) = \frac{(X+1)^2}{4X}.$$

The tower ξ *Given recursively by the equation*

$$Y^2 = \varphi(X), \text{ with } \varphi(X) = \frac{X^2+1}{2X}.$$

We stress again that all three towers above are considered here over the finite field $\mathbb{F}_{p^2}$, p being an odd prime. We will just indicate why this last tower ξ is optimal, that is

$$\lambda(\xi) = p - 1.$$

¿From the equality above it follows that the other two towers ξ_1 and ξ_2 are also optimal, since they are subtowers of ξ (see [GS2] and [GS3]). Denoting by β an element of $\mathbb{F}_{p^2}$ such that $\beta^2 = -1$, one can prove that the ramification set $S(\xi)$ has $s = 6$ elements, more precisely one has

$$S(\xi) = \{0, \infty, \pm 1, \pm\beta\}.$$

The optimality of the tower ξ will follow if we show that the cardinality of the completely splitting set $T(\xi)$ is

$$t = 2(p-1).$$

In fact we would then have

$$\lambda(\xi) \geq \frac{2t}{2g(E_1) + s - 2} = \frac{t}{2} = p - 1,$$

but also $\lambda(\xi) \leq p - 1$ as follows from the Drinfeld-Vladut bound. The proof that $t = 2(p-1)$ is the core of the matter and it envolves Deuring's polynomial $H(Z)$ whose roots give the supersingular elliptic curves in Legendre's form:

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

To complete the proof of the optimality of the tower ξ one then needs the following two new results about the polynomial $H(Z)$: 1) *Each root of* $H(Z)$ *is a fourth power in* $\mathbb{F}_{p^2}$. 2) *One has that the following polynomial identity holds*:

$$H(Z^4) = Z^{p-1} \cdot H\left(\left(\frac{Z^2+1}{2Z}\right)^2\right).$$

¿From these two results one then deduces that (see [GS3]):

$$T(\xi) = \{\alpha \in \mathbb{F}_{p^2} \mid H(\alpha^4) = 0\}.$$

References

[A] Artin, E. – *Quadratische Körper im Gebiet der höheren Kongruenzen*; Math. Z. **19** (1924), 153–246.

[DV] Drinfeld, V.; Vladut, S. – *Number of points of an algebraic curve*; Funct. Anal. **17** (1983), 53–54.

[E1] Elkies, N. – *Explicit modular towers*; Proc. 35th Annual Allerton Conference on Communication, Control and Computing held in Univ. Illinois at Urbana (1998), pp. 23–32.

[E2] Elkies, N. – *Explicit towers of Drinfeld modular curves*; to appear in Proc. 3rd European Congress of Math. held in Barcelona (2000).

[Ga] Garcia, A. – *Curves over finite fields attaining the Hasse-Weil upper bound*; to appear in Proc. 3rd European Congress of Math. held in Barcelona (2000).

[GS1] Garcia, A.; Stichtenoth, H. – *A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound*; Inventiones Math. **121** (1995), 211–222.

[GS2] Garcia, A.; Stichtenoth, H. – *On the asymptotic behaviour of some towers of function fields over finite fields*; J. Number Theory **61** (1996), 248–273.

[GS3] Garcia, A.; Stichtenoth, H. – *On tame towers over finite fields*; preprint (2000).

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

[Ge] van der Geer, G. – *Curves over finite fields and Codes*; to appear in Proc. 3rd European Congress of Math. held in Barcelona (2000).

[H] Hasse, H. – *Zur Theorie der abstrakten elliptischen Funktionenkörper*; J. Reine Angew. Math. **175** (1936), 69–88 and 193–208.

[I] Ihara, Y. – *Some remarks on the number of rational points of algebraic curves over finite fields*; J. Fac. Sci. Tokyo **28** (1981), 721–724.

[L] Lenstra, H.W. – *On a problem of Garcia, Stichtenoth and Thomas*; preprint (2000).

[S] Serre, J.-P. – *Sur le nombre des points rationnels d'une courbe algebrique sur un corps fini*; C.R. Acad. Sci. Paris **296** (1983), 397–402.

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

[W] Weil, A. – *Courbes algebriques et variétés abéliennes*; Herman, Paris (1971).