BULLETIN OF THE BRAZILIAN MATHEMATICAL SOCIETY

Bull Braz Math Soc, New Series 36(3), 393-401

A Class of Artin-Schreier Towers with Finite Genus

San Ling, Henning Stichtenoth and Siman Yang

Abstract. We study the asymptotic behaviour of the genus in some Artin-Schreier towers of function fields over a finite field, and we present a new class of Artin-Schreier towers having finite genus.

Keywords: function fields, finite fields, towers of function fields, Artin-Schreier extensions of function fields.

Mathematical subject classification: 11R58, 14H05, 11D59, 14G15.

1 Introduction

A *tower* $\mathcal{F} = (F_0, F_1, \ldots)$ *of function fields* over the finite field $\mathbb{F}_q$ is an infinite sequence of function fields $F_i/\mathbb{F}_q$ with $F_0 \subseteq F_1 \subseteq F_2 \subseteq \ldots$, having the following properties:

(i) The extensions F_{i+1}/F_i are separable of degree $[F_{i+1} : F_i] > 1$, and $\mathbb{F}_q$ is algebraically closed in F_i, for all $i \geq 0$.

(ii) For some $j \geq 0$, the genus of F_j satisfies $g(F_j) \geq 2$.

It follows from the Hurwitz genus formula that $g(F_i) \to \infty$ for $i \to \infty$, and the following limits do exist (we denote by $N(F)$ the number of $\mathbb{F}_q$-rational places of a function field $F/\mathbb{F}_q$):

$$\gamma(\mathcal{F}) = \lim_{i\to\infty} \frac{g(F_i)}{[F_i : F_0]}, \quad \nu(\mathcal{F}) = \lim_{i\to\infty} \frac{N(F_i)}{[F_i : F_0]} \qquad (1.1)$$

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

Received 10 March 2005.

We call $\lambda(\mathcal{F})$ the *limit of the tower*, $\gamma(\mathcal{F})$ is the *genus of the tower*, and $\nu(\mathcal{F})$ is the *splitting rate of the tower*. By the Drinfeld-Vladut bound [2] one has

$$0 \leq \lambda(\mathcal{F}) \leq \sqrt{q} - 1. \tag{1.2}$$

The tower $\mathcal{F}$ is said to be *asymptotically good* if $\lambda(\mathcal{F}) > 0$, otherwise it is said to be *asymptotically bad*.

The interest in asymptotically good towers comes from various applications of function fields with "many" rational places (with respect to the genus) in Coding theory, Cryptography, etc. (see [10], [12]). This motivates the search for asymptotically good towers. However, it turns out that it is a non-trivial problem to provide examples of asymptotically good towers. The first examples are due to Ihara [8], Tsfasman-Vladut-Zink [13] and Serre [11]. These examples come from modular curves or from classfield theory, and the function fields in these towers are not given by simple explicit equations.

Garcia, Stichtenoth and others have constructed some explicit asymptotically good towers in a *recursive* manner as follows: There is given a polynomial $f(X,Y) \in \mathbb{F}_q[X,Y]$ such that $F_0 = \mathbb{F}_q(x_0)$ is the rational function field over $\mathbb{F}_q$ and $F_{i+1} = F_i(x_{i+1})$, where the irreducible equation for x_{i+1} over the field F_i is just the equation

$$f(x_i, x_{i+1}) = 0\ , \quad \text{for all } \ i \geq 0. \tag{1.3}$$

In this situation we say that the tower $\mathcal{F} = (F_0, F_1, \ldots)$ is *recursively defined* by the polynomial $f(X,Y)$. If the polynomial $f(X,Y)$ has the special form

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

where $\varphi(Y) \in \mathbb{F}_q[Y]$ is a separable *additive* polynomial over $\mathbb{F}_q$,

$$\varphi(Y) = \sum_{j=0}^{m} a_j Y^{p^j} \ \text{ with } \ p = char(\mathbb{F}_q),\ a_j \in \mathbb{F}_q,\ a_0 \cdot a_m \neq 0,$$

and $\psi_0(X), \psi_1(X) \in \mathbb{F}_q[X]$, the tower $\mathcal{F}$ is called a *recursive Artin-Schreier tower* (AS *tower* for short). We say then that $\mathcal{F}$ is defined recursively by the equation

$$\varphi(Y) = \psi_0(X)/\psi_1(X) =: \psi(X) \in \mathbb{F}_q(X). \tag{1.4}$$

If all roots of the polynomial $\varphi(Y)$ are in $\mathbb{F}_q$, then the extensions F_{i+1}/F_i are Artin-Schreier extensions of degree $p^m = \deg \varphi(Y)$. The class of recursive AS towers is especially interesting since it contains examples of towers $\mathcal{F}$ whose limit $\lambda(\mathcal{F})$ attains or is close to the Drinfeld-Vladut bound (1.2), see [4], [7]. It is therefore a natural problem to study AS towers more closely.

Beelen, Garcia and Stichtenoth investigated recursive AS towers of prime degree $p = char(\mathbb{F}_q)$; i.e., where the defining equation of the tower has the form

$$Y^p + bY = \psi(X) \tag{1.5}$$

with $0 \neq b \in \mathbb{F}_q$ and $\psi(X) \in \mathbb{F}_q(X)$. Their main result is as follows (see [1], Thm. 4.1 and Thm. 4.6): If Eq. (1.5) defines an asymptotically good recursive tower over $\mathbb{F}_q$, then the rational function $\psi(X)$ is of one of the following three types:

Type I: $\psi(X) = (X-c)^p/\psi_1(X) + a$, with $a, c \in \mathbb{F}_q$ and a separable polynomial $\psi_1(X) \in \mathbb{F}_q[X]$ of degree $\deg\ \psi_1(X) \leq p$.

Type II: $\psi(X) = \psi_0(X)/(X-a)^p$ with $a \in \mathbb{F}_q$ and a separable polynomial $\psi_0(X) \in \mathbb{F}_q[X]$ of degree $\deg\ \psi_0(X) \leq p$.

Type III: $\psi(X) = 1/\psi_1(X) + a$, with $a \in \mathbb{F}_q$ and a separable polynomial $\psi_1(X) \in \mathbb{F}_q[X]$ of degree $\deg\ \psi_1(X) = p$.

As it was observed in [1], all hitherto known examples of asymptotically good recursive AS towers of degree p are of Type I, and it is an open problem if there exist good towers of Type II or Type III. The situation is somewhat similar as for towers of *Kummer type*, which are recursively defined by an equation of the form

$$Y^m = h(X) \in \mathbb{F}_q[X], \text{ with } gcd(m,q) = 1.$$

Lenstra [9] proved that asymptotically good towers of this type do not exist over the prime field $\mathbb{F}_p$.

Since the limit $\lambda(\mathcal{F})$ of a tower $\mathcal{F}$ satisfies $\lambda(\mathcal{F}) = \nu(\mathcal{F})/\gamma(\mathcal{F})$ (see (1.1)), the tower is asymptotically good if and only if its genus $\gamma(\mathcal{F})$ is finite and its splitting rate $\nu(\mathcal{F})$ is strictly positive. Therefore a necessary first step towards the construction of good AS towers is to find examples where the genus $\gamma(\mathcal{F})$ is finite. It is the aim of this note to provide a class of recursive AS towers of Type III with this property.

2 Artin-Schreier towers of Type III with finite genus

In this section we consider a sequence $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ of function fields $F_i/\mathbb{F}_q$ which is recursively defined by the equation

$$Y^p + bY = 1/(X^p + cX) \tag{2.1}$$

with $b, c \in \mathbb{F}_q \setminus \{0\}$ and $b \neq c$. This means that $F_0 = \mathbb{F}_q(x_0)$ is the rational function field, and for $i \geq 0$ we have $F_{i+1} = F_i(x_{i+1})$ with

$$x_{i+1}^p + bx_{i+1} = 1/(x_i^p + cx_i). \tag{2.2}$$

First we have to prove that this sequence of function fields is indeed a tower, see Prop. 2.2 below. We need

Lemma 2.1. *Let $K = \bar{\mathbb{F}}_q$ be the algebraic closure of $\mathbb{F}_q$ and consider the function field $F = K(x, y)$, where x, y satisfy* Eq. (2.1) *with $b, c \in \mathbb{F}_q \setminus \{0\}$ and $b \neq c$. Then the extensions $F/K(x)$ and $F/K(y)$ are Galois of degree p, and the following holds:*

(i) *Over $K(x)$ exactly the zeroes of $x - \alpha$ with $\alpha^p + c\alpha = 0$ are ramified, each with ramification index p and different exponent* $2(p-1)$. *All these places are poles of y.*

(ii) *Over $K(y)$ exactly the zeroes of $y - \beta$ with $\beta^p + b\beta = 0$ are ramified, each with ramification index p and different exponent* $2(p-1)$. *All these places are poles of x.*

Proof. This follows immediately from the theory of Artin-Schreier extensions of function fields, cf. [12], Ch.III.7.8. □

Proposition 2.2. *The sequence $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ of function fields over $\mathbb{F}_q$ which is defined recursively by* Eq. (2.1) *is a tower.*

Proof. First we have to show that the equation $Y^p + bY = 1/(x_i^p + cx_i)$ is absolutely irreducible over F_i, for all $i \geq 0$. So we consider the constant field extensions $F_i' := F_i \cdot K$ over the algebraic closure $K = \bar{\mathbb{F}}_q$, and we must show that $[F_{i+1}' : F_i'] = p$. The case $i = 0$ follows from Lemma 2.1. Now let $i \geq 1$. We choose elements $\alpha_i, \alpha_{i-1}, \ldots, \alpha_1, \alpha_0 \in K$ such that

$$\alpha_i^p + c\alpha_i = 0, \quad \alpha_i^p + b\alpha_i \neq 0 \tag{2.3}$$

and

$$\alpha_j^p + c\alpha_j = 1/(\alpha_{j+1}^p + b\alpha_{j+1}), \quad \alpha_j^p + b\alpha_j \neq 0 \tag{2.4}$$

for all $j < i$. These choices are possible since $b \neq c$. There exists a place Q of F_i' which is a common zero of the functions $x_i - \alpha_i, x_{i-1} - \alpha_{i-1}, \ldots, x_0 - \alpha_0$, and

Q is unramified in the extension $F_i'/K(x_i)$ by Lemma 2.1(ii). Let P denote the restriction of Q to $K(x_i)$. By (2.3) and Lemma 2.1(i), the place P is ramified in $K(x_i, x_{i+1})/K(x_i)$ with ramification index p, and it follows from Abhyankar's Lemma (see [12], III.8.9) that Q is ramified in F_{i+1}'/F_i' with ramification index p, so $[F_{i+1}' : F_i'] = p$. This proves that the polynomial $Y^p + bY = 1/(x_i^p + cx_i)$ is irreducible over F_i', which implies that the field extension F_{i+1}/F_i is of degree $[F_{i+1} : F_i] = p$ and that the field $\mathbb{F}_q$ is algebraically closed in F_{i+1}.

By Lemma 2.1(i), the degree of the different of F_1/F_0 is $\deg \mathrm{Diff}(F_1/F_0) = 2p(p-1)$, hence the genus of F_1 is $g(F_1) = (p-1)^2$. So we have $g(F_1) \geq 2$ for all $p \neq 2$. In the case $p = 2$ it is easy to see that $g(F_2) \geq 2$. □

For any tower $\mathcal{F} = (F_0, F_1, \ldots)$ over $\mathbb{F}_q$, the *ramification locus* $V(\mathcal{F})$ is defined as

$$V(\mathcal{F}) = \{P \mid P \text{ is a place of } F_0 \text{ which ramifies in } F_n/F_0 \text{ for some } n \geq 1\}.$$

If the ramification locus is finite, we set

$$\deg V(\mathcal{F}) = \sum_{P \in V(\mathcal{F})} \deg P.$$

Proposition 2.3. *Let $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ be the tower over $\mathbb{F}_q$ which is recursively defined by*

$$Y^p + bY = 1/(X^p + cX), \tag{2.1}$$

with the additional condition

$$bc(b-c)^{2p-2} = 1. \tag{2.5}$$

Then the ramification locus $V(\mathcal{F})$ is finite and has degree $\deg V(\mathcal{F}) \leq 1 + p^2$.

Proof. Since the degree of the ramification locus is invariant under constant field extensions, we can assume that the following sets Δ, Ω are contained in $\mathbb{F}_q$:

$$\Delta := \{\delta \in \bar{\mathbb{F}}_q \mid \delta^p + c(b-c)^{p-1}\delta = 0\},$$
$$\Omega := \{\alpha \in \bar{\mathbb{F}}_q \mid \alpha^p + b\alpha \in \Delta\}.$$

Now let $P \in V(\mathcal{F})$. There is some $n \geq 1$ and a place Q of F_n lying above P, such that Q is ramified in the extension F_n/F_{n-1}. Then Q is a pole of x_n by Lemma 2.1; i.e., $x_n(Q) = \infty$. For $i = 0, 1, \ldots, n$ we set

$$\alpha_i := x_{n-i}(Q) \in \bar{\mathbb{F}}_q \cup \{\infty\},$$

and we want to prove the following claim:

$$\alpha_i \in \Omega \cup \{\infty\}, \quad \text{for } i = 0, \dots, n. \tag{2.6}$$

Since $x_0(Q) = \alpha_n$, this will imply that

$$P \in V(\mathcal{F}) \implies x_0(P) \in \Omega \cup \{\infty\},$$

and therefore $\deg V(\mathcal{F}) \leq 1 + |\Omega| = 1 + p^2$, as desired.

We show (2.6) by induction over i (with n fixed). By definition we have $\alpha_0 = x_n(Q) = \infty$. Suppose now that $\alpha_i \in \Omega \cup \{\infty\}$, for some $i \leq n-1$. If $\alpha_i = \infty$, it follows from Eq. (2.2) that $\alpha_{i+1}^p + c\alpha_{i+1} = 0$. Setting

$$\delta_{i+1} := \alpha_{i+1}^p + b\alpha_{i+1} = (\alpha_{i+1}^p + c\alpha_{i+1}) + (b-c)\alpha_{i+1} = (b-c)\alpha_{i+1}$$

we see that

$$\delta_{i+1}^p + c(b-c)^{p-1}\delta_{i+1} = (b-c)^p(\alpha_{i+1}^p + c\alpha_{i+1}) = 0\ ,$$

hence $\alpha_{i+1} \in \Omega$.

Now we assume that $\alpha_i \in \Omega$. If $\alpha_{i+1} = \infty$ then Claim (2.6) holds also for $i+1$ and we are done. So it remains to consider the case where $\alpha_i \in \Omega$ and $\alpha_{i+1} \neq \infty$. From Eq. (2.2) we obtain

$$\alpha_{i+1}^p + c\alpha_{i+1} = 1/(\alpha_i^p + b\alpha_i). \tag{2.7}$$

By induction hypothesis, the element $\delta_i := \alpha_i^p + b\alpha_i \neq 0$ satisfies the equation

$$\delta_i^p + c(b-c)^{p-1}\delta_i = 0, \tag{2.8}$$

and we have to prove that $\delta_{i+1} = \alpha_{i+1}^p + b\alpha_{i+1}$ also satisfies this equation. From Eq. (2.7) follows

$$\delta_{i+1} = \delta_i^{-1} + (b-c)\alpha_{i+1}\ ,$$

hence

$$\begin{aligned}
&\delta_{i+1}^p + c(b-c)^{p-1}\delta_{i+1} \\
&= \delta_i^{-p} + (b-c)^p\alpha_{i+1}^p + c(b-c)^{p-1}(\delta_i^{-1} + (b-c)\alpha_{i+1}) \\
&= (\delta_i^{-p} + c(b-c)^{p-1}\delta_i^{-1}) + (b-c)^p(\alpha_{i+1}^p + c\alpha_{i+1}) \\
&= \delta_i^{-p} + b(b-c)^{p-1}\delta_i^{-1} \\
&= b(b-c)^{p-1}\delta_i^{-(p+1)}(\delta_i^p + \delta_i/b(b-c)^{p-1}) \\
&= b(b-c)^{p-1}\delta_i^{-(p+1)}(\delta_i^p + c(b-c)^{p-1}\delta_i) = 0.
\end{aligned}$$

Observe that in the last line we have used Eq. (2.5) and (2.8). □

It is well known that in the case of tamely ramified towers finite ramification locus implies finite genus, since the different exponent is bounded by the ramification index (see [5]). This is in general not true for wildly ramified towers (cf. [4], Example 4.1). However, in our case we can show that the different exponents of ramified places in the extensions F_i/F_0 are small enough to ensure finite genus. The key point is the following proposition from [6]. A detailed exposition of calculations of different exponents in the tower in Proposition 2.3 can also be found in [14].

Proposition 2.4. (See [6], Lemma 2.) *Let E_1 and E_2 be distinct cyclic function field extensions of F of degree p, and let E be the composite field of E_1 and E_2. Then E/F is a Galois extension of degree p^2. Suppose that P is a place of F which is ramified both in E_1 and E_2 and suppose that the different exponent in both extensions is $2p-2$. Then P is either unramified in E/E_i $(i = 1, 2)$, or in case of ramification the different exponent in E/E_i is also $2p-2$.*

By Lemma 2.1 we can use Proposition 2.4 to calculate the different exponents of all ramified places in the towers $\mathcal{F}$ which are defined by Eq. (2.1). Using the transitivity of different exponents we obtain: for all $P \in V(\mathcal{F})$ and all places Q of F_n lying above P, the different exponent of $Q|P$ is $d(Q|P) = 2(p^t - 1)$ if $e(Q|P) = p^t$. Thus, in any tower recursively defined by Eq. (2.1), the different exponents of ramified places in the extensions F_i/F_0 are bounded by the ramification index multiplied by two (see also [6], Lemma 3).

Now we can prove our main result:

Theorem 2.5. *Let $q = p^r$ (p is a prime number), and assume that $b, c \in \mathbb{F}_q$ satisfy the condition $bc(b-c)^{2p-2} = 1$. Then the equation*

$$Y^p + bY = \frac{1}{X^p + cX}$$

defines recursively a tower $\mathcal{F}$ over $\mathbb{F}_q$ with finite genus

$$\gamma(\mathcal{F}) = \lim_{n\to\infty} g(F_n)/[F_n : F_0] \le p^2.$$

Proof. The Hurwitz genus formula yields

$$\begin{aligned} 2g(F_n) - 2 &= [F_n : F_0](2g(F_0) - 2) + \deg \operatorname{Diff}(F_n/F_0) \\ &< 2[F_n : F_0](\deg V(\mathcal{F}) - 1) \le 2p^2[F_n : F_0]. \qquad \square \end{aligned}$$

Remark 2.6. One can easily see that all results also hold if we replace the prime number p by a power p^s.

References

[1] P. Beelen, A. Garcia and H. Stichtenoth, *On towers of function fields of Artin-Schreier type*. Bull. Braz. Math. Soc. **35** (2004), 151–164.

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

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

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

[5] A. Garcia and H. Stichtenoth, *On tame towers over finite fields.* J. Reine Angew. Math. **557** (2003), 53–80.

[6] A. Garcia and H. Stichtenoth, *Some Artin-Schreier towers are easy*. Moscow Math. J., to appear.

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

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

[9] H.W. Lenstra, *On a problem of Garcia, Stichtenoth, and Thomas*. Finite Fields Appl. **8** (2001), 166–170.

[10] H.Niederreiter and C.P.Xing, Rational Points on Curves over Finite Fields: Theory and Applications. Cambridge University Press, Cambridge, 2001.

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

[12] H. Stichtenoth, Algebraic Function Fields and Codes. Springer Universitext, Berlin-Heidelberg, 1993.

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

[14] S. M. Yang, *On explicit towers of function fields over finite fields*. PhD thesis, National University of Singapore, 2004.

San Ling
Division of Mathematical Sciences
School of Physical and Mathematical Sciences
Nanyang Technological University
Singapore 637616
SINGAPORE

E-mail: lingsan@ntu.edu.sg

Henning Stichtenoth
Fachbereich Mathematik
Universität Duisburg-Essen, Campus Essen,
45117 Essen
GERMANY

E-mail: stichtenoth@uni-essen.de
and
Sabanci University, MDBF
Orhanli, Tuzla 34956, Istanbul
TURKEY

e-mail: henning@sabanciuniv.edu

Siman Yang
Department of Mathematics
East China Normal University
Shanghai, 200062. P.R.
CHINA

E-mail: smyang@math.ecnu.edu.cn