BULLETIN OF THE BRAZILIAN MATHEMATICAL SOCIETY

Bull Braz Math Soc, New Series 35(2), 151-164

On towers of function fields of Artin-Schreier type

Peter Beelen, Arnaldo Garcia[1,2] and Henning Stichtenoth[1]

Abstract. In this article we derive strong conditions on the defining equations of asymptotically good Artin-Schreier towers. We will show that at most three kinds of defining equations can give rise to a recursively defined good tower, if we restrict ourselves to prime degrees.

Keywords: function fields, finite fields, towers of function fields, rational places, genus, limits of towers, Artin-Schreier extensions.

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

0 Introduction

The search for explicit equations of function fields over finite fields, specially the ones coming from modular curves, has attracted interest since the works of Fricke and Klein. Recently the interest on towers of function fields over finite fields was renewed because of its applications to Coding Theory: via Goppa's construction of linear codes from algebraic function fields, Tsfasman-Vladut-Zink showed the existence of long linear codes above the so-called Gilbert-Varshamov bound (see [11], Section VII.2).

We will consider here towers of Artin-Schreier type; i.e., towers $\mathcal{F} = (F_0, F_1, F_2, \dots)$ of function fields F_n over a finite field $K = \mathbb{F}_q$ in which every extension F_n/F_{n-1} is an Artin-Schreier extension. In the last few years several asymptotically good towers of function fields of Artin-Schreier type (precise definitions will be given below) have been found (see [4, 5, 9]). After it turned out that some of these towers are explicit models of certain modular

Received 16 January 2004.

[1]A. Garcia and H. Stichtenoth did part of this work during their stay at Sabanci University, Istanbul, Turkey (Sept. 2002).

[2]A. Garcia was partially supported by PRONEX # 662408/1996-3 (CNPq-Brazil).

curves (see [2, 3]), the significance of them has become even more apparent. In this paper we derive strong restrictions on the defining equations of asymptotically good Artin-Schreier towers (see Theorems 2.1 and 4.6). Particularly interesting is the statement in Theorem 3.1 that a certain extension of rational function fields is wild, which leads to the classification result in Theorem 4.1. If a certain divisor is p-free (see Cor. 2.2) we show that the tower $\mathcal{F}$ is a bad tower. We then consider recursive Artin-Schreier towers $\mathcal{F}$ given by

$$\varphi(Y) = \psi(X) = \frac{\psi_0(X)}{\psi_1(X)},$$

where $\varphi(Y)$ is an additive and separable polynomial, and where $\psi(X)$ is a rational function. If the tower $\mathcal{F}$ is a good tower, then the extension $\mathbb{F}_q(X)/\mathbb{F}_q(\psi(X))$ is a wild extension (see Theor. 3.1). As a consequence we get Theor. 4.1 describing, for good recursive towers of Artin-Schreier type, the possibilities for the rational functions $\psi(X)$ in case deg $\psi(X) = p$, where p denotes the characteristic. Prop. 4.4 and 4.5 show that the case where $\psi(X)$ is a polynomial leads always to a bad tower (see [10] for a similar result in the case of towers of Kummer type over prime fields $\mathbb{F}_p$). All known asymptotically good, recursive towers of Artin-Schreier type of degree p are of the first kind; i.e., they all fall under the item i) of Theor. 4.1.

1 Preliminaries

We give some details concerning notation and definitions, as well as some first properties of towers. Throughout this note, K is a perfect field of characteristic $p > 0$, and $\mathcal{F} = (F_0, F_1, \dots)$ is a *tower of function fields* over K. This means that

i) F_0 is a function field (of one variable) over K, and $F_0 \subset F_1 \subset F_2 \subset \dots$

ii) For all $n \geq 1$ the extension F_n/F_{n-1} is finite and separable of degree $[F_n : F_{n-1}] > 1$.

iii) The field K is the full constant field of F_n, for all $n \geq 0$.

iv) The genus $g(F_n)$ of F_n tends to infinity, for $n \to \infty$.

Towers of function fields are of particular interest in the case when K is the finite field $\mathbb{F}_q$ where q is a power of the characteristic p. In this case we denote by

$N(F_n)$ the number of $\mathbb{F}_q$-rational places (i.e., the number of places of degree one) of $F_n/\mathbb{F}_q$, by $g(F_n)$ the genus of the function field F_n, and by

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

the *limit* of the tower $\mathcal{F}$. This limit $\lambda(\mathcal{F}) \geq 0$ always exists [8], and one has the well-known Drinfeld-Vladut bound [1]:

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

We say that the tower $\mathcal{F}$ is *asymptotically good* (resp. *asymptotically bad*, resp. *asymptotically optimal*) if $\lambda(\mathcal{F}) > 0$ (resp. $\lambda(\mathcal{F}) = 0$, resp. $\lambda(\mathcal{F}) = \sqrt{q} - 1$).

When studying the limit $\lambda(\mathcal{F})$ of a tower over $\mathbb{F}_q$ it is convenient to consider the asymptotic behaviour of the genus and the asymptotic behaviour of the number of rational places separately: i.e., one introduces the quantities

$$\gamma(\mathcal{F}) := \lim_{n\to\infty} \frac{g(F_n)}{[F_n : F_0]} \text{ and } \nu(\mathcal{F}) := \lim_{n\to\infty} \frac{N(F_n)}{[F_n : F_0]}.$$

It is easily seen that the above limits exist, and that we have

$$0 < \gamma(\mathcal{F}) \leq \infty \text{ and } 0 \leq \nu(\mathcal{F}) \leq N(F_0) < \infty.$$

The following lemma follows easily from the definitions above.

Lemma 1.1. *Let $\mathcal{F}$ be a tower of function fields over $\mathbb{F}_q$. Then we have*

i) $\lambda(\mathcal{F}) = \nu(\mathcal{F})/\gamma(\mathcal{F})$.

ii) *The tower $\mathcal{F}$ is asymptotically good if and only if $\nu(\mathcal{F}) > 0$ and $\gamma(\mathcal{F}) < \infty$.* □

There is a simple criterion which implies in many cases that $\nu(\mathcal{F}) > 0$, namely the following: call a rational place P_0 of the function field F_0 *completely splitting* in the tower $\mathcal{F}$ if the place P_0 splits completely in all extensions F_n/F_0 (i.e., the place P_0 has exactly $[F_n : F_0]$ places of F_n above it, for all $n \geq 1$).

Lemma 1.2. *Let $\mathcal{F}$ be a tower of function fields over $\mathbb{F}_q$ and let $t := \#\{P_0 | P_0$ is a rational place of $F_0/\mathbb{F}_q$ which splits completely in the tower $\mathcal{F}\}$. Then we have $\nu(\mathcal{F}) \geq t$. In particular, if $t > 0$ then $\nu(\mathcal{F}) > 0$.*

Proof. Obvious. □

Let F be a function field with K as its full constant field. An irreducible polynomial in $F[Y]$ is called *absolutely irreducible* if this polynomial is also irreducible as an element of $E[Y]$, where E is the compositum field of F and an algebraic closure of K.

As before we consider a tower $\mathcal{F} = (F_0, F_1, F_2, \dots)$ of function fields over the finite field $\mathbb{F}_q$. Assume there is a polynomial in two variables $\Phi(X, Y) \in \mathbb{F}_q[X, Y]$ and elements $x_r \in F_r$ $(r \geq 0)$ such that $F_0 = \mathbb{F}_q(x_0)$ is the rational function field and, for all $n \geq 1$, the following holds:

i) $F_n = F_{n-1}(x_n)$ and $\Phi(x_{n-1}, x_n) = 0$.

ii) The polynomial $\Phi(x_{n-1}, Y) \in F_{n-1}[Y]$ is absolutely irreducible.

Then we say that the tower $\mathcal{F}$ is *defined recursively* by the equation $\Phi(X, Y) = 0$. In case the polynomial $\Phi(X, Y)$ has the specific form $\Phi(X, Y) = \varphi_0(Y)\cdot\psi_1(X) - \varphi_1(Y) \cdot \psi_0(X)$, with polynomials in one variable $\varphi_0(Y), \varphi_1(Y) \in \mathbb{F}_q[Y]$ and $\psi_0(X), \psi_1(X) \in \mathbb{F}_q[X]$, we also say that the tower $\mathcal{F}$ is *defined recursively* by the equation

$$\frac{\varphi_0(Y)}{\varphi_1(Y)} = \frac{\psi_0(X)}{\psi_1(X)}.$$

Many interesting towers of function fields in the literature are of this type, see [4, 5, 7, 8, 9].

Example 1.3. Consider the tower $\mathcal{F}$ of Artin-Schreier type defined recursively over $\mathbb{F}_q$ by the equation

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

where the characteristic p of the finite field $\mathbb{F}_q$ satisfies $p \geq 3$. If the cardinality of the field $\mathbb{F}_q$ satisfies $q = p^p$, then the places of the rational function field $F_0 = \mathbb{F}_q(x_0)$ which are zeros of $x_0^p - x_0 - 1$, are completely splitting in the tower over $\mathbb{F}_q$. Hence $\nu(\mathcal{F}) \geq p$ over $\mathbb{F}_{p^p}$. It will follow from our results, that this tower is asymptotically bad (see Example 4.3 below).

We say that the tower $\mathcal{F}$ has *finite genus* if $\gamma(\mathcal{F}) < \infty$. Now we give a criterion which implies that $\mathcal{F}$ has finite genus. We call the set

$$V(\mathcal{F}) := \{Q_0 | Q_0 \text{ is a place of } F_0/\mathbb{F}_q \text{ ramified in some extension } F_n/F_0\}$$

the *ramification locus* of the tower $\mathcal{F}$. The tower is said to be *tame* if all extensions F_n/F_0 are tame (which means that the ramification index $e(P|Q_0)$ is relatively prime to the characteristic p, for all places Q_0 of the function field F_0 and for all extensions P of Q_0 in F_n). Otherwise the tower $\mathcal{F}$ is said to be *wild*.

Lemma 1.4. *A tame tower $\mathcal{F}$ with finite ramification locus $V(\mathcal{F})$ has finite genus.*

Proof. This is a simple consequence of the Hurwitz genus formula, applied to the extensions F_n/F_0. See also [8]. □

Combining the above results one obtains:

Corollary 1.5. *Let $\mathcal{F}$ be a tower of function fields over $\mathbb{F}_q$ having the following properties:*

i) *The tower $\mathcal{F}$ is tame.*

ii) *The ramification locus $V(\mathcal{F})$ is finite.*

iii) *At least one rational place P_0 of the function field F_0 splits completely in the tower $\mathcal{F}$.*

Then the tower $\mathcal{F}$ is asymptotically good.

We will see in Section 2 that the conclusion of Corollary 1.5 does not hold in general for wild towers.

2 Towers of Artin-Schreier type

We keep all notations from Section . A tower $\mathcal{F} = (F_0, F_1, F_2, \dots)$ of function fields over $\mathbb{F}_q$ is said to be a *tower of Artin-Schreier type* if for all $n \geq 1$ one has $F_n = F_{n-1}(x_n)$, where the minimal polynomial of x_n over F_{n-1} has the form

$$\varphi_n(T) - z_{n-1}$$

with a separable additive polynomial $\varphi_n(T) \in \mathbb{F}_q[T]$ and with some element $z_{n-1} \in F_{n-1}$ (recall that a polynomial $\varphi(T)$ of the form $\sum_{i\geq 0} a_i T^{p^i}$ is called *additive*; it is separable if $a_0 \neq 0$). Note that from the assumption that $\mathcal{F}$ is a tower it follows that the polynomial $\varphi_n(T) - z_{n-1}$ is absolutely irreducible in $F_{n-1}[T]$. It is clear that if there occurs ramification in F_n/F_{n-1} then it is wild ([11]). Examples of asymptotically good towers of Artin-Schreier type are given in [4, 5, 9].

Our main result here (see Theorem 2.1) says that if a Artin-Schreier tower is asymptotically good, then the determination of the genera of the function fields in the tower will require pole-order reductions (see [11], Proposition III.7.8) essentially at all relevant places. In order to state Theorem 2.1 properly, we introduce the following notation: Given a divisor D in a function field of characteristic $p > 0$, one has a unique decomposition $D = p \cdot A + B$, where the supports of the divisors A and B are disjoint and

$$B = \sum b_P \cdot P, \quad \gcd(b_P, p) = 1 \text{ for all places } P \text{ with } b_P \neq 0.$$

We call B the *p-free part* of D. If $B = D$ the divisor D is said to be *p-free*.

Theorem 2.1. *Let $\mathcal{F} = (F_0, F_1, F_2, \dots)$ be a tower of function fields over $\mathbb{F}_q$ of Artin-Schreier type. Suppose that for all $n \geq 1$ we have*

$$F_n = F_{n-1}(x_n) \text{ with } \varphi_n(x_n) - z_{n-1} = 0,$$

where $z_{n-1} \in F_{n-1}$, $\varphi_n(T) \in \mathbb{F}_q[T]$ is an additive separable polynomial and $\varphi_n(T) - z_{n-1} \in F_{n-1}[T]$ is absolutely irreducible. Suppose moreover that the functions $z_r \in F_r$ satisfy the following extra condition: There exists a constant $\epsilon > 0$ such that

$$\deg B_r \geq \epsilon \cdot \deg D_r, \text{ for infinitely many values of the index } r,$$

where D_r is the pole divisor of the function z_r in the field F_r and B_r is the p-free part of the divisor D_r. Then the tower $\mathcal{F}$ is asymptotically bad.

Proof. Assume that the tower $\mathcal{F}$ is asymptotically good, then $\nu(\mathcal{F}) > 0$ by Lemma 1.1. As the sequence $(N(F_n)/[F_n : F_0])_{n \geq 0}$ is monotonously decreasing, we have for all $n \geq 0$ that

$$N(F_n) \geq \nu(\mathcal{F}) \cdot [F_n : F_0].$$

On the other hand the obvious inequality $N(F_n) \leq (q+1)[F_n : \mathbb{F}_q(z_n)]$ holds and we conclude for all $n \geq 0$ that

$$[F_n : \mathbb{F}_q(z_n)] \geq c_1 \cdot [F_n : F_0], \text{ with } c_1 := \nu(\mathcal{F})/(q+1) > 0. \tag{1}$$

Now we choose an infinite sequence of indices $0 \leq r_1 < r_2 < r_3 < \dots$ such that the p-free part B_{r_j} of the pole divisor of z_{r_j} in the field F_{r_j} satisfies

$$\deg B_{r_j} \geq \epsilon \cdot [F_{r_j} : \mathbb{F}_q(z_{r_j})], \text{ for all } j \geq 1. \tag{2}$$

It follows from Equations (1) and (2), taking $c_2 = \epsilon \cdot c_1 > 0$, that

$$\deg B_{r_j} \geq c_2[F_{r_j} : F_0], \text{ for all } j \geq 1. \tag{3}$$

Write $B_{r_j} = \sum b_l P_l$ with places P_l of the function field $F_{r_j}/\mathbb{F}_q$ and $b_l > 0$. Using for example [11], Prop. III.7.10 (d), we see that the different degree of F_{r_j+1}/F_{r_j} is bounded from below by

$$\begin{aligned} \deg \mathrm{Diff}(F_{r_j+1}/F_{r_j}) &\geq \sum (b_l + 1)([F_{r_j+1} : F_{r_j}] - 1) \cdot \deg P_l \\ &\geq \tfrac{1}{2}[F_{r_j+1} : F_{r_j}] \cdot \sum b_l \deg P_l \\ &= \tfrac{1}{2}[F_{r_j+1} : F_{r_j}] \cdot \deg B_{r_j} \geq c_3 \cdot [F_{r_j+1} : F_0] \end{aligned}$$

with $c_3 = c_2/2$. Using the transitivity of the different, we obtain by induction the following:

$$\deg \mathrm{Diff}(F_{r_s+1}/F_{r_1}) \geq s \cdot c_3 \cdot [F_{r_s+1} : F_0], \text{ for all values of the index } s.$$

Without loss of generality we can assume that the genus of the function field F_{r_1} satisfies $g(F_{r_1}) > 0$; then the Hurwitz genus formula for the extension F_{r_s+1}/F_{r_1} implies that

$$g(F_{r_s+1}) \geq \frac{1}{2} \cdot s \cdot c_3 \cdot [F_{r_s+1} : F_0], \text{ for all values of the index } s.$$

Hence $\gamma(\mathcal{F}) = \lim_{s\to\infty} g(F_{r_s+1})/[F_{r_s+1} : F_0] = \infty$. This is a contradiction to Lemma 1.1. □

The proof of Theorem 2.1 shows that if there is a nonzero real constant c such that $\deg \mathrm{Diff}(F_{r+1}/F_r) \geq c \cdot [F_{r+1} : F_0]$, for infinitely many values of the index r, then the tower has an infinite genus. So Theorem 2.1 holds under the more general assumption that there are infinitely many Artin-Schreier steps in the tower satisfying this extra condition in the statement of Theorem 2.1.

As a particular case of Theorem 2.1 we have

Corollary 2.2. *Let the hypotheses and notations be as in Theorem 2.1 apart from the extra condition. Suppose that for all $r \geq 0$, the pole divisor of the function z_r in the function field F_r is p-free (i.e., $B_r = D_r$ for all indices $r \geq 0$). Then the tower $\mathcal{F}$ is asymptotically bad.*

Proof. The extra condition in Theorem 2.1 is satisfied with $\epsilon = 1$ for all indices $r \geq 0$. □

3 Recursive towers of Artin-Schreier type

In this section we want to study the asymptotic behaviour of *recursive Artin-Schreier towers* $\mathcal{F}$ over the finite field $\mathbb{F}_q$; i.e., towers $\mathcal{F}$ defined recursively by equations of the form

$$\varphi(Y) = \frac{\psi_0(X)}{\psi_1(X)}, \tag{4}$$

where $\varphi(Y) \in \mathbb{F}_q[Y]$ is a separable additive polynomial and where $\psi_0(X)$, $\psi_1(X) \in \mathbb{F}_q[X]$ are relatively prime polynomials. Observe that we assume tacitly that, for all $n \geq 1$, the polynomial $\varphi(Y) - \psi_0(x_{n-1})/\psi_1(x_{n-1}) \in F_{n-1}[Y]$ is absolutely irreducible. Examples of equations of the form (4) leading to asymptotically good recursive Artin-Schreier towers are given by (see [5] and [9]):

$$Y^q + Y = \frac{X^q}{X^{q-1}+1} \text{ over } \mathbb{F}_{q^2},$$

or by

$$Y^2 + Y = \frac{X^2}{X+1} + 1 \text{ over } \mathbb{F}_8.$$

Theorem 3.1. *Suppose that $\mathcal{F}$ is an asymptotically good recursive tower over $\mathbb{F}_q$ of Artin-Schreier type, defined by Equation* (4) *as above. Assume in addition that the rational function $\psi(X) := \psi_0(X)/\psi_1(X)$ satisfies $\psi(X) \notin \mathbb{F}_q(X^p)$, where $p = \text{char}(\mathbb{F}_q)$. Then the following holds:*

i) $\deg \varphi(Y) = \deg \psi(X)$, *where* $\deg \psi(X) := \max\{\deg \psi_0(X), \deg \psi_1(X)\}$.

ii) The extension of rational function fields $\mathbb{F}_q(X)/\mathbb{F}_q(\psi(X))$ is wild (i.e., at least one place is wildly ramified).

Proof. i) By our assumptions, the polynomial $\Phi(X, Y) = \varphi(Y) \cdot \psi_1(X) - \psi_0(X)$ is separable in both variables X, Y. Hence assertion i) follows immediately from [6].

ii) Assume that the extension $\mathbb{F}_q(X)/\mathbb{F}_q(\psi(X))$ is tame, i.e. that assertion ii) does not hold. We show by induction that, for all $n \geq 1$, the extension $F_n/\mathbb{F}_q(x_n)$ is tame. For $n = 1$, the function field F_1 is the compositum of $\mathbb{F}_q(x_0)$ and $\mathbb{F}_q(x_1)$. Since the extension $\mathbb{F}_q(x_0)/\mathbb{F}_q(\psi(x_0))$ is tame by assumption, it follows from Abhyankar's lemma (see [11], Prop. III.8.9.) that $F_1/\mathbb{F}_q(x_1)$ is tame. Now we prove the induction step. With the same argument as before

one sees that $\mathbb{F}_q(x_n, x_{n+1})/\mathbb{F}_q(x_{n+1})$ is tame. The induction hypothesis states that $F_n/\mathbb{F}_q(x_n)$ is tame; again from Abhyankar's lemma we conclude that the extension $F_{n+1}/\mathbb{F}_q(x_n, x_{n+1})$ is tame. Since the extension $\mathbb{F}_q(x_n, x_{n+1})/\mathbb{F}_q(x_{n+1})$ is also tame, it follows that the extension $F_{n+1}/\mathbb{F}_q(x_{n+1})$ is tame. Assuming that $\mathbb{F}_q(X)/\mathbb{F}_q(\psi(X))$ is tame, we have thus proved that all extension $F_n/\mathbb{F}_q(x_n)$ are tame. Denoting by $z_n = \psi(x_n)$, we see that all extensions $F_n/\mathbb{F}_q(z_n)$ are tame extension and hence that the pole divisor of the function z_n in F_n is a p-free divisor. The theorem now follows from Corollary 2.2. □

In the next section we will investigate in more detail the case $\deg \psi(X) = p$.

4 Recursive towers of Artin-Schreier type of degree p

We keep the notations of the previous sections. In particular $\mathbb{F}_q$ denotes the finite field with q elements and $p = \mathrm{char}(\mathbb{F}_q)$. According to Theorem 3.1 rational functions $\psi(X)$ such that the extension $\mathbb{F}_q(X)/\mathbb{F}_q(\psi(X))$ is wild, are interesting for the construction of recursive towers. In case $\deg \psi(X) = p$, we give in the next theorem a complete list of all rational functions $\psi(X)$ such that the extension $\mathbb{F}_q(X)/\mathbb{F}_q(\psi(X))$ is wild.

Theorem 4.1. *Let $\psi(X) = \psi_0(X)/\psi_1(X) \in \mathbb{F}_q(X)\backslash\mathbb{F}_q(X^p)$, with $\psi_0(X)$, $\psi_1(X)$ relatively prime polynomials in $\mathbb{F}_q[X]$ satisfying the additional property that $\max\{\deg \psi_0(X), \deg \psi_1(X)\} = p$, where $p = \mathrm{char}(\mathbb{F}_q)$. Then the extension $\mathbb{F}_q(X)/\mathbb{F}_q(\psi(X))$ is wild if and only if one of the following cases holds:*

i) *$\psi(X) = (X-b)^p/\psi_1(X) + a$, with elements $a, b \in \mathbb{F}_q$ and a polynomial $\psi_1(X) \in \mathbb{F}_q[X]\backslash\mathbb{F}_q[X^p]$ of degree $\deg \psi_1(X) \leq p$ and $\psi_1(b) \neq 0$.*

ii) *$\psi(X) = \psi_0(X)/(X-a)^p$, with an element $a \in \mathbb{F}_q$ and with a polynomial $\psi_0(X) \in \mathbb{F}_q[X]\backslash\mathbb{F}_q[X^p]$, where $\deg \psi_0(X) \leq p$ and $\psi_0(a) \neq 0$.*

iii) *$\psi(X) = 1/\psi_1(X) + a$, with an element $a \in \mathbb{F}_q$ and with a polynomial $\psi_1(X) \in \mathbb{F}_q[X]\backslash\mathbb{F}_q[X^p]$, where $\deg \psi_1(X) = p$.*

iv) *$\psi(X) \in \mathbb{F}_q[X]\backslash\mathbb{F}_q[X^p]$ and $\deg \psi(X) = p$.*

Proof. For simplicity we write $\psi := \psi(X)$. Observe that the extension $\mathbb{F}_q(X)/\mathbb{F}_q(\psi)$ is separable since $\psi \notin \mathbb{F}_q(X^p)$. We assume first that the extension $\mathbb{F}_q(X)/\mathbb{F}_q(\psi)$ is wild. It follows from the Hurwitz genus formula that there is exactly one place Q of the field $\mathbb{F}_q(\psi)$ of degree one which is wildly ramified in $\mathbb{F}_q(X)/\mathbb{F}_q(\psi)$. Let P be the unique place of $\mathbb{F}_q(X)$ lying above Q.

Then we distinguish the following four cases which correspond to the cases in the statement of Theorem 2.1:

i) Q is the zero of $\psi - a$ in $\mathbb{F}_q(\psi)$ and P is the zero of $X - b$ in $\mathbb{F}_q(X)$.

ii) Q is the pole of ψ in $\mathbb{F}_q(\psi)$ and P is the zero of $X - a$ in $\mathbb{F}_q(X)$.

iii) Q is the zero of $\psi - a$ in $\mathbb{F}_q(\psi)$ and P is the pole of X in $\mathbb{F}_q(X)$.

iv) Q is the pole of ψ in $\mathbb{F}_q(\psi)$ and P is the pole of X in $\mathbb{F}_q(X)$.

Conversely, it is obvious that in all four cases there is a wildly ramified place in the extension $\mathbb{F}_q(X)/\mathbb{F}_q(\psi)$. □

Definition 4.2. *We define a recursive tower of Artin-Schreier type to be of* the first, second, third*, or* fourth kind *if its defining equation corresponds to case one, two, three, or four in Theorem 4.1.*

Note that till now all known asymptotically good, recursive towers of Artin-Schreier type of degree p are of the first kind ([5, 9]). We will show later that recursive towers of Artin-Schreier type of the fourth kind are asymptotically bad. We do not know whether or not there exist asymptotically good towers of Artin-Schreier type of the second or third kind.

Example 4.3 (Example 1.3 continued). We show that the tower considered in Example 1.3 is asymptotically bad. This follows directly from Theorem 4.1, since for p odd the rational function

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

is not of one of the four forms mentioned in that theorem. More generally for q a power of an odd prime number p, one can show using Corollary 2.2 that the Artin-Schreier tower defined recursively by

$$Y^q + Y = \psi(X) = (X + 1)(X^{q-1} - 1)/X^{q-1}$$

is bad, since all pole orders of $\psi(x_r)$ are of the form $2^t(q - 1)$.

We will now start our investigation of recursive towers of Artin-Schreier type of the fourth kind.

Proposition 4.4. *Let $\mathcal{F}$ be a recursive tower of Artin-Schreier type over the finite field $\mathbb{F}_q$ defined by the equation*

$$Y^p + aY = \psi(X),$$

with $a \in \mathbb{F}_q \backslash \{0\}$ *and* $\psi(X) \in \mathbb{F}_q[X] \backslash \mathbb{F}_q[X^p]$ *such that* $\deg \psi(X) = p$. *If* $\mathcal{F}$ *is an asymptotically good tower, then*

$$\psi(X) = bX^p + cX + d,$$

for certain $b, c \in \mathbb{F}_q \backslash \{0\}$ *and* $d \in \mathbb{F}_q$.

Proof. For simplicity we write $z := \psi(x_0)$ and we define inductively $G_0 := \mathbb{F}_q(x_1)$ and $G_n := G_{n-1}(x_{n+1})$, with $x_{n+1}^p + a \cdot x_{n+1} = \psi(x_n)$. We will first prove the claim that, with the exception of the pole of z, every place of the function field $\mathbb{F}_q(z)$ is unramified in the extension $\mathbb{F}_q(x_0)/\mathbb{F}_q(z)$. For that we assume that $\overline{\mathbb{F}}_q$, an algebraic closure of $\mathbb{F}_q$, is the full constant field of the function fields in the tower; i.e., we have performed a constant field extension to an algebraic closure of $\mathbb{F}_q$. Suppose that the place P of $\mathbb{F}_q(z)$ is ramified in the extension $\mathbb{F}_q(x_0)/\mathbb{F}_q(z)$ and that $z \equiv A \pmod{P}$ for some $A \in \overline{\mathbb{F}}_q$. Let Q be a place of the function field $\mathbb{F}_q(x_0)$ lying above P such that the ramification index $e(Q|P) > 1$ and define $e := e(Q|P)$. There exists $\alpha \in \overline{\mathbb{F}}_q$ such that $x_0 \equiv \alpha \pmod{Q}$. From the defining equation of $\mathcal{F}$ we see that the place Q is unramified in any extension F_n/F_0. Choose R to be one of the p^n places of the function field F_n lying above Q. Further write $S := R \cap G_{n-1}$. Note that $S \cap \mathbb{F}_q(z) = P$, since $R \cap \mathbb{F}_q(z) = (R \cap F_0) \cap \mathbb{F}_q(z) = Q \cap \mathbb{F}_q(z) = P$. Again from the defining equation of the tower we see that $e(S|P) = 1$ and hence that $e(R|S) = e$. Since we chose R lying above Q arbitrarily, we see that there exist at least p^n pairs (R, S), with R a place of F_n and S a place of G_{n-1} such that R lies above S and such that $e(R|S) > 1$.

Define the tower $\widehat{\mathcal{F}}$ inductively by $\widehat{F}_0 = \mathbb{F}_q(y_0)$ and $\widehat{F}_n = \widehat{F}_{n-1}(y_n)$, with $\psi(y_n) = y_{n-1}^p + a \cdot y_{n-1}$. Note that since $\mathcal{F}$ is a tower, so is $\widehat{\mathcal{F}}$. Further observe that $\mathcal{F}$ has the same genus as $\widehat{\mathcal{F}}$ and that $\nu(\widehat{\mathcal{F}}) = \nu(\mathcal{F})$. Since for every $n \geq 1$ the extension $\widehat{F}_n/\widehat{F}_{n-1}$ is isomorphic to the extension F_n/G_{n-1}, we see from the above that ramification occurs at least p^n times in $\widehat{F}_n/\widehat{F}_{n-1}$. This means that $\deg \mathrm{Diff}(\widehat{F}_n/\widehat{F}_{n-1}) \geq p^n$, for all $n \geq 1$. However, it then follows from Proposition 2.5 of [5] that $\widehat{\mathcal{F}}$ (and hence $\mathcal{F}$) is asymptotically bad. This proves the claim that, with the exception of the pole of z, every place of the function field $\mathbb{F}_q(z)$ is unramified in the extension $\mathbb{F}_q(x_0)/\mathbb{F}_q(z)$.

Now let α be zero of $\psi'(X)$ and write Q for the place of the function field F_0 defined by $x_0 \equiv \alpha \pmod{Q}$. Further write $P := Q \cap \mathbb{F}_q(z)$ and $A := z \pmod{P}$. Since $\psi'(\alpha) = 0$ we see that α is a multiple zero of $\psi(X) - A$. This means that $e(Q|P) > 1$, contrary to what we have seen above. Hence $\psi'(X)$ does not have zeros, which means that it is a constant. This proves the proposition. □

Similarly as in Proposition 4.4 one can show that if $\mathcal{F}$ is an asymptotically good, recursive Artin-Schreier tower defined by the equation $\varphi(Y) = \psi(X)$, with $\varphi(Y)$ an additive separable polynomial and $\psi(X) \in \mathbb{F}_q[X] \backslash \mathbb{F}_q[X^p]$ a polynomial such that $\deg \psi(X) = \deg \varphi(Y)$, then $\psi(X)$ is of the form $a \cdot X + \vartheta(X^p)$, for a certain $a \in \mathbb{F}_q \backslash \{0\}$ and some polynomial $\vartheta(X)$.

Proposition 4.4 gives a strong restriction on the form the defining equation of an asymptotically good, recursive tower of Artin-Schreier type of the fourth kind can have. Now we investigate if an equation of this form can define a tower.

Proposition 4.5. *Let $a, b, c \in \mathbb{F}_q \backslash \{0\}$ and $d \in \mathbb{F}_q$. A recursive tower of Artin-Schreier type with defining equation*

$$Y^p + aY = bX^p + cX + d$$

does not exist.

Proof. Suppose that a tower $\mathcal{F} = (F_0, F_1, \dots)$ does exist with defining equation as in the proposition. Define by induction on n the functions $t_0^{(i)} := x_i$ and

$$t_n^{(i)} := t_{n-1}^{(i+1)} - b^{1/p^n} \cdot t_{n-1}^{(i)}.$$

Further we define $c_1 := d$ and for all n bigger than one $c_n := d \cdot \prod_{j=1}^{n-1} (1 - b^{1/p^j})$. We show that for all $n \geq 1$ the following holds:

$$(t_n^{(i)})^p + a \cdot t_n^{(i)} = (c - a \cdot b^{1/p^n}) \cdot t_{n-1}^{(i)} + c_n, \text{ for all } i \geq 0. \tag{5}$$

For $n = 1$, this is clear from the equation $x_{i+1}^p + a \cdot x_{i+1} = b \cdot x_i^p + c \cdot x_i + d$. Assuming the result for n, we find:

$$\begin{aligned}(t_{n+1}^{(i)})^p + a \cdot t_{n+1}^{(i)} &= (t_n^{(i+1)})^p + a \cdot t_n^{(i+1)} - b^{1/p^n} \cdot \left((t_n^{(i)})^p + a \cdot t_n^{(i)}\right) - \\ &\quad a \cdot (b^{1/p^{n+1}} - b^{1/p^n}) \cdot t_n^{(i)} = (c - a \cdot b^{1/p^{n+1}}) \cdot t_n^{(i)} + c_{n+1}.\end{aligned}$$

Here we first used the inductive definition of $t_{n+1}^{(i)}$ and then the induction hypothesis in combination with the definitions of $t_n^{(i)}$ and c_{n+1}. Note that $t_n^{(i)}$ is a linear combination of $x_1, x_2, \dots, x_{n+i}$ with coefficient of x_{n+i} equal to one. This and Equation (5) imply that if an n exists such that $c = a \cdot b^{1/p^n}$, $\mathcal{F}$ is not a tower. For in this case the minimal polynomial of $t_n^{(0)}$ over F_{n-1} is not absolutely irreducible, which implies either that the constant field of F_n is larger than that of F_{n-1} or that $F_n = F_{n-1}$. Hence we can assume that for all n the inequality $c \neq a \cdot b^{1/p^n}$ holds.

Define the place P of the function field $\mathbb{F}_q(x_0)$ to be the pole of the function x_0. It is easy to prove by induction (using Equation (5)) that for all $n \geq 1$ the place P is totally ramified in the extension F_n/F_0. Define P_n to be the unique extension of P in the function field F_n. It also follows easily that for all $n \geq 0$ we have $v_{P_n}(t_n^{(0)}) = -1$. However, by construction, the function $t_n^{(0)} \in F_n$ does not have poles apart from P_n, while at P_n the pole is simple. This implies that $F_n = \mathbb{F}_q(t_n^{(0)})$ and hence that for all $n \geq 0$ the genus of the function field F_n is equal to zero. This implies that $\mathcal{F}$ is not a tower, contrary to our assumption. Therefore the proposition follows. □

The above propositions lead to the following theorem (see Definition 4.2):

Theorem 4.6. *Let $\mathcal{F}$ be a recursive tower of Artin-Schreier type of degree p. If $\mathcal{F}$ is asymptotically good, then it is of the first, second, or third kind.*

Proof. By Theorems 3.1 and 4.1, the tower $\mathcal{F}$ is of the first, second, third, or fourth kind. However, by Propositions 4.4 and 4.5 towers of the fourth kind are asymptotically bad. □

References

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

[2] N.D. Elkies, Explicit Modular Towers, Proceedings of the Thirtyt-Fifth Annual Allerton Conference on Communication, Control and Computing, T. Basar and A. Vardy, eds. (1997), 23–32.

[3] N.D. Elkies, Explicit towers of Drinfeld modular curves, Proceedings of the 3rd European Congress of Mathematics, Barcelona, 7/2000.

[4] A. Garcia 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. Garcia 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. Garcia and H. Stichtenoth, Skew pyramids of function fields are asymptotically bad, Coding Theory, Cryptography and Related Areas, J. Buchmann, T. Høholdt, H. Stichtenoth, H. Tapia-Recillas (eds.), Springer Verlag, (2000).

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

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

[9] 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.

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

[11] H. Stichtenoth, Algebraic function fields and codes, Springer-Verlag, Berlin, (1993).

Peter Beelen
Fachbereich 6 Mathematik
Universität Duisburg-Essen, 45117 Essen
GERMANY
E-mail: peter.beelen@uni-essen.de

Arnaldo Garcia
Instituto de Matemática Pura e Aplicada – IMPA
Estrada Dona Castorina 110
22460-320 Rio de Janeiro RJ
BRAZIL
E-mail: garcia@impa.br

Henning Stichtenoth
Fachbereich 6 Mathematik
Universität Duisburg-Essen, 45117 Essen
GERMANY
and
Sabanci University
MDBF, Orhanli, Tuzla
34956, Istanbul
TURKEY
E-mail: stichtenoth@uni-essen.de