On the splitting rate of a tower of Artin-Schreier type
Sobre la tasa de descomposición de una torre de tipo Artin-Schreier
Horacio Navarro
Departamento de Matemáticas, Universidad del Valle, Cali, Colombia

Abstract
In this note we study the asymptotic behaviour of the number of rational places in a tower of function fields of Artin-Schreier type over a finite field with \(2^s\) elements, where \(s > 0\) is an odd integer.

Keywords: Towers of function fields; Splitting rate; Asymptotic behaviour; Number of rational places.

Resumen
En este artículo estudiamos el comportamiento asintótico del número de lugares racionales en una torre de tipo Artín-Schreier sobre un cuerpo finito con \(2^s\) elementos, donde \(s > 0\) es un entero impar.

Palabras clave: Torres de cuerpos de funciones; Tasa de descomposición; Comportamiento asintótico; Número de lugares racionales.

Introduction
Let \(\mathbb{F}_q\) be a finite field with \(q = p^n\) elements, where \(p\) is a prime and \(n \geq 1\) an integer. Let \(F/\mathbb{F}_q\) be an algebraic function field whose constant field is \(\mathbb{F}_p\). (Weil, 1948) proved that the number \(N = N(F)\) of rational places of \(F/\mathbb{F}_q\) is bounded by

\[
N \leq q + 1 + 2g\sqrt{q},
\]

where \(g = g(F)\) denotes the genus of \(F\). (Ihara, 1981) observed that the Weil bound can be improved if \(g\) is large with respect to \(q\). In order to study how many rational places a function field \(F/\mathbb{F}_q\) of large genus can have, he introduced the function

\[
A(q) := \limsup_{g \to \infty} \frac{N_q(g)}{g},
\]

where

\[
N_q(g) := \max \{ N(F) : F \text{ is a function field over } \mathbb{F}_q \text{ of genus } g \}.
\]

In the same paper he used reduction of Shimura curves to prove that \(A(q) \geq \sqrt{q} - 1\) for \(q = p^{2m}\). He also gave the upper bound \(A(q) \leq 1/2 \sqrt{8q + 1}\) which is better that the upper bound for \(A(q)\) obtained from the Weil bound. This result was improved by (Drinfel’d & Vladut, 1983) showing the inequality

\[
0 \leq A(q) \leq \sqrt{q} - 1,
\]

which is still the best known upper bound. Using class field theory, (Serre, 1983) showed that \(A(q) > 0\) for any \(q\). The exact value of \(A(q)\) is however unknown when \(q\) is not a square. (Tsfasman, et al., 1982) showed the existence of linear codes with parameters improving the so-called Gilbert-Varshamov bound using a sequence of modular curves over \(\mathbb{F}_{q^2}\).
that reaches the Drinfel’d-Vladut bound and a construction of linear codes due to Goppa. After that, the interest in the study of the quantity $A(q)$ increased. However, the techniques involved are far from being elementary and the curves (function fields) used are not explicit, which is crucial for potential applications in coding theory.

(Garcia & Stichtenoth, 1995) introduced the concept of recursive towers of function fields over finite fields, i.e., towers defined by bivariate equations $f(x, y) = 0$. However, not any $f(x, y)$ defines a tower, so a convenient choice of $f(x, y)$ must be made. The limit of a recursive tower of function fields over $\mathbb{F}_q$ is a real non-negative real number. One can see that it is a lower bound for $A(q)$. (See section 2 for details).

While the main purpose in this theory is to construct recursive towers with positive limit to obtain non-trivial lower bounds for $A(q)$, this search can be reduced by showing when a recursive tower has limit equal to zero. According to (Garcia & Stichtenoth, 2000), a recursive tower has limit equal to zero if it is skew in the sense that the degree of the equation defining the tower is not the same in each variable. Since a tower with infinite genus has limit equal to zero, (Chara & Toledano, 2015) gave conditions to prove the infiniteness of the genus and noticed that many known examples of non-skew recursive towers with infinite genus are particular cases of these conditions. However, there is not an easy way to determine the limit of a recursive tower non-skew of finite genus.

Among the class of recursive towers there is an important one, namely the class of Artin-Schreier type towers which are recursively defined by equations of the form

$$y^p + by = f(x)$$

for some suitable rational function $f(x) \in \mathbb{F}_q(x)$, where $p = \text{char} \mathbb{F}_q$ and $0 \neq b \in \mathbb{F}_q$. (Beelen et al., 2004) gave necessary conditions on the form of $f(x)$ in order to have a tower with positive limit. Unfortunately, those conditions are not sufficient, so if one chooses one of these $f(x) \in \mathbb{F}_q(x)$ still one has to prove that the equation (1) defines a tower and also to determine the limit of the tower, which is a non-trivial task. For instance, (Ling et al., 2005) showed that the equation (1) defines a tower over $\mathbb{F}_q$, where

$$f(x) = \frac{1}{x^p + cx},$$

$0 \neq c \in \mathbb{F}_q$ and $c \neq b$. Moreover, adding the condition $bc(b - c)^{2p-2} = 1$ they proved that it has finite genus, but so far it has not been possible the determination of the limit of this class of towers.

In (Chara et al., 2018) was proven that sequence $\mathcal{H} = \{F_i\}_{i=0}^m$ of function fields defined by the Artin-Schreier equation

$$y^2 + y = \frac{x}{x^2 + x + 1}$$

is a tower with finite genus over $\mathbb{F}_{2^s}$ for any positive integer $s$ and it is asymptotically good when $s$ is even. In particular, this tower reaches the Drinfeld-Vladut bound when $s = 2$. The main motivation to study this tower over $\mathbb{F}_{2^s}$ for any $s$ odd is that recursive towers over fields with two and three elements with positive limit are not known. The aim of this note is to show that the number of rational places of each function field $F_i$ of the tower $\mathcal{H}$ over $\mathbb{F}_{2^s}$, when $s$ is a positive integer odd, is constant. As a consequence the tower $\mathcal{H}$ over $\mathbb{F}_{2^s}$ for any $s$ odd has limit equal to zero.

1 Notations and Preliminaries

An algebraic function field $F$ over $\mathbb{F}_q$ is a finite algebraic extension $F$ of the rational function field $\mathbb{F}_q(x)$, where $x$ is a transcendental element over $\mathbb{F}_q$. 

1168
Let \( F \) be a function field over \( \mathbb{F}_q \). The symbol \( \mathbb{P}(F) \) stands for the set of all places of \( F \) and \( g(F) \) for the genus.

Let \( F' \) be a finite extension of \( F \) and let \( Q \in \mathbb{P}(F') \). We will write \( Q\mid P \) when the place \( Q \) of \( F' \) lies over the place \( P \) of \( F \), i.e., \( P = Q \cap F \).

A tower \( \mathcal{F} \) of function fields over a finite field \( \mathbb{F}_q \) is a sequence \( \mathcal{F} = \{ F_i \}_{i=0}^\infty \) of function fields over \( F_i/\mathbb{F}_q \) satisfying the following conditions:

1. \( F_i \subset F_{i+1} \) for all \( i \geq 0 \).
2. The extension \( F_{i+1}/F_i \) is finite and separable, for all \( i \geq 1 \).
3. The field \( \mathbb{F}_q \) is algebraically closed in \( F_i \), for all \( i \geq 0 \).
4. The genus \( g(F_i) \to \infty \) as \( i \to \infty \).

A tower of function field \( \mathcal{F} = \{ F_i \}_{i=0}^\infty \) over \( \mathbb{F}_q \) is called a recursive tower if there exist a sequence of transcendental elements \( \{ x_i \}_{i=0}^\infty \) over \( \mathbb{F}_q \) and a bivariate polynomial \( f(x,y) \in \mathbb{F}_q[x,y] \) such that \( F_0 = \mathbb{F}_q(x_0) \) and

\[
F_{i+1} = F(x_i),
\]

where \( f(x_i, x_{i+1}) = 0 \) for all \( i \geq 0 \). In this case we say that the tower \( \mathcal{F} \) is defined by the equation

\[
f(x,y) = 0.\]

The limit \( \lambda(\mathcal{F}) \), the splitting rate \( \nu(\mathcal{F}) \) and the genus of a tower \( \mathcal{F} = \{ F_i \}_{i=0}^\infty \) over \( \mathbb{F}_q \) are defined as

\[
\lambda(\mathcal{F}) := \lim_{i \to \infty} \frac{N(F_i)}{g(F_i)},
\]

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

respectively, where \( N(F_i) \) denote the number of \( \mathbb{F}_q \)-rational points of \( F_i \).

**Proposition 1.1.** *(Stichtenoth, 2009, chap 7)* Let \( \mathcal{F} = \{ F_i \}_{i=0}^\infty \) be a tower over \( \mathbb{F}_q \). Then

i. \( 0 \leq \lambda(\mathcal{F}) \leq A(q) \).

ii. \( 0 \leq \nu(\mathcal{F}) < \infty \).

iii. \( 0 < \gamma(\mathcal{F}) \leq \infty \).

A tower \( \mathcal{F} \) over \( \mathbb{F}_q \) is called asymptotically good if \( \lambda(\mathcal{F}) > 0 \), asymptotically optimal if \( \lambda(\mathcal{F}) = A(q) \) and asymptotically bad if \( \lambda(\mathcal{F}) = 0 \).

As an immediate consequence of the Proposition 1.1 and of the definitions above, one can see that a tower \( \mathcal{F} \) over \( \mathbb{F}_q \) is asymptotically good if and only if \( \nu(\mathcal{F}) > 0 \) and \( \lambda(\mathcal{F}) < \infty \).

In the following theorem we summarize the mean properties of the tower \( \mathcal{H} = \{ F_i \}_{i=0}^\infty \) defined by the equation (2).

**Theorem 1.2.** *(Chara et al., 2018)* Consider the tower \( \mathcal{H} \) over \( \mathbb{F}_{2^s} \), where \( s \) is a positive integer.

i. \( [F_i : F_0] = 2^i \).

ii. \( \mathcal{H} \) has finite genus.
2 The splitting rate of the tower \( \mathcal{H} \)

Throughout this section \( k = \mathbb{F}_{2^s} \) will be a finite field with \( 2^s \) elements where \( s \) is an odd integer and \( \text{Tr} \) denotes the trace map from \( \mathbb{F}_{2^s} \) to \( \mathbb{F}_2 \).

We begin with the following technical lemma.

**Lemma 2.1.** Let \( \theta, \beta \in k \) such that \( \theta^2 + \theta = \frac{\beta}{\beta^2 + \beta + 1} \). Then

\[
\text{Tr}\left(\frac{\theta}{\theta^2 + \theta + 1}\right) \neq \text{Tr}\left(\frac{\theta + 1}{\theta^2 + \theta + 1}\right).
\]

**Proof.** Suppose that

\[
\text{Tr}\left(\frac{\theta}{\theta^2 + \theta + 1}\right) = \text{Tr}\left(\frac{\theta + 1}{\theta^2 + \theta + 1}\right)
\]

then

\[
\text{Tr}\left(\frac{1}{\theta^2 + \theta + 1}\right) = 0. \tag{3}
\]

On the other hand, by hypothesis

\[
\theta^2 + \theta = \frac{\beta}{\beta^2 + \beta + 1}
\]

then

\[
\frac{1}{\theta^2 + \theta + 1} = \frac{\beta^2 + \beta + 1}{\beta^2 + 1} = 1 + \frac{\beta}{\beta^2 + 1} + \left(\frac{\beta}{\beta + 1}\right)^2.
\]

Finally, since \( \text{Tr}(1) = 1 \) and \( \text{Tr}(\alpha) = \text{Tr}(\alpha^2) \) for all \( \alpha \in k \), we have

\[
\text{Tr}\left(\frac{1}{\theta^2 + \theta + 1}\right) = \text{Tr}(1) + \text{Tr}\left(\frac{\beta}{\beta + 1}\right) + \text{Tr}\left(\left(\frac{\beta}{\beta + 1}\right)^2\right) = 1,
\]

contradicting (3).

**Lemma 2.2.** Let \( F \) be a function field over \( k \) such that \( k \) is its full field of constants and let \( x \in F \setminus k \). Consider the Artin-Schreier extensions \( F_1 = F(y) \) and \( F_2 = F_1(z) \) defined by the equations

\[
y^2 + y = \frac{x}{x^2 + x + 1} \quad \text{and} \quad z^2 + z = \frac{y}{y^2 + y + 1},
\]

and the set

\[
S = \left\{ \beta \in k : \text{Tr}\left(\frac{\beta}{\beta^2 + \beta + 1}\right) = 0 \right\}.
\]

Then

i. A rational place \( P \) of \( F \) such that \( x(P) = \infty \) or \( x(P) = \beta \) for some \( \beta \in S \) splits completely in \( F_1 \) into two rational places \( Q_\theta \) and \( Q_{\theta+1} \) such that \( y(Q_\theta) = \theta \) and \( y(Q_{\theta+1}) = \theta + 1 \), for some \( \theta \in k \).

ii. For each pair of rational places \( Q_\theta \) and \( Q_{\theta+1} \) of \( F_1 \) one and only one of them splits completely in \( F_2 \) into two rational places \( Q_\delta \) and \( Q_{\delta+1} \) such that \( z(Q_\delta) = \delta \) and \( z(Q_{\delta+1}) = \delta + 1 \), for some \( \delta \in k \).

iii. The number of rational places \( N(F_i) \) of \( F_i, i = 1, 2 \), is

\[
N(F_i) = 2(|S| + 1).
\]
On the splitting rate of a tower of Artin-Schreier type

doi: https://doi.org/10.18257/raccefyn.1140

F₁ Qβ₁ Qβ₁+1 Q Q Qβ₁ Qβ₁+1
F₂ Qβ Qβ+1 Pβ Pβ

Figure 1. Behaviour of a rational place in \( F_2/F \).

Proof. Let \( P \) be a rational place of \( F \). Then \( x(P) = \beta \) for some \( \beta \in k \) or \( x(P) = \infty \). We write \( P := P_\beta \) or \( P := P_\infty \). Since the extension \( F_1/F \) is defined by the polynomial \( \phi = T^2 + T + \frac{x}{x^2 + x + 1} \in F[T] \) and \( \beta^2 + \beta + 1 \neq 0 \) because \( k = \mathbb{F}_{2^s} \) with \( s \) odd, we have that the reduction modulo \( P \) of \( \phi \) is the polynomial

\[
\phi_\beta = T^2 + T + \frac{\beta}{\beta^2 + \beta + 1} \in k[T],
\]

in the first case, and

\[
\phi_\infty = T^2 + T \in k[T],
\]

in the second one. On the other hand, we know that \( \phi_\beta \) is irreducible over \( k \) if and only if

\[
\text{Tr} \left( \frac{\beta}{\beta^2 + \beta + 1} \right) = 1 \tag{4}
\]

and \( \phi_\beta \) splits completely over \( k \) if and only if

\[
\text{Tr} \left( \frac{\beta}{\beta^2 + \beta + 1} \right) = 0. \tag{5}
\]

Note that \( \beta \notin S \) if and only if \( \beta \) satisfies (4). Hence, by Kummer’s Theorem (Stichtenoth, 2009, Theorem 3.3.7), there is only one place of degree 2 of \( F_1 \) lying over \( P_\beta \) when \( \beta \notin S \) (see figure 1). Now, for \( \beta \in S \cup \{\infty\} \) the polynomial \( \phi_\beta \) splits into two different linear factors over \( k \). Clearly if \( \theta \in k \) is a root of \( \phi_\beta \) then we have that \( \phi_\beta(T) = (T + \theta)(T + (\theta + 1)) \). Again by Kummer’s Theorem, there are exactly two rational places \( Q_\theta, Q_{\theta+1} \) of \( F_1 = F(\gamma) \) lying over \( P_\beta \) such that \( \gamma(Q_\theta) = \theta \) and \( \gamma(Q_{\theta+1}) = \theta + 1 \). This proves (i), and since a rational place of \( F_1 \) lying over a rational place of \( F \), we also have

\[
N(F_1) = 2(|S| + 1).
\]

Now, consider two rational places \( Q_\theta \) and \( Q_{\theta+1} \) of \( F_1 \), for some \( \theta \in k \). For the proof of (i)

\[
\theta^2 + \theta = \frac{\beta}{\beta^2 + \beta + 1},
\]
for some $\beta \in S$. It is clear that the extension $F_2/F_1$ is defined by the polynomial

$$\varphi = T^2 + T + \frac{y}{y^2 + y + 1} \in F_1[T]$$

and the reduction of $\varphi$ modulo $Q_\theta$ and modulo $Q_{\theta+1}$ is the polynomial

$$\varphi_\theta = T^2 + T + \frac{\theta}{\theta^2 + \theta + 1} \quad \text{and} \quad \varphi_{\theta+1} = T^2 + T + \frac{\theta + 1}{\theta^2 + \theta + 1},$$

respectively. By Lemma 2.1, we can assume w.l.o.g. that

$$\text{Tr} \left( \frac{\theta}{\theta^2 + \theta + 1} \right) = 1 \quad \text{and} \quad \text{Tr} \left( \frac{\theta + 1}{\theta^2 + \theta + 1} \right) = 0.$$

This implies that $\varphi_\theta$ is irreducible over $k$ and $\varphi_{\theta+1}$ splits completely over $k$. Hence, by Kummer’s Theorem there is only one place of degree two of $F_2$ lying over $Q_\theta$ and the place $Q_{\theta+1}$ splits completely in $F_2$ into two rational places of the form $Q_\delta$ and $Q_{\delta+1}$ such that $z(Q_\delta) = \delta$ and $z(Q_{\delta+1}) = \delta + 1$, where $\delta \in k$ is a root of $\varphi_{\theta+1}$. (See figure 1). It remains to prove that

$$N(F_2) = 2(|S| + 1).$$

As each rational place $R$ of $F_2$ lies over a rational place of $F_1$, then $R$ lies over a place of the form $Q_\theta$ or $Q_{\theta+1}$ for some $\theta \in k$. By ii), one and only one of these places splits completely in $F_2$. On the other hand, we have seen in the proof of i) that $N(F_1) = 2(|S| + 1)$. Thus, we obtain

$$N(F_2) = N(F_1) = 2(|S| + 1).$$

Now we are in a position to state and prove one of our main results.

**Theorem 2.3.** Consider the tower $\mathcal{H} = \{F_i\}_{i=0}^\infty$ over $k$. The number of rational places $N(F_i)$ of $F_i$ is

$$N(F_i) = 2(|S| + 1),$$

for all $i \geq 1$, where $S$ is defined as in Lemma 2.2.

**Proof.** Let $P_0$ be the only zero of $x_0 + \alpha$ in $F_0 = k(x_0)$ and $P_\infty$ be the only pole of $x_0$ in $F_0$. We show by induction that a place $P_\alpha$, with $\alpha \in S \cup \{\infty\}$, has exactly two rational places in $F_i$ for all $i \geq 1$. It is true for $i = 1$ by Lemma 2.2, and we assume now that the assertion holds for some $i$. Let $R_1$ and $R_2$ the two rational places in $F_i$ lying over $P_\alpha$. We have proved in Lemma 2.2 that both places $R_1$ and $R_2$ lying over a rational place $P_\beta$ of $F_{i-1}$ for some $\beta \in S$, and one and only one place between $R_1$ and $R_2$ has two rational places in $F_{i+1}$. Hence, there exist two rational places in $F_{i+1}$ lying over $P_\alpha$. Finally, we conclude that

$$N(F_i) = 2(|S| + 1)$$

for all $i \geq 1$. \(\square\)

As an immediate consequence of the above result we have:

**Theorem 2.4.** The splitting rate of the tower $\mathcal{H}$ over $k$ is zero.

**Proof.** From Theorem 2.3 we have that

$$\nu(\mathcal{H}) = \lim_{i \to \infty} \frac{N(F_i)}{[F_i:F_0]} = \lim_{i \to \infty} \frac{2(|S| + 1)}{2^i} = 0.$$ \(\square\)
Corollary 2.5. The tower $\mathcal{H}$ over $k$ is asymptotically bad.

Proof. Since

$$\lambda(\mathcal{H}) = \lim_{i \to \infty} \frac{N(F_i)}{g(F_i)} = \frac{v(\mathcal{H})}{\gamma(\mathcal{H})},$$

we conclude $\lambda(\mathcal{H}) = 0$.

3 Conclusions

In this note we have completed the classification of the asymptotic behavior of the tower $\mathcal{H}$ over a finite field with $2^s$ in terms of the parity of $s$. This work was started by (Chara et al., 2018). As stated by (Beelen et al., 2006) there are only four recursive towers of Artin-Schreier type over a field with two elements including the tower $\mathcal{H}$. As a future work, one can study the remaining three in order to determine if is possible a classification such as the one given above.

4 Conflict of interest

The author declares that he has no conflict of interest.

References


