Towards a Classification of Recursive Towers of Function Fields over Finite Fields*

Peter Beelen, Arnaldo Garcia and Henning Stichtenoth

Abstract: In this paper we derive "normal forms" for the defining equations of recursive towers of function fields over finite fields, under certain weak hypotheses. Specially interesting are the cases of towers of Kummer type and towers of Artin-Schreier type.

1 Introduction

The interest in solutions of polynomial equations over finite fields has a long history in mathematics, going back at least to C.F. Gauß. When the polynomial equations define an absolutely irreducible algebraic curve (projective and nonsingular), we have the famous theorem of A. Weil bounding the number of solutions with all coordinates in a finite field, in terms of the genus g of the curve and of the cardinality q of the finite field. Denote by $N_q(g)$ the largest number of rational points over the finite field $\mathbb{F}_q$ on an irreducible curve (projective and nonsingular) defined over $\mathbb{F}_q$ with genus g. Then we have the following bound (the so-called Hasse-Weil upper bound):

$$N_q(g) \leq q + 1 + 2\sqrt{q} \cdot g. \tag{1.1}$$

Ihara noticed that this bound can be improved significantly if the genus of the curve is large; he introduced the quantity $A(q)$ in order to study the asymptotics of curves over a fixed finite field $\mathbb{F}_q$:

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

From Equation (1.1) we clearly have $A(q) \leq 2\sqrt{q}$. The best upper bound known for $A(q)$ is the so-called Drinfeld-Vladut bound, see [5]:

$$A(q) \leq \sqrt{q} - 1. \tag{1.2}$$

To deal with the quantity $A(q)$, one considers towers of curves or of function fields over finite fields, specially recursive towers (see Definition 2.2).

*This work was partially done when the authors visited Sabancı University, İstanbul, Turkey in the period Sept. 2003–Jan. 2004. A. Garcia was also supported by PRONEX # 662408/1996-3(CNPq-Brazil).

The aim of this paper is to show how to transform the defining equation of a recursive tower of function fields

$$f(Y) = g(X), \quad \text{with rational functions} \quad f(T), g(T) \in \mathbb{F}_q(T)$$

obtaining another defining equation for the same tower

$$\tilde{f}(Y) = \tilde{g}(X)$$

where the rational functions $\tilde{f}(T), \tilde{g}(T) \in \mathbb{F}_q(T)$ have very special forms (see Theorems 4.3, 5.2, 6.2, 6.4 and 7.3).

Our results can be considered as a way of classifying recursive towers over $\mathbb{F}_q$. They are also a first step in tackling the "fantasia" of N. Elkies which states that every recursively defined tower which attains the Drinfeld-Vladut bound is modular, see [6]. Finally we hope that our results will lead to the discovery of new examples of asymptotically good towers.

2 Preliminaries

Let $\mathbb{F}_q$ denote the finite field of cardinality q. An algebraic function field $F/\mathbb{F}_q$ is a finite algebraic extension of the rational function field $\mathbb{F}_q(t)$. We will always assume implicitly that the field $\mathbb{F}_q$ is algebraically closed in F; i.e., the only elements of F which are algebraic over $\mathbb{F}_q$ are the elements of $\mathbb{F}_q$. We denote by $g(F)$ the genus of the function field F and by $N(F)$ the number of rational places (i.e., places of degree one) of $F/\mathbb{F}_q$.

Definition 2.1 A *tower of function fields over* $\mathbb{F}_q$ is an infinite sequence $\mathcal{F} = (F_0, F_1, F_2, \dots)$ of function fields $F_n/\mathbb{F}_q$ having the following properties:

(1) $F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots$, and for all $n \geq 0$ the extension F_{n+1}/F_n is separable of degree $[F_{n+1} : F_n] > 1$.

(2) For some $r \geq 0$ the function field $F_r/\mathbb{F}_q$ has genus $g(F_r) > 1$.

Observe that $g(F_n) \to \infty$ as $n \to \infty$; this follows easily from conditions (1) and (2) using the Hurwitz genus formula (see [12, Thm.III.4.12]).

Of particular interest are "asymptotically good" towers $\mathcal{F} = (F_n)_{n\geq 0}$ over $\mathbb{F}_q$, which means that each function field F_n has many rational places compared to its genus. To make this definition precise, we first remark that for any tower $\mathcal{F} = (F_n)_{n\geq 0}$ over $\mathbb{F}_q$ the limit

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

exists (see [8]). From the Drinfeld-Vladut bound (1.2) we derive $\lambda(\mathcal{F}) \leq \sqrt{q} - 1$. The tower $\mathcal{F}$ is said to be *asymptotically good* (resp. *asymptotically bad*) if $\lambda(\mathcal{F}) > 0$ (resp. $\lambda(\mathcal{F}) = 0$).

We say that a tower $\mathcal{F} = (F_n)_{n\geq 0}$ is *given explicitly* if there are given elements $x_i \in F_i$ and polynomials $0 \neq \varphi_i(T) \in F_i[T]$ such that $F_{n+1} = F_n(x_{n+1})$ and $\varphi_n(x_{n+1}) = 0$, for all $n \geq 0$. It is a non-trivial problem to provide explicitly given asymptotically good towers. Most examples to be found in the literature are of the following type, cf. Section 3 below:

Definition 2.2 Let $\mathcal{F} = (F_n)_{n\geq 0}$ be a tower of function fields over $\mathbb{F}_q$, and let $f(T), g(T) \in \mathbb{F}_q(T)$ be two separable rational functions with coefficients in the field $\mathbb{F}_q$. We say that the tower $\mathcal{F}$ *can be described recursively* by the equation

$$f(Y) = g(X) \tag{2.1}$$

if there are elements x_i, for all $i \geq 0$, such that the following holds:

(1) $F_0 = \mathbb{F}_q(x_0)$ is the rational function field.

(2) $F_{n+1} = F_n(x_{n+1})$ and $f(x_{n+1}) = g(x_n)$, for all $n \geq 0$.

(3) $[F_{n+1} : F_n] = \deg f(T)$, for all $n \geq 0$.

Recall that the function $f(T)$ is called separable if $f \notin \mathbb{F}_q(T^p)$, where p denotes the characteristic of $\mathbb{F}_q$, and also recall that the degree of a rational function $f(T) = a(T)/b(T)$, with relatively prime polynomials $a(T), b(T) \in \mathbb{F}_q[T]$, is defined as $\deg f(T) = \max\{\deg a(T), \deg b(T)\}$.

Definition 2.3 If the tower is recursively described by Equation (2.1), we say that $\mathcal{F}$ is an (f, g)-*tower* over $\mathbb{F}_q$, and we define the *corresponding basic function field* of Equation (2.1) as

$$F := \mathbb{F}_q(x, y) \quad \text{with} \quad f(y) = g(x). \tag{2.2}$$

Note that the extensions $F/\mathbb{F}_q(x)$ and $F/\mathbb{F}_q(y)$ are separable and that $\mathbb{F}_q$ is algebraically closed in F by our general assumption. Moreover, defining for convenience $z := f(y) = g(x)$ we have $\mathbb{F}_q(z) = \mathbb{F}_q(x) \cap \mathbb{F}_q(y)$ and

$$[F : \mathbb{F}_q(x)] = [\mathbb{F}_q(y) : \mathbb{F}_q(z)] = \deg f(T),$$

$$[F : \mathbb{F}_q(y)] = [\mathbb{F}_q(x) : \mathbb{F}_q(z)] = \deg g(T).$$

Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2, \mathbb{F}_q)$ (i.e., $a, b, c, d \in \mathbb{F}_q$ and $ad \neq bc$), and let u be an element in some extension field of $\mathbb{F}_q$, with $cu + d \neq 0$. Then we set

$$A \cdot u := \frac{au + b}{cu + d}.$$

If the tower $\mathcal{F} = (F_n)_{n\geq 0}$ is described recursively by the equation $f(Y) = g(X)$, we can perform a transformation of the variables $x_0, x_1, \ldots$ by setting $x_i = A \cdot \tilde{x}_i$,

for all $i \geq 0$. It is then clear that $F_0 = \mathbb{F}_q(\tilde{x}_0)$ and $F_{n+1} = F_n(\tilde{x}_{n+1})$, and that the functions $\tilde{x}_i$ satisfy the equation

$$\tilde{f}(\tilde{x}_{n+1}) = \tilde{g}(\tilde{x}_n), \text{ with } \tilde{f}(T) := f(A \cdot T) \text{ and } \tilde{g}(T) := g(A \cdot T). \tag{2.3}$$

This means that the tower $\mathcal{F}$ can also be described recursively by the equation $\tilde{f}(Y) = \tilde{g}(X)$.

A necessary condition for an (f, g)-tower $\mathcal{F}$ to be asymptotically good is that $\deg f(T) = \deg g(T)$, see [7]. There are, however, more delicate restrictions: the ramification behaviour of the two extensions $F/\mathbb{F}_q(x)$ and $F/\mathbb{F}_q(y)$ (where $F = \mathbb{F}_q(x, y)$ is the corresponding basic function field) should be "similar". For a precise formulation of this statement see [2]. In Section 4–7 we will show that - under rather weak assumptions about ramification in the extensions $F/\mathbb{F}_q(x)$ and $F/\mathbb{F}_q(y)$ - an (f, g)-tower $\mathcal{F}$ can be described recursively by an equation $\tilde{f}(Y) = \tilde{g}(X)$, where $\tilde{f}(T)$ and $\tilde{g}(T)$ have a very special form.

3 Examples of recursive towers

In this section we assemble a list of known examples of asymptotically good (f, g)-towers over $\mathbb{F}_q$. These examples serve as motivation and illustration for our results in Sections 4–7.

Example 3.1 ([9, 10]) Let $m \geq 2$ and $\gcd(m, q) = 1$, and let $a, b, c \in \mathbb{F}_q \backslash \{0\}$. Then the equation

$$Y^m = a(X + b)^m + c \tag{3.1}$$

recursively defines a tower $\mathcal{F}_1$ of function fields over $\mathbb{F}_q$; we call $\mathcal{F}_1$ a tower of *Fermat type*. For various choices of q, m, a, b, c such towers provide examples for many phenomena that can occur in the theory of recursive towers. For example, some towers of Fermat type are completely splitting, some have finite ramification locus, others have infinite ramification locus (for precise definitions see [9, Sec. 2]). Among the towers of Fermat type there are asymptotically good and also asymptotically bad towers. Particularly interesting are the following two cases of asymptotically good towers, whose limits attain the Drinfeld-Vladut bound $\lambda(\mathcal{F}) = \sqrt{q} - 1$, see [10]:

$$Y^3 = (X + 1)^3 + 1 \quad \text{over} \quad \mathbb{F}_4, \tag{3.2}$$

$$Y^2 = -(X + 1)^2 + 1 \quad \text{over} \quad \mathbb{F}_9. \tag{3.3}$$

Example 3.2 For any prime power $q = p^{2s} \equiv 1 \bmod 2$, the equation

$$Y^2 = \frac{X^2 + 1}{2X} \tag{3.4}$$

defines an asymptotically good tower $\mathcal{F}_2$ over the finite field $\mathbb{F}_q$. Over the finite field $\mathbb{F}_{p^2}$ (p an odd prime) this tower attains the Drinfeld-Vladut bound

$\lambda(\mathcal{F}_2) = p-1$, see [9]. Some other examples of interesting towers defined by a quadratic equation

$$Y^2 = g(X) \quad \text{with} \quad g(X) \in \mathbb{F}_q(X) \quad \text{and} \quad \deg g(X) = 2 \tag{3.5}$$

are given in [6, 9].

Example 3.3 ([6, 13]) For some values of q and m (with $\gcd(m, q) = 1$), the equation

$$Y^m = 1 - \left(\frac{X}{X-1}\right)^m \tag{3.6}$$

defines an asymptotically good tower $\mathcal{F}_3 = (F_0, F_1, F_2, \dots)$ over $\mathbb{F}_q$. The interesting feature here is that this tower $\mathcal{F}_3$ is unramified over the third field F_2 in the tower.

Example 3.4 ([6]) Let p be a prime number, $p \neq 5$, and consider the polynomial $f(T) = T^5 + 5T^3 - 5T - 11 \in \mathbb{F}_p[T]$. Then the equation

$$f(Y) = \frac{125}{f\left(\frac{X+4}{X-1}\right)} \tag{3.7}$$

defines a tower $\mathcal{F}_4$ over $\mathbb{F}_{p^2}$ whose limit attains the Drinfeld-Vladut bound; i.e., we have $\lambda(\mathcal{F}_4) = p-1$.

Example 3.5 ([8]) For any prime power q, the equation

$$Y^q + Y = \frac{X^q}{X^{q-1}+1} \tag{3.8}$$

defines an asymptotically good tower $\mathcal{F}_5$ over $\mathbb{F}_{q^2}$, whose limit attains the Drinfeld-Vladut bound.

Example 3.6 ([11]) The equation

$$Y^2 + Y = X + 1 + \frac{1}{X} \tag{3.9}$$

defines an asymptotically good tower $\mathcal{F}_6$ over the field $\mathbb{F}_8$. Its limit is given by $\lambda(\mathcal{F}_6) = 3/2$. This tower was the first known explicit example of a tower over a field $\mathbb{F}_q$ with non-square cardinality whose limit is large. In fact, its limit attains Zink's bound, see [14].

Example 3.7 ([3]) The equation

$$\frac{Y-1}{Y^q} = \frac{X^q - 1}{X} \tag{3.10}$$

defines a tower $\mathcal{F}_7$ over the field $\mathbb{F}_{q^2}$ whose limit attains the Drinfeld-Vladut bound. For the corresponding basic function field $F = \mathbb{F}_{q^2}(x, y)$, both extensions $F/\mathbb{F}_{q^2}(x)$ and $F/\mathbb{F}_{q^2}(y)$ are non-Galois for $q > 2$.

Example 3.8 ([4]) The equation

$$\frac{1-Y}{Y^q} = \frac{X^q + X - 1}{X} \tag{3.11}$$

defines an asymptotically good tower $\mathcal{F}_8$ over the field $\mathbb{F}_{q^3}$. This interesting tower generalizes Example 3.6 to arbitrary cubic fields. Its limit satisfies Zink's bound (see [14]):

$$\lambda(\mathcal{F}_8) \geq \frac{2(q^2-1)}{q+2}.$$

As in Example 3.7, the extensions $F/\mathbb{F}_{q^3}(x)$ and $F/\mathbb{F}_{q^3}(y)$ in the corresponding basic function field $F = \mathbb{F}_{q^3}(x, y)$ are non-Galois for $q > 2$.

Definition 3.9 Given an (f, g)-tower $\mathcal{F}$ over $\mathbb{F}_q$, we define its *dual tower* $\mathcal{G}$ as the tower recursively given by the equation

$$g(Y) = f(X);$$

i.e., by interchanging the variables X and Y (see [2]).

It is clear that an (f, g)-tower $\mathcal{F}$ and its dual $\mathcal{G}$ have the same limit $\lambda(\mathcal{F}) = \lambda(\mathcal{G})$.

As an example of this concept we consider below the dual tower of the tower in Example 3.6.

Example 3.10 The dual tower $\mathcal{G}$ of the tower $\mathcal{F}_6$ in Example 3.6 is defined by the equation

$$Y + 1 + \frac{1}{Y} = X^2 + X. \tag{3.12}$$

The substitution $Y = (\tilde{Y}+1)/\tilde{Y}$ and $X = (\tilde{X}+1)/\tilde{X}$ transforms Equation (3.12) into the equation $\tilde{Y}^2 + \tilde{Y} = \tilde{X}^2/(\tilde{X}^2 + \tilde{X} + 1)$. Hence the tower $\mathcal{G}$ can also be described by the equation

$$Y^2 + Y = \frac{X^2}{X^2 + X + 1}. \tag{3.13}$$

Considering the examples above, we make the following interesting observation:

Observation 3.11 We remark that all defining equations $f(Y) = g(X)$ for the towers given in Examples 3.1–3.10 can be written in the form

$$f(Y) = A \cdot f(B \cdot X) \quad \text{with} \quad A, B \in \mathrm{GL}(2, \mathbb{F}_q). \tag{3.14}$$

This remark is obvious for the towers given in Examples 3.1, 3.3 and 3.4. In Example 3.5 we have $f(Y) = Y^q + Y$ and

$$g(X) = \frac{X^q}{X^{q-1}+1} = A \cdot f(B \cdot X) \quad \text{with} \quad A = B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

The proof of this remark in the other examples is left to the reader; we will come back to Observation 3.11 in Section 4.

4 Transformations of the defining equation of a recursive tower

In this section we study the effect of variable transformations on the defining equation of a recursive tower. The following result is crucial.

Theorem 4.1 *Let $\mathcal{F}$ be a tower of function fields over $\mathbb{F}_q$ which can be described recursively by the equation $f_1(Y) = g_1(X)$, with rational functions $f_1(T), g_1(T) \in \mathbb{F}_q(T)$. Denote by $F = \mathbb{F}_q(x, y)$ the corresponding basic function field and set $z := f_1(y) = g_1(x) \in F$. Suppose that $f(T), g(T) \in \mathbb{F}_q(T)$ are rational functions with the following properties:*

(1) $\deg f(T) = \deg f_1(T)$ *and* $\deg g(T) = \deg g_1(T)$.

(2) *There exist elements $\overline{x}$ and $\overline{y}$ in the field F such that $\mathbb{F}_q(x) = \mathbb{F}_q(\overline{x})$, $\mathbb{F}_q(y) = \mathbb{F}_q(\overline{y})$, $f(\overline{y}) \in \mathbb{F}_q(z)$ and $g(\overline{x}) \in \mathbb{F}_q(z)$.*

Then the tower $\mathcal{F}$ can also be described recursively by an equation of the form

$$f(Y) = A \cdot g(B \cdot X)$$

for suitable matrices $A, B \in \mathrm{GL}(2, \mathbb{F}_q)$.

Proof. It is clear from (1) and (2) that $\mathbb{F}_q(z) = \mathbb{F}_q(f(\overline{y})) = \mathbb{F}_q(g(\overline{x}))$. Hence there exists a matrix $A \in \mathrm{GL}(2, \mathbb{F}_q)$ such that

$$f(\overline{y}) = A \cdot g(\overline{x}).$$

We write $\overline{y} = C \cdot y$ and $\overline{x} = D \cdot x$ with $C, D \in \mathrm{GL}(2, \mathbb{F}_q)$. Then

$$f(C \cdot y) = A \cdot g(D \cdot x) = A \cdot g((DC^{-1}) \cdot (C \cdot x)).$$

Setting $B = DC^{-1}$, $\tilde{y} = C \cdot y$ and $\tilde{x} = C \cdot x$, we see that

$$f(\tilde{y}) = A \cdot g(B \cdot \tilde{x}).$$

□

The observation at the end of Section 3 shows that many interesting towers can be defined by an equation of the form $f(Y) = A \cdot f(B \cdot X)$. This motivates the following definition.

Definition 4.2 Let $f(T) \in \mathbb{F}_q(T)$ be a rational function. A tower $\mathcal{F}$ of function fields over $\mathbb{F}_q$ is called an *f-tower* if there exist matrices $A, B \in \mathrm{GL}(2, \mathbb{F}_q)$ such that $\mathcal{F}$ can be described recursively by the equation $f(Y) = A \cdot f(B \cdot X)$.

All towers in Examples 3.1–3.10 are in fact f-towers for an appropriate choice of the rational function $f(T)$. We have the following immediate consequence of Theorem 4.1:

Theorem 4.3 *Let $\mathcal{F}$ be a tower of function fields over $\mathbb{F}_q$ which can be described recursively by the equation $f_1(Y) = g_1(X)$ with $f_1(T), g_1(T) \in \mathbb{F}_q(T)$. Let $F = \mathbb{F}_q(x,y)$ be the corresponding basic function field and set $z := f_1(y) = g_1(x) \in F$. Suppose that $f(T) \in \mathbb{F}_q(T)$ is another rational function with the properties:*

(1) $\deg f(T) = \deg f_1(T) = \deg g_1(T)$.

(2) *There exist elements $\overline{x}$ and $\overline{y}$ in the field F such that $\mathbb{F}_q(x) = \mathbb{F}_q(\overline{x})$, $\mathbb{F}_q(y) = \mathbb{F}_q(\overline{y})$, $f(\overline{x}) \in \mathbb{F}_q(z)$ and $f(\overline{y}) \in \mathbb{F}_q(z)$.*

Then the tower $\mathcal{F}$ is an f-tower; i.e., it can be described recursively by

$$f(Y) = A \cdot f(B \cdot X)$$

for suitable matrices $A, B \in \mathrm{GL}(2, \mathbb{F}_q)$.

In Sections 5–7 we will apply Theorem 4.1 and 4.3 in specific cases; in particular we will consider the case where both extensions $F/\mathbb{F}_q(x)$ and $F/\mathbb{F}_q(y)$ are Galois extensions.

5 Towers of Kummer type

Let $\mathcal{F}$ be an (f,g)-tower of function fields over $\mathbb{F}_q$ and denote by $F = \mathbb{F}_q(x,y)$ the corresponding basic function field. Here we investigate the case where both extensions $F/\mathbb{F}_q(x)$ and $F/\mathbb{F}_q(y)$ are Galois extensions of degree m, with m relatively prime to q.

Lemma 5.1 *Let $\mathbb{F}_q(u) \supseteq \mathbb{F}_q(z)$ be an extension of rational function fields of degree $[\mathbb{F}_q(u) : \mathbb{F}_q(z)] = m > 1$ with $m \mid (q-1)$. Then the following conditions are equivalent:*

(i) *The extension $\mathbb{F}_q(u)/\mathbb{F}_q(z)$ is Galois, and there exists a rational place of $\mathbb{F}_q(z)$ which is totally ramified in $\mathbb{F}_q(u)$.*

(ii) *At least two places of $\mathbb{F}_q(z)$ are totally ramified in the extension $\mathbb{F}_q(u)/\mathbb{F}_q(z)$.*

(iii) *There is an element $\tilde{u} \in \mathbb{F}_q(u)$ such that $\mathbb{F}_q(\tilde{u}) = \mathbb{F}_q(u)$ and $\tilde{u}^m \in \mathbb{F}_q(z)$.*

If one (and hence all) of the three conditions above holds, then the Galois group of $\mathbb{F}_q(u)/\mathbb{F}_q(z)$ is cyclic, exactly two rational places of $\mathbb{F}_q(z)$ are totally ramified and all other places of $\mathbb{F}_q(z)$ are unramified in the extension $\mathbb{F}_q(u)/\mathbb{F}_q(z)$.

Proof. (i) $\Rightarrow$ (ii): Let P be a rational place of $\mathbb{F}_q(z)$ which is totally ramified, and let $P_1, \ldots, P_r$ be the other places of $\mathbb{F}_q(z)$ which are ramified in the extension $\mathbb{F}_q(u)/\mathbb{F}_q(z)$. Denote by e_j the ramification index of P_j in $\mathbb{F}_q(u)/\mathbb{F}_q(z)$ and by $\deg P_j$ the degree of the place P_j, for $j = 1, \ldots, r$. Since ramification is tame, the Hurwitz genus formula for the extension $\mathbb{F}_q(u)/\mathbb{F}_q(z)$ gives

$$-2 = -2m + (m-1) + \sum_{j=1}^{r} \frac{m}{e_j} \cdot (e_j - 1) \cdot \deg P_j,$$

hence

$$\sum_{j=1}^{r} \left(1 - \frac{1}{e_j}\right) \cdot \deg P_j = 1 - \frac{1}{m}.$$

Since $1/e_j \leq 1/2$, we obtain

$$1 > 1 - \frac{1}{m} \geq \sum_{j=1}^{r} \frac{\deg P_j}{2},$$

and therefore $r = \deg P_1 = 1$ and $e_1 = m$. This proves item (ii).

(ii) $\Rightarrow$ (iii): Let P_1, Q_1 be places of $\mathbb{F}_q(z)$ which are totally ramified in the extension $\mathbb{F}_q(u)/\mathbb{F}_q(z)$, and denote by P (resp. Q) the place of $\mathbb{F}_q(u)$ lying above P_1 (resp. Q_1). As above it follows from the Hurwitz genus formula that the places P_1 and Q_1 (hence also the places P and Q) are rational places. In a rational function field, any divisor of degree 0 is principal, hence we can find elements $\tilde{u} \in \mathbb{F}_q(u)$ and $\tilde{z} \in \mathbb{F}_q(z)$ with principal divisors

$$(\tilde{u})_{\mathbb{F}_q(u)} = P - Q \quad \text{and} \quad (\tilde{z})_{\mathbb{F}_q(z)} = P_1 - Q_1.$$

Above we have denoted by $(t)_E$ the principal divisor of the function t in the function field E. It follows that

$$(\tilde{u}^m)_{\mathbb{F}_q(u)} = mP - mQ = (\tilde{z})_{\mathbb{F}_q(u)},$$

and hence $\tilde{u}^m = c \cdot \tilde{z}$ with $0 \neq c \in \mathbb{F}_q$. The element $\tilde{u}$ is a generator of the function field $\mathbb{F}_q(u)$, since its pole divisor has degree one. We have thus proved item (iii).

(iii) $\Rightarrow$ (i): Observing that the field $\mathbb{F}_q$ contains the m-th roots of unity, this implication is obvious: the automorphisms of the extension $\mathbb{F}_q(u)/\mathbb{F}_q(z)$ are given by $\sigma(\tilde{u}) = \zeta \cdot \tilde{u}$ with $\zeta^m = 1$ and the zero of $\tilde{u}$ is totally ramified in the extension $\mathbb{F}_q(u)/\mathbb{F}_q(z)$. □

Now we come to the main result of this section.

Theorem 5.2 *Let $\mathcal{F}$ be an (f_1, g_1)-tower of function fields over $\mathbb{F}_q$ and denote by $F = \mathbb{F}_q(x, y)$ the corresponding basic function field. Suppose that the following conditions hold:*

(1) $\deg f_1(T) = \deg g_1(T) = m$ *and* m *divides* $(q-1)$.

(2) *Both extensions $\mathbb{F}_q(x)/\mathbb{F}_q(g_1(x))$ and $\mathbb{F}_q(y)/\mathbb{F}_q(f_1(y))$ satisfy the equivalent conditions* (i)–(iii) *of Lemma 5.1.*

Then $\mathcal{F}$ is an f-tower with $f(T) = T^m$. More specifically, the tower $\mathcal{F}$ can be described recursively by an equation of the form

$$Y^m = \frac{a(X+1)^m + b(X+\gamma)^m}{c(X+1)^m + d(X+\gamma)^m} \tag{5.1}$$

with $a, b, c, d, \gamma \in \mathbb{F}_q$, $\gamma \neq 1$ and $ad \neq bc$.

Proof. By Theorem 4.3 and Lemma 5.1, the tower $\mathcal{F}$ is an f-tower with $f(T) = T^m$. This means that $\mathcal{F}$ can be described recursively by an equation

$$Y^m = \frac{a_1 \left(\dfrac{\alpha_1 X + \beta_1}{\gamma_1 X + \delta_1} \right)^m + b_1}{c_1 \left(\dfrac{\alpha_1 X + \beta_1}{\gamma_1 X + \delta_1} \right)^m + d_1} = \frac{a_1(\alpha_1 X + \beta_1)^m + b_1(\gamma_1 X + \delta_1)^m}{c_1(\alpha_1 X + \beta_1)^m + d_1(\gamma_1 X + \delta_1)^m} \tag{5.2}$$

with $a_1 d_1 \neq b_1 c_1$ and $\alpha_1 \delta_1 \neq \beta_1 \gamma_1$.

We first consider the case where $\alpha_1 \neq 0$ and $\gamma_1 \neq 0$. Then it follows that $\beta_1 \neq 0$ or $\delta_1 \neq 0$, and we can assume that $\beta_1 \neq 0$. Substituting $Y = \alpha_1^{-1}\beta_1 \tilde{Y}$ and $X = \alpha_1^{-1}\beta_1 \tilde{X}$ we obtain

$$\left(\frac{\beta_1}{\alpha_1} \right)^m \tilde{Y}^m = \frac{a_1(\beta_1 \tilde{X} + \beta_1)^m + b_1(\alpha_1^{-1}\beta_1\gamma_1 \tilde{X} + \delta_1)^m}{c_1(\beta_1 \tilde{X} + \beta_1)^m + d_1(\alpha_1^{-1}\beta_1\gamma_1 \tilde{X} + \delta_1)^m},$$

hence

$$\tilde{Y}^m = \frac{a(\tilde{X} + 1)^m + b(\tilde{X} + \gamma)^m}{c(\tilde{X} + 1)^m + d(\tilde{X} + \gamma)^m} \tag{5.3}$$

It is clear that $\gamma \neq 1$ and $ad \neq bc$, since otherwise Equation (5.3) is not absolutely irreducible.

Next we consider the case where $\alpha_1 = 0$ or $\gamma_1 = 0$ in Equation (5.2). We can assume that $\gamma_1 = 0$ and $\alpha_1 \neq 0$, and then Equation (5.2) takes the form

$$Y^m = \frac{a_2(X + \beta_2)^m + b_2}{c_2(X + \beta_2)^m + d_2} \quad \text{with} \quad a_2, b_2, c_2, d_2, \beta_2 \in \mathbb{F}_q. \tag{5.4}$$

Suppose that $\beta_2 = 0$; then Equation (5.4) can be written as $Y^m = C \cdot X^m$ with a matrix $C \in \mathrm{GL}(2, \mathbb{F}_q)$. For the functions $x_0, x_1, x_2, \dots$ in the tower $\mathcal{F} = (F_0, F_1, F_2, \dots)$ this means that

$$x_1^m = C \cdot x_0^m\,, \quad x_2^m = C \cdot x_1^m = C^2 \cdot x_0^m\,, \ \dots\ , \quad x_n^m = C^n \cdot x_0^m$$

for all $n \geq 1$. Since $\mathrm{GL}(2, \mathbb{F}_q)$ is a finite group, we have $C^n = \mathrm{id}$ for some $n \geq 1$, and therefore $x_n^m = x_0^m$, $x_{n+1}^m = x_1^m$, etc. It follows that we have the equalities $F_{n-1} = F_n = F_{n+1} = \cdots$, a contradiction. We have thus shown that $\beta_2 \neq 0$ in Equation (5.4). The substitution $X = \beta_2/\tilde{X}$ and $Y = \beta_2/\tilde{Y}$ then transforms Equation (5.4) into

$$\tilde{Y}^m = \frac{a_3(\tilde{X} + 1)^m + b_3 \tilde{X}^m}{c_3(\tilde{X} + 1)^m + d_3 \tilde{X}^m}$$

which has the form as in Equation (5.1). □

We remark that Equation (5.1) can also be written as

$$f(Y) = A \cdot f(B \cdot X) \quad \text{with} \quad f(T) = T^m,\ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix},\ B = \begin{pmatrix} 1 & 1 \\ 1 & \gamma \end{pmatrix},$$

where $ad \neq bc$ and $\gamma \neq 1$.

A tower $\mathcal{F}$ which can be recursively described by Equation (5.1) is called a *tower of Kummer type*, since both extensions $F/\mathbb{F}_q(x)$ and $F/\mathbb{F}_q(y)$ are Kummer extensions, where we again denote by $F = \mathbb{F}_q(x,y)$ the corresponding basic function field. This class of towers contains the towers of Fermat type (see Example 3.1) and some other towers discussed in Section 3 (see Equations (3.4), (3.5) and (3.6)).

6 Towers of Artin-Schreier type

Some of the examples of towers in Section 3 are described recursively by an equation of the form $Y^\ell + aY = g(X)$, where ℓ is a power of $p = \mathrm{char}(\mathbb{F}_q)$, and with $0 \neq a \in \mathbb{F}_q$ and $g(X) \in \mathbb{F}_q(X)$. In this section we will discuss equations of this type. Let $p = \mathrm{char}(\mathbb{F}_q)$ denote the characteristic of $\mathbb{F}_q$. Recall that a monic polynomial $\wp(T) \in \mathbb{F}_q[T]$ of the form

$$\wp(T) = \sum_{i=0}^{r} a_i T^{p^i}, \quad \text{with} \quad a_i \in \mathbb{F}_q \quad \text{and} \quad a_r = 1,$$

is called an *additive polynomial* over $\mathbb{F}_q$. It is separable if and only if $a_0 \neq 0$ (since its derivative is $\wp'(T) = a_0$). A finite field extension E/F with $F \supseteq \mathbb{F}_q$ is called an *Artin-Schreier extension* if there exists an element $u \in E$ with $E = F(u)$ whose irreducible polynomial over F has the form $h(T) = \wp(T) - z$, with $z \in F$ and $\wp(T)$ a separable additive polynomial over $\mathbb{F}_q$.

The following lemma is an analogue to Lemma 5.1.

Lemma 6.1 *Let $\mathbb{F}_q(u) \supseteq \mathbb{F}_q(z)$ be an extension of rational function fields of degree $[\mathbb{F}_q(u) : \mathbb{F}_q(z)] = p^r$, with $p = \mathrm{char}(\mathbb{F}_q)$ and $r \geq 1$. Then the following conditions are equivalent:*

(i) *The extension $\mathbb{F}_q(u)/\mathbb{F}_q(z)$ is Galois.*

(ii) *There is an element $\tilde{u} \in \mathbb{F}_q(u)$ with $\mathbb{F}_q(u) = \mathbb{F}_q(\tilde{u})$ and a separable additive polynomial $\wp(T) \in \mathbb{F}_q[T]$ of degree $\deg \wp(T) = p^r$ such that $\wp(\tilde{u}) \in \mathbb{F}_q(z)$ and all roots of $\wp(T) = 0$ are in $\mathbb{F}_q$.*

If one (and hence both) of the conditions above holds, then the Galois group of $\mathbb{F}_q(u)/\mathbb{F}_q(z)$ is elementary abelian of type $(p, \ldots, p)$, exactly one rational place of $\mathbb{F}_q(z)$ is totally ramified in $\mathbb{F}_q(u)/\mathbb{F}_q(z)$ and all other places of $\mathbb{F}_q(z)$ are unramified in $\mathbb{F}_q(u)$. Moreover, the irreducible polynomial over $\mathbb{F}_q(z)$ of the element $\tilde{u}$ in condition (ii) *above is $h(T) := \wp(T) - w$ with $w \in \mathbb{F}_q(z)$ and $\mathbb{F}_q(z) = \mathbb{F}_q(w)$.*

Proof. (i) $\Rightarrow$ (ii): We assume that the extension $\mathbb{F}_q(u)/\mathbb{F}_q(z)$ is Galois of degree p^r and denote by $\mathrm{Gal}(\mathbb{F}_q(u)/\mathbb{F}_q(z))$ its Galois group. First we show that there is exactly one place of $\mathbb{F}_q(z)$ which ramifies in $\mathbb{F}_q(u)$. Suppose this is wrong. Then at least two places $P_0 \neq Q_0$ of $\mathbb{F}_q(z)$ are ramified in the extension $\mathbb{F}_q(u)/\mathbb{F}_q(z)$.

Denote by $P_1, \ldots, P_n$ (resp. $Q_1, \ldots, Q_m$) all places of $\mathbb{F}_q(u)$ lying above P_0 (resp. Q_0), and by $e(P_i)$ (resp. $e(Q_j)$) the ramification index of P_i (resp. Q_j) in $\mathbb{F}_q(u)$. Since all ramification is wild, the different exponents of $P_i|P_0$ satisfy $d(P_i|P_0) \geq e(P_i)$ and similarly $d(Q_j|Q_0) \geq e(Q_j)$. Now the Hurwitz genus formula for the extension $\mathbb{F}_q(u)/\mathbb{F}_q(z)$ gives

$$\begin{aligned} -2 &\geq -2p^r + \sum_{i=1}^{n} e(P_i) \cdot \deg P_i + \sum_{j=1}^{m} e(Q_j) \cdot \deg Q_j \\ &= -2p^r + p^r \cdot \deg P_0 + p^r \cdot \deg Q_0 \\ &\geq 0, \end{aligned}$$

a contradiction. It follows that exactly one place P_0 of $\mathbb{F}_q(z)$ is ramified in $\mathbb{F}_q(u)$ and that $\deg P_0 = 1$; i.e., P_0 is a rational place. It is now easily seen that the place P_0 is totally ramified in the extension $\mathbb{F}_q(u)/\mathbb{F}_q(z)$ (otherwise, by Hilbert's ramification theory, there would exist an intermediate field $\mathbb{F}_q(z) \subsetneq E \subsetneq \mathbb{F}_q(u)$ such that $E/\mathbb{F}_q(z)$ is unramified - a contradiction).

Denote by P the unique place of $\mathbb{F}_q(u)$ lying above P_0. Since $P|P_0$ is totally ramified, P is a rational place of $\mathbb{F}_q(u)$. Choose $\tilde{u} \in \mathbb{F}_q(u)$ with pole divisor P, then $\tilde{u}$ also generates the field $\mathbb{F}_q(u)$. Any automorphism $\sigma \in \mathrm{Gal}(\mathbb{F}_q(u)/\mathbb{F}_q(z))$ fixes the place P, so $\sigma(\tilde{u}) = c_\sigma \cdot \tilde{u} + d_\sigma$ with $c_\sigma, d_\sigma \in \mathbb{F}_q$. Then $\sigma^i(\tilde{u}) = c_\sigma^i \cdot \tilde{u} + d_i$ for all $i \geq 1$ (with some element $d_i \in \mathbb{F}_q$), and since $\sigma^{p^r} = \mathrm{id}$ we conclude that $c_\sigma^{p^r} = 1$, hence $c_\sigma = 1$. The map

$$\begin{aligned} \mathrm{Gal}(\mathbb{F}_q(u)/\mathbb{F}_q(z)) &\to \mathbb{F}_q \\ \sigma &\mapsto d_\sigma \end{aligned}$$

(with $\sigma(\tilde{u}) = \tilde{u} + d_\sigma$) is then a monomorphism from $\mathrm{Gal}(\mathbb{F}_q(u)/\mathbb{F}_q(z))$ onto an additive subgroup $\mathcal{U} \subseteq \mathbb{F}_q$, hence $\mathrm{Gal}(\mathbb{F}_q(u)/\mathbb{F}_q(z))$ is elementary abelian of type $(p, \ldots, p)$. The polynomial

$$\wp(T) := \prod_{d \in \mathcal{U}} (T - d) \in \mathbb{F}_q[T]$$

is an additive polynomial of degree p^r (since $\mathcal{U}$ is an additive subgroup of $\mathbb{F}_q$, cf. [12, III.7.9]), and the element

$$w := \wp(\tilde{u}) = \prod_{d \in \mathcal{U}} (\tilde{u} - d)$$

is invariant under $\mathrm{Gal}(\mathbb{F}_q(u)/\mathbb{F}_q(z))$. It follows that $w \in \mathbb{F}_q(z)$, and since the pole order of w at the place P is equal to $p^r = [\mathbb{F}_q(u) : \mathbb{F}_q(z)]$, we conclude that $\mathbb{F}_q(w) = \mathbb{F}_q(z)$. Thus we have proved item (ii) and all claims stated at the end of Lemma 6.1.

(ii) $\Rightarrow$ (i): Let $\tilde{u}$ and $\wp(T)$ be as in (ii). It is clear that the polynomial $h(T) := \wp(T) - \wp(\tilde{u}) \in \mathbb{F}_q(z)[T]$ is the irreducible polynomial of $\tilde{u}$ over $\mathbb{F}_q(z)$. The equation $\wp(T) = 0$ has p^r distinct roots $d \in \mathbb{F}_q$ and for any such d we have $h(\tilde{u} + d) = \wp(\tilde{u} + d) - \wp(\tilde{u}) = \wp(\tilde{u}) + \wp(d) - \wp(\tilde{u}) = \wp(d) = 0$. Hence $h(T) = 0$ has p^r roots in $\mathbb{F}_q(u)$ and the extension $\mathbb{F}_q(u)/\mathbb{F}_q(z)$ is Galois. $\square$

Combining Theorem 4.1 and Lemma 6.1 we obtain the following result:

Theorem 6.2 *Let $\mathcal{F}$ be a tower over $\mathbb{F}_q$ which can be described recursively by the equation $f(Y) = g(X)$, with rational functions $f(T)$ and $g(T)$ in $\mathbb{F}_q(T)$ satisfying $\deg f(T) = \deg g(T) = p^r$, where p denotes the characteristic of $\mathbb{F}_q$. Denote by $F = \mathbb{F}_q(x, y)$ the corresponding basic function field. Suppose that both extensions $F/\mathbb{F}_q(x)$ and $F/\mathbb{F}_q(y)$ are Galois. Then there exist monic additive polynomials $\wp_1(T), \wp_2(T) \in \mathbb{F}_q[T]$ of degree p^r having all roots in $\mathbb{F}_q$ and non-singular matrices $A, B \in \mathrm{GL}(2, \mathbb{F}_q)$ such that the tower $\mathcal{F}$ can be described recursively by the equation*

$$\wp_2(Y) = A \cdot \wp_1(B \cdot X).$$

A typical example for Theorem 6.2 is the tower $\mathcal{F}_5$ from Example 3.5 which is given recursively by Equation (3.8):

$$Y^q + Y = \frac{X^q}{X^{q-1} + 1}.$$

Setting $\wp_1(T) := \wp_2(T) := T^q + T$ we see that

$$\wp_2(Y) = A \cdot \wp_1(B \cdot X) \quad \text{with} \quad A = B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

For Artin-Schreier extensions of degree p we can sharpen Lemma 6.1 and thereby we obtain a stronger version of Theorem 6.2:

Lemma 6.3 *Let $\mathbb{F}_q(u) \supseteq \mathbb{F}_q(z)$ be an extension of rational function fields of degree $[\mathbb{F}_q(u) : \mathbb{F}_q(z)] = p = \mathrm{char}(\mathbb{F}_q)$. Then the following conditions are equivalent:*

(i) *The extension $\mathbb{F}_q(u)/\mathbb{F}_q(z)$ is Galois.*

(ii) *There exists an element $u_1 \in \mathbb{F}_q(u)$ such that $u_1^p - u_1 \in \mathbb{F}_q(z)$ and $\mathbb{F}_q(u_1) = \mathbb{F}_q(u)$.*

(iii) *There exists an element $u_2 \in \mathbb{F}_q(u)$ and an element $0 \neq a \in \mathbb{F}_q$ such that $\mathbb{F}_q(u_2) = \mathbb{F}_q(u)$ and $u_2^p - a^{p-1}u_2 \in \mathbb{F}_q(z)$.*

(iv) *For all elements $0 \neq b \in \mathbb{F}_q$ there is some element $u_3 \in \mathbb{F}_q(u)$ such that $\mathbb{F}_q(u_3) = \mathbb{F}_q(u)$ and $u_3^p - b^{p-1}u_3 \in \mathbb{F}_q(z)$.*

Proof. It is sufficient to prove the implications (i) $\Rightarrow$ (iii) $\Rightarrow$ (iv).

(i)$\Rightarrow$ (iii): Let $\mathbb{F}_q(u)/\mathbb{F}_q(z)$ be Galois of degree p. By Lemma 6.1 there is an element $\tilde{u}$ with $\mathbb{F}_q(\tilde{u}) = \mathbb{F}_q(u)$ and a polynomial $\wp(T) = T^p - cT$ with $0 \neq c \in \mathbb{F}_q$ such that $\wp(\tilde{u}) \in \mathbb{F}_q(z)$ and $\wp(T) = T^p - cT = T(T^{p-1} - c) = 0$ has all roots in $\mathbb{F}_q$. This means that $c = a^{p-1}$ for some $a \in \mathbb{F}_q \backslash \{0\}$. The element $u_2 := \tilde{u}$ therefore has the desired properties.

(iii)⇒ (iv): We now assume that there is an element $u_2 \in \mathbb{F}_q(u)$ with $\mathbb{F}_q(u_2) = \mathbb{F}_q(u)$ and an element $0 \neq a \in \mathbb{F}_q$ such that $u_2^p - a^{p-1}u_2 \in \mathbb{F}_q(z)$. Let $b \in \mathbb{F}_q \setminus \{0\}$ be given. We then set $u_3 := a^{-1}bu_2$ and obtain

$$u_3^p - b^{p-1}u_3 = a^{-p}\, b^p\, u_2^p - b^{p-1}\, a^{-1}\, b\, u_2 = a^{-p}\, b^p\, (u_2^p - a^{p-1}u_2),$$

hence $\mathbb{F}_q(u_3) = \mathbb{F}_q(u)$ and $u_3^p - b^{p-1}u_3 \in \mathbb{F}_q(z)$. □

Theorem 6.4 *Let $\mathcal{F}$ be a tower over $\mathbb{F}_q$ which can be described recursively by the equation $f(Y) = g(X)$, with rational functions $f(T)$ and $g(T)$ in $\mathbb{F}_q(T)$ satisfying $\deg f(T) = \deg g(T) = p^r$, where p denotes the characteristic of $\mathbb{F}_q$. Denote by $F = \mathbb{F}_q(x, y)$ the corresponding basic function field. Suppose that both extensions $F/\mathbb{F}_q(x)$ and $F/\mathbb{F}_q(y)$ are Galois. Let $0 \neq e \in \mathbb{F}_q$ and set*

$$\wp(T) := T^p - e^{p-1}T \in \mathbb{F}_q[T].$$

Then the tower $\mathcal{F}$ is a $\wp$-tower; more precisely, the tower can be described recursively by one of the following equations:

$$\wp(Y) = \begin{cases} \dfrac{a}{\wp(\alpha X) + b} + c & (Case\ 1) \\ a \cdot \wp\left(\dfrac{\alpha}{X}\right) + b & (Case\ 2) \\ \dfrac{a}{\wp\,(\alpha/X) + b} + c & (Case\ 3) \end{cases}$$

with $a, b, c, \alpha \in \mathbb{F}_q$ and $a \neq 0$, $\alpha \neq 0$. In Case 1 we can further assume that $\alpha \notin \mathbb{F}_p$, and in Case 2 we can assume that $a \notin \mathbb{F}_p$.

Proof. By Theorem 4.3 and Lemma 6.3 we can describe the tower $\mathcal{F}$ recursively by an equation

$$\wp(Y) = A \cdot \wp(B \cdot X) \quad \text{with} \quad A, B \in \mathrm{GL}(2, \mathbb{F}_q),$$

where $\wp(T) = T^p - e^{p-1}T$ as above. This means that

$$\wp(Y) = \frac{a \cdot \wp\left(\dfrac{\alpha X + \beta}{\gamma X + \delta}\right) + b}{c \cdot \wp\left(\dfrac{\alpha X + \beta}{\gamma X + \delta}\right) + d} \quad \text{with} \quad ad \neq bc \text{ and } \alpha\delta \neq \beta\gamma. \tag{6.1}$$

We distinguish four possible cases:

(Case 1): $c \neq 0$ and $\gamma = 0$. We may assume that $c = 1$ and obtain from Equation (6.1)

$$\begin{aligned} \wp(Y) &= \frac{a_1 \cdot \wp(\alpha_1 X + \beta_1) + b_1}{\wp(\alpha_1 X + \beta_1) + d_1} = \frac{a_1 \cdot \wp(\alpha_1 X) + b_2}{\wp(\alpha_1 X) + d_2} \\ &= \frac{a_2}{\wp(\alpha_1 X) + d_2} + b_3 \end{aligned}$$

with certain elements $a_i, b_j, \cdots \in \mathbb{F}_q$.

(Case 2): $c = 0$ and $\gamma \neq 0$. Now we may assume that $\gamma = 1$ and obtain from Equation (6.1)

$$\wp(Y) = a_1 \cdot \wp\left(\frac{\alpha X + \beta}{X + \delta}\right) + b_1.$$

We substitute $Y = \tilde{Y} - \delta$ and $X = \tilde{X} - \delta$. This gives

$$\begin{aligned}
\wp(\tilde{Y}) - \wp(\delta) &= a_1 \cdot \wp\left(\frac{\alpha_1 \tilde{X} + \beta_1}{\tilde{X}}\right) + b_1 \\
&= a_1 \cdot \wp\left(\frac{\alpha_2}{\tilde{X}} + \beta_2\right) + b_1 \\
&= a_1 \cdot \wp\left(\beta_2\right) + a_1 \cdot \wp\left(\frac{\alpha_2}{\tilde{X}}\right) + b_1,
\end{aligned}$$

hence

$$\wp(\tilde{Y}) = a_1 \cdot \wp\left(\frac{\alpha_2}{\tilde{X}}\right) + b_2$$

with $a_i, b_j, \cdots \in \mathbb{F}_q$.

(Case 3): $c \neq 0$ and $\gamma \neq 0$, and we may assume that $c = \gamma = 1$. In this case, Equation (6.1) gives

$$\begin{aligned}
\wp(Y) &= \frac{a \cdot \wp\left(\frac{\alpha X + \beta}{X + \delta}\right) + b}{\wp\left(\frac{\alpha X + \beta}{X + \delta}\right) + d} = \frac{a \cdot \wp\left(\frac{\alpha_1}{X + \delta} + \beta_1\right) + b}{\wp\left(\frac{\alpha_1}{X + \delta} + \beta_1\right) + d} \\
&= \frac{a \cdot \wp\left(\frac{\alpha_1}{X + \delta}\right) + b_1}{\wp\left(\frac{\alpha_1}{X + \delta}\right) + d_1} = \frac{a_2}{\wp\left(\frac{\alpha_1}{X + \delta}\right) + d_1} + b_2.
\end{aligned}$$

We substitute $Y = \tilde{Y} - \delta$ and $X = \tilde{X} - \delta$ and find

$$\wp(\tilde{Y}) = \frac{a_2}{\wp\left(\frac{\alpha_1}{\tilde{X}}\right) + d_1} + b_3,$$

as desired.

(Case 4): $c = \gamma = 0$. In this case Equation (6.1) yields

$$\wp(Y) = a_1 \cdot \wp(\alpha_1 X + \beta_1) + b_1 = a_1 \cdot \wp(\alpha_1 X) + b_2. \tag{6.2}$$

We have shown in [1, Prop.4.5] that Equation (6.2) does not define a tower.

It is clear that in Cases 1–3 the constants a and α are non-zero. Assume now that in Case 1 the recursive equation of the tower is

$$\wp(Y) = \frac{a}{\wp(\alpha X) + b} + c \quad \text{with} \quad \alpha \in \mathbb{F}_p. \tag{6.3}$$

Then $\wp(\alpha X) = \alpha \cdot \wp(X)$, and we can rewrite Equation (6.3) as

$$\wp(Y) = C \cdot \wp(X) \quad \text{with a matrix} \quad C \in \mathrm{GL}(2, \mathbb{F}_q).$$

For some $n \geq 1$ we have $C^n = \mathrm{id}$, and as in the proof of Theorem 5.2 we conclude that Equation (6.3) does not define a tower.

Finally we consider Case 2 and assume that $a \in \mathbb{F}_p$. Then the defining equation of $\mathcal{F}$ is

$$\wp(Y) = \wp\left(\frac{a\alpha}{X}\right) + b, \tag{6.4}$$

hence $\wp(Y - a\alpha/X) = b$. This shows that Equation (6.4) is not absolutely irreducible, contrary to our definition of recursive towers. □

As an application of Theorem 6.4 we obtain a complete list of all (f, g)-towers with $\deg f = \deg g = 2$ over the field $\mathbb{F}_2$ with two elements. By Theorem 6.4 such a tower can be described recursively by an equation

$$Y^2 + Y = \frac{1}{\left(\frac{1}{X}\right)^2 + \left(\frac{1}{X}\right) + b} + c \tag{6.5}$$

with $b, c \in \mathbb{F}_2$.

For $b = c = 0$, Equation (6.5) becomes

$$Y^2 + Y = \frac{1}{\left(\frac{1}{X}\right)^2 + \left(\frac{1}{X}\right)} = \frac{X^2}{X+1}.$$

This is the tower $\mathcal{F}_5$ from Example 3.5 for $q = 2$. It attains the Drinfeld-Vladut bound over $\mathbb{F}_4$.

Next we consider the case $b = 0$, $c = 1$. Then Equation (6.5) becomes $Y^2 + Y = (X^2 + X + 1)/(X + 1)$, and with the transformation $\tilde{X} = X + 1$, $\tilde{Y} = Y + 1$ we obtain

$$\tilde{Y}^2 + \tilde{Y} = \tilde{X} + 1 + \frac{1}{\tilde{X}}.$$

This tower was considered in Example 3.6; it is asymptotically good over the field $\mathbb{F}_8$.

Similarly for $b = 1$, $c = 0$ we get the equation

$$Y^2 + Y = \frac{X^2}{X^2 + X + 1}.$$

This tower was considered in Example 3.10; it is dual to the previous tower, and hence it is asymptotically good over $\mathbb{F}_8$.

Finally, for $b = c = 1$ we find the equation

$$Y^2 + Y = \frac{X+1}{X^2+X+1}.$$

With the substitution $\tilde{Y} = Y + 1$, $\tilde{X} = X + 1$ this gives

$$\tilde{Y}^2 + \tilde{Y} = \frac{\tilde{X}}{\tilde{X}^2+\tilde{X}+1}. \tag{6.6}$$

This equation has not yet been considered in the literature. It would be interesting to study the tower $\mathcal{F}$ which is recursively defined by Equation (6.6). In particular: is $\mathcal{F}$ asymptotically good over $\mathbb{F}_q$ with $q = 2^s$, for some $s \geq 1$?

7 Some non-Galois f-towers

The concept of an f-tower is useful not only in case the extensions $F/\mathbb{F}_q(x)$ and $F/\mathbb{F}_q(y)$ are Galois (with $F = \mathbb{F}_q(x, y)$ denoting the corresponding basic function field). In this section we consider a situation where both these extensions are non-Galois. Among other things, this leads to a more natural representation and a better understanding of the towers in Examples 3.7 and 3.8.

Let us consider in more details the tower in Example 3.8, which is given recursively by the equation $f(Y) = g(X)$ with

$$f(Y) = \frac{1-Y}{Y^q} \quad \text{and} \quad g(X) = \frac{X^q + X - 1}{X}. \tag{7.1}$$

We set $z := f(y) = g(x)$.

Remark 7.1 There are places P,Q of $\mathbb{F}_q(z)$ and places $\tilde{P}$, $\tilde{Q}$ of $\mathbb{F}_q(x)$ with $\tilde{P}|P$ and $\tilde{Q}|Q$ such that

$$e(\tilde{P}|P) = q \quad \text{and} \quad e(\tilde{Q}|Q) = q - 1;$$

indeed, this follows from the fact that the element $z - 1 = (x-1)^q/x$ has a zero of order q and a pole of order $q-1$ in $\mathbb{F}_q(x)$. Also, there are places R, S of $\mathbb{F}_q(z)$ and places $\tilde{R}$, $\tilde{S}$ of $\mathbb{F}_q(y)$ with $\tilde{R}|R$ and $\tilde{S}|S$ such that

$$e(\tilde{R}|R) = q \quad \text{and} \quad e(\tilde{S}|S) = q - 1.$$

This shows that the extensions $\mathbb{F}_q(x)/\mathbb{F}_q(z)$ and $\mathbb{F}_q(y)/\mathbb{F}_q(z)$ have a similar ramification structure.

Keeping the remark above in mind, we return to the general case of an (f, g)-tower $\mathcal{F}$ over $\mathbb{F}_q$. We begin with an analogue of Lemmas 5.1 and 6.1.

Lemma 7.2 *Let $\mathbb{F}_\ell(u) \supseteq \mathbb{F}_\ell(z)$ be an extension of rational function fields of degree $[\mathbb{F}_\ell(u) : \mathbb{F}_\ell(z)] = q > 1$, and assume that $p = \mathrm{char}(\mathbb{F}_\ell)$ divides q. Set*

$$h(T) := T^q - T^{q-1} \in \mathbb{F}_\ell[T].$$

Assume that there are places $\tilde{P}$ and $\tilde{Q}$ of $\mathbb{F}_\ell(u)$ such that

$$e(\tilde{P}|P) = q \quad \text{and} \quad e(\tilde{Q}|Q) = q - 1,$$

where P and Q denote the restrictions of $\tilde{P}$ and $\tilde{Q}$ to the subfield $\mathbb{F}_\ell(z)$. Then there is an element $\tilde{u} \in \mathbb{F}_\ell(u)$ such that $\mathbb{F}_\ell(\tilde{u}) = \mathbb{F}_\ell(u)$ and $h(\tilde{u}) \in \mathbb{F}_\ell(z)$.

Proof. Let P, Q, $\tilde{P}$, $\tilde{Q}$ be as in the lemma. It follows from the Hurwitz genus formula that all these places are rational. We choose a generator $\tilde{z}$ of $\mathbb{F}_\ell(z)$ whose principal divisor in the field $\mathbb{F}_\ell(z)$ is

$$(\tilde{z})_{\mathbb{F}_\ell(z)} = Q - P.$$

Then the principal divisor of $\tilde{z}$ in $\mathbb{F}_\ell(u)$ has the form

$$(\tilde{z})_{\mathbb{F}_\ell(u)} = (q-1)\tilde{Q} + \tilde{Q}_1 - q\tilde{P} \tag{7.2}$$

with another place $\tilde{Q}_1$ of $\mathbb{F}_\ell(u)$ of degree one. We can choose an element $\tilde{u} \in \mathbb{F}_\ell(u)$ with the following properties: the pole of $\tilde{u}$ in $\mathbb{F}_\ell(u)$ is $\tilde{P}$, the zero of $\tilde{u}$ is $\tilde{Q}$ and the zero of $\tilde{u}-1$ is $\tilde{Q}_1$. We then consider the element $h(\tilde{u}) = \tilde{u}^q - \tilde{u}^{q-1} = \tilde{u}^{q-1}(\tilde{u}-1)$. Its principal divisor in the field $\mathbb{F}_\ell(u)$ is by construction

$$(h(\tilde{u}))_{\mathbb{F}_\ell(u)} = (q-1)\tilde{Q} + \tilde{Q}_1 - q\tilde{P}, \tag{7.3}$$

and it follows from Equations (7.2) and (7.3) that $h(\tilde{u}) = c \cdot \tilde{z}$ for some $0 \neq c \in \mathbb{F}_\ell$. □

Combining Lemma 7.2 and Theorem 4.3 we obtain immediately:

Theorem 7.3 *Let $\mathcal{F}$ be an (f,g)-tower over $\mathbb{F}_\ell$ such that $\deg f(T) = \deg g(T) = q > 1$ and suppose that the characteristic of $\mathbb{F}_\ell$ divides q. Denote by $F = \mathbb{F}_\ell(x,y)$ the corresponding basic function field with $f(y) = g(x) =: z$. Assume that both extensions $\mathbb{F}_\ell(x)/\mathbb{F}_\ell(z)$ and $\mathbb{F}_\ell(y)/\mathbb{F}_\ell(z)$ satisfy the assumptions of Lemma 7.2; i.e., there are places P, Q, R, S of $\mathbb{F}_\ell(z)$ and $\tilde{P}$, $\tilde{Q}$ of $\mathbb{F}_\ell(x)$ and $\tilde{R}$, $\tilde{S}$ of $\mathbb{F}_\ell(y)$ with $\tilde{P}|P$, $\tilde{Q}|Q$, $\tilde{R}|R$ and $\tilde{S}|S$ whose ramification indices are*

$$e(\tilde{P}|P) = e(\tilde{R}|R) = q \quad \text{and} \quad e(\tilde{Q}|Q) = e(\tilde{S}|S) = q - 1.$$

Set $h(T) := T^q - T^{q-1}$. Then the tower $\mathcal{F}$ is an h-tower over $\mathbb{F}_\ell$; i.e., $\mathcal{F}$ can be described recursively by the equation

$$h(Y) = A \cdot h(B \cdot X)$$

for suitable matrices $A, B \in \mathrm{GL}(2, \mathbb{F}_\ell)$.

As an example for Theorem 7.3 we consider once again the tower $\mathcal{F}_8$ from Example 3.8 which is defined by $f(Y) = g(X)$ with $f(Y)$ and $g(X)$ as in Equation (7.1). It follows from Remark 7.1 and Theorem 7.3 that the tower $\mathcal{F}_8$ is an h-tower; indeed, setting $\tilde{Y} = 1/Y$ and $\tilde{X} = 1/X$, Equation (7.1) becomes

$$h(\tilde{Y}) = \frac{1 + \tilde{X}^{q-1} - \tilde{X}^q}{\tilde{X}^{q-1}} = 1 - \frac{1}{h\left(\dfrac{\tilde{X}}{\tilde{X}-1}\right)}.$$

Hence the tower $\mathcal{F}_8$ can also be described recursively by the equation

$$h(Y) = 1 - \frac{1}{h\left(\dfrac{X}{X-1}\right)} = A \cdot h(B \cdot X) \tag{7.4}$$

with

$$A = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}.$$

An important step in [4] is to show that the tower $\mathcal{F}_8 = (F_0, F_1, F_2, \dots)$ over $\mathbb{F}_{q^3}$ has the following property: there are $q^2 + q$ rational places of the field F_0 which split completely in all extensions F_n/F_0, for $n \geq 1$. Using the recursive description of $\mathcal{F}_8$ by Equation (7.4) we can give a much simpler proof of this property than the proof in [4] which is based on the recursive description of $\mathcal{F}_8$ by Equation (7.1). First of all we have the following polynomial identity which can be checked easily:

$$(T-1)^{q^2+q+1} + 1 = T \cdot \left(h(T)^{q+1} - h(T) + 1\right). \tag{7.5}$$

Denoting by $\overline{\mathbb{F}}_q$ the algebraic closure of $\mathbb{F}_q$, we then define the set $\Omega \subseteq \overline{\mathbb{F}}_q$ by

$$\Omega := \{\alpha \in \overline{\mathbb{F}}_q \,;\, (\alpha - 1)^{q^2+q+1} = -1\} \backslash \{0\}. \tag{7.6}$$

It is clear that $\Omega \subseteq \mathbb{F}_{q^3}$ and that the cardinality of Ω is $q^2 + q$.

Recall that the function $x_0 \in F_0$ is a generator of the rational function field $F_0/\mathbb{F}_{q^3}$, see Definition 2.2. We want to show that the zero of $x_0 - \alpha$, for $\alpha \in \Omega$, splits completely in all extensions F_n/F_0 (which proves the desired property of the tower $\mathcal{F}_8$). By Equation (7.4) it is enough to prove the following claim:

Claim: *Let $\beta \in \overline{\mathbb{F}}_q$ be an element such that*

$$h(\beta) = 1 - \frac{1}{h\left(\dfrac{\alpha}{\alpha-1}\right)} \quad \textit{for some} \quad \alpha \in \Omega. \tag{7.7}$$

Then the element β also belongs to the set Ω.

Proof of the Claim. Let $\alpha \in \Omega$, then $\gamma := \alpha/(\alpha-1) \in \Omega$ by the definition in (7.6). We now consider an element $\beta \in \overline{\mathbb{F}_q}$ which satisfies Equation (7.7), so

$$h(\beta) = 1 - \frac{1}{h(\gamma)} \quad \text{for some } \ \gamma \in \Omega. \tag{7.8}$$

In order to prove that $\beta \in \Omega$ we have to check (by Equation (7.5)) the identity $h(\beta)^{q+1} - h(\beta) + 1 = 0$; i.e.,

$$h(\beta)^q = \frac{h(\beta)-1}{h(\beta)}. \tag{7.9}$$

Now

$$\begin{aligned} h(\beta)^q &= 1 - \frac{1}{h(\gamma)^q} && \text{(by (7.8))} \\ &= 1 - \frac{h(\gamma)}{h(\gamma)-1} && \text{(since } \gamma \in \Omega\text{)} \\ &= \frac{1}{1-h(\gamma)} = \frac{1}{1-\dfrac{1}{1-h(\beta)}} && \text{(by (7.8))} \\ &= \frac{h(\beta)-1}{h(\beta)}. \end{aligned}$$

This proves Equation (7.9) and finishes the proof of the claim. □

Remark 7.4 The tower $\mathcal{F}_7$ given in Example 3.7 is asymptotically good over the quadratic field $\mathbb{F}_{q^2}$, and by Theorem 7.3 it can also be described by an equation $h(Y) = A \cdot h(B \cdot X)$ with $h(T) = T^q - T^{q-1}$ and with matrices $A, B \in \mathrm{GL}(2, \mathbb{F}_{q^2})$. One checks that this equation is

$$h(Y) = \frac{1}{h\left(\dfrac{X}{X-1}\right)}. \tag{7.10}$$

References

[1] P. Beelen, A. Garcia and H. Stichtenoth, *On towers of function fields of Artin-Schreier type*, to appear in Bulletin Braz. Math. Soc.

[2] P. Beelen, A. Garcia and H. Stichtenoth, *On ramification and genus of recursive towers*, preprint (2004).

[3] J. Bezerra and A. Garcia, *A tower with non-Galois steps which attains the Drinfeld-Vladut bound*, to appear in J. Number Theory.

[4] J. Bezerra, A. Garcia and H. Stichtenoth, *An explicit tower of function fields over cubic finite fields and Zink's lower bound*, preprint (2003).

[5] V.G. Drinfeld and S.G. Vladut, *The number of points of an algebraic curve*, Funktsional. Anal. i Prilozhen. **17** (1983), 68–69. [Funct. Anal. Appl. **17** (1983), 53–54].

[6] N. D. Elkies, *Explicit Modular Towers*, in *Proceedings of the 35th Annual Allerton Conference on Communication, Control and Computing* (Urbana, 1997), 23–32, 1998.

[7] A. Garcia and H. Stichtenoth, *Skew pyramids of function fields are asymptotically bad*, in *Coding Theory, Cryptography and Related Areas* (Guanajuato, 1998), 111–113, Springer, 2000.

[8] 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.

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

[10] 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.

[11] 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.

[12] H. Stichtenoth, *Algebraic function fields and codes*, Springer, Berlin, 1993.

[13] J. Wulftange, *Zahme Türme algebraischer Funktionenkörper*, Ph.D. Thesis, University of Essen, 2003.

[14] T. Zink, *Degeneration of Shimura surfaces and a problem in coding theory*, in *Fundamentals of Computation Theory*, Lecture Notes in Computer Science, Vol. **199**, Springer, Berlin, 503–511, 1985.

Authors' addresses:

Peter Beelen, Fachbereich 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 Mathematik, Universität Duisburg-Essen, 45117 Essen, Germany. e-mail: stichtenoth@uni-essen.de