Journal of Algebra and Its Applications
Vol. 14, No. 3 (2015) 1550028 (12 pages)
© World Scientific Publishing Company
DOI: 10.1142/S0219498815500280

World Scientific
www.worldscientific.com

New examples of asymptotically good Kummer type towers

María Chara
Instituto de Matemática Aplicada del Litoral (UNL-CONICET)
Güemes 3450 S3000GLN, Santa Fe, Argentina
mchara@santafe-conicet.gov.ar

Ricardo Toledano
Departamento de Matemática, Facultad de Ingeniera Química (UNL)
Santiago del Estero 2829, S3000AOM, Santa Fe, Argentina
rtoledano@santafe-conicet.gov.ar

Received 6 May 2013
Accepted 14 May 2014
Published 17 October 2014

Communicated by K. Lauter

In this work, we give sufficient conditions in order to have finite ramification locus in sequences of function fields defined by different kind of Kummer extensions. These conditions can be easily implemented in a computer to generate several examples. We present some new examples of asymptotically good towers of Kummer type and we show that many known examples can be obtained from our general results.

Keywords: Function fields; Kummer extension; towers.

Mathematics Subject Classification: 11G, 11R, 14H05

1. Introduction

Asymptotically good towers of function fields have received much attention in theoretical considerations related to coding theory and Cryptography after the work of Tsfasman, Vladut and Zink in [8]. They showed the existence of linear codes with parameters improving the so-called Gilbert–Varshamov bound using asymptotically good towers of modular curves (in fact, optimal) and a construction of linear codes due to Goppa. However, they did not give a method for constructing them. This motivated the search for asymptotically good towers of function fields over finite fields defined in an explicit way. It turns out that it is a non-trivial problem to provide examples of such towers. This line of research was initiated by Garcia and Stichtenoth. They established all the fundamental results of the theory of asymptotically good towers (see, for example, [2]) and made one of their most important contributions with the study of the so-called recursive towers (see Sec. 2 for details).

The aim of this paper is to continue the investigation (initiated in [1]) of the asymptotic behavior of towers of function fields defined by a Kummer equation of the form

$$y^m = \frac{x^m - \alpha f(x) + \alpha}{f(x)}, \tag{1.1}$$

where $f \in \mathbb{F}_q[x]$ is a suitable polynomial and $\alpha \in \mathbb{F}_q^*$. More precisely, in [1] we obtained conditions in order to have non-empty splitting locus of towers recursively defined by (1.1), and now we will deal with the ramification locus. The finiteness of the ramification locus of towers recursively defined by (1.1) will suffice to prove their good asymptotic behavior because an important and well-known result of Garcia and Stichtenoth states that if a tame tower has non-empty splitting locus and finite ramification locus, then the tower is asymptotically good [4, Theorem 2.1]. We will show new examples of asymptotically good towers recursively defined by (1.1).

In Sec. 2, we give the basic definitions and we establish the notation to be used throughout the paper. In Sec. 3, we prove our main results. In particular, in Theorem 3.4, we give sufficient conditions to have asymptotically good Kummer type towers recursively defined by (1.1). The first part of Sec. 3 is devoted to prove some auxiliary results needed in the proof of Theorem 3.4. An interesting feature of these results is that they can be easily implemented in a computer so that we were able to search for many equations of the form (1.1) defining good towers. Consequently, we show different examples of asymptotically good towers of Kummer type and we observe that some known examples can be obtained from our general results. In particular, in Example 3.14, we present new interesting examples of asymptotically good Kummer type towers whose defining equations have coefficients in $\mathbb{F}_9 \backslash \mathbb{F}_3$.

2. Preliminaries

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

Let $\mathcal{F} = (F_0, F_1, \ldots)$ be a sequence of function fields over $\mathbb{F}_q$. We shall say that $\mathcal{F}$ is *admissible* if

(1) $F_0 \subsetneq F_1 \subsetneq F_2 \subsetneq \cdots$,
(2) the field extension F_{i+1}/F_i is finite and separable for all $i \geq 0$, and
(3) the field $\mathbb{F}_q$ is algebraically closed in F_i for all $i \geq 0$, i.e. the only elements of F_i which are algebraic over $\mathbb{F}_q$ are the elements of $\mathbb{F}_q$. In this case, we shall say that $\mathbb{F}_q$ is the full constant field of each F_i.

If the genus $g(F_i)$ grows to infinity as $i \to \infty$, we say that the admissible sequence $\mathcal{F}$ is a *tower of function fields over* $\mathbb{F}_q$.

We shall say that an admissible sequence $\mathcal{F}$ is *recursively defined* if there exist a bivariate polynomial $H \in \mathbb{F}_q[S, T]$ and transcendental elements x_i, such that for all $i \geq 0$ the following holds:

(1) $F_0 = \mathbb{F}_q(x_0)$ is the rational function field.
(2) $F_{i+1} = F_i(x_{i+1})$ with $H(x_i, x_{i+1}) = 0$.
(3) $[F_{i+1} : F_i] = \deg_T H$.

Let $\mathbb{P}(F)$ denote the set of all places of a function field $F/\mathbb{F}_q$. The following definitions are important in the study of the asymptotic behavior of sequences of function fields. Let $\mathcal{F} = (F_0, F_1, \ldots)$ be an admissible sequence of function fields over $\mathbb{F}_q$. A place $P \in \mathbb{P}(F_i)$ *splits completely* in $\mathcal{F}$ if P splits completely in each extension F_j/F_i. The *splitting locus* of $\mathcal{F}$ over F_0 is defined as

$$\mathrm{Split}(\mathcal{F}/F_0) := \{P \in \mathbb{P}(F_0) : \deg(P) = 1 \text{ and } P \text{ splits completely in } \mathcal{F}\},$$

where $\deg(P)$ is the degree of the place P. A place $P \in \mathbb{P}(F_i)$ is *ramified* in $\mathcal{F}$ if P is ramified in any extension F_j/F_i. The *ramification locus* of $\mathcal{F}$ over F_0 is the set

$$\mathrm{Ram}(\mathcal{F}/F_0) := \{P \in \mathbb{P}(F_0) : P \text{ ramified in some extension } F_n/F_0\}.$$

A place $P \in \mathbb{P}(F_i)$ *is totally ramified* in $\mathcal{F}$ if P is totally ramified in each extension F_j/F_i. The *complete ramification locus* of $\mathcal{F}$ over F_0 is defined as

$$\mathrm{Cram}(\mathcal{F}/F_0) := \{P \in \mathbb{P}(F_0) : \deg(P) = 1 \text{ and } P \text{ is totally ramified in } \mathcal{F}\}.$$

Since every place $Q \in \mathbb{P}(F_i)$ lying above a place in $\mathrm{Split}(\mathcal{F}/F_0) \cup \mathrm{Cram}(\mathcal{F}/F_0)$ is a rational place (i.e. of degree one), we have that

$$N(F_i) \geq [F_i : F_0]|\mathrm{Split}(\mathcal{F}/F_0)| + |\mathrm{Cram}(\mathcal{F}/F_0)|, \tag{2.1}$$

where $N(F_i)$ is the number of rational places of F_i.

Notice that if for an admissible sequence of function fields $\mathcal{F} = (F_0, F_1, \ldots)$ we have that $\mathrm{Split}(\mathcal{F}/F_0) \neq \emptyset$ (in other words, there is a rational place P in F_0 that splits completely in each extension F_i/F_0) then, by the Hasse–Weil bound, we have that $g(F_i) \to \infty$ as $i \to \infty$ so that $\mathcal{F}$ is actually a tower.

Given a finite extension E/F and a place $P \in \mathbb{P}(F)$ there are finitely many places $Q \in \mathbb{P}(E)$ lying above P. We will write $Q \mid P$ when Q lies over P. The extension E/F is said to be *tame* if the ramification index $e(Q \mid P)$ is relatively prime to the characteristic of $\mathbb{F}_q$, for all places $P \in \mathbb{P}(F)$ and all $Q \mid P$. We shall say that an admissible sequence $\mathcal{F} = (F_0, F_1, \ldots)$ of function fields over $\mathbb{F}_q$ is *tame* if all the extensions F_i/F_0 are tame.

3. Kummer Type Towers

As we said in Sec. 1, it is well-known that a tame recursive tower is asymptotically good if it has non-empty splitting locus and finite ramification locus. The next result, proved in [1], gives sufficient conditions in order to have non-empty splitting locus, in the particular class of sequences of Kummer type recursively defined by (1.1).

We will use the following notation. For a given rational function $f \in \mathbb{F}_q(T)$ the set of zeros of f in an algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$ will be denoted either by Z_f, or by $Z_{f(T)}$ in case we need to specify $f(T)$.

Proposition 3.1. *Let $m > r \geq 1$ be such that $\gcd(m, m-r) = 1$ and $\gcd(m, q) = 1$. Let $\alpha \in \mathbb{F}_q^*$ and consider the rational functions*

$$a(T) = T^m \quad \textit{and} \quad b(T) = \frac{T^m - \alpha f(T) + \alpha}{f(T)},$$

where $f(T) \in \mathbb{F}_q[T]$ is a polynomial of degree r. If $\mathbb{F}_q$ is a splitting field for $T^m + \alpha$ and $Z_f \cap Z_{T^m+\alpha} = \emptyset$, then for the (a, b)-recursive sequence of function fields $\mathcal{F} = (F_0, F_1, \ldots)$ we have that

$$|\mathrm{Split}(\mathcal{F}/F_0)| \geq m$$

and

$$N(F_i) \geq m^{i+1} + 1.$$

Since we have non-empty splitting locus for the Kummer sequences recursively defined by (1.1), we shall focus, from now on, in finding sufficient conditions in order to ensure finite ramification. First, we give a simple result which will be useful later. We will denote by $x(P)$ the residue class mod P of $x \in F$.

Lemma 3.2. *Let $\mathcal{F} = (F_0, F_1, \ldots)$ be an admisible recursive sequence of function fields over $\mathbb{F}_q$ defined by the equation $H(S, T) = 0$, where $H \in \mathbb{F}_q[S, T]$. Assume that there is a set $S_0 \subset \overline{\mathbb{F}}_q$ such that if $\gamma \in S_0$ and $H(\beta, \gamma) = 0$ then $\beta \in S_0$. Let $\{x_i\}_{i \geq 0}$ be a sequence of transcendental elements over $\mathbb{F}_q$ such that $F_0 = \mathbb{F}_q(x_0)$ and $F_{i+1} = F_i(x_{i+1})$ where $H(x_i, x_{i+1}) = 0$ for all $i \geq 0$. Let Q be a place in $\mathbb{P}(F_i)$ such that $x_i(Q) \in S_0$. Then $x_0(Q) \in S_0$.*

Proof. Let Q be a place of F_i such that $x_i(Q) \in S_0$. Since $\mathcal{F}$ is recursively defined by H, we have that $H(x_{i-1}, x_i) = 0$ for all $i \geq 0$. By reducing this equation modulo Q we obtain $H(x_{i-1}(Q), x_i(Q)) = 0$, and by hypothesis $x_{i-1}(Q) \in S_0$. Now, since $H(x_{i-2}, x_{i-1}) = 0$, the reduction modulo Q of this equation shows that $x_{i-2}(Q) \in S_0$. Continuing in this way, we arrive to the desired conclusion. □

Next we prove a proposition giving sufficient conditions for the finiteness of the ramification locus of a particular class of recursive sequences of Kummer type. Recall that if $g(T) \in \mathbb{F}_q[T]$, we denote by Z_g the set of zeros of $g(T)$ in an algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$.

Proposition 3.3. *Let $m \geq 2$ be an integer with $q \equiv 1 \bmod m$. Consider the sequence $\mathcal{F} = (F_0, F_1, \ldots)$ of function fields over $\mathbb{F}_q$ defined recursively by the* *equation*

$$y^m = \frac{b_1(x)}{b_2(x)}, \tag{3.1}$$

where $b_1(T), b_2(T) \in \mathbb{F}_q[T]$ *are coprime polynomials such that* $\deg(b_1(T)) = m$ *and* $\deg(b_2(T)) = m - r$ *with* $\gcd(m, r) = 1$. *Then* $\mathcal{F}$ *is a tame admissible sequence. Assume now that there is a finite set* $S_0 \subset \mathbb{F}_q$ *with the following properties*:

(1) $Z_{b_1} \subset S_0$.
(2) $Z_{b_2} \subset S_0$.
(3) $Z_{\sigma_\gamma} \subset S_0$, *for all* $\gamma \in S_0$, *where* $\sigma_\gamma(T) = b_2(T)\gamma^m - b_1(T)$.

Then $\mathrm{Ram}(\mathcal{F}/F_0)$ *is a finite set. More precisely, if* $P \in \mathbb{P}(\mathbb{F}_0)$ *is a ramified place in the sequence* $\mathcal{F}$ *then either* $P = P_\infty$ *is the pole of* x_0 *in* F_0, *or* P *is the zero of* $x_0 - \gamma$, *for some* $\gamma \in S_0$.

Proof. By hypothesis each extension F_n/F_{n-1} is cyclic of degree m. It is also easy to see that the pole P_∞ of x_0 in F_0 is totally ramified in the sequence $\mathcal{F}$. Therefore, $\mathbb{F}_q$ is the full constant field of each F_n, and then $\mathcal{F}$ is admissible and tame.

Suppose that $P \in \mathbb{P}(F_0)$ is ramified in F_n/F_0. Choose $Q \in \mathbb{P}(F_n)$ above P such that $e(Q \mid P) > 1$ and let $P_i = Q \cap F_i$ be the restriction of Q to F_i, for each $i = 0, 1, \ldots, n$. Since $Q \mid P$ is ramified, then $P_{i+1} \mid P_i$ is ramified for some index i.

From the defining equation,

$$x_{i+1}^m = \frac{b_1(x_i)}{b_2(x_i)},$$

and from the ramification theory of Kummer extensions (see, for example, [7, Proposition 3.7.3]), it follows that P_{i+1} is either a zero or a pole of x_{i+1} in F_{i+1}.

If P_{i+1} is a zero of x_{i+1}, we have that $x_{i+1}(Q) = 0$. By reducing the equation $x_{i+1}^m b_2(x_i) = b_1(x_i)$, modulo Q we obtain

$$0 = x_{i+1}(Q)^m b_2(x_i(Q)) = b_1(x_i(Q)),$$

and this implies that $x_i(Q) = \gamma$ for some $\gamma \in \overline{\mathbb{F}}_q$ such that $b_1(\gamma) = 0$. Thus $x_i(Q) \in S_0$ by (1).

Suppose now that P_{i+1} is a pole of x_{i+1}. Then $x_{i+1}^{-1} \in P_{i+1} \subset Q$. Hence $x_{i+1}^{-1}(Q) = 0$. Since $b_2(x_i) = b_1(x_i)x_{i+1}^{-m}$, by reducing modulo Q we have that $b_2(x_i(Q)) = b_1(x_i(Q))(x_{i+1}^{-1}(Q))^m = 0$ and this implies that $x_i(Q) = \gamma$ for some $\gamma \in \overline{\mathbb{F}}_q$ such that $b_2(\gamma) = 0$. Therefore $x_i(Q) \in S_0$ by (2). By (3) and Lemma 3.2 we have that $x_0(Q) \in S_0$.

Now we can easily see that if $P \in \mathbb{P}(F_0)$ is a ramified place in $\mathcal{F}$ then, $P = P_\infty$ if $v_{P_1}(x_1) < 0$ and P is the zero of $x_0 - \gamma$, for some $\gamma \in S_0$, if $v_{P_1}(x_1) \geq 0$. Hence $\mathrm{Ram}(\mathcal{F}/F_0) \subset \{P_{x_0 - \gamma} : \gamma \in S_0\} \cup \{P_\infty\}$ and since S_0 is finite, $\mathcal{F}$ has finite ramification locus. □

Now we can prove one of our main results.

Theorem 3.4. *Let $m \geq 2$ be an integer and q a prime power such that $q \equiv 1 \bmod m$. Let $\alpha \in \mathbb{F}_q$ such that $T^m + \alpha$ splits into linear factors in $\mathbb{F}_q$ and let $f(T) \in \mathbb{F}_q[T]$ be a separable polynomial of degree $m - r$ with $\gcd(m, r) = 1$ such that $Z_{T^m+\alpha} \cap Z_f = \emptyset$. Assume that there is a finite set $S_0 \subset \overline{\mathbb{F}}_q$ with the following properties*:

(1) $Z_{T^m - \alpha f(T) + \alpha} \subset S_0$.
(2) $Z_f \subset S_0$.
(3) $Z_{\sigma_\gamma} \subset S_0$, *for all* $\gamma \in S_0$, *where* $\sigma_\gamma(T) = f(T)(\gamma^m + \alpha) - (T^m + \alpha) \in \overline{\mathbb{F}}_q[T]$.

Then the sequence $\mathcal{F} = (F_0, F_1, \ldots)$ of function fields defined by the equation

$$y^m = \frac{x^m - \alpha f(x) + \alpha}{f(x)} \tag{3.2}$$

is an asymptotically good tower of Kummer type over $\mathbb{F}_q$ and

$$\lambda(\mathcal{F}) \geq \frac{2m}{|S_0| - 1} > 0.$$

Proof. As in Proposition 3.3, we have by hypothesis that each extension F_n/F_{n-1} is cyclic of degree m, and the pole P_∞ of x_0 in F_0 is totally ramified in the sequence $\mathcal{F}$. Therefore, $\mathbb{F}_q$ is the full constant field of each F_n, and then $\mathcal{F}$ is admissible and tame.

Using Proposition 3.1 we have that $|\mathrm{Split}(\mathcal{F}/F_0)| \geq m$ and then $\mathcal{F}$ is a tower over $\mathbb{F}_q$.

The fact that $S_0 \subset \overline{\mathbb{F}}_q$ is finite, implies that for some integer s we have that $S_0 \subset \mathbb{F}_{q^s}$ and satisfies the conditions in Proposition 3.3. Therefore, we have that if $P \in \mathbb{P}(\mathbb{F}_0)$ is a ramified place in the tower $\mathcal{F}$, then $P = P_\infty$ or P is the zero of $x_0 - \gamma$, for some $\gamma \in S_0$. Then the ramification locus is finite and thus the tower has a finite genus over $\mathbb{F}_{q^s}$. Since the genus of a tower does not change in constant field extensions, we conclude that $\mathcal{F}$ has finite genus over $\mathbb{F}_q$.

Finally, since $\mathcal{F}$ is a tame recursive tower with non-empty splitting locus and finite ramification locus, [4, Theorem 2.1] implies that $\mathcal{F}$ is an asymptotically good tower of Kummer type over $\mathbb{F}_q$. Moreover, since $|\mathrm{Split}(\mathcal{F}/F_0)| \geq m$ and $\mathrm{Ram}(\mathcal{F}/F_0) \subset S_0 \cup \{\infty\}$ then

$$\lambda(\mathcal{F}) \geq \frac{2m}{|S_0| + 1 - 2},$$

as desired. □

Example 3.5. Let $m = 2, q = 9$. Let $\mathcal{G} = (G_0, G_1, \ldots)$ be defined recursively by

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

This equation is of the form (1.1) with $f(x) = x$ and $\alpha = 1$. In this case, $T^2 + 1$ has two simple roots in $\mathbb{F}_9$ and $f(T)$ is a separable polynomial of degree 1 with no common roots with $T^2 + 1$. Then

$$|\mathrm{Split}(\mathcal{G}/G_0)| \geq 2,$$

by Proposition 3.1. The set $S_0 = \mathbb{F}_3 \subset \mathbb{F}_9$ satisfies conditions (1)–(3) of Theorem 3.4. Hence

$$\mathrm{Ram}(\mathcal{G}/G_0) \subseteq \{P_\infty, P_{x_0}, P_{x_0-1}, P_{x_0-2}\},$$

then $\mathcal{G}$ is an asymptotically good tower of Kummer type over $\mathbb{F}_9$ with

$$\lambda(\mathcal{G}) \geq 2.$$

Since

$$2 \geq A(9) \geq \lambda(\mathcal{G}) \geq 2,$$

we see that this tower over $\mathbb{F}_9$ is asymptotically optimal, i.e. $\lambda(\mathcal{G}) = A(9)$.

Remark 3.6. Note that the tower $\mathcal{G}$ in the previous example has, in fact, finite ramification locus over $\mathbb{F}_3$. However, Theorem 3.4 only allow us to say that $\mathcal{F}$ has positive splitting over $\mathbb{F}_9$. Notice that $\mathcal{G}$ can be described also by

$$y^2 = \frac{(x+1)^2}{4x}.$$

By [3, Remark 5.9] we have that $\mathcal{G}$ is a subtower of

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

which is optimal over $\mathbb{F}_{p^2}$.

Example 3.7. Let $m = 2, q = 9$. Let $\mathcal{H} = (H_0, H_1, \ldots)$ be defined recursively by

$$y^2 = \frac{x(x-1)}{x+1}.$$

This equation is of the form (1.1) with $f(x) = x + 1$ and $\alpha = 1$. Again in this case we have that $|\mathrm{Split}(\mathcal{H}/H_0)| \geq 2$. The finite field $\mathbb{F}_9$ can be represented as $\mathbb{F}_9 = \mathbb{F}_3(\delta)$ with $\delta^2 + 2\delta + 2 = 0$. The set $S_0 = \{0, 1, 2, \delta, \delta^3, \delta^5, \delta^7\} \subset \mathbb{F}_9$ satisfies conditions (1)–(3) of Theorem 3.4, and then $\mathcal{H}$ is an asymptotically good Kummer type tower over $\mathbb{F}_9$ with

$$\lambda(\mathcal{H}) \geq \frac{2}{3}.$$

Remark 3.8. Notice that the tower $\mathcal{H}$ in the previous example can be described also by

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

Using this equation in [3, Example 4.3] the authors proved that $\mathcal{H}$ is an asymptotically good tower and the same bound for its limit was obtained.

Theorem 3.4 is stated for towers whose defining equations have coefficients in any finite field. Hence we can find examples of towers whose defining equations have coefficients in non-prime fields. In fact, if we perform a computer search for all possible equations of the type (3.2) satisfying the conditions of Theorem 3.4 for $q = 9$ we obtain a long list of equations, and therefore of towers, which at first glance seem totally different from each other. In particular, we obtain some equations whose coefficients are purely in $\mathbb{F}_3$ while the vast majority has coefficients in $\mathbb{F}_9$. However, by a suitable change of variables, it can be shown that all of them are either equivalent to the tower in Example 3.5 or to the tower in Example 3.7. That is, the towers in the above examples are the only two towers with defining equations of the type (3.2) and satisfying the conditions of Theorem 3.4 with a finite set $S_0 \subset \mathbb{F}_9$.

For example, other equations defining the asymptotically optimal Kummer tower of Example 3.5 are given in Table 1.

Given that all the equations in Table 1 define the same tower and satisfy the conditions of Theorem 3.4 we wonder in which cases different equations satisfying these conditions will give us the same tower. As a response to this question we have the following proposition.

Proposition 3.9. *Let $\alpha \in \mathbb{F}_q^*$ and $f(T) \in \mathbb{F}_q[T]$ be such that the equation*

$$y^m = \frac{x^m - \alpha f(x) + \alpha}{f(x)} \tag{3.3}$$

defines a tower which satisfies the conditions of Theorem 3.4. *Then, if for $c \in \mathbb{F}_q^*$ we consider $\beta = c^{-m}\alpha \in \mathbb{F}_q^*$ and $g(T) = f(cT) \in \mathbb{F}_q[T]$, we have that the equation*

$$y^m = \frac{x^m - \beta g(x) + \beta}{g(x)}$$

defines the same tower as the one defined by (3.3) *and also satisfies Theorem* 3.4.

Proof. By applying to (3.3) the change of variables $x = cX, y = cY$ we get

$$c^m Y^m = \frac{c^m X^m - \alpha f(cX) - \alpha}{f(cX)}.$$

Table 1. Other examples of equations defining the same tower as in Example 3.5.

α	$f(T)$	Defining equation	Change of variables
$\delta + 1$	$(\delta + 2)T$	$y^2 = \frac{x^2-(\delta+1)(\delta+2)x+\delta+1}{(\delta+2)x}$	$X = \delta x; Y = \delta y$
$\delta + 1$	$(2\delta + 1)T$	$y^2 = \frac{x^2-(\delta+1)(2\delta+1)x+\delta+1}{(2\delta+1)x}$	$X = \delta^4 x; Y = \delta^4 y$
2	$(\delta + 1)T$	$y^2 = \frac{x^2-2(\delta+1)x+2}{(\delta+1)x}$	$X = \delta^3 x; Y = \delta^3 y$
$2\delta + 2$	$2\delta T$	$y^2 = \frac{x^2-(2\delta+2)2\delta x+2\delta+2}{2\delta x}$	$X = 2x; Y = 2y$
1	$2T$	$y^2 = \frac{x^2-2x+1}{2x}$	$X = \delta^5 x; Y = \delta^5 y$
$2\delta + 2$	δT	$y^2 = \frac{x^2-(2\delta+2)\delta x+2\delta+2}{\delta x}$	$X = \delta^2 x; Y = \delta^2 y$

Thus

$$Y^m = \frac{X^m - c^{-m}\alpha g(X) + c^{-m}\alpha}{g(X)} = \frac{X^m - \beta g(X) + \beta}{g(X)}$$

defines the same tower.

Moreover, since $Z_{T^m+\alpha} \cap Z_f = \emptyset$ then $Z_{T^m+\beta} \cap Z_g = \emptyset$. Otherwise, if $x \in Z_{T^m+\beta} \cap Z_g$ then $x^m + \beta = 0$ and $g(x) = 0$. This means that $x^m + c^{-m}\alpha = 0$ and $f(cx) = 0$, and since $c \in \mathbb{F}_q^*$ we get $(cx)^m + \alpha = 0$. But in this case $cx \in Z_{T^m+\alpha} \cap Z_f$ which is a contradiction.

Let S_0 be the set of Theorem 3.4 for f. We define $S_0^g = \{c^{-1}\lambda : \lambda \in S_0\} \subset \mathbb{F}_q$. Then S_0^g satisfies:

(1)

$$\begin{aligned} Z_{T^m - \beta g(T) + \beta} &= \{x : x^m - \beta g(x) + \beta = 0\} \\ &= \{x : x^m - c^{-m}\alpha f(cx) + c^{-m}\alpha = 0\} \\ &= \{c^{-1}(cx) : (cx)^m - \alpha f(cx) + \alpha = 0\} \\ &\subset \{c^{-1}\lambda : \lambda \in S_0\} = S_0^g. \end{aligned}$$

(2) $Z_g = \{x : g(x) = 0\} = \{c^{-1}(cx) : f(cx) = 0\} \subset \{c^{-1}\lambda : \lambda \in S_0\} = S_0^g$.

(3) For all $\gamma \in S_0^g$ we have that $\gamma = c^{-1}\delta$ with $\delta \in S_0$ and

$$\begin{aligned} Z_{\sigma_\gamma} &= \{x : g(x)(\gamma^m + \beta) - (x^m + \beta) = 0\} \\ &= \{x : f(cx)((c^{-1}\delta)^m + \alpha) - ((cx)^m + \alpha) = 0\} \\ &= \{c^{-1}\lambda : f(\lambda)(\delta^m + \alpha) - (\lambda^m + \alpha) = 0\} \\ &= \{c^{-1}\lambda : \sigma_\delta(\lambda) = 0\} \\ &\subset \{c^{-1}\lambda : \lambda \in S_0\} = S_0^g. \end{aligned}$$

Therefore, for each element in $\mathbb{F}_q^*$ we have an equation which defines the same tower as (3.3) and satisfies the conditions of Theorem 3.4. □

For those cases where $c^m = 1$, we have the following direct consequence of the above proposition.

Corollary 3.10. *For each mth root c of* 1 *in $\mathbb{F}_q$, we have that the equation*

$$y^m = \frac{x^m - \alpha g(x) + \alpha}{g(x)},$$

with $g(T) = f(cT) \in \mathbb{F}_q[T]$, defines the same tower as (3.3) *and satisfies the conditions of Theorem* 3.4.

Proposition 3.9 has an important computational consequence. Namely when making a computer search for all possible equations that define towers satisfying the conditions of Theorem 3.4 over $\mathbb{F}_q$, we will actually find $q-1$ equations representing the same tower. Moreover, the above corollary tells us that for every α there are as many equations that define the same tower as mth roots of 1 in $\mathbb{F}_q$.

Let us now look at some other examples of towers whose defining equations have coefficients in non-prime fields. We consider first the case $m = 2$ and $q = 25$.

Example 3.11. Let us represent the finite field $\mathbb{F}_{25}$ as $\mathbb{F}_5(\delta)$ with $\delta^2 + 4\delta + 2 = 0$. Consider the sequence $\mathcal{K} = (K_0, K_1, \ldots)$ of function fields over $\mathbb{F}_{25}$ defined recursively by the equation

$$y^2 = \frac{x^2 - (\delta + 2)x}{(\delta + 2)x + 1}.$$

We have that $\mathbb{F}_{25}$ is a splitting field for $T^2 + 4$ and it is easy to check that $S_0 = \{0, 2\delta + 4, 4\delta + 3, \delta + 2, 3\delta + 1\}$ satisfies the conditions of Theorem 3.4. Then $\mathcal{K}$ is a tame Kummer type tower over $\mathbb{F}_{25}$ with

$$|\mathrm{Split}(\mathcal{K}/K_0)| \geq 2$$

and

$$|\mathrm{Ram}(\mathcal{K}/K_0)| \leq 5.$$

Therefore, by Theorem 3.4 we have that

$$\lambda(\mathcal{K}) \geq \frac{2 \cdot 2}{5 - 1} = 1.$$

Remark 3.12. By using a suitable change of variables it can be shown that the tower $\mathcal{K}$ can also be defined by the equation

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

which was studied by Garcia, Stichtenoth and Rück in [3], where it is also shown that its limit is at least 1.

Remark 3.13. Again in this case, making a computer search for all possible equations over $\mathbb{F}_{25}$ defining towers satisfying Theorem 3.4, we find 24 different equations, but all of them represent the tower $\mathcal{K}$ of Example 3.11. There is no other tower of this type with a finite set $S_0 \subset \mathbb{F}_{25}$.

Now we show new examples of asymptotically good Kummer type towers over $\mathbb{F}_9$.

Example 3.14. Let us represent the finite field $\mathbb{F}_{81}$ as $\mathbb{F}_3(\delta)$ with $\delta^4 + 2\delta^3 + 2 = 0$. When looking for all possible equations

$$y^2 = \frac{x^2 - \alpha f(x) + \alpha}{f(x)},$$

defining towers of function fields over $\mathbb{F}_{81}$ with, for example, $\alpha = 2\delta^3 + 2\delta^2 + 1$, we arrive to eight different possible candidates for $f(T)$. But since $\mathbb{F}_{81}$ has two 2th roots of unity, Corollary 3.10 tells us that only four of these equations represent different towers. Two of them are the towers of Examples 3.5 and 3.7, and we find two more new towers:

$$\mathcal{I} = (I_0, I_1, \ldots) \quad \text{with } f(T) = (2\delta^3 + 2\delta^2 + 2)T + (\delta^3 + \delta^2 + 2)$$

and

$$\mathcal{J} = (J_0, J_1, \ldots) \quad \text{with } f(T) = (\delta^3 + \delta^2)T + (2\delta^3 + 2\delta^2).$$

In both cases we find a finite set S_0 with nine elements and by Theorem 3.4 we have that

$$\lambda(\mathcal{I}) \geq \frac{2 \cdot 2}{9-1} = \frac{1}{2} \quad \text{and} \quad \lambda(\mathcal{J}) \geq \frac{2 \cdot 2}{9-1} = \frac{1}{2}.$$

Remark 3.15. Again as before, if we look (computationally) for all possible equations of the type (3.2) satisfying the conditions of Theorem 3.4 for $q = 81$ we obtain a long list of candidates. Interestingly in this case, there are no other equations representing the towers $\mathcal{I}$ or $\mathcal{J}$ with coefficients in $\mathbb{F}_3$. Moreover, it is easy to check that the coefficients in both equations are actually in $\mathbb{F}_9$. However, the corresponding sets S_0 are in $\mathbb{F}_{81}$ and not in $\mathbb{F}_9$. Since the genus of a tower does not change in constant field extensions and recalling that the towers $\mathcal{I}$ and $\mathcal{J}$ both have non-empty splitting locus in $\mathbb{F}_9$, we see that in fact, they are asymptotically good towers over $\mathbb{F}_9$, each one with limit at least 1/2. From this and the list of asymptotically good tame towers over $\mathbb{F}_9$ given in [6], we can say that $\mathcal{I}$ and $\mathcal{J}$ are new examples.

As we mentioned in Sec. 1, in this paper we have worked with towers defined recursively by equation of the form (1.1) because they have non-empty splitting locus under the conditions of Proposition 3.1 which are easy to check. Another equation in which is already known that the splitting locus is non-empty is

$$y^m = x^{m-r} f(x), \tag{3.4}$$

where $f \in \mathbb{F}_q[x]$ is a suitable polynomial of degree r with $f(0) \neq 0$ and $\gcd(m, r) = 1$. In [4], Garcia, Stichtenoth and Thomas studied towers defined recursively by (3.4), giving conditions in order to have finite ramification locus. Interestingly, and somehow surprisingly, when performing a computational search for this type of equations, the only examples that appeared are the so-called Fermat type towers (see [3]). So we are tempted to conjecture that these are the only ones of the form (3.4) which are asymptotically good. Recall that Lenstra [5] proved that over a prime fields, for equations of the form (3.4) there is not a finite set $S_0 \subset \overline{\mathbb{F}}_p$ containing the ramification locus of the tower.

We end with the following observation. Making the change of variables $X = 1/x$ and $Y = 1/y$ in (3.4), we obtain the equation

$$y^m = \frac{x^m}{h(x)},$$

with $h \in \mathbb{F}_q[x]$. In particular, for $q = 9$ and $h(x) = x - 1$ we have a tower recursively defined by

$$y^2 = \frac{x^2}{x-1},$$

which is asymptotically optimal (see [3, Example 14.9]). However, this example is not new as claimed in [3]. It is, in fact, a Fermat type tower of the form (3.4) given by

$$y^2 = x(x-1),$$

over $\mathbb{F}_9$.

Acknowledgment

The first author was supported by Departamento de Matemáticas, Facultad de Ingeniería Química (UNL) and Instituto de Matemática Aplicada del Litoral (UNL-CONICET).

References

[1] M. Chara and R. Toledano, Rational places in extensions and sequences of function fields of kummer type, *J. Pure Appl. Algebra* **215**(11) (2011) 2603–2614.

[2] A. Garcia and H. Stichtenoth, Explicit towers of function fields over finite fields, in *Topics in Geometry*, *Coding Theory and Cryptography*, Algebras and Applications, Vol. 6 (Springer, Dordrecht, 2007), pp. 1–58.

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

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

[5] H. W. Lenstra, Jr., On a problem of Garcia, Stichtenoth, and Thomas, *Finite Fields Appl.* **8**(2) (2002) 166–170.

[6] H. Maharaj and J. Wulftange, On the construction of tame towers over finite fields, *J. Pure Appl. Algebra* **199**(1–3) (2005) 197–218.

[7] H. Stichtenoth, *Algebraic Function Fields and Codes*, 2nd edn., Graduate Texts in Mathematics, Vol. 254 (Springer-Verlag, Berlin, 2009).

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