Available online at www.sciencedirect.com
SCIENCE DIRECT®
Journal of Pure and Applied Algebra 199 (2005) 197–218
JOURNAL OF PURE AND APPLIED ALGEBRA
www.elsevier.com/locate/jpaa

On the construction of tame towers over finite fields

Hiren Maharaj[a,*], Jörg Wulftange[b]

[a] *Department of Mathematical Sciences, Clemson University, Clemson, SC 29634-0975, USA*
[b] *Mathematics and Computer Science, University of Essen, 45117 Essen, Germany*

Received 1 October 2003; received in revised form 5 November 2004
Available online 13 January 2005
Communicated by J. Walker

Abstract

Recently, W.-C. W. Li, et al. (Lect. Notes in Comput. Sci. 2369 (2002) 372) developed a non-deterministic algorithm to perform a computer search for polynomials that recursively define asymptotically good sequences of function fields. In this paper, we build on this work by refining this algorithm. We give many sufficient conditions for the construction of such sequences and we describe the techniques used in the search. Many examples are given. The resulting towers are important for the construction of asymptotically good sequences of codes and they could provide further numerical evidence for Elkies' modularity conjecture.

MSC: Primary: 11R58; secondary: 11G20; 12F05; 12Y05

1. Introduction

Much work has been devoted to the construction of asymptotically good sequences of function fields over a finite field, that is, sequences of function fields over a fixed finite field with asymptotically many rational places relative to the genus. The main motivation for such constructions is their usefulness in the construction of sequences of arbitrarily long codes with parameters exceeding or close to the Gilbert–Varshamov bound. For applications to coding theory, one requires an explicit presentation of these function fields. Explicit constructions began in 1995 in a paper by Garcia and Stichtenoth [10]. Subsequent work

* Corresponding author: Tel.: 864 656 4566; fax: 864 656 5230.
E-mail addresses: hmahara@clemson.edu (H. Maharaj), wulftange@hotmail.com (J. Wulftange).

0022-4049/$ - see front matter © 2004 Elsevier B.V. All rights reserved.
doi:10.1016/j.jpaa.2004.12.008

on this topic include, among others, [4,5,10–14,16,17]. For a reference describing non-explicit constructions, using class field theoretic techniques, we recommend the book by Niederreiter and Xing [20]. Recently, in [17], a non-deterministic algorithm is developed to perform a systematic computer search for polynomials that recursively define explicit asymptotically good sequences of function fields. In this paper, we build on this work by refining this algorithm. In this section, we give some background and a detailed description of the algorithm. In Section 2 we give many sufficient conditions for the construction of such sequences. In Section 3 we describe some of the techniques used in the search and in Section 4 we describe the computer implementation and improvements of the algorithm. Finally, in Section 5 we present many new examples. Unless otherwise mentioned, we will use the same notation as in [21], for example, we denote the set of places of a function field F by $\mathbb{P}(F)$ and its number of rational places by $N(F)$.

A *tower of function fields over* $\mathbb{F}_q$ is defined to be a sequence $\mathscr{F} = (F_0, F_1, F_2, \ldots)$ of function fields, having the following properties:

(i) $F_0 \subseteq F_1 \subseteq F_2 \subseteq \ldots$.
(ii) For each $n \geqslant 0$, the extension F_{n+1}/F_n is separable of degree $[F_{n+1} : F_n] > 1$.
(iii) The genus $g(F_j) > 1$ for some $j \geqslant 1$.
(iv) $\mathbb{F}_q$ is the full field of constants of each F_n.

As noted in [10], the conditions (ii), (iii) and the Hurwitz genus formula imply that $g(F_n) \to \infty$ as $n \to \infty$. A tower $\mathscr{F} = (F_0, F_1, F_2, \ldots)$ is called *tame* if each extension F_{n+1}/F_n, $n = 0, 1, \ldots$, is a tame extension. For any tower $\mathscr{F} = (F_0, F_1, F_2, \ldots)$ of function fields over $\mathbb{F}_q$, let

$$\lambda(\mathscr{F}) := \lim_{i\to\infty} N(F_i)/g(F_i).$$

It is shown in [13] that this limit is well defined. A tower $\mathscr{F}$ is said to be *asymptotically good* (respectively *asymptotically bad*) if $\lambda(\mathscr{F}) > 0$ (respectively $\lambda(\mathscr{F}) = 0$). It is clear that $\lambda(\mathscr{F}) \leqslant A(q)$ where $A(q) = \limsup_{g\to\infty} N_q(g)/g$ where $N_q(g)$ is the maximum number of rational places of a function field with genus g and with the finite field $\mathbb{F}_q$ as the full field of constants. Drinfeld and Vladut [3] showed that $A(q) \leqslant \sqrt{q} - 1$. It was also shown by Ihara [15], and Tsfasman et al. [22] in special cases, that $A(q) = \sqrt{q} - 1$ when q is a square. When q is not a square, the exact value of $A(q)$ is currently unknown. We say that the tower $\mathscr{F}$ over $\mathbb{F}_q$ is *optimal* if $\lambda(\mathscr{F}) = A(q)$.

In the case that q is a square, Garcia and Stichtenoth [9] discovered the first explicit optimal tower over $\mathbb{F}_q$—thus providing a more elementary proof of the Ihara result that $A(q) = \sqrt{q} - 1$ if q is a square. Subsequently in [10], Garcia and Stichtenoth found another optimal tower $\mathscr{G} := (F_i)$ over $\mathbb{F}_q$, q a square, with the following simpler description: let $q_0^2 = q$ and put $F_0 := \mathbb{F}_q(x_0)$; for $n > 0$ we have $F_n := F_{n-1}(x_n)$ where

$$x_n^{q_0} + x_n = \frac{x_{n-1}^{q_0}}{x_{n-1}^{q_0-1} + 1}. \tag{1}$$

In these towers wild ramification occurs and so the genus computation is difficult. Subsequently in [14,4] explicit towers with tame ramification were found. In [4], using modular

curve constructions, Elkies found entire families of explicit optimal towers with tame ramification. Tame towers have the advantage that the genus computation is simpler. In fact, for a tame tower $\mathscr{F}$, under additional assumptions, we have the following lower bound for $\lambda(\mathscr{F})$:

Theorem 1.1 (*Garcia et al. [14]*). *Let $\mathscr{F} = (F_0, F_1, F_2, \ldots)$ be a tower of function fields over $\mathbb{F}_q$ satisfying the following conditions*:

(i) *All extensions F_{n+1}/F_n are tame.*
(ii) *The set $R_{\mathscr{F}} = \{P \in \mathbb{P}(F_0) | P$ is ramified in F_n/F_0 for some $n \geqslant 1\}$ is finite.*
(iii) *The set $S_{\mathscr{F}} = \{P \in \mathbb{P}(F_0) | \deg P = 1$, and P splits completely in all extensions $F_n/F_0\}$ is non-empty.*

Then $\mathscr{F}$ is an asymptotically good tower and

$$\lambda(\mathscr{F}) \geqslant \frac{2s}{2g(F_0) - 2 + r}, \tag{2}$$

where $s := \#S_{\mathscr{F}}$ and $r := \sum_{P \in R_{\mathscr{F}}} \deg P$.

Given $f(x, y) \in \mathbb{F}_q[x, y]$, a tower $\mathscr{F} = (F_0, F_1, \ldots)$ over $\mathbb{F}_q$ is said to be (recursively) defined by $f(x, y)$ if $F_0 = \mathbb{F}_q(x_0)$ is the rational function field and for each $n > 0$, $F_n = \mathbb{F}_q(x_0, x_1, \ldots, x_n)$, where $f(x_i, x_{i+1}) = 0$ for $1 \leqslant i < n$. For brevity, we usually specify a tower by stating the polynomial $f(x, y)$ which defines the recursion. Thus the Garcia–Stichtenoth tower $\mathscr{G}$ above would be presented by

$$f(x, y) = (x^{q_0 - 1} + 1)(y^{q_0} + y) - x^{q_0}.$$

Next we describe the algorithm used in [17] to perform a search for asymptotically good recursively defined tame towers. The main idea for the algorithm comes from the proof in [10] that the recursion (1) gives an optimal tower. Essentially, the algorithm checks if the conditions of Theorem 1.1 are satisfied. Given $f(x, y) \in \mathbb{F}_q[x, y]$, the most difficult conditions to check for are: whether $f(x, y)$ gives rise to a tower and condition (ii) of Theorem 1.1.

Let $K = \overline{\mathbb{F}}_q$ denote a fixed algebraic closure of $\mathbb{F}_q$. Observe that if $\mathscr{F} = (F_0, F_1, F_2, \ldots)$ is a tower over $\mathbb{F}_q$ then the composite $\mathscr{F} \cdot K := (F_0 \cdot K, F_1 \cdot K, \ldots)$ satisfies conditions (i), (ii) and (iii) in the definition of a tower. Also note that the set $R_{\mathscr{F}}$ of Theorem 1.1 is finite if and only if the set $R_{\mathscr{F} \cdot K}$ is finite. Thus, we may take K to be the field of constants for $\mathscr{F}$ and we let $F := K(x, y)$, $f(x, y) = 0$ where $f(x, y) \in K[x, y]$ is irreducible.

Define $\mathbb{P}^1$ to be the set $K \cup \{\infty\}$ where ∞ is a formal symbol which does not belong to K; for a given rational function field $K(z)$ and $v \in \mathbb{P}^1$, we denote by $P_v(z)$ the zero of $z - v$ in $K(z)$ if $v \in K$; otherwise $P_v(z)$ denotes the pole of z in $K(z)$. If $v, \mu \in \mathbb{P}^1$, we write $v \leftarrow \mu$ if there exists a place Q in F such that Q extends both the places $P_v(x)$ and $P_\mu(y)$.

In [12], it is shown that a necessary condition for f to define an asymptotically good tower is that the degrees of f in both variables are equal, so we assume this about f. Let m be the degree of f in both variables. Let M denote the set of all $v \in \mathbb{P}^1$ such that $P_v(x)$ is totally ramified in the extension $F/K(x)$ and let N denote the set of all $\mu \in \mathbb{P}^1$ such

that the place $P_\mu(y)$ is ramified in the extension $F/K(y)$ with ramification index e such that g.c.d$(e, m) > 1$ or p divides e where p is the characteristic of $\mathbb{F}_q$. Then condition (ii) is checked as follows:

(1) Put $R_0 := \{v \in \mathbb{P}^1 | P_v(x)$ ramifies in $F/K(x)\}$.
(2) $R_{i+1} := \{\mu \in \mathbb{P}^1 | \mu \leftarrow v$ for some $v \in R_i\}$ for $i = 0, 1, 2, \ldots$
(3) Put $R := \bigcup_{i=0}^{\infty} R_i$.
(4) If the set R is finite then $R_{\mathscr{F}}$ is finite (see Theorem 2.6).

Computationally, each successive R_i is computed and if for some $j > 0$ we have that

$$R_j \subseteq \bigcup_{i=0}^{j-1} R_i, \tag{3}$$

then we conclude that $R = \bigcup_{i=0}^{j-1} R_i$ is finite. This explains why the algorithm is not deterministic: we do not know the smallest j for which (3) may hold. Also we have no way of deciding at the outset in which finite field to do all the computations. It may well happen that (3) holds while the smallest finite field containing R is too large to do computations in a reasonable running time.

Next we show how we checked for condition (iii). In this case, the set $S_{\mathscr{F}}$ is easily computed as follows: For each $v \in \mathbb{F}_q$ let

$$S(v) = \{\mu \in \mathbb{F}_q \cup \{\infty\} | v \leftarrow \mu\}.$$

Let

$$S_0 := \{[v, S(v)] | v \in \mathbb{F}_q \cup \{\infty\} \text{ and } P_v(x) \text{ splits completely in } \mathbb{F}_q(x, y)/\mathbb{F}_q(x)\}.$$

For $i \geqslant 1$ we define sets S_i and S_i' recursively as follows:

$$S_{i-1}' := \{v : [v, S(v)] \in S_{i-1}\}$$

and

$$S_i := \{[v, S(v)] \in S_{i-1} | S(v) \subseteq S_{i-1}'\}.$$

Note that the sequence (S_i) satisfies $S_0 \supseteq S_1 \supseteq S_2 \supseteq \ldots$. If for some i we have that $S_i = S_{i+1}$ then the sequence stabilizes: $S_i = S_{i+1} = S_{i+2} = \ldots$ and if $S_i \neq \emptyset$ then the places $P_v(x_0)$ $(v \in S_i')$ split completely in each extension F_n/F_0. We set

$$S_{\mathscr{F}} = \{P_v(x_0) : v \in S_i'\}.$$

After checking that conditions (ii) and (iii) of Theorem 1.1 are satisfied, the next step is to determine if the sequence (F_i) is infinite. In order to do this, we choose only those equations which result in towers where there is ramification in each step F_{n+1}/F_n as it is an easy matter to automatically check for this condition while searching for the set R. The above algorithm was implemented using the algebraic number theory package KASH [2].

The following new towers were found in [17]:

Theorem 1.2 (*Li et al. [17]*). *Each of the polynomials below defines an optimal tower over the indicated finite field*:

- $2xy^2 + (x^2 + x + 1)y + x^2 + x + 2$ *over* $\mathbb{F}_9$,
- $(4x + 1)y^2 + (x^2 + x + 2)y + x + 3$ *over* $\mathbb{F}_{25}$,
- $(x^2 + 6)y^2 + xy + x^2 + 4$ *over* $\mathbb{F}_{49}$,
- $x^2y^3 + (x^3 + x^2 + x)y^2 + (x + 1)y + x^3 + x$ *over* $\mathbb{F}_4$.

In [17] it is shown that the above towers are new in the sense that they cannot be embedded in any of the known towers. In the appendix of [17], Elkies proves that the four towers described above define new modular towers and that they dominate known modular towers. He [4,5] has shown that every currently known explicit optimal tower over $\mathbb{F}_{q^2}$ is either elliptic modular or Drinfeld modular. In particular the Garcia–Stichtenoth tower above is Drinfeld modular. He further conjectures that all the optimal towers over $\mathbb{F}_{q^2}$ constructed recursively should be modular. Every new tower found in this paper dominates a tower which is known to be modular. As pointed out by Elkies [17], this strongly suggests that they are also modular. The modularity of the new towers are yet to be determined.

It should be pointed out that while our computer searches are extensive, they are not exhaustive. In this paper we focused only on towers defined by degree two polynomials. There are two most striking observations from the accumulated data: the first is the above-mentioned fact that every asymptotically good tower found dominates a known modular tower. The other is that we found no asymptotically good towers over prime fields $\mathbb{F}_p$ for $p = 3, 5, 7, 11, 13$. This leads to the question whether there are any. In [16], Lenstra gives an elegant proof that a construction of Garcia et al. presented in [14] (for every finite field which is not prime) cannot work over prime fields. This, coupled with our data, suggests that there are no asymptotically good towers over prime fields defined by degree two polynomials.

Further outputs from the algorithm, especially for higher degree polynomials, will be recorded on a web page [19].

2. On the construction of recursively defined towers

Throughout this section we use the following notation. Let $f(x, y) \in \mathbb{F}_q[x, y]$ and let m be the degree of f in the y variable. Let $F_0 := \mathbb{F}_q(x_0)$ be the rational function field. We will only consider extensions of F_0 in a fixed algebraic closure of F_0. For $n > 0$ define $F_n := F_{n-1}(x_n)$ where x_n is a solution to $f(x_{n-1}, T) = 0$. We will say that the resulting sequence $F_0, F_1, \ldots$ is recursively defined by $f(x, y)$ and we put $\mathscr{F} := \bigcup_{i \geqslant 0} F_i$. It is clear that a given $f(x, y)$ may recursively define more than one such sequence of function fields and the corresponding field $\mathscr{F}$ could possibly be different in each case. A crucial condition to check in the search for good towers is that $[\mathscr{F} : \mathbb{F}_q(x_0)] = \infty$. Once this condition is satisfied and if it is further known that at least one rational place of F_0 splits completely in $\mathscr{F}$, then the Hasse Weil bound guarantees that $g(F_n) \to \infty$. In this section we present many sufficient conditions for the extension $\mathscr{F}/F_0$ to be infinite. As before, let K denote the algebraic closure of $\mathbb{F}_q$. Since the extension $\mathscr{F}/F_0$ is infinite if and only if the extension

$\mathscr{F} \cdot K$ over $F_0 \cdot K$ is infinite, we may take K to be the field of constants for $\mathscr{F}$. Moreover, the quantity r in Theorem 1.1 remains unchanged over constant field extensions—typically (but not always) we work in the smallest constant field extension such that all places in set $R_{\mathscr{F}}$ all have degree one. The following result will be used repeatedly in the sequel (see also [23]).

Lemma 2.1. *Let F'/F be a finite extension of function fields. Suppose that $F' = F_1F_2$ is the compositum of two intermediate fields $F \subseteq F_1$, $F_2 \subseteq F'$ and that $F = F_1 \cap F_2$. Assume that F_1 and F_2 are linearly disjoint over F. Let P be a place of F and let P_1 and P_2 be respective places over P in F_1 and F_2. Then there exists a place P' in F' with $P'|P_1$ and $P'|P_2$.*

Proof. First assume that the extensions F_1/F and F_2/F are separable. Let $\tilde{F}$ be the Galois closure of F' over F. Let $Q_1(:= P_1)$, Q_2, ..., Q_n be the places of F_1 that lie over P. We choose an element $t \in F_1$ such that $v_{Q_1}(t) > 0$ and $v_{Q_i}(t) < 0$ for $i = 2, \ldots, n$ (such a choice is possible by the weak approximation theorem).

We consider a place $\tilde{P}$ of $\tilde{F}$over P_2 and let $\tilde{Q}$ be a place of $\tilde{F}$ that lies over Q_1. Since the Galois group of $\tilde{F}/F$ acts transitively on the places over P, there is a $\sigma \in Gal(\tilde{F}/F)$ with $\tilde{Q}^\sigma = \tilde{P}$. Then, we have $t^\sigma \in \tilde{P}$.

Let f be the minimal polynomial of t over F. Since F_1 and F_2 are linearly disjoint over F, the polynomial f is irreducible over F_2. The Galois group of $\tilde{F}/F_2$ acts transitively on the zeroes of f. As t and t^σ are zeroes of f, there is a $\tau \in \tilde{G} := Gal(\tilde{F}/F_2)$ with $t^{\sigma\tau} = t$.

Let $P' := \tilde{P}^\tau \cap F'$. Since $\tilde{G}$ fixes F_2 element-wise, it follows that $P'|P_2$. Since $t \in P'$, it follows from $P' \cap F_1 = Q_j$ for some $j \in \{1, \ldots, n\}$, that $P'|P_1$.

Now, if F_1/F or F_2/F is not separable, for $i = 1, 2$ let $F \subseteq E_i \subseteq F_i$ such that E_i/F separable, and F_i/E_i purely inseparable. Define $E' := E_1E_2$ and $Q_i := P_i \cap E_i$. Due to the first part of the proof, there is a place Q' of E' with $Q'|Q_i$. Since the extension F'/E' is purely inseparable and all places in purely inseparable extensions are totally ramified, the result follows in this case too. □

Corollary 2.2. *Suppose for each k $(0 \leqslant k < n)$ that $f(x_k, T)$ is absolutely irreducible over F_k. For $0 \leqslant i \leqslant j \leqslant n$ define $F_{i,j} = K(x_i, x_{i+1}, \ldots, x_j)$. For $0 \leqslant i \leqslant j \leqslant k \leqslant l \leqslant n$ let P, P_1 and P_2 be places of $F_{j,k}$, $F_{i,k}$ and $F_{j,l}$ respectively, such that $P_1|P$ and $P_2|P$. Then, there exists a place P' in $F_{i,l}$ with $P'|P_1$ and $P'|P_2$.*

Proof. As the polynomial $f(x_k, Y)$ is irreducible over F_k for $k = 0, \ldots, n-1$, it follows from the recursive definition of the intermediate fields $F_{i,j}$, that

$$m^{l-k} = [F_{j,l} : F_{j,k}] = [F_{i,l} : F_{i,k}].$$

Thus, $[F_{i,l} : F_{j,l}] = [F_{i,k} : F_{j,k}]$ and the fields $F_{i,k}$ and $F_{j,l}$ are linear disjoint over $F_{j,k}$. Now, the claim follows from lemma 2.1. □

Let M and N be the sets defined in Section 1. Define a sequence of function fields as follows: put $F_0 := K(x_0)$, and for each $k \geqslant 0$, let x_{k+1} be a solution to $f(x_k, T) = 0$; put $F_k := K(x_0, x_1, \ldots, x_k)$. The next result gives a condition for $[F_k : F_0] \to \infty$ as $k \to \infty$.

Theorem 2.3. *Suppose that for some $\mu_0 \in M\backslash N$, there is a sequence $(\mu_i)_{i\geqslant 0}$ in $\mathbb{P}^1\backslash N$ such that $\mu_{i+1} \leftarrow \mu_i$ for all $i \geqslant 0$. Then for each $k = 0, 1, \ldots$, there is a place in F_k which is totally ramified in the extension F_{k+1}/F_k with ramification index m so that $[F_{k+1} : F_k] = m$. In particular, this implies that $[F_k : F_0] \to \infty$ as $k \to \infty$. If, in addition, we also assume that m is relatively prime with the characteristic of K, then each extension F_{k+1}/F_k is also separable.*

Proof. We prove by induction on k that there exists a place P in each F_k which ramifies in F_{k+1}/F_k with index m. For the field F_0 the result is true as the place $P \in \mathbb{P}_{F_0}$ with $x_0(P) = \mu_0$ is totally ramified in F_1/F_0. Now, suppose the claim is true for $0 \leqslant i < k$. By assumption, there exists a place Q_i in $K(x_i, x_{i+1})$, such that $x_i(Q_i) = \mu_{k-i}$ and $x_{i+1}(Q_i) = \mu_{k-i-1}$ for $0 \leqslant i < k$. It follows from the induction that the polynomials $f(x_i, Y)$ are irreducible over F_i for $0 \leqslant i < k$. By repeated application of Corollary 2.2 we obtain a place Q of F_k, which lies over all the places Q_i with $0 \leqslant i < k$. By Abhyankar's Lemma [21, Proposition III.8.9], the place Q over $Q \cap K(x_k)$ has ramification index r with $\gcd(r, m) = 1$. Since $Q \cap K(x_k)$ is totally ramified in $K(x_k, x_{k+1})/K(x_k)$, it follows again by Abhyankar's Lemma that Q ramifies in F_{k+1}/F_k with ramification index m. □

The smallest field containing sequence $(\mu_i)_{i\geqslant 0}$ may be large thus making it difficult to compute. The following corollary however has an effective version which is explained in Section 2.1.

Corollary 2.4. *Suppose that $M \nsubseteq N$ and that for each $\mu \in \mathbb{P}^1\backslash N$ there is a $\nu \in \mathbb{P}^1\backslash N$ such that $\nu \leftarrow \mu$. Then for each k there is a place in F_k which is totally ramified in the extension F_{k+1}/F_k with ramification index m so that $[F_{k+1} : F_k] = m$. In particular, this implies that $[F_k : F_0] \to \infty$ as $k \to \infty$. If, in addition, we also assume that m is relatively prime with the characteristic of K, then each extension F_{k+1}/F_k is also separable.*

Define the sets $M' := M \cap K$ and $N' := N \cap K$.

Corollary 2.5. *Suppose that $f(x, y)$ is monic in y, $M' \nsubseteq N'$ and that for some $\mu_0 \in M'\backslash N'$ there is a sequence $(\mu_i)_{i\geqslant 0}$ in $K\backslash N'$ such that $f(\mu_{i+1}, \mu_i) = 0$ for each $i = 0, 1, \ldots$. Then for each k there is a place in F_k which is totally ramified in the extension F_{k+1}/F_k with ramification index m so that $[F_{k+1} : F_k] = m$. In particular, this implies that $[F_k : F_0] \to \infty$ as $k \to \infty$. If, in addition, we also assume that m is relatively prime with the characteristic of K, then each extension F_{k+1}/F_k is also separable.*

Proof. The result follows because Kummer's Theorem [21, Theorem III.3.7] guarantees that the conditions $\mu_{i+1} \leftarrow \mu_i$ $(i \geqslant 0)$ of Theorem 2.3 are satisfied. □

Theorem 2.6. *Let $\mathscr{F}$ be a tower recursively defined by a polynomial $f(x, y)$ and let $R = \bigcup_{i=0}^{\infty} R_i$ be the set defined in Section 1. Then*

$$R_{\mathscr{F}} \subseteq \{P_\mu(x_0) : \mu \in R\}.$$

Thus, if R is finite then $R_{\mathscr{F}}$ is finite.

Proof. Using the notation of Section 1, we may assume that the field of constants is K. Let $P \in R_{\mathscr{F}}$. Then there is an $n > 0$ such that there is a place $P' \in \mathbb{P}(F_{n-1})$ lying above P that ramifies in the extension F_n/F_{n-1}. By Abhyankar's Lemma [21, Proposition III.8.9], $P' \cap K(x_{n-1})$ is ramified in the extension $K(x_{n-1}, x_n)/K(x_{n-1})$ and so $P' \cap K(x_{n-1}) = P_\mu(x_{n-1})$ for some $\mu \in R_0$. From the definition of the sets R_i, it follows that $P = P' \cap K(x_0) = P_\nu(x_0)$ for some $\nu \in R_{n-1}$. This shows that $R_{\mathscr{F}} \subseteq \{P_\mu(x_0) : \mu \in R\}$. Thus, since R is finite, so is the set $R_{\mathscr{F}}$. □

2.1. An effective version of Corollary 2.4

A priori, checking the conditions of Corollary 2.4 is computationally intensive. On the computer one has to work with a finite field instead of K—so one has to guess the right finite field to work with to check the conditions as stated in Corollary 2.4. In this subsection we present a finite version of this result. Theorem 2.7 below contains an obvious algorithm that indicates from the outset exactly which finite field we should consider. All the conditions of Theorem 2.7 are easily checked with KASH.

Let $f(X, Y) \in K[X, Y]$ be an irreducible polynomial of degree m in each of the variables X and Y. Define the function field $F := K(x, y)$ by $f(x, y) = 0$. We assume that F is a separable extension of $K(x)$ and $K(y)$. Let M and N be defined as above and define the polynomial

$$\Delta(X) := \prod_{\mu \in N \cap K} (X - \mu),$$

where we take the empty product to be 1.

Next define the following set

$$B_\infty := \{\nu \in \mathbb{P}^1 : \nu \leftarrow \infty\}.$$

Now viewing $f(X, Y)$ as a polynomial in X with coefficients in $K[Y]$ we define the polynomial $R(Y)$ as the resultant of the polynomials $f(X, Y)$ and $\Delta(X)$, i.e.,

$$R(Y) := \mathrm{Res}(f(X, Y), \Delta(X)).$$

Finally, let Z be the set of zeroes of $R(Y)$ in K. Observe that Z is a finite set, otherwise one can show that $f(X, Y)$ is not irreducible.

Theorem 2.7. *Define a sequence of function fields as follows*: *put* $F_0 := K(x_0)$, *and for each* $k \geqslant 0$, let x_{k+1} *be a solution to* $f(x_k, T) = 0$; *put* $F_k := K(x_0, x_1, \ldots, x_k)$.

Assume that $M \not\subseteq N$ *and the following*:

(a) *if* $\infty \notin N$ *assume that* $B_\infty \not\subseteq N$.
(b) *if* $Z \not\subseteq N$ *Then for each* $\mu \in Z \setminus N$ *assume that* $f(X, \mu)$ *has a zero that does not belong to* $N \cap K$.

Then for each k *there is a place in* F_k *which is totally ramified in the extension* F_{k+1}/F_k *with ramification index* m *so that* $[F_{k+1} : F_k] = m$. *In particular, this implies that* $[F_k : F_0] \to \infty$ *as* $k \to \infty$. *If, in addition, we also assume that* m *is relatively prime with the characteristic of* K, *then each extension* F_{k+1}/F_k *is also separable.*

Proof. We show that the conditions of Corollary 2.4 are satisfied, that is, we show that for each $\mu \in \mathbb{P}^1 \backslash N$ there exists a $v \in \mathbb{P}^1 \backslash N$ such that $v \leftarrow \mu$. Choose $\mu \in \mathbb{P}^1 \backslash N$. If $\mu = \infty$ then condition (a) guarantees the existence of v. Thus assume that $\mu \neq \infty$. If $\mu \notin Z$ then $R(\mu) \neq 0$ and the polynomials $f(X, \mu)$ and $\Delta(X)$ have no common non-constant factors (cf. [18, p. 41, Lemma 2.6]) so that any $v \in K$ such that $f(v, \mu) = 0$ does not belong to N as required. If $\mu \in Z$ then condition (b) guarantees the existence of v. This completes the proof. □

We remark that the conditions for Theorem 2.7 are equivalent to the conditions of Corollary 2.4.

Consider the following example: let $f(x, y) = x^2y^2 + xy + 4x^2 + 2x + 4 \in \mathbb{F}_5[x, y]$. Using the notation of Theorem 2.7, we have $M = \{0, 2\}$ and $N = \{0, \infty\}$ so that $\Delta(X) = X$ and $R(Y) = 4$ so that $Z = \emptyset$ and the conditions of Theorem 2.7 are trivially satisfied.

The following polynomials can also be shown to give rise to towers by verifying the conditions of Theorem 2.7: $x^2y^2 + 2xy + 4x^2 + x + 1$, $x^2y^2 + (x^2 + x)y + x^2 + 4x + 4 \in \mathbb{F}_5[x, y]$ and $x^2y^2 + 3xy + 2x^2 + 2x + 4$, $x^2y^2 + 3xy + 4x^2 + x + 4 \in \mathbb{F}_7[x, y]$.

3. Elimination techniques

In the above section we gave several sufficient conditions to guarantee that a polynomial gives rise to a tower. In this section we discuss four methods which proved very effective in eliminating potential candidates for towers. The first method is an application of a technique that Elkies used to recognize the modular towers in [17]. This method depends on the defining polynomials possessing certain non-trivial fractional linear transform symmetries. In Section 3.2 we present another simple method that depends on the polynomial remaining unchanged after interchanging the variables. In Section 3.3 we present a method that uses elimination theory of Groebner bases. Finally, in Section 3.4 we present a criterion for Galois polynomials to define asymptotically bad towers.

3.1. Elkies' technique

Let $\mathscr{F} = \bigcup_{k \geqslant 0} F_k$ be a tame tower recursively defined by $f(x, y) = 0$. Suppose there is a non-trivial fractional linear transformation ε (so $\varepsilon(x) = \frac{ax+b}{cx+d}$ for some $a, b, c, d \in K$), such that

$$f(\varepsilon(x), \varepsilon(y)) = 0 \text{ iff } f(x, y) = 0. \tag{4}$$

The fractional linear transformation gives rise to an automorphism σ_0 of F_0 with $\sigma_0(x_0) = \varepsilon(x_0)$. It follows from Eq. (4), that σ_0 can be extended to an automorphism σ_k of F_k with $\sigma_k(x_j) = \varepsilon(x_j)$ for $0 \leqslant j \leqslant k$. We denote the fixed field of F_k under $\langle \sigma_k \rangle$ with E_k. Then $\mathscr{E} := \bigcup_{k \geqslant 0} E_k$ is a Galois subtower of $\mathscr{F}$ with $[\mathscr{F} : \mathscr{E}] = \mathrm{o}(\varepsilon)$, where $\mathrm{o}(\varepsilon)$ is the order of ε when considered as an element of $GL(2, K)$. It is called the quotient subtower of $\mathscr{F}$ (under ε).

The tower $\mathscr{E}$ is recursively defined by

$$F(X, Y) = 0,$$

where $X = x + \varepsilon(x) + \varepsilon^2(x) + \cdots + \varepsilon^{o(\varepsilon)-1}(x)$, $Y = y + \varepsilon(y) + \varepsilon^2(y) + \cdots + \varepsilon^{o(\varepsilon)-1}(y)$, and F is obtained from f by eliminating x and y. Computationally this can be realized by using Gröbner Basis.

As an example, consider the polynomial

$$f(x, y) = xy^2 + (2x^2 + x + 1)y + 2x$$

over $\mathbb{F}_3$. Assuming that $f(x, y)$ gives rise to a tower $\mathscr{T}$, it is not hard to show that the ramification locus is $R = \{x_0^4 + x_0^3 + 2x_0^2 + 1, x_0^4 + 2x_0^3 + x_0 + 1, x_0^2 + 1\}$ and the places $S=\{x_0, 1/x_0\}$ split completely. It follows then from Theorem 1.1 that $\lambda(\mathscr{T}) \geqslant 1/2$. However, the tower is finite: observe that $f(x, y)=0$ if and only if $f(\varepsilon(x), \varepsilon(y))=0$ where $\varepsilon(x) := 2/x$. Next we form the quotient subtower by introducing the variables $X=x+\varepsilon(x)$, $Y=y+\varepsilon(y)$, and eliminate x,y from $f(x, y) = 0$ to obtain $F(X, Y) = 0$ where $F(X, Y) = X + 2Y + 2$ but it is obvious that $F(X, Y)$ does not give rise to a tower. Hence $\mathscr{T}$ is not a tower.

The above approach proved extremely useful to eliminate many possible candidates for towers: for example, the following polynomials which can be shown not to give rise to towers over the indicated finite fields:

$(x^2 + 1)y^2 + (x^2 + x)y + 1 + 2x$ over $\mathbb{F}_3$,
$(x^2 + 1)y^2 + (x^2 + 2x + 2)y + 2 + x$ over $\mathbb{F}_3$,
$x^2y^2 + (x^2 + 2x + 2)y + x^2 + 2x + 2$ over $\mathbb{F}_3$,
$xy^2 + (4x^2 + x + 4)y + x$ over $\mathbb{F}_5$,
$xy^2 + (4x^2 + x + 2)y + 3x$ over $\mathbb{F}_5$,
$xy^2 + (4x^2 + x + 1)y + 4x$ over $\mathbb{F}_5$
$xy^2 + (2x^2 + x + 4)y + 2x$ over $\mathbb{F}_5$,
$xy^2 + (2x^2 + x + 3)y + 4x$ over $\mathbb{F}_5$,
$x^2y^2 + (x^2 + x + 6)y + 6x^2 + 6x + 3$ over $\mathbb{F}_{11}$,
$(x^2 + 1)y^2 + (x^2 + x + 4)y + 4x^2 + 3x + 2$ over $\mathbb{F}_{11}$,
$(x^2 + 1)y^2 + (2x^2 + 4x + 1)y + 6x^2 + 10x + 9$ over $\mathbb{F}_{11}$.

That same technique applies, if there is a fractional linear transformation $\varepsilon \in GL(2, K)$ such that

$$f(\varepsilon(x), y) = \mu f(x, y) \text{ for some } \mu \in K^*.$$

Again, ε induces an automorphism $\sigma_0 \in Aut(F_0/\mathbb{F}_q)$, which in this case can be extended to an automorphism of F_k with $\sigma_k(x_j) = x_j$ for $1 \leqslant j \leqslant k$.

As an example, consider the tower $\mathscr{M}$ defined by

$$x_{i+1}^2 = \frac{x_i^2 + 1}{2x_i} \text{ for } i \geqslant 0, \tag{5}$$

which leads to an asymptotically optimal tower, cf. [13]. The right-hand side of Eq. (5) has the involution $\varepsilon : x_i \mapsto 1/x_i$. We form the quotient subtower by introducing $y_i = x_i + 1/x_i$. Then, from Eq. (5), we get $x_{i+1}^2 = \frac{1}{2}y_i$ and

$$y_{i+1}^2 = \frac{(y_i + 2)^2}{2y_i},$$

which defines the same degree two subtower $\mathscr{N}$ as

$$y_{i+1}^2 = \frac{(y_i + 1)^2}{4y_i} \tag{6}$$

given in [13]. The same involution as above applies now to Eq. (6), which leads to another (optimal) degree two subtower $\mathscr{L}$ defined by [4]:

$$z_{i+1}^2 = \frac{(z_i + 3)^2}{8(z_i + 1)}.$$

3.2. Symmetric polynomials do not define towers

Let $f(x, y) \in \mathbb{F}_q[x, y]$ be an absolutely irreducible polynomial. Next we show that if $f(x, y) = f(y, x)$ and the extension $\mathbb{F}_q(x, y)/\mathbb{F}_q(x)$ ($f(x, y) = 0$) is Galois, then $f(x, y)$ does not define a tower. This simple result eliminates many possibilities and thus helps to reduce the total running time. For example, if one considers only degree 2 polynomials, then immediately q^6 polynomials are eliminated out of a possible q^9 polynomials. As examples, consider the polynomials $xy^2 + (x^2 + 1)y + x + 1$, $xy^2 + (x^2 + x + 2)y + 2x$ and $(x^2 + 1)y^2 + 2xy + x^2 + 2$ over $\mathbb{F}_3$. Each of these polynomials remain unchanged after interchanging the variables and thus do not give rise to towers.

Lemma 3.1. *Let $f(x, y) \in \mathbb{F}_q[x, y]$ be an absolutely irreducible polynomial. Suppose that the extension $\mathbb{F}_q(x, y)/\mathbb{F}_q(x)$ ($f(x, y) = 0$) is Galois and that $f(x, y) = f(y, x)$. Then the polynomial $f(x, y)$ does not give rise to a tower.*

Proof. Define a sequence of function fields $F_0, F_1, \ldots$ as follows: $F_0 := \mathbb{F}_q(x_0)$ and for $n > 0$, $F_n := F_{n-1}(x_n)$ where x_n is a solution to $f(x_{n-1}, T) = 0$. First we show that $\mathbb{F}_q(x_0, x_1) = \mathbb{F}_q(x_1, x_2)$. Observe that since $f(x, y) = f(y, x)$, we have that $f(x_1, x_0) = f(x_1, x_2) = 0$. Thus x_0 and x_2 are conjugates over $\mathbb{F}_q(x_1)$. Since the extension $\mathbb{F}_q(x_0, x_1)/\mathbb{F}_q(x_1)$ is Galois, it follows that $x_2 \in \mathbb{F}_q(x_0, x_1)$. Thus $\mathbb{F}_q(x_1, x_2) \subseteq \mathbb{F}_q(x_0, x_1)$. Since both these function fields are of the same degree over $\mathbb{F}_q(x_1)$, they must be equal. Similarly, we have that $\mathbb{F}_q(x_i, x_{i+1}) = \mathbb{F}_q(x_{i+1}, x_{i+2})$ for all $i \geqslant 0$. But this implies that $x_0, x_1, x_2, \ldots$ all belong to $F_1 = \mathbb{F}_q(x_0, x_1)$ so that $F_i \subseteq F_1$ for all $i \geqslant 1$. Thus the sequence $F_0, F_1, \ldots$ is not a tower. □

3.3. Identifying bad towers using elimination theory

We illustrate this method by example without all the computational details. The reader may easily fill in the missing computation.

Assume that the polynomial

$$f(x, y) = x^2y^2 + (x^2 + x + 1)y + x^2 + x + 2 \tag{7}$$

gives rise to a tower $\mathscr{T}$ over $\mathbb{F}_3$. Let w_1 be a primitive element of $\mathbb{F}_{27}$ satisfying $w_1^3 + 2w_1 + 1 = 0$ and let w be a primitive element of $\mathbb{F}_{3^5}$ satisfying $w^5 + 2w + 1 = 0$. It can be shown that the ramification set (using the notation of Theorem 1.1) is given by the zeroes of the polynomials in the set $R_{\mathscr{T}.\mathbb{F}_{27}} = \{1/x_0,\ x_0 - w_1^j,\ j = 1,\ 2,\ 3,\ 5,\ 6,\ 7,\ 9,\ 11,\ 14,\ 15,\ 16\ 17,\ 18,\ 19,\ 21,\ 22,\ 23,\ 25\}$ and the splitting set (again using the notation of Theorem 1.1) is given by $S_{\mathscr{T}.\mathbb{F}_{3^5}} = \{x_0 - w^j \mid j = 198,\ 110,\ 196,\ 88,\ 104,\ 136,\ 215,\ 22, 70,\ 166,\ 161,\ 166,\ 66,\ 146,\ 233, 136,\ 210,\ 239,\ 22,\ 66, 42,\ 241,\ 198,\ 126,\ 241,\ 14,\ 161,\ 215,\ 233,\ 239\}$.

It follows from Theorem 1.1 that $\lambda(\mathscr{T}) \geqslant \frac{30}{-1+19/2} = 60/17$. It can be shown, using techniques from Groebner bases that the curve defined by f is not closed under any fractional linear transforms over $\overline{\mathbb{F}}_3$. Thus Elkies' technique is not applicable.

Define $F_0 := \mathbb{F}_{3^5}(x_0)$ and, for $n > 0$, $F_n := F_{n-1}(x_n)$ where x_n is a solution of the equation $f(x_{n-1}, T) = 0$. Of course, we work in a fixed algebraic closure of F_1. However, using elimination theory, by successively eliminating the variables $x_1, x_2, \ldots$, it can be shown that the functions $x_1, x_2, \ldots$ all belong to the (finite) set of zeroes of the polynomials $P_i(T)$ below where $u := x_0$. This contradicts the assumption that $f(x, y)$ defines a tower.

$$\begin{aligned}
P_0(T) &= f(u, T),\\
P_1(T) &= T + 2u,\\
P_2(T) &= (u^2 + u + 1)T^2 + (u + 1)T + u + 2,\\
P_3(T) &= u^2T^2 + (2u + 2)T + 2u,\\
P_4(T) &= (u^2 + u + 1)T^2 + u^2T + u^2 + 1,\\
P_5(T) &= (u^4 + 2u^2 + 1)T^4 + (2u^4 + 2u^3 + 2u^2 + 2u + 2)T^3\\
&\quad + (2u^4 + 2u^3 + 2u^2 + 2)T^2 + (u^4 + u^3 + 2u + 2)\\
&\quad T + u^4 + u^3 + 2u^2 + u + 1,\\
P_6(T) &= (u^4 + u^3 + u + 1)T^4 + (u^4 + u^3 + u + 1)T^3 + (2u^2 + u)T^2\\
&\quad + (u^4 + u^3 + u^2 + 1)T + u^4 + u^3 + u + 2,\\
P_7(T) &= (u^4 + 2u^2 + 1)T^4 + (u^3 + 2u^2 + u)T^3 + (2u^4 + 2u^3 + 2u^2 + 2)T^2\\
&\quad + (u^3 + u + 2)T + u^4 + 2u^2 + 2u + 2,\\
P_8(T) &= (u^4 + 2u^3 + 2u^2 + u + 1)T^4 + (2u^3 + 2u^2 + u + 1)T^3\\
&\quad + (2u^4 + 2u^3 + 2u^2 + 2)T^2 + (2u^3 + 2u + 1)\\
&\quad T + u^4 + 2u^3 + 2u^2 + 2u + 1,\\
P_9(T) &= (u^4 + 2u^3 + 2u^2 + u + 1)T^4 + (2u^4 + 2u^3 + 2u^2 + u + 1)T^3\\
&\quad + (2u^4 + 2u^3 + 2u^2 + 2)T^2 + (u^4 + u^3)T + u^4 + u^3 + 2u^2.
\end{aligned}$$

Similarly, it can be shown that the polynomials $xy^2 + (2x^2 + x + 4)y + 4x + 1 \in \mathbb{F}_7[x, y]$, and $xy^2 + (2x^2 + x + 9)y + 7x^2 + 6x + 10 \in \mathbb{F}_{11}[x, y]$ do not give rise to towers. Without this crucial fact, both these polynomials would seem to give rise to asymptotically good towers

over their respective prime fields. Unfortunately, after extensive computational search for recursively defined asymptotically good towers over prime fields, we still have not found any. The search was done using degree two polynomials and for the primes 3, 5, 7, 11, 13.

3.4. Asymptotically bad towers defined by a family of Galois polynomials

Let $f(x, y) \in \mathbb{F}_q[x, y]$ be absolutely irreducible with the same degree m in both variables. We assume that m is relatively prime with q. Define the function field $F := \mathbb{F}_q(x, y)$ by $f(x, y) = 0$. Let M be the set of places of $\mathbb{F}_q(x)$ which are totally ramified in the extension $F/\mathbb{F}_q(x)$ and let N be the set of places of $\mathbb{F}_q(y)$ that ramify in the extension $F/\mathbb{F}_q(y)$. Assume $M \neq \emptyset$ and that both extensions $F/\mathbb{F}_q(x)$ and $F/\mathbb{F}_q(y)$ are Galois. In this section we prove the following result, under the above hypothesis.

Lemma 3.2. *Assume that there is a place Q in M with $gcd(\deg Q, m) = 1$ and which has the property that for each P in N, $\deg Q$ does not divide $\deg P$ ... (†).*

Define sequence $\mathscr{F} := (F_i)$ by $F_0 = \mathbb{F}_q(x_0)$ and for $i > 0$, $F_i := F_{i-1}(x_i)$ where x_i is any solution to

$$f(x_{i-1}, Y) = 0.$$

Then we have the following:

(i) *The sequence $\mathscr{F} := (F_0, F_1, F_2, \ldots)$ is a tower over $\mathbb{F}_q$ such that for each k, there is at least one place in F_k that is totally ramified in the extension F_{k+1}/F_k.*
(ii) *The tower $\mathscr{F}$ is asymptotically bad.*

Proof. (i) Let $n \geqslant 1$ and choose a place Q in $\mathbb{F}_q(x_n)$ with property (†), that is Q is totally ramified in the extension $\mathbb{F}_q(x_n, x_{n+1})/\mathbb{F}_q(x_n)$ and the degree of Q is relatively prime to m and does not divide the degree of any place of $\mathbb{F}_q(x_n)$ which ramifies in the extension $\mathbb{F}_q(x_{n-1}, x_n)/\mathbb{F}_q(x_n)$. Let Q' be a place of F_n that lies over the place Q. Consider the respective restrictions $Q_0, Q_1, \ldots, Q_n(=Q)$ of Q' to $\mathbb{F}_q(x_0), \mathbb{F}_q(x_1), \ldots, \mathbb{F}_q(x_n)$.

We claim that the degree of each place Q_i is divisible by the degree of Q: Let Q'_n denote the restriction of Q' to $\mathbb{F}_q(x_{n-1}, x_n)$. Observe that

$$\deg Q'_n = f(Q'_n|Q_{n-1}) \deg Q_{n-1} = f(Q'_n|Q) \deg Q, \tag{8}$$

where $f(Q'_n|Q_{n-1})$ and $f(Q'_n|Q)$ are the relative degrees of the place Q_n in the extensions $\mathbb{F}_q(x_{n-1}, x_n)/\mathbb{F}_q(x_n)$ and $\mathbb{F}_q(x_{n-1}, x_n)/\mathbb{F}_q(x_{n-1})$. Since these extensions are Galois, it follows that the relative degrees $f(Q'_n|Q_{n-1})$ and $f(Q'_n|Q)$ both divide m. Now from Eq. (8) and the fact that $\deg Q$ is relatively prime with m, it follows that $\deg Q$ divides $\deg Q_{n-1}$. Now let Q'_{n-1} denote the restriction of Q' to $\mathbb{F}_q(x_{n-2}, x_{n-1})$. Observe that

$$\deg Q'_{n-1} = f(Q'_{n-1}|Q_{n-2}) \deg Q_{n-2} = f(Q'_{n-1}|Q_{n-1}) \deg Q_{n-1}. \tag{9}$$

Since $\deg Q$ divides the right-most side of Eq. (9) it follows that $\deg Q$ divides

$$f(Q'_{n-1}|Q_{n-2}) \deg Q_{n-2}$$

and hence also deg Q_{n-2}, using the facts that m and deg Q are relatively prime and that the extension $\mathbb{F}_q(x_{n-2}, x_{n-1})/\mathbb{F}_q(x_{n-2})$ is Galois so that $f(Q'_{n-1}|Q_{n-2})$ divides m. Continuing in this way, by an inductive argument, we see that deg Q divides deg Q_i for $i=0, 1, \ldots, n-1$ as claimed.

Now, by assumption (†), it follows that none of the places Q_i can ramify in the extension $\mathbb{F}_q(x_{i-1}, x_i)/\mathbb{F}_q(x_i)$. By Abhyankar's lemma [21, Proposition III.8.9], it follows that $e(Q'|Q) = 1$ so that, again by Abhyankar's lemma, we have that Q' is totally ramified in the extension F_{n+1}/F_n. That $g(F_n) \to \infty$ as $n \to \infty$ follows from the proof of (ii).

(ii) It is easily shown, by repeated application of the different formula for towers that

$$\mu(\mathscr{F}) := \lim_{n\to\infty} \frac{g(F_n)}{[F_n : F_0]} = g(F_0) - 1 + \frac{1}{2}\sum_{i=1}^{\infty} \frac{\deg \operatorname{Diff}(F_i/F_{i-1})}{[F_i : F_0]}.$$

It is shown in [13] that $\lambda(\mathscr{F}) = \nu(\mathscr{F})/\mu(\mathscr{F})$ where $\nu(\mathscr{F}) = \lim_{n\to\infty} N(F_n)/[F_n : F_0]$ $(< \infty)$. We will show that $\mu(\mathscr{F}) = \infty$. Let $n > 1$ be given. Let Q denote the place of $\mathbb{F}_q(x_n)$ with the property in the statement of the theorem for the extension $\mathbb{F}_q(x_n, x_{n+1})/\mathbb{F}_q(x_n)$. Now let Q' be any place in F_n which lies over Q. From the proof of (i), Q' is unramified in the extension $F_n/\mathbb{F}_q(x_n)$. It is clear that the quantity $\mu(\mathscr{F})$ remains invariant under change of constant field. Thus, without loss of generality, we may increase the constant field so that we may assume that Q has degree one and splits completely in the extension $F_n/\mathbb{F}_q(x_n)$. Each of the m^n places of F_n which lie above Q are totally ramified in F_{n+1}/F_n. It follows that

$$\frac{\deg \operatorname{Diff}(F_{n+1}/F_n)}{[F_{n+1} : F_0]} \geqslant \frac{m^n(m-1)}{m^{n+1}} = \frac{m-1}{m} \not\to 0$$

as $n \to \infty$. Thus $\mu(\mathscr{F}) = \infty$. □

As an example consider the following rational function:

$$f(x, y) := y^3 - 1 + \left(\frac{x-1}{x+1}\right)^3 = y^3 - 2\frac{3x^2+1}{(x+1)^3} \tag{10}$$

over $\mathbb{F}_p$ where p is a prime congruent to 1 or 7 modulo 12. Modulo any such prime $-\frac{1}{3}$ is not a square so that $3x^2 + 1$ is irreducible. Also, since 3 divides $p - 1$, $\mathbb{F}_p$ contains cube roots of unity. Thus, using the notation of Lemma 3.2, we have $N = \{y - \alpha | \alpha \in \mathbb{F}_p, \alpha^3 = 1\}$ and $M = \{1/x, x^2 + 1/2\}$. Since the conditions of Lemma 3.2 are satisfied with $Q = 3x^2 + 1$, it follows that $f(x, y)$ defined in (10) gives rise to an asymptotically bad tower.

4. The computer implementation

The KASH implementation is essentially the same as outlined in [17] but differs in the following important ways. Let $\mathscr{T}$ be a tower defined by an equation $f(x, y) = 0$. Since the polynomials $f(x_k, T)$ are irreducible for each $k \geqslant 0$, we obtain for the degrees of the field extensions (using the notation of Corollary 2.2)

$$[F_{k+1} : F_k] = [F_{1,k+1} : F_{1,k}].$$

Thus,

$$[F_{k+1} : F_{1,k+1}] = [F_k : F_{1,k}],$$

and the equation $f(y_{k+1}, y_k) = 0$ defines a sequence $(E_k)_{k \geqslant 0}$, $E_k := \mathbb{F}_q(y_0, y_1, ..., y_k)$, of algebraic function fields, such that $f(T, y_k)$ is irreducible over E_k for all $k \geqslant 0$. In this way, we obtain a tower $\mathscr{S} := \bigcup_{k \geqslant 0} E_k$, the *dual tower* with respect to $\mathscr{T}$ [1]. The towers $\mathscr{T}$ and $\mathscr{S}$ satisfy $\lambda(\mathscr{T}) = \lambda(\mathscr{S})$. Thus, for computational purposes, we need only consider one of the polynomials $f(x, y)$ or $f(y, x)$. Moreover, $\mathscr{T}'$ it a tower defined by $f(\varepsilon(x), \varepsilon(y))$ where $\varepsilon(x)$ is a fractional linear transform with coefficients in $\mathbb{F}_p$, then $\lambda(\mathscr{T}) = \lambda(\mathscr{T}')$. Define the following relation $\sim$ on the set $\mathscr{P}$ of polynomials of degree m (in both variables) in $\mathbb{F}_p[x, y]$: $f \sim g$ if and only if $f(x, y) = \lambda g(y, x)$, $f(x, y) = \lambda g(x, y)$ or $f(x, y) = (cx + d)^m (cy + d)^m g(\varepsilon(x), \varepsilon(y))$ for some fractional linear transformation $\varepsilon(x) = (ax + b)/(cx+d)$ with coefficients in $\mathbb{F}_p$. It is clear that $\sim$ is an equivalence relation. Occasionally, we need to consider linear fractional transforms over $\overline{\mathbb{F}}_p$. In this case we say that f and g are $\sim$ related over $\overline{\mathbb{F}}_p$ if the aboveconditions are satisfied. Consider a lexicographic ordering on the coefficients of polynomials in $\mathbb{F}_p[x, y]$ of degree m (in both variables). From each equivalence class, we choose the smallest element—and do all computation with that polynomial. This considerably reduced the number of polynomials that we did all the computations with and allowed us to more efficiently analyze the results without having the overabundance of data.

In [17], in order to determine whether a polynomial defines a tower, we checked if the conditions of Theorem 2.3 are satisfied (although the proof of this general lemma was not known at the time of writing the paper [17]—these conditions are implied in the proofs of the paper [10]). This had the major drawback that it was not possible to determine the smallest possible finite field to work with to check this condition. The new feature in the program is a check for the conditions of Theorem 2.7. While more restrictive than Theorem 2.3, it has the advantage that the conditions can be checked in a finite number of steps.

The techniques of Section 3 were incorporated in the program. In order to implement Elkies' technique, we use the Groebner basis features of the computer algebra system Maple.

5. Examples

The aim of this section is to present a clear picture of the towers found and how they compare with each other. In order to do this efficiently, we omit many details in the computations. However, we refer the reader to [17] where the computations are similar and done in detail. All those polynomials listed below without a reference are new in the sense that they are not $\sim$-related (over the algebraic closure of the respective finite field) to any of the currently known polynomials that define optimal towers. Note that we make repeated use of theorems in Section 2 without indication. We will occasionally use some notation and terminology from [13]. In addition, we will also use the following terminology: given two towers $\mathscr{F} = (F_1, F_2, F_3, \ldots)$ and $\mathscr{E} = (E_1, E_2, E_3, \ldots)$ over $\mathbb{F}_q$, the tower $\mathscr{E}$ is said to be a *subtower* [10] of $\mathscr{F}$ or that $\mathscr{F}$ is a *supertower* of $\mathscr{E}$ if there exists an embedding

$$\iota : \bigcup_{i \geqslant 1} E_i \to \bigcup_{i \geqslant 1} F_i$$

over $\mathbb{F}_q$. We denote this by: $\mathscr{E} \prec \mathscr{F}$.

$q = 9$:

The polynomial

$$f(x, y) = (x^2 + 1)y^2 + 2xy + 2x^2 + 1 \tag{11}$$

gives rise to a tower $\mathscr{T}$ over $\mathbb{F}_9$ with ramification set given by $R_{\mathscr{T}} = \{\text{zeroes of} x_0^4 + x_0^2 + 2, \text{ zeroes of } x_0^4 + 2x_0^2 + 2\}$.

It can be shown that the zeroes of $x_0^4 + x_0^2 + 2$ are totally ramified in the tower. Let w be a (primitive) element of $\mathbb{F}_9$ which satisfies $w^2 + 2w + 2 = 0$. Then $S = \{1/x, x, x - w^j \text{ for } j = 2, 4, 6, 8\}$ is a set of six places of F_1 which split completely in the tower. We conclude from Theorem 2.1 that $\lambda(\mathscr{T}) \geqslant 2 \cdot 6/(-2 + 8) = 2$. Since $A(9) = 2$ it follows that the tower $\mathscr{T}^{(9)}$ is optimal over $\mathbb{F}_9$ with $\lambda(\mathscr{T}) = 2$.

Now, it is shown in [17] that the tower $\mathscr{T}_1$ over $\mathbb{F}_9$ given by the equation $g(x, y) = 2xy^2 + (x^2 + x + 1)y + x^2 + x + 2$ is optimal. Moreover, it is shown in [17] that $\mathscr{T}_1$ is "new" in the sense that all previously known towers over $\mathbb{F}_9$ are not subtowers of $\mathscr{T}_1$. In the same way as in [17], it can be shown that none of the previously known towers (except possibly $\mathscr{T}_1$) is a subtower of $\mathscr{T}$. Comparison of $\mathscr{T}$ and $\mathscr{T}_1$ though does not appear to be easy. However, it can be shown, for example using computer algebra software with Groebner basis capabilities, that f is not $\sim$-related *over* $\bar{\mathbb{F}}_3$.

Consider the following polynomials in $\mathbb{F}_3[x, y]$. It can be shown that for each i, $1 \leqslant i \leqslant 7$, $f_i(x, y)$ gives rise to an asymptotically good tower, which we denote by $\mathscr{T}_i$; the corresponding lower bound for $\lambda(\mathscr{T}_i)$ (in all cases, except for $i = 11, 10$ obtained by using Theorem 1.1) is indicated in the last column.

Ref:		$f_i(x, y)$:	$\lambda(\mathscr{T}_i) \geqslant$
[14]	$\mathscr{T}_1$:	$f_1(x, y) = y^2 + x^2 + x$	2
	$\mathscr{T}_2$:	$f_2(x, y) = y^2 + xy + 2x^2 + 1$	2/3
	$\mathscr{T}_3$:	$f_3(x, y) = y^2 + xy + 2x^2 + 2$	2/3
[4]	$\mathscr{T}_4$:	$f_4(x, y) = y^2 + x^2y + 1$	2
[13]	$\mathscr{T}_5$:	$f_5(x, y) = y^2 + (x^2 + 1)y + 1$	2
	$\mathscr{T}_6$:	$f_6(x, y) = y^2 + (x^2 + 1)y + 2x^2$	2/3
[17]	$\mathscr{T}_7$:	$f_7(x, y) = xy^2 + (2x^2 + x + 2)y + x^2 + 2x + 2$	2
	$\mathscr{T}_8$:	$f_8(x, y) = x^2y^2 + (2x + 1)y + x^2 + 2x + 1$	2/3
	$\mathscr{T}_9$:	$f_9(x, y) = (x^2 + 1)y^2 + 2xy + 2x^2 + 1$	2
[17]	$\mathscr{T}_{10}$:	$f_{10}(x, y) = xy^2 + 2x^2y + x^2 + 2x + 1$	2
[17]	$\mathscr{T}_{11}$:	$f_{11}(x, y) = y^2 + (x^2 + 1)y + x^2 + x + 1$	2

The towers $\mathscr{T}_1$, $\mathscr{T}_4$ and $\mathscr{T}_5$ are respectively special cases of the towers $\mathscr{L}$, $\mathscr{M}$ and $\mathscr{N}$ in [13]. It is shown in [23] (Beispiel 3.2.6) that the lower bounds given for $\lambda(\mathscr{T}_i)$, $i = 2, 3, 6, 8$ are exact so that these towers are not optimal. Using Elkies' technique, it can be shown that

- $\mathscr{T}_1 \prec \mathscr{T}_2, \mathscr{T}_3$,
- $\mathscr{T}_5 \prec \mathscr{T}_6, \mathscr{T}_8$,
- $\mathscr{T}_{11} \prec \mathscr{T}_{10} \prec \mathscr{T}_7, \mathscr{T}_9$.

Moreover, in [17], it is shown that $\mathscr{T}_1 \prec \mathscr{T}_5 \prec \mathscr{T}_4$. Since $\mathscr{T}_{10}$ and $\mathscr{T}_{11}$ are subtowers of optimal towers, it follows that they are optimal. The polynomial f_9 is not $\sim$ related to any other known degree two polynomial which defines an optimal tower.

$q = 25$:

Consider the following polynomials in $\mathbb{F}_5[x, y]$. It can be shown that for each i, $1 \leqslant i \leqslant 19$, $f_i(x, y)$ gives rise to an asymptotically good tower, which we denote by $\mathscr{T}_i$; the corresponding lower bound for $\lambda(\mathscr{T}_i)$ (in all cases, except for $i = 2, 19, 28$ obtained using Theorem 1.1) is indicated in the last column.

Ref:		$f_i(x, y)$:	$\lambda(\mathscr{T}_i) \geqslant$
[13]	$\mathscr{T}_1$:	$f_1(x, y) = y^2 + x^2y + 4$	4
[7]	$\mathscr{T}_2$:	$f_2(x, y) = y^2 + x^2y + x$	4
[7]	$\mathscr{T}_3$:	$f_3(x, y) = y^2 + x^2y + 3x$	4
[13]	$\mathscr{T}_4$:	$f_4(x, y) = y^2 + (x^2 + 2)y + 1$	4
[8]	$\mathscr{T}_5$:	$f_5(x, y) = y^2 + (x^2 + 2)y + x^2$	4
[4]	$\mathscr{T}_6$:	$f_6(x, y) = y^2 + (x^2 + 2)y + 2x^2 + 1$	4
[7]	$\mathscr{T}_7$:	$f_7(x, y) = y^2 + (x^2 + 2)y + 3x^2 + 4x + 4$	4
	$\mathscr{T}_8$:	$f_8(x, y) = y^2 + (x^2 + 3)y + 4x^2$	1
[17]	$\mathscr{T}_9$:	$f_9(x, y) = xy^2 + (4x^2 + x + 1)y + x^2 + 2x + 3$	4
	$\mathscr{T}_{10}$:	$f_{10}(x, y) = xy^2 + (4x^2 + x + 2)y + 3x^2 + x + 4$	4
	$\mathscr{T}_{11}$:	$f_{11}(x, y) = x^2y^2 + (x^2 + 3)y + 4$	4
	$\mathscr{T}_{12}$:	$f_{12}(x, y) = x^2y^2 + (x^2 + 3x + 3)y + 4$	3
	$\mathscr{T}_{13}$:	$f_{13}(x, y) = x^2y^2 + (x^2 + 4x + 2)y + 4$	4
	$\mathscr{T}_{14}$:	$f_{14}(x, y) = x^2y^2 + (x^2 + 4x + 2)y + 4x^2 + 2$	3
	$\mathscr{T}_{15}$:	$f_{15}(x, y) = x^2y^2 + (x^2 + 4x + 4)y + 4x^2 + 3x + 2$	3
	$\mathscr{T}_{16}$:	$f_{16}(x, y) = (x^2 + 1)y^2 + (x + 1)y + 2x^2 + 4x + 1$	1
	$\mathscr{T}_{17}$:	$f_{17}(x, y) = (x^2 + 1)y^2 + (x^2 + 3x + 3)y + x^2 + 4$	4
	$\mathscr{T}_{18}$:	$f_{18}(x, y) = (x^2 + 1)y^2 + (2x^2 + 2x + 4)y + 3x^2 + 3$	4
[8]	$\mathscr{T}_{19}$:	$f_{19}(x, y) = y^2 + x^2y + 3x^2 + 2$	4
	$\mathscr{T}_{20}$:	$f_{20}(x, y) = y^2 + 2xy + 4x^2 + 1$	1
	$\mathscr{T}_{21}$:	$f_{21}(x, y) = y^2 + 2xy + 4x^2 + 2$	1
[7]	$\mathscr{T}_{22}$:	$f_{22}(x, y) = y^2 + 4xy + x^2 + x$	2
[7]	$\mathscr{T}_{23}$:	$f_{23}(x, y) = y^2 + x^2y + 2x^2 + 2x$	4
	$\mathscr{T}_{24}$:	$f_{24}(x, y) = xy^2 + (4x^2 + x + 2)y + 2x^2 + 2x + 3$	4
	$\mathscr{T}_{25}$:	$f_{25}(x, y) = x^2y^2 + xy + 4x^2 + 1$	4
	$\mathscr{T}_{26}$:	$f_{26}(x, y) = x^2y^2 + 2xy + 2x^2 + 4$	4
[7]	$\mathscr{T}_{27}$:	$f_{27}(x, y) = y^2 + (x^2 + 1)y + x^2 + 4x + 4$	4

The towers $\mathscr{T}_1$, $\mathscr{T}_4$ and $\mathscr{T}_6$ are respectively special cases of the towers $\mathscr{M}$, $\mathscr{N}$ and $\mathscr{L}$ in [13]. All these towers except possibly $\mathscr{T}_i$, $i = 8, 16, 12, 14, 15, 20, 21$ are optimal. (Are the given lower bounds for these also exact?) The tower $\mathscr{T}_{22}$ is actually optimal, and the indicated lower bound is due to the non-determinism of the algorithm.

Using Elkies' technique and results from [13], it can be shown that each of the towers above is a super tower of one of $\mathscr{T}_i$, $i = 2,\ 6,\ 22,\ 27,\ 19$. More specifically we have

- $\mathscr{T}_2 \prec \mathscr{T}_i$ for $i = 7, 12, 14, 15$; and $\mathscr{T}_7 \prec \mathscr{T}_i$ for $i = 3, 13$
- $\mathscr{T}_6 \prec \mathscr{T}_i$, $i = 8,\ 16$
- $\mathscr{T}_{19} \prec \mathscr{T}_i$ for $i = 5, 10, 11, 18$; and $\mathscr{T}_{10} \prec \mathscr{T}_i$ for $i = 9, 17$.
- $\mathscr{T}_{27} \prec \mathscr{T}_i$ for $i = 23,\ 24,\ 25,\ 26$,
- $\mathscr{T}_{22} \prec \mathscr{T}_{21}, \mathscr{T}_{20}$.

Moreover, in [13] is shown that $\mathscr{T}_6 \prec \mathscr{T}_4 \prec \mathscr{T}_1$.

The embeddings $\mathscr{T}_{19} \prec \mathscr{T}_{10} \prec \mathscr{T}_9$ were shown by Elkies in [17]. The fact that $\mathscr{T}_i$, $i = 2,\ 19,\ 27$ are optimal now follows because they are subtowers of optimal towers.

Now $\gamma(\mathscr{T}_i)$ in each case is easily computed and from this it follows that $\gamma(\mathscr{T}_i)$ is some integer power of 2 for $i \neq 2,\ 19,\ 8,\ 16$.

Proposition 5.1. *None of the towers $\mathscr{T}_2$, $\mathscr{T}_{19}$, $\mathscr{T}_{27}$ is isomorphic to any of the towers $\mathscr{T}_i$, $i \neq 2,\ 8,\ 16,\ 19,\ 27$.*

Proof. We show that $\mathscr{T}_2$ is not isomorphic to any of $\mathscr{T}_i$ for $i \neq 2,\ 8,\ 16,\ 19$; and we do this in detail for $i = 1$ as the proof is similar in the other case. The proof for $\mathscr{T}_{19}$, $\mathscr{T}_{27}$ is similar.

Suppose that $(F_0, F_1, F_2, \ldots)$ and $(E_0, E_1, E_2, \ldots)$ represents $\mathscr{T}_2$ and $\mathscr{T}_1$, respectively. Suppose that $\iota : \mathscr{T}_1 \cong \mathscr{T}_2$ is an isomorphism. We denote the image of E_i under ι again by E_i so that $\bigcup_{i=0}^{\infty} E_i = \bigcup_{i=0}^{\infty} F_i$. Now choose j such that F_j contains E_0; and i such that E_i contains F_j. Then $[F_j : E_0]$ divides $[E_i : E_0] = 2^i$. Now, from Lemma 2.6 in [13] we have

$$[F_j : E_0] \cdot \gamma_{E_0}(\mathscr{T}_1) = [F_j : F_0] \cdot \gamma_{F_0}(\mathscr{T}_2). \tag{12}$$

Now $\gamma_{E_0}(\mathscr{T}_1) = 2$ and $\gamma_{F_0}(\mathscr{T}_2) = 3/2$ (note that $\gamma_{\mathbb{F}_{25}(x_0)}(\mathscr{T}_\ell) = 3/2$, $\ell = 19,\ 27$ as well). From (12) it now follows that $[F_j : E_0] = 3 \cdot 2^{j-2}$, a contradiction. □

While it is unknown if any pair of $\mathscr{T}_2$, $\mathscr{T}_{19}$, $\mathscr{T}_{27}$ are isomorphic, it can be shown that no two of f_2, f_{19}, f_{27} are $\sim$-related *over* $\overline{\mathbb{F}}_5$.

$q = 49$:

Ref:		$f_i(x, y)$:	$\lambda(\mathscr{T}_i) \geqslant$
[13]	$\mathscr{T}_1$:	$f_1(x, y) = y^2 + x^2 y + 4$	6
[7]	$\mathscr{T}_2$:	$f_2(x, y) = y^2 + x^2 y + 5x$	6
[8]	$\mathscr{T}_3$:	$f_3(x, y) = y^2 + x^2 y + 5x^2 + 5$	4
	$\mathscr{T}_4$:	$f_4(x, y) = y^2 + x^2 y + 6x^2 + 3x$	6
[13]	$\mathscr{T}_5$:	$f_5(x, y) = y^2 + (x^2 + 1)y + 6x^2 + 2$	6
[8]	$\mathscr{T}_6$:	$f_6(x, y) = y^2 + (x^2 + 4)y + x^2$	6

Ref:		$f_i(x, y)$:	$\lambda(\mathscr{T}_i) \geqslant$
[13]	$\mathscr{T}_7$:	$f_7(x, y) = y^2 + (x^2 + 6)y + 2$	6
	$\mathscr{T}_8$:	$f_8(x, y) = y^2 + (x^2 + 6)y + x^2$	6
[7]	$\mathscr{T}_9$:	$f_9(x, y) = y^2 + (x^2 + 6)y + 4x^2 + 6x + 4$	6
	$\mathscr{T}_{10}$:	$f_{10}(x, y) = xy^2 + (6x^2 + 1)y + x^2 + 5x + 2$	6
	$\mathscr{T}_{11}$:	$f_{11}(x, y) = xy^2 + (6x^2 + x + 2)y + 4x^2 + 6x + 6$	6
	$\mathscr{T}_{12}$:	$f_{12}(x, y) = xy^2 + (6x^2 + x + 5)y + x^2 + 4$	6
	$\mathscr{T}_{13}$:	$f_{13}(x, y) = x^2y^2 + xy + 2x^2 + 1$	6
	$\mathscr{T}_{14}$:	$f_{14}(x, y) = x^2y^2 + xy + 3x^2 + 4$	6
	$\mathscr{T}_{15}$:	$f_{15}(x, y) = x^2y^2 + xy + 4x^2 + 4$	6
	$\mathscr{T}_{16}$:	$f_{16}(x, y) = x^2y^2 + xy + 5x^2 + 1$	6
	$\mathscr{T}_{17}$:	$f_{17}(x, y) = x^2y^2 + 3xy + 6x^2 + 2$	6
	$\mathscr{T}_{18}$:	$f_{18}(x, y) = x^2y^2 + (x^2 + 2)y + 4$	6
	$\mathscr{T}_{19}$:	$f_{19}(x, y) = x^2y^2 + (x^2 + 6)y + 1$	6
	$\mathscr{T}_{20}$:	$f_{20}(x, y) = x^2y^2 + (x^2 + 3x + 6)y + x^2 + 2x + 1$	6
[17]	$\mathscr{T}_{21}$:	$f_{21}(x, y) = (x^2 + 1)y^2 + xy + 6x^2 + 4$	6
	$\mathscr{T}_{22}$:	$f_{22}(x, y) = (x^2 + 1)y^2 + 6xy + 6x^2 + 4$	6
	$\mathscr{T}_{23}$:	$f_{23}(x, y) = (x^2 + 1)y^2 + (x^2 + x + 6)y + 3x^2 + 6x + 5$	6
	$\mathscr{T}_{24}$:	$f_{24}(x, y) = (x^2 + 1)y^2 + (x^2 + 2x + 2)y + 5x^2 + 5$	6
	$\mathscr{T}_{25}$:	$f_{25}(x, y) = (x^2 + 1)y^2 + (2x^2 + 6x + 1)y + 6x^2 + 1$	6
	$\mathscr{T}_{26}$:	$f_{26}(x, y) = (x^2 + 1)y^2 + (3x^2 + 2x + 6)y + 5x^2 + 5$	6
	$\mathscr{T}_{27}$:	$f_{27}(x, y) = y^2 + (x^2 + 4)y + 3x^2 + 4x + 5$	6
[8]	$\mathscr{T}_{28}$:	$f_{28}(x, y) = y^2 + x^2y + 5x^2 + 5$	6
[7]	$\mathscr{T}_{29}$:	$f_{29}(x, y) = y^2 + (x^2 + 4)y + 6x^2 + x + 1$	6
	$\mathscr{T}_{30}$:	$f_{30}(x, y) = xy^2 + (6x^2 + x + 4)y + 2x^2 + 4x + 3$	6
[7]	$\mathscr{T}_{31}$:	$f_{31}(x, y) = y^2 + x^2y + 2x$	6
[17]	$\mathscr{T}_{32}$:	$f_{32}(x, y) = y^2 + (x^2 + x + 6)y + 2x^2 + 5x + 6$	6
[7]	$\mathscr{T}_{33}$:	$f_{33}(x, y) = y^2 + (x^2 + 6)y + 4x^2 + 2x + 2$	6
	$\mathscr{T}_{34}$:	$f_{34}(x, y) = y^2 + (x^2 + 4)y + 3x^2 + 4x + 1$	6

The tower $\mathscr{T}_4$ is isomorphic to the modular tower defined by $y^2 - (x^2 - 4x + 1)y - x^2$ (this tower is modular and corresponds to $\Gamma_1(8) \cap \Gamma_0(2^k)$, [6]). The towers $\mathscr{T}_1$, $\mathscr{T}_5$ and $\mathscr{T}_7$ are respectively special cases of the towers $\mathscr{M}$, $\mathscr{L}$ and $\mathscr{N}$ in [13].

Using Elkies' technique and results from [13], it can be shown that each of the towers above is a super tower of one of $\mathscr{T}_i$, $i = 3, 5, 27, 28, 31, 33$. More specifically we have

- $\mathscr{T}_3 \prec \mathscr{T}_{18}$.
- $\mathscr{T}_5 \prec \mathscr{T}_7 \prec \mathscr{T}_i$ for $i = 1, 4, 10, 14, 15$ and $\mathscr{T}_1 \prec \mathscr{T}_j$ for $j = 8, 11, 19, 26$.
- $\mathscr{T}_{27} \prec \mathscr{T}_2$.
- $\mathscr{T}_{28} \prec \mathscr{T}_i$ for $i = 6, 23, 24$.
- $\mathscr{T}_{29} \prec \mathscr{T}_i$ for $i = 9, 13, 16, 17$.
- $\mathscr{T}_{31} \prec \mathscr{T}_{30}$, $\mathscr{T}_{37}$, and $\mathscr{T}_{30} \prec \mathscr{T}_{20}$, $\mathscr{T}_{12}$, and $\mathscr{T}_{37} \prec \mathscr{T}_{25}$.
- $\mathscr{T}_{33} \prec \mathscr{T}_{32} \prec \mathscr{T}_i$ for $i = 21, 22$.

$q = 7^4$:

Increasing the constant field to $\mathbb{F}_{7^4}$ yields the following additional towers. Curiously the asymptotic limit does not increase: it remains 6.

	$f_i(x, y)$:	$\lambda(\mathscr{F}_i) \geqslant$
$\mathscr{F}_1$:	$f_1(x, y) = y^2 + (x^2 + 3)y + 5x + 4$	6
$\mathscr{F}_2$:	$f_2(x, y) = y^2 + (x^2 + 5)y + 5x + 2$	6
$\mathscr{F}_3$:	$f_3(x, y) = x^2y^2 + (x^2 + 4x + 5)y + 5x^2 + x + 6$	6
$\mathscr{F}_4$:	$f_4(x, y) = y^2 + (x^2 + 4)y + 6x^2 + 3x + 6$	6

Using Elkies' technique, it can be shown that

- $\mathscr{T}_{33} \prec \mathscr{F}_4 \prec \mathscr{F}_1$,
- $\mathscr{T}_8 \prec \mathscr{F}_2$,
- $\mathscr{T}_{18} \prec \mathscr{F}_3$,

where the first towers refer to those over $\mathbb{F}_{49}$.

$q = 121$:

Ref:		$f_i(x, y)$:	$\lambda(\mathscr{T}_i) \geqslant$
[13]	$\mathscr{T}_1$:	$f_1(x, y) = y^2 + x^2y + 4$	10
[7]	$\mathscr{T}_2$:	$f_2(x, y) = y^2 + x^2y + 9x$	10
[7]	$\mathscr{T}_3$:	$f_3(x, y) = y^2 + (x^2 + 8)y + 3x^2 + 4x + 5$	10
[7]	$\mathscr{T}_4$:	$f_4(x, y) = y^2 + x^2y + 5x$	10
[13]	$\mathscr{T}_5$:	$f_5(x, y) = y^2 + (x^2 + 3)y + 5$	10
	$\mathscr{T}_6$:	$f_6(x, y) = y^2 + (x^2 + 7)y + 9x + 4$	10
[7]	$\mathscr{T}_7$:	$f_7(x, y) = y^2 + (x^2 + 8)y + 10x^2 + 7x + 6$	10
[7]	$\mathscr{T}_8$:	$f_8(x, y) = y^2 + (x^2 + 3)y + 4x^2 + 5x + 5$	10
[8]	$\mathscr{T}_9$:	$f_9(x, y) = y^2 + (x^2 + 7)y + 3x^2 + 4$	10
[7]	$\mathscr{T}_{10}$:	$f_{10}(x, y) = y^2 + (x^2 + 7)y + 8x^2 + 3x + 5$	10
	$\mathscr{T}_{11}$:	$f_{11}(x, y) = y^2 + (x^2 + 9)y + 6x^2 + 9x + 6$	10
[8]	$\mathscr{T}_{12}$:	$f_{12}(x, y) = y^2 + (x^2 + 8)y + x^2$	10
[8]	$\mathscr{T}_{13}$:	$f_{13}(x, y) = y^2 + x^2y + 9x^2 + 1$	10
	$\mathscr{T}_{14}$:	$f_{14}(x, y) = y^2 + (x^2 + 9)y + 9x + 2$	10
	$\mathscr{T}_{15}$:	$f_{15}(x, y) = x^2y^2 + xy + 4x^2 + 1$	10
	$\mathscr{T}_{16}$:	$f_{16}(x, y) = x^2y^2 + 2xy + 3x^2 + 4$	10
	$\mathscr{T}_{17}$:	$f_{17}(x, y) = x^2y^2 + 2xy + 8x^2 + 4$	10
	$\mathscr{T}_{18}$:	$f_{18}(x, y) = x^2y^2 + (x^2 + 7)y + 5$	10
	$\mathscr{T}_{19}$:	$f_{19}(x, y) = x^2y^2 + (x^2 + 2x + 1)y + 1$	10
	$\mathscr{T}_{20}$:	$f_{20}(x, y) = x^2y^2 + (x^2 + 3x + 6)y + 9x^2 + 8x + 3$	10
	$\mathscr{T}_{21}$:	$f_{21}(x, y) = x^2y^2 + (x^2 + 3x + 9)y + 4$	10
	$\mathscr{T}_{22}$:	$f_{22}(x, y) = x^2y^2 + (x^2 + 8x + 4)y + 5$	10
	$\mathscr{T}_{23}$:	$f_{23}(x, y) = (x^2 + 1)y^2 + (x^2 + 4x + 3)y + 10x^2 + 3$	10

Ref:	$f_i(x, y)$:	$\lambda(\mathscr{T}_i) \geqslant$
$\mathscr{T}_{24}$:	$f_{24}(x, y) = (x^2+1)y^2 + (3x^2+4x+9)y + 8x^2 + 8$	10
$\mathscr{T}_{25}$:	$f_{25}(x, y) = (x^2+1)y^2 + (3x^2+5x+8)y + 7x^2 + x + 8$	10
$\mathscr{T}_{26}$:	$f_{26}(x, y) = (x^2+1)y^2 + (4x^2+5x+4)y + 5x + 8$	10

The towers $\mathscr{T}_1$, $\mathscr{T}_3$ and $\mathscr{T}_5$ are respectively special cases of the towers $\mathscr{M}$, $\mathscr{N}$ and $\mathscr{L}$ in [13]. Thus, from [13], we have $\mathscr{T}_5 \prec \mathscr{T}_3 \prec \mathscr{T}_1$. In this case, in order for the program to finish in a tolerable time, we relaxed many of the conditions. This explains why we found fewer towers here. Using Elkies' technique, the following can be shown:

$\mathscr{T}_4 \prec \mathscr{T}_3 \prec \mathscr{T}_2, \mathscr{T}_{22}$, $\quad \mathscr{T}_8 \prec \mathscr{T}_7 \prec \mathscr{T}_6, \mathscr{T}_{23}$,
$\mathscr{T}_{11} \prec \mathscr{T}_{10}$, $\quad \mathscr{T}_{13} \prec \mathscr{T}_{12} \prec \mathscr{T}_{14}, \mathscr{T}_{19}$,
$\mathscr{T}_{11} \prec \mathscr{T}_{15}, \mathscr{T}_{16}, \mathscr{T}_{17}$, $\quad \mathscr{T}_{13} \prec \mathscr{T}_{18}, \mathscr{T}_{24}, \mathscr{T}_{25}$.
$\mathscr{T}_8 \prec \mathscr{T}_{21} \prec \mathscr{T}_{20}, \mathscr{T}_{26}$,

Acknowledgements

The authors are very grateful to Mike Zieve and the referee for their detailed reading of this paper and for all their comments and corrections.

References

[1] P. Beelen, A. Garcia, H. Stichtenoth, On ramification and genus of recursive towers, Portugaliae Math, to appear.
[2] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, K. Wildanger, KANT V4, J. Symbolic Comput. 24 (1997) 267–283.
[3] V.G. Drinfel'd, S.G. Vladut, Number of points of an algebraic curve, Funct. Anal. 17 (1983) 53–54.
[4] N.D. Elkies, Explicit modular towers, in: T. Basar, A. Vardy (Eds.), Proceedings of the 35th Annual Allerton Conference on Communication, Control and Computing (1997), pp. 23–32.
[5] N.D. Elkies, Explicit towers of Drinfeld modular curves, Proceedings of the Third European Congress of Mathematics, Barcelona, 2000.
[6] N.D. Elkies, email correspondence.
[7] N.D. Elkies, http://www.math.harvard.edu/~elkies/tower2_1.html
[8] N.D. Elkies, http://www.math.harvard.edu/~elkies/tower2_2.html
[9] A. Garcia, H. Stichtenoth, A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound, Invent. Math. 121 (1995) 211–222.
[10] A. Garcia, H. Stichtenoth, On the asymptotic behaviour of some towers of function fields over finite fields, J. Number Theory 61 (1996) 248–273.
[11] A. Garcia, H. Stichtenoth, Asymptotically good towers of function fields over finite fields, C. R. Acad. Sci. Paris I 322 (1996) 1067–1070.
[12] A. Garcia, H. Stichtenoth, Skew pyramids of function fields are asymptotically bad, in: J. Buchmann et al., (Eds.), Coding Theory, Cryptography and Related Topics, Proceedings of a Conference in Guanajuato, 1998, Springer, Berlin, 2000, pp. 111–113.
[13] A. Garcia, H. Stichtenoth, H.-G. Rück, On tame towers over finite fields, J. Reine Angew. Math. 557 (2003) 53–80.
[14] A. Garcia, H. Stichtenoth, M. Thomas, On towers and composita of towers of function fields over finite fields, Finite Fields Appl. 3 (3) (1997) 257–274.

[15] Y. Ihara, Some remarks on the number of rational points of algebraic curves over finite fields, J. Fac. Sci. Univ. Tokyo Sect. IA Math. 28 (1981) 721–724.
[16] H.W. Lenstra Jr., On a problem of Garcia, Stichtenoth and Thomas, Finite Fields Appl. 8 (2001) 1–5.
[17] W.-C.W. Li, H. Maharaj, H. Stichtenoth, with an appendix by N.D. Elkies, New optimal tame towers of function fields over small finite fields, in: C. Fieker, D.R. Kohel (Eds.), Proceedings of ANTS-5, Lect. Notes in Comput. Sci. 2369, 2002, pp. 372–389.
[18] D. Lorenzini, An invitation to arithmetic geometry, Graduate Studies in Mathematics, 9, American Mathematical Society, Providence, RI, 1996.
[19] H. Maharaj, http://people.clemson.edu/∼hmahara/
[20] H. Niederreiter, C.P. Xing, Rational Points on Curves over Finite Fields: Theory and Applications, Cambridge University Press, Cambridge, 2001.
[21] H. Stichtenoth, Algebraic Function Fields and Codes, Springer, Berlin, Heidelberg, New York, 1993.
[22] M.A. Tsfasman, S.G. Vladut, T. Zink, Modular curves, Shimura curves and Goppa codes better than the Varshamov–Gilbert bound, Math. Nachr. 109 (1982) 21–28.
[23] J. Wulftange, Zahme Türme algebraischer funktionenkörper, Ph.D. Thesis, Universität Essen, 2003.