

1-1-2015

Quadratic recursive towers of function fields over \mathbb{F}_2

HENNING STICHTENOTH

SEHER TUTDERE

Follow this and additional works at: <https://dctubitak.researchcommons.org/math>



Part of the [Mathematics Commons](#)

Recommended Citation

STICHTENOTH, HENNING and TUTDERE, SEHER (2015) "Quadratic recursive towers of function fields over \mathbb{F}_2 ," *Turkish Journal of Mathematics*: Vol. 39: No. 5, Article 6. <https://doi.org/10.3906/mat-1411-42>

Available at: <https://dctubitak.researchcommons.org/math/vol39/iss5/6>

This Article is brought to you for free and open access by TÜBİTAK Academic Journals. It has been accepted for inclusion in Turkish Journal of Mathematics by an authorized editor of TÜBİTAK Academic Journals.

Quadratic recursive towers of function fields over \mathbb{F}_2

Henning STICHTENOTH¹, Seher TUTDERE^{2,*}

¹Faculty of Engineering and Natural Sciences, Sabanci University, Orhanlı, Tuzla, İstanbul, Turkey

²Department of Mathematics, Gebze Technical University, Çayirova Campus, Gebze, Kocaeli, Turkey

Received: 20.11.2014

Accepted/Published Online: 07.05.2015

Printed: 30.09.2015

Abstract: Let $\mathcal{F} = (F_n)_{n \geq 0}$ be a quadratic recursive tower of algebraic function fields over the finite field \mathbb{F}_2 , i.e. \mathcal{F} is a recursive tower such that $[F_n : F_{n-1}] = 2$ for all $n \geq 1$. For any integer $r \geq 1$, let $\beta_r(\mathcal{F}) := \lim_{n \rightarrow \infty} B_r(F_n)/g(F_n)$, where $B_r(F_n)$ is the number of places of degree r and $g(F_n)$ is the genus, respectively, of F_n/\mathbb{F}_2 . In this paper we give a classification of all rational functions $f(X, Y) \in \mathbb{F}_2(X, Y)$ that may define a quadratic recursive tower \mathcal{F} over \mathbb{F}_2 with at least one positive invariant $\beta_r(\mathcal{F})$. Moreover, we estimate $\beta_1(\mathcal{F})$ for each such tower.

Key words: Towers of algebraic function fields, genus, number of places

1. Introduction

Throughout this paper we use basic facts and notations as in [15]. We will consider (algebraic) function fields F/\mathbb{F}_q of one variable over the finite field \mathbb{F}_q . In all cases, \mathbb{F}_q will be the full constant field of F/\mathbb{F}_q . We denote by $g(F)$, $B_r(F)$ (for $r \in \mathbb{N}$), and $\mathbb{P}(F)$ the genus, the number of places of degree r , and the set of all places, respectively, of F/\mathbb{F}_q .

An infinite sequence $\mathcal{F} = (F_n)_{n \geq 0}$ of function fields F_n/\mathbb{F}_q is called a *tower* over \mathbb{F}_q , if

$$F_0 \subsetneq F_1 \subsetneq F_2 \subsetneq \dots,$$

all extensions F_{n+1}/F_n are finite separable, and $g(F_n) \rightarrow \infty$ as $n \rightarrow \infty$. For brevity, we denote it by \mathcal{F}/\mathbb{F}_q . Let $\mathcal{F} = (F_n)_{n \geq 0}$ be a tower. For any $r \geq 1$ the limit

$$\beta_r(\mathcal{F}) := \lim_{n \rightarrow \infty} \frac{B_r(F_n)}{g(F_n)}$$

is called a *global invariant* of \mathcal{F}/\mathbb{F}_q . These invariants were studied, for instance, in [8, 9, 11, 17]. For those invariants, the generalized Drinfeld–Vladut bound says that $\beta_r(\mathcal{F}) \leq (q^{r/2} - 1)/r$ for all $r \geq 1$. Moreover, for any tower \mathcal{F}/\mathbb{F}_q , one has that $\beta_1(\mathcal{F}) \leq A(q)$, where $A(q)$ is the well-known Ihara constant, which is quite important in coding theory and cryptography. Notice that $\beta_1(\mathcal{F}) = \lambda(\mathcal{F})$ is often called *the limit* of the tower \mathcal{F}/\mathbb{F}_q . Hence, the case $r = 1$ has been extensively studied by many researchers; see [1, 3, 4, 13]. More recently, towers with many positive invariants were studied; see [8, 9, 11, 17].

*Correspondence: stutdere@gmail.com

2010 AMS Mathematics Subject Classification: 11R58, 14H05.

In this paper, we are interested in a particular type of towers, namely recursive towers (for the definition of a recursive tower see Definition 1.3(a)). There are some interesting examples of such towers as given in [3, 7]. In the literature, there are many known recursive towers of function fields having positive β_1 over the finite field \mathbb{F}_q , where $q = p^k$ with p prime and $k \geq 2$; for instance, see [1]. However, the existence of recursive towers of function fields having positive β_1 over prime fields \mathbb{F}_p is not known. This is one of the open problems in the theory of recursive towers of function fields over finite fields.

Lenstra [12] showed that the construction of Kummer towers with $\beta_1 > 0$ over nonprime fields given by Garcia et al. [6] does not work over prime fields. That means that the towers over prime fields obtained by that construction have $\beta_1 = 0$. In [16] we investigated the recursive tower \mathcal{F} defined by the polynomial $f(X, Y) = Y^2X + Y + X^2 + 1$ over \mathbb{F}_2 and obtained some bounds for the invariant $\beta_1(\mathcal{F})$.

In this paper, we investigate the polynomials $f(X, Y) \in \mathbb{F}_2[X, Y]$ that yield quadratic recursive towers $\mathcal{F} = (F_n)_{n \geq 0}$, i.e. $[F_n : F_{n-1}] = 2$ for all $n \geq 1$, of function fields over \mathbb{F}_2 . Our main goal is to give a classification of polynomials $f(X, Y) \in \mathbb{F}_2[X, Y]$ that *recursively* define a *potentially good quadratic* tower over \mathbb{F}_2 (i.e. quadratic recursive towers that have at least one positive invariant β_r over \mathbb{F}_2).

The organization of our paper is as follows. We first introduce some basic results and some notions, and then we give our main results in Section 2.

We now give some more notations that will be used throughout this paper. For $f \in F$ and $P \in \mathbb{P}(F)$, we denote by $v_P(f)$ the valuation of f at P . Moreover, for a rational function field $\mathbb{F}_q(x)$ we will write $(x = a)$ for the place that is the zero of $x - a$ (where $a \in \mathbb{F}_q$) and $(x = \infty)$ for the pole of x .

Let E/F be a finite separable extension, and P and Q be places of F/\mathbb{F}_q and E/\mathbb{F}_q , respectively. We will write $Q|P$ if the place Q lies above P . In this case, we will denote by

$$e(Q|P), f(Q|P), \text{ and } d(Q|P)$$

the ramification index, the relative degree, and the different exponent, respectively, of $Q|P$. Moreover, since $P = Q \cap F$, the place P is called the *restriction* of Q to F .

We now give some definitions and recall the following limits whose existence is well known (for instance, see [15, Lemma 7.2.3], [9, Corollary 2.7]).

Definition 1.1 Let $\mathcal{F} = (F_n)_{n \geq 0}$ be a tower over \mathbb{F}_q and $r \in \mathbb{N}$. The real numbers

$$\nu_r(\mathcal{F}) = \lim_{n \rightarrow \infty} \frac{B_r(F_n)}{[F_n : F_0]}, \quad \beta_r(\mathcal{F}) = \lim_{n \rightarrow \infty} \frac{B_r(F_n)}{g(F_n)}, \text{ and } \gamma(\mathcal{F}) = \lim_{n \rightarrow \infty} \frac{g(F_n)}{[F_n : F_0]}$$

are called the *global invariants* of \mathcal{F}/\mathbb{F}_q and the *genus* of the tower \mathcal{F} over F_0 , respectively.

Obviously, $\beta_r(\mathcal{F}) = \nu_r(\mathcal{F})/\gamma(\mathcal{F})$ for all $r \geq 1$.

Definition 1.2 For any tower \mathcal{F}/\mathbb{F}_q , if $\beta_r(\mathcal{F}) > 0$ for some $r \in \mathbb{N}$, we say that \mathcal{F}/\mathbb{F}_q is a *potentially good tower*.

Definition 1.3 Let $\mathcal{F} = (F_n)_{n \geq 0}$ be a tower over \mathbb{F}_q and $f(X, Y) \in \mathbb{F}_q[X, Y]$ be an *absolutely irreducible polynomial*.

(a) Suppose that there exist elements $x_n \in F_n$ (for $n \geq 0$) such that $F_0 = \mathbb{F}_q(x_0)$ is the rational function field and

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

Then we say that the tower \mathcal{F} is recursively defined over \mathbb{F}_q by the equation $f(X, Y) = 0$.

(b) If $[F_{n+1} : F_n] = 2$ for all $n \geq 0$ we say that \mathcal{F}/\mathbb{F}_q is a quadratic tower.

(c) The function field F/\mathbb{F}_q with $F := \mathbb{F}_q(x, y)$, where x, y satisfy the equation $f(x, y) = 0$, is called the basic function field of \mathcal{F}/\mathbb{F}_q (note that $F \cong F_1$).

(d) The tower \mathcal{G}/\mathbb{F}_q , which is recursively defined by the equation $f(Y, X) = 0$, is called the dual tower of \mathcal{F}/\mathbb{F}_q .

We call two towers $\mathcal{F} = (F_n)_{n \geq 0}$ and $\mathcal{G} = (G_n)_{n \geq 0}$ isomorphic if for every $n \geq 0$, F_n is isomorphic to G_n . In particular, every recursive tower is isomorphic to its dual tower. It is clear that isomorphic towers have the same invariants, i.e. for all $r \geq 1$:

$$\nu_r(\mathcal{F}) = \nu_r(\mathcal{G}), \quad \gamma(\mathcal{F}) = \gamma(\mathcal{G}), \quad \text{and} \quad \beta_r(\mathcal{F}) = \beta_r(\mathcal{G}).$$

From now on, by a tower \mathcal{F} over \mathbb{F}_q , we mean a recursive tower, i.e. a tower that is recursively defined by an equation $f(X, Y) = 0$ or in other words by a polynomial $f(X, Y) \in \mathbb{F}_q[X, Y]$. In this paper we are in general interested in potentially good quadratic recursive towers over \mathbb{F}_2 . However, our main interest is the case $r = 1$. We here give a classification of potentially good towers over \mathbb{F}_2 , up to isomorphism. Our main result is as follows:

Theorem 1.4 *Suppose that \mathcal{F}/\mathbb{F}_2 is a potentially good quadratic recursive tower. Then the basic function field F/\mathbb{F}_2 of \mathcal{F}/\mathbb{F}_2 is an elliptic function field with $B_1(F) \in \{2, 3, 4, 5\}$ and, up to isomorphism, we have the following:*

- (a) *If $B_1(F) = 2$, then there exists only one equation that can define \mathcal{F}/\mathbb{F}_2 . In this case, $\beta_3(\mathcal{F}) = \frac{1}{2}$ and $\beta_r(\mathcal{F}) = 0$ for all $r \neq 3$.*
- (b) *If $B_1(F) = 3$, then there are exactly three equations that can define \mathcal{F}/\mathbb{F}_2 . In all cases, $\beta_1(\mathcal{F}) = 0$.*
- (c) *If $B_1(F) = 4$, then there are exactly six equations that can define \mathcal{F}/\mathbb{F}_2 . In all cases, $\beta_1(\mathcal{F}) = 0$.*
- (d) *If $B_1(F) = 5$, then there are exactly four equations that can define \mathcal{F}/\mathbb{F}_2 .*

Proof The proof will follow from Remark 2.3; Theorems 2.4, 2.5, 2.9, and 2.14; and Corollaries 2.8 and 2.13. \square

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

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

Let \mathcal{F}/\mathbb{F}_q be a tower defined by the equation $f(X) = g(Y)$, where $f(T), g(T) \in \mathbb{F}_q(T)$. In [2] it was proved that for any $A \in GL(2, \mathbb{F}_q)$ the equation $f(A \cdot X) = g(A \cdot Y)$ also defines the tower \mathcal{F} . In Remark 1.5, we give a more general observation, which can be shown in a similar way as in [2].

Remark 1.5 Let \mathcal{F}/\mathbb{F}_q be a tower defined by the equation $f(X, Y) = 0$. For any $A \in GL(2, \mathbb{F}_2)$, the equation $f(A \cdot X, A \cdot Y) = 0$ also defines the tower \mathcal{F}/\mathbb{F}_q . Moreover, it is clear that the equations $f(X, Y) = \frac{f_1(X, Y)}{f_2(X, Y)} = 0$, where $f_1(X, Y), f_2(X, Y) \in \mathbb{F}_2[X, Y]$ are relatively prime, and $f_1(X, Y) = 0$ recursively define the same sequence of function fields over \mathbb{F}_q .

Lemma 1.6 Let $\mathcal{F} = (F_n)_{n \geq 0}$ be a tower over \mathbb{F}_q defined by the equation $f(X, Y) = 0$ such that $g(F_{k-1}) = 0$ and $g(F_k) \geq 1$ for some $k \geq 1$. We set $G_i := F_{i+k-1}$ for all $i \geq 0$. The sequence $\mathcal{G} := (G_i)_{i \geq 0}$ of function fields G_i/\mathbb{F}_q is also a recursive tower, and its basic function field is nonrational.

Proof The field F_{k-1} has genus 0, and hence it is rational, say $F_{k-1} = \mathbb{F}_q(u_0)$ for some transcendental element u_0 . We write $u_0 = \phi(x_0, \dots, x_{k-1})$ where ϕ is a rational function in k variables and define $u_i := \phi(x_i, \dots, x_{i+k-1})$ for any $i \geq 0$. Let $h(u_0, u_1) = 0$ be the irreducible equation for u_1 over F_{k-1} . Then $h(u_i, u_{i+1}) = 0$ for all $i \geq 0$, which implies that the tower $\mathcal{G} = (F_{k-1}, F_k, \dots)$ can be defined recursively by the equation $h(U, V) = 0$. Thus, the lemma follows. □

Remark 1.7 By Lemma 1.6, it is enough to consider only towers \mathcal{F}/\mathbb{F}_q whose basic function field F/\mathbb{F}_q has genus strictly greater than zero. For the rest of the paper, we will always assume this.

Let $f(X, Y) \in \mathbb{F}_q[X, Y]$ be a polynomial. For $T = X$ (or $T = Y$) we set $\deg_T f(X, Y) := \max\{\deg_T f_1(X, Y), \deg_T f_2(X, Y)\}$ and call it the degree of $f(X, Y)$ in the variable X (or Y , respectively).

Lemma 1.8 Suppose that \mathcal{F}/\mathbb{F}_q is a tower defined by the equation $f(X, Y) = 0$ where $\deg_X f(X, Y) \neq \deg_Y f(X, Y)$. Then $\beta_r(\mathcal{F}) = 0$ for all $r \geq 1$.

The proof of Lemma 1.8 can be omitted; one can prove it by using the same method used for the proof of the case $r = 1$ in [5] and the following formula (c.f. [15, p.207]): for all $r, d \geq 1$,

$$r\beta_r(\mathcal{F}/\mathbb{F}_q) = \sum_{d|r} \mu\left(\frac{r}{d}\right) \beta_1(\mathcal{F} \cdot \mathbb{F}_{q^d}/\mathbb{F}_{q^d}), \tag{1}$$

where μ is the Möbius function and $\mathcal{F} \cdot \mathbb{F}_{q^d} := (F_n \mathbb{F}_{q^d})_{n \geq 0}$ is the tower of constant field extensions $F_n \mathbb{F}_{q^d}/\mathbb{F}_{q^d}$ of F_n/\mathbb{F}_q .

Suppose now that \mathcal{F} is a potentially good quadratic tower defined by the equation $f(X, Y) = 0$ over \mathbb{F}_2 . It follows from Lemma 1.8 that $\deg_X f(X, Y) = \deg_Y f(X, Y) = 2$. In other words, for the basic function field F/\mathbb{F}_2 of the tower \mathcal{F}/\mathbb{F}_2 , we have that $F = \mathbb{F}_2(x, y)$ with $f(x, y) = 0$ such that $[F : \mathbb{F}_2(x)] = [F : \mathbb{F}_2(y)] = 2$. Now it follows from Riemann’s inequality [15, Corollary 3.11.4] that the function field F/\mathbb{F}_2 has genus $g \leq 1$ and hence $g = 1$ (because of our assumption in Remark 1.7). Therefore, F/\mathbb{F}_2 is an elliptic function field. We also note that by the Hasse–Weil bound [15, Theorem 5.2.3], we have $1 \leq B_1(F) \leq 5$.

Proposition 1.9 Up to isomorphism over \mathbb{F}_2 , for each $n \in \{1, 2, 3, 4, 5\}$, there exists exactly one elliptic function field $F = \mathbb{F}_2(x, y)$ over \mathbb{F}_2 having $B_1(F) = n$. These function fields can be described explicitly as follows:

- (i) $B_1(F) = 1$ and $y^2 + y = x^3 + x + 1$,
- (ii) $B_1(F) = 2$ and $y^2 + y = (x^2 + x + 1)/x$,
- (iii) $B_1(F) = 3$ and $y^2x + yx^2 + 1 = 0$,
- (iv) $B_1(F) = 4$ and $y^2 + y = x/(x^2 + x + 1)$,
- (v) $B_1(F) = 5$ and $y^2x + y = x^2 + 1$.

Proof It follows from [10, Proposition 6.4, p.79] or [15, Proposition 6.1.2] that up to isomorphism over \mathbb{F}_2 there are five elliptic function fields F/\mathbb{F}_2 . Hence, it is enough to show that the given equations define elliptic function fields with the desired number of rational places. We first consider the equation in (iii). Multiplying both sides of that equation by y^2x yields that $y^4x^2 + y^3x^3 + y^2x = 0$. Now set $t := yx$ and $z := y^2x = ty$. Clearly, $\mathbb{F}_2(x, y) = \mathbb{F}_2(z, t)$ and $z^2 + z = t^3$. Similarly, by multiplying both sides of the equation in (v) by x and setting $w := xy$, we obtain that $\mathbb{F}_2(x, w) = \mathbb{F}_2(x, y)$ and $w^2 + w = x^3 + x$. Now by applying the Artin–Schreier extensions theorem [15, Proposition 3.7.8] and Kummer’s theorem [15, p. 86, Theorem 3.3.7], all assertions follow. \square

We summarize as follows:

Theorem 1.10 *Suppose that $\mathcal{F} = (F_n)_{n \geq 0}$ is a potentially good quadratic recursive tower defined by the equation $f(X, Y) = 0$ over \mathbb{F}_2 . Then the following hold:*

- (a) *If \mathcal{G}/\mathbb{F}_2 is the dual tower of \mathcal{F}/\mathbb{F}_2 , then $\beta_r(\mathcal{F}) = \beta_r(\mathcal{G})$ for all $r \geq 1$,*
- (b) *for any $A \in GL(2, \mathbb{F}_2)$, the equation $f(A \cdot X, A \cdot Y) = 0$ also defines the tower \mathcal{F} ,*
- (c) $\deg_X f(X, Y) = \deg_Y f(X, Y) = 2$,
- (d) *w.l.o.g. the basic function field F_1/\mathbb{F}_2 is an elliptic function field with $B_1(F_1) \in \{1, 2, 3, 4, 5\}$,*
- (e) $f(X, Y) \neq f(Y, X)$.

Proof (a)–(d) follow from our previous discussions and (e) follows from [14, Lemma 3.1]. \square

2. Potentially good quadratic recursive towers over \mathbb{F}_2

In this section we will find all equations that up to isomorphism recursively define a potentially good quadratic recursive tower over \mathbb{F}_2 . We will make a classification of those equations by using Theorem 1.10.

From now on, unless otherwise stated, we suppose that $\mathcal{F} = (F_n)_{n \geq 0}$ is a potentially good quadratic recursive tower defined by an equation $f(X, Y) = 0$ over \mathbb{F}_2 with the basic function field F_1/\mathbb{F}_2 . For simplicity, we set $F := F_1$. By Theorem 1.10(d), w.l.o.g. $F = \mathbb{F}_2(x, y)$ for some $x, y \in F$ with $f(x, y) = 0$ and F/\mathbb{F}_2 is an elliptic function field with $B_1(F) = n$ for some $n \in \{1, 2, 3, 4, 5\}$. It follows from Proposition 1.9 that up to isomorphism F/\mathbb{F}_2 is unique with n rational places. It is clear that the equations in the following set S_n also define the function field F/\mathbb{F}_2 :

$$S_n := \{f(A \cdot X, B \cdot Y) = 0 \mid A, B \in GL(2, \mathbb{F}_2)\}.$$

It follows from Theorem 1.10(b) that for any $A, B \in GL(2, \mathbb{F}_2)$ and $f(X, Y) \in \mathbb{F}_2[X, Y]$ the equations $f(A \cdot X, B \cdot Y) = 0$ and $f(X, A^{-1} \cdot (B \cdot Y)) = 0$ define the same sequence of function fields over \mathbb{F}_2 . Therefore, it is enough to investigate all equations $f(X, A \cdot Y) = 0$ with $A \in GL(2, \mathbb{F}_2)$ for each $f(X, Y) \in \mathbb{F}_2[X, Y]$ such that $f(x, y) = 0$ and the following holds:

$$\deg_X f(X, Y) = [F : \mathbb{F}_2(x)] = [F : \mathbb{F}_2(y)] = \deg_Y f(X, Y) = 2.$$

We will make a classification of the desired equations according to the number of rational places of the basic function field F/\mathbb{F}_2 for which $B_1(F) \in \{1, 2, 3, 4, 5\}$. Throughout the subsequent subsections we will use the following notations:

Notations: (1) For any rational function $f(X, Y) \in \mathbb{F}_q(X, Y)$ we denote by $\hat{f}(X, Y)$ the numerator of $f(X, Y)$.

(2) We assign the elements of the group $GL(2, \mathbb{F}_2)$ as follows:

$$A_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, A_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, A_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, A_3 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, A_4 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, A_5 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

Note that A_0 is the identity of the group $GL(2, \mathbb{F}_2)$.

Definition 2.1 Let F be a field and suppose that it has a subfield $\mathbb{F}_2(x)$ such that $[F : \mathbb{F}_2(x)] = 2$. We say that $\mathbb{F}_2(x)$ is a degree-2 rational subfield of F .

Observe that in our situation the basic function field F/\mathbb{F}_2 is generated by x and y , and the rational function fields $\mathbb{F}_2(x)$ and $\mathbb{F}_2(y)$ are degree-2 rational subfields of F . To prove Theorem 1.4, we first need to prove the following theorem:

Theorem 2.2 Suppose that F/\mathbb{F}_2 is an elliptic function field with $B_1(F) = n$. Then $n \in \{1, 2, 3, 4, 5\}$ and there are exactly n degree-2 rational subfields of F/\mathbb{F}_2 . Moreover, when $n \in \{2, 3, 4, 5\}$, one can write F as follows:

(i) If $n = 2$, then $F = \mathbb{F}_2(x, y)$ with $x(y^2 + y) = x^2 + x + 1$.

(ii) If $n = 3$, then $F = \mathbb{F}_2(u, v)$ with distinct $u, v \in \{x, y, z\}$, where

$$z := \frac{x^2+x+1}{xy+x}, \text{ with}$$

$$y^2x + yx^2 + 1 = 0 \quad \text{and} \quad y^2 + zy^2 + yz^2 + y + 1 = 0. \tag{2}$$

(iii) If $n = 4$, then $F = \mathbb{F}_2(u, v)$ with distinct $u, v \in \{x, y, z, t\}$, where

$$z := \frac{1}{y(x^2+x+1)+x+1} \quad \text{and} \quad t := \frac{1}{y(x^2+x+1)+x^2+1}, \text{ with}$$

$$(y^2 + y)(x^2 + x + 1) = x \quad \text{and} \quad z(t^2 + t) = z^2 + 1. \tag{3}$$

(iv) If $n = 5$, then $F = \mathbb{F}_2(u, v)$ with distinct $u, v \in \{x, y, z, t, w\}$, where

$$z := \frac{xy+x+1}{x^2}, \quad t := \frac{x}{xy+1}, \quad \text{and} \quad w := \frac{y+1}{x}, \text{ with}$$

$$uw^2 + v = u^2 + 1 \text{ for } (u, v) \in \{(x, y), (w, y)\} \text{ and } z^2t^2 + z = t^2 + t. \tag{4}$$

Proof It follows from the Hasse–Weil bound [15, Theorem 5.2.3] that $n \in \{1, 2, 3, 4, 5\}$. We first suppose that $n = 1$. Assume that $\mathbb{F}_2(y)$ is a degree-2 rational subfield of F , which is distinct from $\mathbb{F}_2(x)$. Then we must have that $\mathbb{F}_2(x, y) = F$. Let P be the unique rational place of F/\mathbb{F}_2 . Then $P \cap \mathbb{F}_2(x) = (x = \alpha)$ and $P \cap \mathbb{F}_2(y) = (y = \beta)$ for some $\alpha, \beta \in \mathbb{F}_2 \cup \{\infty\}$. Hence, we have the following cases:

$$(a) \alpha = \beta = \infty, \quad (b) \alpha = \infty, \beta \in \mathbb{F}_2 \text{ or } \beta = \infty, \alpha \in \mathbb{F}_2, \quad (c) \alpha, \beta \in \mathbb{F}_2.$$

First, suppose that (a) holds. As $B_1(F) = 1$, it is clear that place P must be ramified over both of the fields $\mathbb{F}_2(x)$ and $\mathbb{F}_2(y)$. Then by [15, Theorem 1.5.17], the Riemann–Roch space $\mathcal{L}(2P)$ of the divisor $2P$ has dimension two. Since $x, y \in \mathcal{L}(2P)$, we have that $\mathcal{L}(2P) = \langle 1, x \rangle = \langle 1, y \rangle$, and so $x = a + by$ for some $a, b \in \mathbb{F}_2$. This implies that $F = \mathbb{F}_2(x)$, which contradicts the fact that $g(F) = 1$. If (b) or (c) holds, then similarly we get a contradiction. Thus, F has only one degree-2 rational subfield, namely $\mathbb{F}_2(x)$. Next, we prove assertions (i) and (iii), and the proofs of (ii) and (iv) are similar to that of (i):

(i) We know from Proposition 1.9 that up to isomorphism there exists exactly one elliptic function field F/\mathbb{F}_2 with $B_1(F) = 2$ and $F = \mathbb{F}_2(x, y)$ such that the equation given in (i) holds. Hence, $\mathbb{F}_2(x)$ and $\mathbb{F}_2(y)$ are degree-2 rational subfields of F . Denote by R_1 and R_2 the rational places of F/\mathbb{F}_2 . By using Kummer’s theorem [15, Theorem 3.3.7], we have the following ramification structures in $F/\mathbb{F}_2(x)$ and $F/\mathbb{F}_2(y)$, respectively:

- (I) $(x = 0)$ and $(x = \infty)$ are ramified in F , and $(x = 1)$ is inert in F . W.l.o.g. we assume that $R_1|(x = 0)$ and $R_2|(x = \infty)$.
- (II) $(y = \infty)$ splits in F and R_1, R_2 lie above it. The places $(y = 0)$ and $(y = 1)$ are inert in F .

Now let $\mathbb{F}_2(z)$ be a degree-2 rational subfield of F . Since $B_1(F) = 2$, the ramification structure in $F/\mathbb{F}_2(z)$ must be similar to one of the types (I) or (II). That means that in $F/\mathbb{F}_2(z)$ either two rational places are ramified and one rational place is inert, or one rational place splits and two rational places are inert. In the first case, w.l.o.g. we have that $(z = 0) = (x = 0) = 2R_1$, and so $\mathcal{L}(2R_1) = \langle 1, z \rangle = \langle 1, x \rangle$. Hence, $x = a + bz$ for some $a, b \in \mathbb{F}_2$, which implies that $\mathbb{F}_2(z) = \mathbb{F}_2(x)$. In the second case, one similarly gets that $\mathbb{F}_2(z) = \mathbb{F}_2(y)$. Thus, (i) follows.

(iii) By Proposition 1.9(iv), $F = \mathbb{F}_2(x, y)$ such that the first equation given in (iii) holds. Hence, $\mathbb{F}_2(x)$ and $\mathbb{F}_2(y)$ are distinct degree-2 rational subfields of F . By the Artin–Schreier extensions theorem [15, Proposition 3.7.8] we have the following ramification structure in $F/\mathbb{F}_2(x)$ and $F/\mathbb{F}_2(y)$, respectively:

- (I) $(x = 0)$ and $(x = \infty)$ split, and $(x = 1)$ is inert in F . The zero of $x^2 + x + 1$, say P_1 , in $\mathbb{F}_2(x)$ is ramified in F . Let Q_1 and Q_2 be places of F/\mathbb{F}_2 lying above $(x = 1)$ and P_1 , respectively.
- (II) $(y = 0)$ and $(y = 1)$ split, and $(y = \infty)$ is inert in F . The zero of $y^2 + y + 1$, say P_2 , in $\mathbb{F}_2(y)$ is ramified in F . Moreover, $Q_1 \cap \mathbb{F}_2(y) = P_2$ and $Q_2 \cap \mathbb{F}_2(y) = (y = \infty)$.

Next, we consider the field $\mathbb{F}_2(z, t)$. By the Artin–Schreier extensions theorem [15, Proposition 3.7.8], $\mathbb{F}_2(z, t)/\mathbb{F}_2$ has genus one and four rational places. Since, up to isomorphism, there is only one elliptic function field with four rational places, w.l.o.g. we can assume that $\mathbb{F}_2(z, t) = F$. Now let R_1, R_2, R_3 , and

R_4 be the rational places of F/\mathbb{F}_2 . By the same theorem, we have the following ramification structure in $F/\mathbb{F}_2(z)$ and $F/\mathbb{F}_2(t)$, respectively:

- (III) $(z = \infty)$ and $(z = 0)$ are ramified, and $(z = 1)$ splits in F . W.l.o.g. we assume that $R_1|(z = \infty)$, $R_2|(z = 0)$, and then R_3 and R_4 lie above $(z = 1)$.
- (IV) $(t = 0)$ and $(t = 1)$ are ramified, and $(t = \infty)$ splits in F . Moreover, $R_3|(t = 0)$ and $R_4|(t = 1)$.

Hence, $\mathbb{F}_2(z), \mathbb{F}_2(t) \notin \{\mathbb{F}_2(x), \mathbb{F}_2(y)\}$ are distinct degree-2 rational subfields of F . It follows from (I) and (II) that for any place Q of F/\mathbb{F}_2 with degree two, we have that $Q \cap \mathbb{F}_2(x) = P_1$ or $(x = 1)$, and $Q \cap \mathbb{F}_2(y) = P_2$ or $(y = \infty)$. Hence, F/\mathbb{F}_2 has exactly two places of degree two, say Q_1, Q_2 . Suppose now that $\mathbb{F}_2(w)$ is a degree-2 rational subfield of F . We then have the following cases:

- c.1. Two rational places of $\mathbb{F}_2(w)$ split in F and one rational place of $\mathbb{F}_2(w)$, w.l.o.g. say $(w = 0)$, is inert in F . Then $Q_i \cap \mathbb{F}_2(w) = (w = 0)$ for $i = 1$ or 2 . If $i = 1$, then $(w = 0) = (x = 1)$ in F . Hence, $v_{Q_1}(w(x - 1)^{-1}) = 0$, which implies that $F_2(w) = \mathbb{F}_2(x)$. If $i = 2$, similarly we then obtain that $F_2(w) = \mathbb{F}_2(y)$.
- c.2. Two rational places of $\mathbb{F}_2(w)$ are ramified and one rational place of $\mathbb{F}_2(w)$ splits in F . W.l.o.g. suppose that $(w = 0)$ is ramified in F . Then $(w = 0) = 2R_i$ for some $i \in \{1, 2, 3, 4\}$. Hence, similar as in c.1., we obtain that $\mathbb{F}_2(w) \in \{\mathbb{F}_2(z), \mathbb{F}_2(t)\}$.

Therefore, (iii) follows. □

Remark 2.3 *It follows from Theorem 2.2 that there is no equation defining a tower of function fields over \mathbb{F}_2 whose basic function field has only one rational place.*

We next investigate towers over \mathbb{F}_2 whose basic function field F/\mathbb{F}_2 has n rational places for each $n = 2, 3, 4, 5$.

2.1. $B_1(F) = 2$

In this subsection we suppose that the basic function field F/\mathbb{F}_2 has two rational places.

Theorem 2.4 *Suppose that \mathcal{F}/\mathbb{F}_2 is a potentially good quadratic recursive tower with the basic function field F/\mathbb{F}_2 having $B_1(F) = 2$. Then, up to isomorphism, \mathcal{F}/\mathbb{F}_2 can be defined by the following equation:*

$$Y^2 + Y = \frac{X^2 + X + 1}{X}. \tag{5}$$

Moreover, $\beta_3(\mathcal{F}) = \frac{1}{2}$ and $\beta_r(\mathcal{F}) = 0$ for all $r \neq 3$.

Proof Suppose that $f(X, Y) = 0$ is an equation defining a tower \mathcal{F}/\mathbb{F}_2 with the desired properties. By Theorem 2.2(i), $F = \mathbb{F}_2(x, y)$ where $x(y^2 + y) = x^2 + x + 1$. It follows from Theorem 1.10 that $f(u', v') = 0$ for some distinct $u', v' \in \{A \cdot x, B \cdot y \mid A, B \in GL(2, \mathbb{F}_2)\}$ and $F = \mathbb{F}_2(u', v')$. Set $g(X, Y) := X(Y^2 + Y) + X^2 + X + 1$ and let $A_i \in GL(2, \mathbb{F}_2)$ for $i = 1, 2, 3, 4, 5$. By the same theorems (see also the discussion and notations of the previous section), we have the following:

$$f(X, Y) = \hat{g}(X, A_i \cdot Y) \text{ for some } 0 \leq i \leq 5 \text{ where}$$

(1) $\hat{g}(X, Y) = \hat{g}(X, A_0 \cdot Y) = \hat{g}(X, A_1 \cdot Y) = g(X, Y) = 0,$

(2) $\hat{g}(X, A_2 \cdot Y) = \hat{g}(X, A_3 \cdot Y) = 0,$

(3) $h(X, Y) := \hat{g}(X, A_4 \cdot Y) = \hat{g}(X, A_5 \cdot Y) = (X^2 + X + 1)Y^2 + XY + X^2 + X + 1 = 0.$

Since $g(A_2 \cdot X, A_2 \cdot (A_3 \cdot Y)) = g(X, Y) = 0$, by Remark 1.5, Eqs. (1) and (2) describe the same tower over \mathbb{F}_2 . Next, we claim that Eq. (3) does not define a tower over \mathbb{F}_2 . To prove this claim first let $E_0 := \mathbb{F}_2(x_0)$ be the rational function field and $E_n := E_{n-1}(x_n)$ for any $n \geq 1$ with $h(x_{n-1}, x_n) = 0$. For $n = 2$, we have that

$$h(x_2, T) = \frac{x_0 x_2}{x_0^2 + 1} \left(T + \frac{1}{x_0} \right) (T + x_0) \in E_2[T].$$

Hence, $E_i = E_2$ for all $i \geq 3$, and so the claim follows. Therefore, we have $f(X, Y) = g(X, Y)$. The rest follows from [7] and [9, Example 4.3]. □

2.2. $B_1(F) = 3$

In this part we suppose that the basic function field F/\mathbb{F}_2 has three rational places.

Theorem 2.5 *Suppose that \mathcal{F}/\mathbb{F}_2 is a potentially good quadratic recursive tower with the basic function field F/\mathbb{F}_2 having $B_1(F) = 3$. Then, up to isomorphism, \mathcal{F}/\mathbb{F}_2 can be defined by one of the following equations:*

(1) $Y^2X + X + YX^2 + X^2 + 1 = 0,$

(2) $YX^2 + Y^2 + X = 0,$

(3) $X^2Y^2 + X^2Y + XY^2 + X + Y^2 = 0.$

Proof Let \mathcal{F}/\mathbb{F}_2 be a tower with the given assumptions and F/\mathbb{F}_2 be its basic function field. Suppose that $f(X, Y) = 0$ is an equation defining the tower \mathcal{F}/\mathbb{F}_2 . By Theorem 2.2(ii) $F = \mathbb{F}_2(u, v)$ where $u, v \in \{x, y, z\}$ as in (2). It follows from Theorem 1.10 that $f(u', v') = 0$ for some distinct $u', v' \in \{A \cdot x, B \cdot y, C \cdot z \mid A, B, C \in GL(2, \mathbb{F}_2)\}$ and $F = \mathbb{F}_2(u', v')$. In addition, we have that $x^2 + zx^2 + xz^2 + x + 1 = 0$. Let $A_i \in GL(2, \mathbb{F}_2)$ for $i = 1, 2, 3, 4, 5$. By the same theorems (see also Section 2), we have the following cases:

c.1. $f(X, Y) = \hat{f}_1(X, A_i \cdot Y)$ for some $1 \leq i \leq 5$, where $f_1(X, Y) := Y^2X + YX^2 + 1 = 0$ and

(i) $\hat{f}_1(X, A_1 \cdot Y) = X^2Y + X^2 + XY^2 + X + 1 = 0,$

(ii) $\hat{f}_1(X, A_2 \cdot Y) = X^2Y + X + Y^2 = 0,$

(iii) $\hat{f}_1(X, A_3 \cdot Y) = X^2Y^2 + X^2Y + XY^2 + X + Y^2 = 0,$

(iv) $\hat{f}_1(X, A_4 \cdot Y) = X^2Y^2 + X^2Y + XY^2 + Y^2 + 1 = 0,$

(v) $\hat{f}_1(X, A_5 \cdot Y) = X^2Y + X^2 + X + Y^2 + 1 = 0$. Note that $\hat{f}_1(X, A_5 \cdot Y) = 0$ and $\hat{f}_1(A_3 \cdot X, A_3 \cdot (A_5 \cdot Y)) = 0$ define the same tower whose dual tower can be defined by the equation $\hat{f}_1(X, A_3 \cdot Y) = 0$.

c.2. $f(X, Y) = \hat{f}_2(X, A_i \cdot Y)$ for some $1 \leq i \leq 5$, where $f_2(X, Y) := X^2 + YX^2 + XY^2 + X + 1$. Note that $f_2(X, Y) = \hat{f}_1(X, A_1 \cdot Y) = 0$.

Therefore, by Theorem 1.10, $f(X, Y) = 0$ must be one of the equations in c.1 (i), (ii), (iii), or (iv). We claim that the equation in c.1(iv) does not define a tower over \mathbb{F}_2 . Obviously, if the claim holds, then we are done. To prove the claim first let $G_0 := \mathbb{F}_2(x_0)$ be the rational function field and $G_i = G_{i-1}(x_i)$ for all $i \geq 1$ with $\hat{f}_1(x_{i-1}, A_4 \cdot x_i) = 0$. We have in $G_2[T]$ that

$$\hat{f}_1(x_2, A_4 \cdot T) = \left[(T + (x_0^4 + x_0)x_1 + (x_0^4 + x_0^3 + x_0^2 + 1))x_2 + (x_0^4 + x_0^3 + x_0)x_1 + A \right] \cdot B \cdot C,$$

where

$$A := \frac{x_0^6 + x_0^5 + x_0^4 + x_0^2}{x_0^2 + x_0 + 1}, \quad B := \left(x_1 + \frac{x_0^3 + x_0 + 1}{x_0^3 + 1} \right) x_2 + \frac{x_1}{x_0 + 1} + \frac{1}{x_0^2 + x_0 + 1},$$

and

$$C := T + ((x_0^4 + x_0)x_1 + (x_0^4 + x_0^3 + x_0^2))x_2 + \frac{x_1(x_0^5 + x_0^4 + 1)}{x_0} + \frac{x_0^6 + x_0^5 + x_0^2 + x_0 + 1}{x_0^2 + x_0}.$$

Hence, $G_i = G_2$ for all $i \geq 3$, and so the claim follows. □

Next, we investigate the invariant $\beta_1(\mathcal{F})$ of the tower \mathcal{F}/\mathbb{F}_2 for each case (1)–(3) in Theorem 2.5 if the given equation defines a tower.

Remark 2.6 We know from [3] and [17, Example 3.2.2] that the equation in Theorem 2.5(2) defines a potentially good quadratic tower \mathcal{F}/\mathbb{F}_2 with $\beta_2(\mathcal{F}) = \frac{1}{2}$ and $\beta_r(\mathcal{F}) = 0$ for all $r \neq 2$.

Proposition 2.7 Each of the following equations recursively defines a tower \mathcal{F}/\mathbb{F}_2 with $\beta_1(\mathcal{F}) = 0$:

(i) $Y^2X + X + YX^2 + X^2 + 1 = 0$, (ii) $X^2Y^2 + X^2Y + XY^2 + X + Y^2 = 0$.

Proof (i) Suppose that $\mathcal{F} = (F_n)_{n \geq 0}$ is a sequence of function fields defined recursively by the equation $f(X, Y) := Y^2X + X + YX^2 + X^2 + 1 = 0$ over \mathbb{F}_2 . By definition, $F_0 = \mathbb{F}_2(x_0)$, where $x_0 \in F_0$ is transcendental over \mathbb{F}_2 , and $F_1 = \mathbb{F}_2(x_0, x_1)$ such that x_0, x_1 satisfy the equation $f(x_0, x_1) = 0$. For simplicity, set $F := \mathbb{F}_2(x, y) = F_1$ where $x := x_0$ and $y := x_1$. Multiplying the equation $f(x, y) = 0$ by $1/x^3$ and letting $z := y/x$ yields that

$$z^2 + z = \frac{x^2 + x + 1}{x^3}.$$

We denote the rational places of F/\mathbb{F}_2 by R_1, R_2 , and R_3 . By the Artin–Schreier extensions theorem [15, Proposition 3.7.8], we have the following:

- (I) $(x = 0)$ is ramified in F , $R_1|(x = 0)$, and $R_1 \cap \mathbb{F}_2(y) = (y = \infty)$;
- (II) $(x = 1)$ is inert in F ;
- (III) $(x = \infty)$ splits in F , R_2 and R_3 lie above it, and $R_2 \cap \mathbb{F}_2(y) = (y = 1)$ and $R_3 \cap \mathbb{F}_2(y) = (y = \infty)$.

By using (I)–(III), and applying Abhyankar’s lemma [15, Theorem 3.9.1] in the Figure, for any $n \geq 1$, we obtain the following:

- Let $P^{(n)} \in \mathbb{P}(F_n)$ with $P^{(n)} \cap \mathbb{F}_2(x_k) = (x_k = \infty)$ for all $0 \leq k < n$ and $P^{(n)} \cap \mathbb{F}_2(x_n) = (x_n = 1)$, and $Q^{(n)} \in \mathbb{P}(F_n)$ with $Q^{(n)} \cap \mathbb{F}_2(x_k) = (x_k = \infty)$ for all $0 \leq k \leq n$. Then $P^{(n)}$ is inert in F_{n+1} and $Q^{(n)}$ splits in F_{n+1} . Thus, $[F_{n+1} : F_n] = 2$ and \mathbb{F}_2 is algebraically closed in F_n , and so the sequence \mathcal{F} is a quadratic tower over \mathbb{F}_2 .
- For any place $R^{(n)}$ of F_n with $R^{(n)} \cap F_0 = (x_0 = 0)$, we have that $R^{(n)} \cap \mathbb{F}_2(x_n) = (x_n = \alpha)$ for some $\alpha \in \{1, \infty\}$. If $\alpha = 1$ (resp. $\alpha = \infty$), then $R^{(n)}$ is inert (resp. splits) in F_{n+1} . Note that conversely for any $\alpha \in \{1, \infty\}$ there exists a place $R^{(n)}$ of F_n that lies above $(x_0 = 0)$ and $(x_n = \alpha)$.
- $B_1(F_n) = 4$ for all $n \geq 2$. Hence, $\nu_1(\mathcal{F}) = 0$, and so $\beta_1(\mathcal{F}) = 0$.

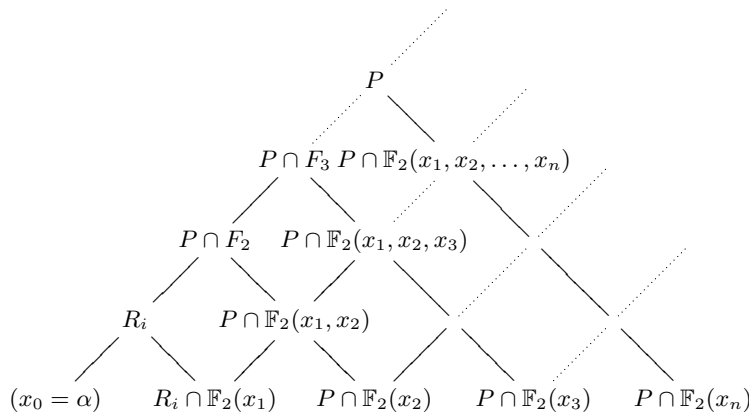


Figure. $\alpha \in \{0, 1, \infty\}$ and $P \in \{P^{(n)}, Q^{(n)}, R^{(n)}\}$.

(ii) We use the same method and notations as in the proof of (i) with $f(X, Y) := X^2Y^2 + X^2Y + XY^2 + X + Y^2 = 0$. Multiplying the equation $f(x, y) = 0$ by $\frac{x^2+x+1}{x^4}$ and setting $z := \frac{y(x^2+x+1)}{x^2}$ yields that $z^2 + z = \frac{x^2+x+1}{x^3}$. In this case, we obtain that $B_1(F_n) = 2$ for all $n \geq 2$. Hence, $\nu_1(\mathcal{F}) = 0$, and so $\beta_1(\mathcal{F}) = 0$.

□

The following corollary is an immediate consequence of Theorem 2.5, Remark 2.6, and Proposition 2.7.

Corollary 2.8 *Suppose that $\mathcal{F} = (F_n)_{n \geq 0}$ is a quadratic recursive tower of function fields over \mathbb{F}_2 such that its basic function field F_1/\mathbb{F}_2 has $B_1(F_1) = 3$. Then $\beta_1(\mathcal{F}) = 0$.*

2.3. $B_1(F) = 4$

In this subsection we suppose that the basic function field F/\mathbb{F}_2 has four rational places.

Theorem 2.9 *Suppose that \mathcal{F}/\mathbb{F}_2 is a potentially good quadratic recursive tower with the basic function field F/\mathbb{F}_2 having $B_1(F) = 4$. Up to isomorphism, \mathcal{F}/\mathbb{F}_2 can be defined by one of the following equations:*

- (1) $(Y^2 + Y)(X^2 + X + 1) + X = 0,$ (4) $X^2Y^2 + X^2Y + XY + X + Y,$
- (2) $XY^2 + XY + X^2 + 1 = 0,$ (5) $X^2Y + XY + X^2 + Y^2 + Y = 0,$
- (3) $X^2Y^2 + X^2Y + XY + Y + 1 = 0,$ (6) $X^2Y + XY + X + Y^2 + Y = 0.$

Proof Suppose that \mathcal{F}/\mathbb{F}_2 is a tower with the given assumptions and let F/\mathbb{F}_2 be its basic function field. Suppose that \mathcal{F}/\mathbb{F}_2 is defined by an equation $f(X, Y) = 0$. By Theorem 2.2(iii) $F = \mathbb{F}_2(u, v)$ where $u, v \in \{x, y, z, t\}$ as in (3). It follows from 1.10 that $f(u', v') = 0$ for some distinct $u', v' \in \{A_1 \cdot x, A_2 \cdot y \mid A_i \in GL(2, \mathbb{F}_2)\}$ for $i = 1, 2, 3, 4, 5$ and $F = \mathbb{F}_2(u', v')$. Because of (3), we have the following equations:

- (a) $(y^2 + y)(x^2 + x + 1) = x,$ (d) $x^2t + xt^2 + xt = t + 1,$
- (b) $z(t^2 + t) = z^2 + 1,$ (e) $y^2z^2 + y^2z + y^2 + yz = z^2 + z,$
- (c) $x^2z^2 + x^2z + xz = z + 1,$ (f) $y^2t^2 + y^2t + y^2 + yt^2 + yt = t + 1.$

Let $A_i \in GL(2, \mathbb{F}_2)$ for $i = 0, 1, 2, 3, 4, 5$. It follows from Theorems 1.10 and 2.2(iii) (see also Section 2) that we have the following cases:

- c.1. $f(X, Y) = \hat{f}_1(X, A_i \cdot Y)$ for some $0 \leq i \leq 5$, where $f_1(X, Y) := (Y^2 + Y)(X^2 + X + 1) + X$ with $f_1(x, y) = 0$ and
 - (i) $\hat{f}_1(X, A_1 \cdot Y) = f_1(X, Y).$
 - (ii) $\hat{f}_1(X, A_2 \cdot Y) = \hat{f}_1(X, A_3 \cdot Y) = \hat{f}_1(A_2 \cdot X, A_2 \cdot Y) = 0.$ Note that this equation defines the same tower as defined by $f_1(X, Y) = 0$.
 - (iii) $g(X, Y) := \hat{f}_1(X, A_4 \cdot Y) = \hat{f}_1(X, A_5 \cdot Y) = X^2Y + XY^2 + XY + X + Y = 0.$ Note that since $g(X, Y) = g(Y, X) = 0$, this equation does not define a tower.
- c.2. $f(X, Y) = \hat{f}_2(X, A_i \cdot Y)$ for some $0 \leq i \leq 5$, where $f_2(X, Y) := XY^2 + XY + X^2 + 1$ with $f_2(z, t) = 0$ and
 - (i) $\hat{f}_2(X, A_1 \cdot Y) = f_2(X, Y).$
 - (ii) $\hat{f}_2(X, A_2 \cdot Y) = \hat{f}_2(X, A_3 \cdot Y) = \hat{f}_2(A_2 \cdot X, A_2 \cdot Y) = 0.$ Note that this equation defines the same tower as defined by $f_2(X, Y) = 0$.
 - (iii) $\hat{f}_2(X, A_4 \cdot Y) = \hat{f}_2(X, A_5 \cdot Y) = X^2Y^2 + X^2 + XY + Y^2 + 1 =: g(X, Y).$ Note that since $g(X, Y) = g(Y, X) = 0$, this equation does not define a tower.
- c.3. $f(X, Y) = \hat{f}_3(X, A_i \cdot Y)$ for some $0 \leq i \leq 5$, where $f_3(X, Y) := X^2Y^2 + X^2Y + XY + Y + 1$ with $f_3(x, z) = 0$ and
 - (i) $\hat{f}_3(X, A_1 \cdot Y) = X^2Y^2 + X^2Y + XY + X + Y.$

(ii) $\hat{f}_3(X, A_2 \cdot Y) = X^2Y + XY + X^2 + Y^2 + Y.$

(iii) $\hat{f}_3(X, A_3 \cdot Y) = X^2Y + X^2 + XY^2 + XY + Y =: g(X, Y).$ Note that $g(X, Y) = \hat{f}_3(A_4 \cdot X, A_4 \cdot (A_2 \cdot Y)).$

(iv) $\hat{f}_3(X, A_4 \cdot Y) = X^2Y + XY^2 + XY + Y + 1.$ Note that $\hat{f}_3(X, A_4 \cdot Y) = \hat{f}_3(A_2 \cdot X, A_2 \cdot (A_1 \cdot Y)).$

(v) $\hat{f}_3(X, A_5 \cdot Y) = X^2Y + XY + X + Y^2 + Y.$

c.4. $f(X, Y) = \hat{f}_3(X, A_i \cdot Y)$ for some $0 \leq i \leq 5$, where $f_4(X, Y) := X^2Y + XY^2 + XY + Y + 1$ with $f_4(x, t) = 0.$ Note that $f_4(X, Y) = \hat{f}_3(X, A_4 \cdot Y) = 0.$

c.5. $f(X, Y) = \hat{f}_5(X, A_i \cdot Y)$ for some $0 \leq i \leq 5$, where $f_5(X, Y) := X^2Y^2 + X^2Y + X^2 + XY + Y^2 + Y$ with $f_5(y, z) = 0.$ Note that $\hat{f}_5(A_4 \cdot X, A_4 \cdot Y) = \hat{f}_3(X, A_3 \cdot Y).$

c.6. $f(X, Y) = \hat{f}_6(X, A_i \cdot Y)$ for some $0 \leq i \leq 5$, where $f_6(X, Y) := X^2Y^2 + X^2Y + X^2 + XY^2 + XY + Y + 1$ with $f_6(y, t) = 0.$ Note that $f_6(X, Y) = \hat{f}_3(A_4 \cdot X, A_4 \cdot Y) = 0.$

Consequently, by Theorem 1.10, we have only the equations c.1(i), c.2(i), $f_3(X, Y) = 0,$ c.3(i), c.3(ii), and c.3(v).

□

Next, we investigate the sequences of function fields that are defined by the equations given in Theorem 2.9(1)–(6).

Remark 2.10 It follows from [4] and [17, Example 3.2.1] that the equation in Theorem 2.9(2) defines a potentially good quadratic tower \mathcal{F}/\mathbb{F}_2 such that $\beta_2(\mathcal{F}) = \frac{1}{2}$ and $\beta_r(\mathcal{F}) = 0$ for all $r \neq 2.$

Proposition 2.11 The following equations define a quadratic recursive tower \mathcal{F} over \mathbb{F}_2 with $\beta_1(\mathcal{F}) = 0:$

(a) $(Y^2 + Y)(X^2 + X + 1) + X = 0,$ (c) $X^2Y + XY + X^2 + Y^2 + Y = 0,$

(b) $X^2Y^2 + X^2Y + XY + Y + 1 = 0,$ (d) $X^2Y + XY + X + Y^2 + Y = 0.$

Proof We use a similar method and the same notations as in Proposition 2.7 in (a)–(d). The proofs of (a)–(d) are all similar, so we omit the details in the proofs of (b)–(d).

(a) Set $f(X, Y) := (Y^2 + Y)(X^2 + X + 1) + X = 0.$ Denote the rational places of F/\mathbb{F}_2 by $R_1, R_2, R_3,$ and $R_4.$ By the Artin–Schreier extensions theorem [15, Proposition 3.7.8], we have the following:

(I) $(x = 0)$ splits in $F,$ R_1 and R_2 lie above it, and $R_1 \cap \mathbb{F}_2(y) = (y = 0)$ and $R_2 \cap \mathbb{F}_2(y) = (y = 1).$

(II) $(x = 1)$ is inert in $F.$

(III) $(x = \infty)$ splits in $F,$ R_3 and R_4 lie above it, and $R_3 \cap \mathbb{F}_2(y) = (y = 0)$ and $R_4 \cap \mathbb{F}_2(y) = (y = 1).$

(IV) The zero of $x^2 + x + 1$ in $\mathbb{F}_2(x)$ is ramified in $F.$

In order to show that \mathcal{F}/\mathbb{F}_2 is a tower, we consider the sequence $\mathcal{F} \cdot \mathbb{F}_4 = (\mathbb{F}_n \mathbb{F}_4)_{n \geq 0}$ of constant field extensions $F_n \mathbb{F}_4/\mathbb{F}_4$ of $F_n/\mathbb{F}_2.$ If the sequence $\mathcal{F} \cdot \mathbb{F}_4/\mathbb{F}_4$ is a quadratic tower, then so is $\mathcal{F}/\mathbb{F}_2.$ By the Artin–Schreier extensions theorem [15, Proposition 3.7.8], the following hold:

(I') same as (I) with $F := F\mathbb{F}_4$.

(II') $(x = 1)$ splits in $F\mathbb{F}_4$. Let R'_1 and R'_2 be extensions of $(x = 1)$ in $F\mathbb{F}_4$. Then $R'_1 \cap \mathbb{F}_4(y) = (y = a)$ and $R'_2 \cap \mathbb{F}_4(y) = (y = b)$, where a, b are roots of the polynomial $g(T) = T^2 + T + 1$.

(III') $(x = a)$ and $(x = b)$ are ramified in $F\mathbb{F}_4$. Let R'_3 and R'_4 be extensions of $(x = a)$ and $(x = b)$, respectively, in $F\mathbb{F}_4$. Then $R'_i \cap \mathbb{F}_4(y) = (y = \infty)$ for $i = 3, 4$.

Claim: For any $n \geq 1$, let P_n be a place of $F_n\mathbb{F}_4$ such that $x_n(P_n) = a$, $x_{n-1}(P_n) = 1$, and $x_k(P_n) = 0$ for all $k \leq n - 2$ and $n \geq 2$. Then P_n is ramified in $F_{n+1}\mathbb{F}_4$ for all $n \geq 0$. If the claim holds, then it follows immediately that \mathbb{F}_4 is algebraically closed in $F_n\mathbb{F}_4$ and $[F_{n+1}\mathbb{F}_4 : F_n\mathbb{F}_4] = 2$ for all $n \geq 1$. Hence, $\mathcal{F} \cdot \mathbb{F}_4/\mathbb{F}_4$ is a quadratic tower.

Proof of the claim: For $n = 0$, the proof follows from (III'). By definition $F_{n+1}\mathbb{F}_4 = F_n\mathbb{F}_4(x_{n+1})$ for all $n \geq 0$, where x_n, x_{n+1} satisfy the equation $f(x_n, x_{n+1}) = 0$. For simplicity, we first set $u := \frac{x_1}{x_1^2 + x_1 + 1}$ and let P be the extension of $(x_0 = 1)$ and $(x_1 = a)$ in F_1 . Then $v_P(u) = -2$. Let $t = x_0 + 1$ be a prime element for P , i.e. $v_P(t) = 1$. Since $v_P(x_1 + a) = 2$, by [15, Theorem 4.2.6], there are elements $a_2, a_3, \dots \in \mathbb{F}_4$ such that $x_1 = a + a_2t^2 + a_3t^3 + \dots$. By inserting these values of x_0 and x_1 in the equation $f(x_0, x_1) = 0$, we obtain that $x_1 = a + t^2 + t^3 + t^4 + \dots$. Now let $z := \frac{a+1}{t}$. Then $v_P(u + z^2 + z) = -1$. Hence, by the Artin-Schreier extensions theorem [15, Proposition 3.7.8], P is ramified in F_2 . The case $n \geq 2$ now follows by chasing a figure, as in the proof of Proposition 2.7, and applying the same theorem.

Next, as in the proof of Proposition 2.7, by using (I)–(III), one can easily obtain that $B_1(F_2) = 6$ and $B_1(F_n) = 4$ for all $n \geq 3$. Hence, $\nu_1(\mathcal{F}) = 0$, and so $\beta_1(\mathcal{F}) = 0$.

(b) Set $f(X, Y) := X^2Y^2 + X^2Y + XY + Y + 1 = 0$. Multiplying the equation $f(x, y) = 0$ by $\frac{x^2}{(x^2+x+1)^2}$ and setting $z := \frac{x^2y}{x^2+x+1}$ yields that $z^2 + z = \frac{x^2}{(x^2+x+1)^2}$. Applying the Artin-Schreier extensions theorem with $u := \frac{x}{x^2+x+1}$ yields that the place $(x^2 + x + 1 = 0)$ is ramified in F_1 . In this case, we obtain that \mathcal{F}/\mathbb{F}_2 is a quadratic tower such that $B_1(F_n) = 4$ for all $n \geq 1$. Hence, $\nu_1(\mathcal{F}) = 0$, and so $\beta_1(\mathcal{F}) = 0$.

(c) Set $f(X, Y) := X^2Y + XY + X^2 + Y^2 + Y = 0$. Multiplying the equation $f(x, y) = 0$ by $\frac{1}{(x^2+x+1)^2}$ and setting $z := \frac{y}{x^2+x+1}$ yields that $z^2 + z = \frac{x^2}{(x^2+x+1)^2}$. In this case, we get that $B_1(F_n) = 4$ for all $n \geq 1$. Hence, $\nu_1(\mathcal{F}) = 0$, and so $\beta_1(\mathcal{F}) = 0$.

(d) Set $f(X, Y) := X^2Y + XY + X + Y^2 + Y = 0$. Multiplying the equation $f(x, y) = 0$ by $\frac{1}{(x^2+x+1)^2}$ and setting $z := \frac{y}{x^2+x+1}$ yields that $z^2 + z = \frac{x}{(x^2+x+1)^2}$. In this case, we obtain that $B_1(F_n) = 2(n + 1)$ for all $n \geq 1$. Hence, $\nu_1(\mathcal{F}) = 0$, and so $\beta_1(\mathcal{F}) = 0$.

□

Proposition 2.12 *The equation $f(X, Y) = X^2Y^2 + X^2Y + XY + X + Y = 0$ defines a quadratic recursive tower \mathcal{F}/\mathbb{F}_2 with $\beta_1(\mathcal{F}) = 0$. Moreover, for all $n \geq 2$, we have that*

$$B_1(F_n) = \frac{\alpha^{n-1}(\alpha^3 + 1) + (-1)^n(\alpha - 1)}{\sqrt{5}},$$

where $\alpha := \frac{\sqrt{5}+1}{2}$ is the golden ratio.

Proof We use the same method and notations as in Proposition 2.11 with $f(X, Y) = X^2Y^2 + X^2Y + XY + X + Y = 0$. Multiplying the equation $f(x, y) = 0$ by $\frac{x^2}{(x^2+x+1)^2}$ and setting $z := \frac{x^2y}{(x^2+x+1)}$ yields that

$$z^2 + z = \frac{x^3}{(x^2 + x + 1)^2}.$$

By the Artin–Schreier extensions theorem [15, Proposition 3.7.8], we have the following:

- (I) $(x = 0)$ splits in F , R_1 and R_2 lie above it, and $R_1 \cap \mathbb{F}_2(y) = (y = 0)$ and $R_2 \cap \mathbb{F}_2(y) = (y = \infty)$.
- (II) $(x = 1)$ is inert in F .
- (III) $(x = \infty)$ splits in F , R_3 and R_4 lie above it, $R_3 \cap \mathbb{F}_2(y) = (y = 0)$, and $R_4 \cap \mathbb{F}_2(y) = (y = 1)$.

By using (I)–(III), as in the proof of Proposition 2.7, one can easily show that the sequence \mathcal{F}/\mathbb{F}_2 is a quadratic tower over \mathbb{F}_2 . To estimate $B_1(F_n)$, for any $n \geq 1$, let

$$\begin{aligned} B_0(n-1) &:= \#\{P \in \mathbb{P}(F_n) : x_{n-1}(P) = 0\}, \\ B_1(n-1) &:= \#\{P \in \mathbb{P}(F_n) : x_{n-1}(P) = 1\}, \text{ and} \\ B_\infty(n-1) &:= \#\{P \in \mathbb{P}(F_n) : x_{n-1}(P) = \infty\}. \end{aligned}$$

By using (I)–(III), we obtain that

$$\begin{aligned} B_\infty(n-1) = B_0(n-2), \quad B_1(n-1) = B_\infty(n-2) \quad \text{and} \\ B_0(n-1) = B_0(n-2) + B_\infty(n-2) = B_0(n-2) + B_0(n-3). \end{aligned} \tag{6}$$

Notice that the sequences $\{B_0(n)\}_n \geq 0$ with $B_0(0) = 1, B_0(1) = 2$, and $\{B_1(n)\}_n \geq 1, \{B_\infty(n)\}_n \geq 0$ with $B_1(1) = B_1(2) = B_\infty(0) = B_\infty(1) = 1$ satisfy the Fibonacci recursion. Hence, one obtains that

$$B_\infty(n) = \frac{\alpha^{2n+2} + (-1)^n}{\sqrt{5}\alpha^{n+1}} \quad \text{where} \quad \alpha := \frac{\sqrt{5} + 1}{2}. \tag{7}$$

Now using (I)–(III) and applying Abhyankar’s lemma [15, Theorem 3.9.1] gives that for any rational place P of F_{n-1} , we have $x_{n-1}(P) \in \{0, \infty\}$, and so P splits in F_n . Conversely, if $x_{n-1}(P) \in \{0, \infty\}$, then P is a rational place of F_{n-1} and it splits in F_n . Hence, it follows from (6) and (7) that

$$\begin{aligned} B_1(F_n) = 2(B_0(n) + B_\infty(n)) &= 2(B_\infty(n+1) + B_\infty(n)) \\ &= \frac{\alpha^{n-1}(\alpha^3 + 1) + (-1)^n(\alpha - 1)}{\sqrt{5}}. \end{aligned}$$

Since $\alpha < 2 = [F_n : F_{n-1}]$ for any $n \geq 1$, we have that $\nu_1(\mathcal{F}) = 0$, and so $\beta_1(\mathcal{F}) = 0$. □

The following consequence follows from Theorem 2.9, Remark 2.10, and Propositions 2.11 and 2.12.

Corollary 2.13 *Suppose that $\mathcal{F} = (F_n)_{n \geq 0}$ is a quadratic recursive tower of function fields over \mathbb{F}_2 such that its basic function field F_1/\mathbb{F}_2 has four rational places. Then $\beta_1(\mathcal{F}) = 0$.*

2.4. $B_1(F) = 5$

In this subsection we suppose that the basic function field F/\mathbb{F}_2 has five rational places.

Theorem 2.14 *Suppose that \mathcal{F}/\mathbb{F}_2 is a potentially good quadratic recursive tower of function fields with the basic function field F/\mathbb{F}_2 having $B_1(F) = 5$. Up to isomorphism, \mathcal{F}/\mathbb{F}_2 can be defined by one of the following equations:*

- (1) $Y^2X + Y + X^2 + 1 = 0,$ (3) $X^2Y^2 + XY^2 + X + Y = 0,$
- (2) $X^2 + XY^2 + X + Y = 0,$ (4) $X^2Y^2 + X^2 + XY^2 + Y + 1 = 0.$

Proof Suppose that \mathcal{F}/\mathbb{F}_2 is a tower with the given assumptions and let F/\mathbb{F}_2 be its basic function field. By Theorem 2.2(iv), $F = \mathbb{F}_2(u, v)$ for some distinct $u, v \in \{x, y, z, t, w\}$ as in (4). Because of (4), the following hold:

- (a) $uv^2 + v = u^2 + 1$ for $(u, v) \in \{(x, y), (w, y)\},$
- (b) $u^2v^2 + u = v + 1$ for $(u, v) \in \{(x, z), (x, w)\},$
- (c) $u^2v^2 + u = v^2 + v$ for $(u, v) \in \{(x, t), (z, t), (t, w)\},$
- (d) $y^2z^2 + z^2 + zy^2 = y,$
- (e) $y^2t^2 + y^2t + y = t^2 + 1,$
- (f) $z^2w^2 + z^2 + z = w^2 + w.$

Suppose now that \mathcal{F}/\mathbb{F}_2 is defined by the polynomial $f(X, Y) \in \mathbb{F}_2[X, Y]$. Then $f(u', v') = 0$ for some distinct $u', v' \in \{A \cdot x, B \cdot y, C \cdot z, D \cdot t, E \cdot w \mid A, B, C, D, E \in GL(2, \mathbb{F}_2) \text{ for } i = 0, 1, 2, 3, 4, 5\}$ and $F = \mathbb{F}_2(u', v')$, by Theorem 1.10. Let $A_i \in GL(2, \mathbb{F}_2)$ as before. By Theorems 1.10 and 2.2(iv) (see also Section 2), we have the following cases:

- c.1. $f(X, Y) = \hat{f}_1(X, A_i \cdot Y)$ for some $0 \leq i \leq 5$, where $f_1(X, Y) := Y^2X + Y = X^2 + 1$ with $f_1(u, v) = 0$ for $(u, v) \in \{(x, y), (w, y)\}.$
 - (i) $\hat{f}_1(X, A_1 \cdot Y) = X^2 + XY^2 + X + Y = 0,$
 - (ii) $\hat{f}_1(X, A_2 \cdot Y) = X^2Y^2 + X + Y^2 + Y = 0,$
 - (iii) $\hat{f}_1(X, A_3 \cdot Y) = X^2Y^2 + XY^2 + X + Y = 0,$
 - (iv) $\hat{f}_1(X, A_4 \cdot Y) = X^2Y^2 + X^2 + XY^2 + Y + 1 = 0,$
 - (v) $\hat{f}_1(X, A_5 \cdot Y) = X^2Y^2 + X^2 + X + Y^2 + Y = 0,$ which is symmetric.
- c.2. $f(X, Y) = \hat{f}_2(X, A_i \cdot Y)$ for some $0 \leq i \leq 5$, where $f_2(X, Y) := X^2Y^2 + X + Y + 1 = 0$ with $f_2(u, v) = 0$ for $(u, v) \in \{(x, z), (x, w)\}.$ Note that $\hat{f}_2(A_1 \cdot X, A_1 \cdot (A_1 \cdot Y)) = \hat{f}_1(X, A_2 \cdot Y) = 0.$
- c.3. $f(X, Y) = \hat{f}_3(X, A_i \cdot Y)$ for some $0 \leq i \leq 5$, where $f_3(X, Y) := X^2Y^2 + X + Y^2 + Y = 0$ with $f_3(u, v) = 0$ for $(u, v) \in \{(x, t), (z, t), (t, w)\}.$ Note that $f_3(X, Y) = \hat{f}_2(X, A_2 \cdot Y) = 0.$

c.4. $f(X, Y) = \hat{f}_4(X, A_i \cdot Y)$ for some $0 \leq i \leq 5$, where $f_4(X, Y) := X^2Y^2 + Y^2 + YX^2 + X = 0$ with $f_4(y, z) = 0$. Note that $f_4(X, Y) = \hat{f}_1(A_2 \cdot X, A_2 \cdot Y) = 0$.

c.5. $f(X, Y) = \hat{f}_5(X, A_i \cdot Y)$ for some $0 \leq i \leq 5$, where $f_5(X, Y) := X^2Y^2 + XY^2 + Y + X^2 + 1 = 0$ with $f_5(t, y) = 0$. Note that $f_5(X, Y) = \hat{f}_1(X, A_4 \cdot Y) = 0$.

c.6. $f(X, Y) = \hat{f}_6(X, A_i \cdot Y)$ for some $0 \leq i \leq 5$, where $f_6(X, Y) := X^2Y^2 + X^2 + X + Y^2 + Y = 0$ with $f_6(z, w) = 0$. Note that $f_6(X, Y) = \hat{f}_1(X, A_5 \cdot Y) = 0$.

By Theorem 1.10, $f(X, Y) = 0$ must be one of the equations $f_1(X, Y) = 0$, c.1.(i)–(iv). We claim that the equation in c.1.(ii) does not define a tower over \mathbb{F}_2 . Obviously, if the claim holds, then we are done. To prove the claim first let $G_0 := \mathbb{F}_2(x_0)$ be the rational function field and $G_i = G_{i-1}(x_i)$ for all $i \geq 1$ with $f_1(x_{i-1}, A_2 \cdot x_i) = 0$. We have that

$$f_1(x_2, A_2 \cdot T) = \left(\frac{x_1 + x_0^2 + x_0 + 1}{x_0^2 + 1} \right) \left(\frac{T + x_0^2 + x_1}{x_0^2 + 1} \right) \left(T + \frac{(x_0^2 + 1)x_1}{x_0^2} + \frac{1}{x_0} \right).$$

Hence, $G_i = G_2$ for all $i \geq 2$, and so the claim follows. □

The following result is given in [16, Theorems 4.4 and 4.6]:

Proposition 2.15 *The equation $f(X, Y) = Y^2X + Y + X^2 + 1 = 0$ defines a quadratic tower $\mathcal{F} = (F_n)_{n \geq 0}$ over \mathbb{F}_2 with the following properties:*

(i) $9 \cdot 2^{n-2} \leq g(F_n) \leq (n - 1) \cdot 2^n + 1$ for all $n \geq 4$,

(ii) $\alpha^n \leq B_1(F_n) \leq 3 \cdot 2^n$, where $\alpha = \frac{\sqrt{5}+1}{2}$ is the golden ratio, for all $n \geq 0$.

We remark here that we do not know whether the equation given in Theorem 2.14(1) defines a quadratic tower \mathcal{F}/\mathbb{F}_2 with $\beta_1(\mathcal{F}) = 0$. We only have the bounds given in Proposition 2.15. Moreover, each of the equations (2)–(4) in Theorem 2.14 also defines a quadratic tower over \mathbb{F}_2 that behaves similarly to the tower in Proposition 2.15. Consequently, Theorem 1.4 holds. As a future work, one can study the invariants $\beta_r(\mathcal{F})$, for $r \geq 2$, of the towers defined by the equations given in Theorems 2.5, 2.9, and 2.14.

Acknowledgment

The first author was partially supported by the Scientific and Technological Research Council of Turkey (TÜBİTAK) under grant no: TBAG-111T234 and the second author was partially supported by TÜBİTAK under grant no: TBAG-112T011.

References

[1] Bassa A, Beelen P, Garcia A, Stichtenoth H. Towers of function fields over non-prime finite fields. *Moscow Math J* 2015; 15: 1-29.
 [2] Beelen P, Garcia A, Stichtenoth H. Towards a classification of recursive towers of function fields over finite fields. *Finite Fields Appl* 2006; 12: 56–77.

- [3] Garcia A, Stichtenoth H. A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound. *Invent Math* 1995; 121: 211–222.
- [4] Garcia A, Stichtenoth H. On the asymptotic behaviour of some towers of function fields over finite fields. *J Number Theory* 1996; 61: 248–273.
- [5] Garcia A, Stichtenoth H. Skew pyramids of function fields are asymptotically bad. In: Buchmann J, editor. *Coding Theory, Cryptography and Related Topics, Proceedings of a Conference in Guanajuato 1998*. Berlin, Germany: Springer-Verlag, 2000, pp. 111–113.
- [6] Garcia A, Stichtenoth H, Thomas M. On towers and composita of towers of function fields over finite fields. *Finite Fields Appl* 1997; 3: 257–274.
- [7] Geer van der G, Vlugt van der M. An asymptotically good tower of function fields over the field with eight elements. *Bull London Math Soc* 2002; 34: 291–300.
- [8] Hasegawa T. Asymptotic behavior of higher degree places in towers of function fields over finite fields. PhD, Waseda University, Tokyo, Japan, 2007.
- [9] Hess F, Stichtenoth H, Tutdere S. On invariants of towers of function fields over finite fields. *J Algebra Appl* 2013; 12: 1250190.
- [10] Husemöller D. *Elliptic Curves*. 2nd ed. Berlin, Germany: Springer-Verlag, 2004.
- [11] Lebacque P. Sur quelques propriétés asymptotiques des corps globaux. PhD, Université de Marseille II, Marseille, France, 2007 (in French).
- [12] Lenstra HW Jr. On a problem of Garcia, Stichtenoth, and Thomas. *Finite Fields Th App* 2002; 8: 166–170.
- [13] Ling S, Stichtenoth H, Yang. A class of Artin-Schreier towers with finite genus. *Bull Braz Math Soc New Series* 2005; 36: 393–401.
- [14] Maharaj H, Wulftange J. On the construction of tame towers over finite fields. *J Pure Appl Algebra* 2005; 199: 197–218.
- [15] Stichtenoth H. *Algebraic Function Fields and Codes*. 2nd ed. Berlin, Germany: Springer-Verlag, 2009.
- [16] Tutdere S. A recursive tower of function fields over \mathbb{F}_2 . MSc, Sabancı University, Turkey, 2009.
- [17] Tutdere S. On the asymptotic theory of towers of function fields over finite fields. PhD, Sabancı University, İstanbul, Turkey, 2012.