

1-1-2014

On a tower of Garcia and Stichtenoth

SEHER TUTDERE

Follow this and additional works at: <https://journals.tubitak.gov.tr/math>



Part of the [Mathematics Commons](#)

Recommended Citation

TUTDERE, SEHER (2014) "On a tower of Garcia and Stichtenoth," *Turkish Journal of Mathematics*: Vol. 38: No. 3, Article 2. <https://doi.org/10.3906/mat-1310-52>
Available at: <https://journals.tubitak.gov.tr/math/vol38/iss3/2>

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. For more information, please contact academic.publications@tubitak.gov.tr.

On a tower of Garcia and Stichtenoth

Seher TUTDERE*

Department of Mathematics, Gebze Institute of Technology, Çayırova Campus, Gebze, Kocaeli, Turkey

Received: 28.10.2013 • Accepted: 13.12.2013 • Published Online: 14.03.2014 • Printed: 11.04.2014

Abstract: In 2003, Garcia and Stichtenoth constructed a recursive tower $\mathcal{F} = (F_n)_{n \geq 0}$ of algebraic function fields over the finite field \mathbb{F}_q , where $q = l^r$ with $r \geq 1$ and $l > 2$ is a power of the characteristic of \mathbb{F}_q . They also gave a lower bound for the limit of this tower. In this paper, we compute the exact value of the genus of the algebraic function field F_n/\mathbb{F}_q for each $n \geq 0$. Moreover, we prove that when $q = 2^k$, with $k \geq 2$, the limit of the tower \mathcal{F} attains the lower bound given by Garcia and Stichtenoth.

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

1. Introduction

Let \mathbb{F}_q be a finite field and F/\mathbb{F}_q be an algebraic function field of one variable with the field \mathbb{F}_q as its full constant field. Throughout this paper, we shall simply refer to F/\mathbb{F}_q as a function field. Here we consider towers of function fields over \mathbb{F}_q (for the definition of a tower, see Section 2). The limit $\lambda(\mathcal{F})$ of a tower $\mathcal{F} = (F_n)_{n \geq 0}$ over \mathbb{F}_q is defined as

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

where $N(F_n)$ and $g(F_n)$ denote the number of rational places and the genus, respectively, of F_n/\mathbb{F}_q . Towers with $\lambda(\mathcal{F}) > 0$ are called *asymptotically good* towers. Such towers are quite useful in cryptography and coding theory. In particular, asymptotically good recursive towers are used to construct algebraic-geometry codes with good parameters (for the definition of a recursive tower, see Definition 2.1). The Drinfeld–Vladut bound says that $\lambda(\mathcal{F}) \leq q^{1/2} - 1$. By using recursive towers with limits attaining this bound, one can construct towers exceeding the Gilbert–Varshamov bound [8]. Moreover, the function fields in such towers have a large class number [1].

For a tower $\mathcal{F} = (F_n)_{n \geq 0}$ over \mathbb{F}_q , usually one can estimate the limit of the tower without knowing the precise value of the genus of each function field F_n/\mathbb{F}_q (for instance, see [4, 6, 7, 10]). There are very few towers for which one knows the exact value of the genus of F_n/\mathbb{F}_q (for instance, see [2, 5, 9]). However, knowing the exact value of the genus of F_n/\mathbb{F}_q is quite useful in some applications. For instance, in [1] it was shown that to have a good estimation for the class number of F_n/\mathbb{F}_q , it is good to know the exact value of the genus of F_n/\mathbb{F}_q . This is the main motivation of this paper. Here, our first aim is to compute the genus of F_n/\mathbb{F}_q (for

*Correspondence: stutdere@gmail.com

2010 AMS Mathematics Subject Classification: .

all $n \geq 0$) for a tower constructed by Garcia and Stichtenoth. This tower is defined as follows: let $q = l^r$ with $r \geq 1$ and $l > 2$ be a power of the characteristic of \mathbb{F}_q . Assume that $r \equiv 0 \pmod 2$ or $l \equiv 0 \pmod 2$. In [3, Theorem 3.11], Garcia and Stichtenoth proved that the polynomial

$$F(X, Y) = Y^{l-1} + (X + b)^{l-1} - 1 \in \mathbb{F}_q[X, Y], \text{ with } b \in \mathbb{F}_l^*,$$

defines a recursive tower \mathcal{F} over \mathbb{F}_q . They also showed that the limit of this tower satisfies the inequality $\lambda(\mathcal{F}) \geq 2/(l-2)$. Our second aim is to prove that when $q = 2^k$, with $k \geq 2$, the limit of the tower \mathcal{F} attains the lower bound given by Garcia and Stichtenoth.

2. Preliminaries

Throughout this paper, we use basic facts and notations as in [7]. We will consider (algebraic) function fields F/\mathbb{F}_q of one variable over \mathbb{F}_q . In all cases, \mathbb{F}_q will be the full constant field of F . We denote by $g(F)$, $N(F)$, and $\mathbb{P}(F)$ the genus, the number of rational places, and the set of all places of F/\mathbb{F}_q , respectively. 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 . We denote them by P_a and P_∞ , respectively. This means we have that $x(P_a) = a$ and $x(P_\infty) = \infty$.

Let E/F be a finite separable extension, and let 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 .

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 $n \rightarrow \infty$.

Definition 2.1 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 a nonconstant polynomial. Suppose that there exist elements $x_n \in F_n$ (for $n \geq 0$) such that

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

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

For a tower $\mathcal{F} = (F_n)_{n \geq 0}$ over \mathbb{F}_q , one has the following [4, Lemma 3.4]:

- (i) The sequence $(g(F_n)/[F_n : F_0])_{n \geq 0}$ is convergent in $\mathbb{R}^{>0} \cup \{\infty\}$. The limit of this sequence is called the *genus of tower* \mathcal{F} and it is denoted by $\gamma(\mathcal{F})$.
- (ii) The sequence $(N(F_n)/[F_n : F_0])_{n \geq 0}$ is convergent in $\mathbb{R}^{\geq 0}$. The limit of this sequence is called the *splitting rate* of \mathcal{F} and it is denoted by $\nu(\mathcal{F})$.

Hence, by using (i) and (ii) it is clear that the sequence $(N(F_n)/g(F_n))_{n \geq 0}$ converges in $\mathbb{R}^{\geq 0}$. Its limit is called the *limit* of the tower \mathcal{F} and denoted by $\lambda(\mathcal{F})$. By definition, $\lambda(\mathcal{F}) = \nu(\mathcal{F})/\gamma(\mathcal{F})$.

A tower $\mathcal{F} = (F_n)_{n \geq 0}$ over \mathbb{F}_q is said to be a *tame* tower if all extensions F_{n+1}/F_n are tame (i.e. all ramification indices in F_{n+1}/F_n are coprime to the characteristic of \mathbb{F}_q). Moreover, we recall that for any tower \mathcal{F} over \mathbb{F}_q the set

$$R(\mathcal{F}) := \{P \in \mathbb{P}(F_0) : P \text{ is ramified in } F_n \text{ for some } n \geq 1\}$$

is called the *ramification locus* of \mathcal{F} .

In this paper, we will study the following tame tower introduced by Garcia and Stichtenoth in [3, Section 3]:

Theorem 2.2 *Let $q = l^r$ with $r \geq 1$ and $l > 2$ be a power of the characteristic of \mathbb{F}_q . Assume that*

$$r \equiv 0 \pmod{2} \text{ or } l \equiv 0 \pmod{2}.$$

Then the polynomial

$$F(X, Y) = Y^{l-1} + (X + b)^{l-1} - 1 \in \mathbb{F}_q[X, Y], \text{ with } b \in \mathbb{F}_l^*, \tag{2.1}$$

defines a recursive tower $\mathcal{F} = (F_n)_{n \geq 0}$ over \mathbb{F}_q with the following properties:

- (i) $[F_n : F_0] = (l - 1)^n$ for all $n \geq 0$.
- (ii) The place $(x_0 = \infty) \in \mathbb{P}(F_0)$ splits completely in \mathcal{F} .
- (iii) Letting $F = F_0 := \mathbb{F}_q(x_0)$ be the rational function field, we have that

$$R(\mathcal{F}) = \{P \in \mathbb{P}(F_0) : x_0(P) = \alpha \text{ for some } \alpha \in \mathbb{F}_l\}.$$

- (iv) The genus of \mathcal{F} satisfies the inequality $\gamma(\mathcal{F}) \leq (l - 2)/2$.
- (v) $\lambda(\mathcal{F}) \geq 2/(l - 2)$.

Proof For the proof, see [3, Theorem 3.11 and Proposition 3.9]. □

3. Main results

From now on, $\mathcal{F} = (F_n)_{n \geq 0}$ will denote the tower given in Theorem 2.2.

Theorem 3.1 *For all $n \geq 0$, we have that*

$$g(F_n) = \begin{cases} \binom{l-2}{2}(l-1)^n - \frac{l}{2}(l-1)^{n/2} + 1 & \text{if } n \equiv 0 \pmod{2} \\ \binom{l-2}{2}(l-1)^n - (l-1)^{(n+1)/2} + 1 & \text{if } n \equiv 1 \pmod{2}. \end{cases}$$

We prove Theorem 3.1 via the Lemmas 3.2, 3.3, and 3.4. First, let

$$f(X) := -(X + b)^{l-1} + 1 \in \mathbb{F}_q[X], \text{ with } b \in \mathbb{F}_l^*.$$

Since the tower \mathcal{F} is recursively defined by (2.1), we can set $F_0 = \mathbb{F}_q(x_0)$ and $F_{n+1} = F_n(x_{n+1})$ where

$$x_{n+1}^{l-1} = f(x_n) \quad \text{for all } n \geq 0. \tag{3.1}$$

Note that $f(\alpha) = 0$ if and only if $\alpha \in \mathbb{F}_l \setminus \{-b\}$. Hence, by Kummer’s extension theorem [7, pp. 122] and Kummer’s theorem [7, pp. 86], we have the following ramification structure in $F_1/\mathbb{F}_q(x_0)$ and $F_1/\mathbb{F}_q(x_1)$:

- (1) Any place $(x_0 = \alpha) \in \mathbb{P}(F_0)$, with $\alpha \in \mathbb{F}_l \setminus \{-b\}$, is totally ramified in F_1 . If $P_\alpha \in \mathbb{P}(F_1)$ is a place lying above $(x_0 = \alpha)$, then $x_1(P_\alpha) = 0$.
- (2) The place $(x_0 = -b) \in \mathbb{P}(F_0)$ splits completely in F_1 . If $P \in \mathbb{P}(F_1)$ is a place lying above $(x_0 = -b)$, then $x_1(P) = \alpha$ for some $\alpha \in \mathbb{F}_l^*$.

From now on, the numbers in the figures will denote the corresponding ramification indices. To sum up (1) and (2), we have the following:

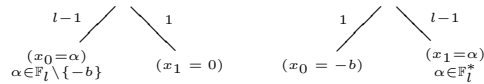


Figure 1. Ramification structure in $F_1/\mathbb{F}_q(x_0)$ and $F_1/\mathbb{F}_q(x_1)$.

Lemma 3.2 Let $S := \{P \in \mathbb{P}(F_0) : x_0(P) = \alpha \text{ for some } \alpha \in \mathbb{F}_l \setminus \{-b\}\}$. All $P \in S$ are totally ramified in \mathcal{F} .

Proof Let $P \in S$. It follows from Eq. (3.1) that for any $Q_n \in \mathbb{P}(F_n)$, $n \geq 1$, $Q_n|P$, we have $x_n(Q_n) = 0$. Hence, by applying Abhyankar’s lemma [7, pp. 137] in Figure 2, we obtain that P is totally ramified in F_n for all $n \geq 1$.

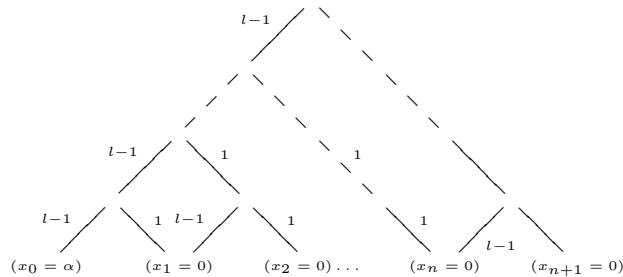


Figure 2. Ramification of $(x_0 = \alpha)$ in \mathcal{F} .

□

Lemma 3.3 Let $P := (x_0 = -b) \in \mathbb{P}(F_0)$ and Q be a place of F_n/\mathbb{F}_q lying above P , for some $n \geq 1$. We have the following cases:

- (i) $x_n(Q) \in \mathbb{F}_l^*$. In this case, $e(Q|P) = 1$.

(ii) $x_n(Q) = 0$. Then there exists $1 \leq k \leq n$ such that at $P' := Q \cap F_k$ we have $x_k(P') = \alpha$ for some $\alpha \in \mathbb{F}_l^* \setminus \{-b\}$ and

$$x_j(Q) = -b \quad \text{for all } 0 \leq j \leq k-1.$$

In this case, if $n < 2k + 1$, then

$$e(Q|P) = 1.$$

If $n \geq 2k + 1$, for any $P'' \in \mathbb{F}_{2k}$ with $P''|P'|P$, we have

$$e(Q|P) = e(Q|P'') = (l-1)^{n-2k}.$$

Proof It follows immediately from Eq. (3.1) and Figure 1 that $x_n(Q) \in \mathbb{F}_l$. Using Figure 1 and applying Abhyankar's lemma [7, pp. 137] in Figure 3 yields the desired results in (i) and (ii).

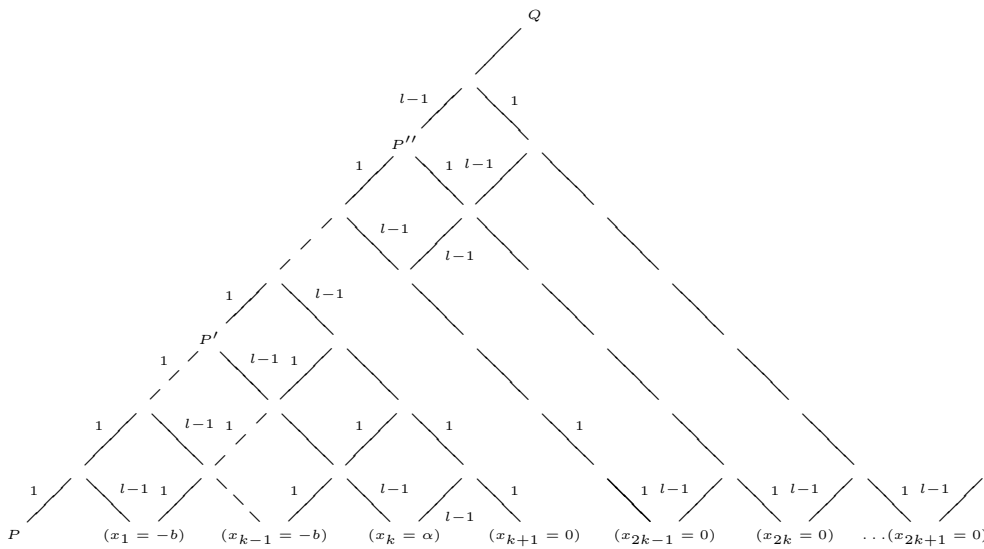


Figure 3. Ramification of $(x_0 = -b)$ in \mathcal{F} .

□

Lemma 3.4 For any $k \geq 0$, set

$$R_k := \{P \in \mathbb{P}(F_k) : x_k(P) = \alpha \text{ for some } \alpha \in \mathbb{F}_l^* \setminus \{-b\}\}.$$

Then the following hold:

- (i) For all $k \geq 1$, the place $(x_k = \alpha)$ of $\mathbb{F}_q(x_k)/\mathbb{F}_q$, with $\alpha \in \mathbb{F}_l^* \setminus \{-b\}$, is totally ramified in F_k .
- (ii) $\#R_k = l - 2$ and $\deg P = 1$ for all $P \in R_k$ with $k \geq 0$.
- (iii) For any $k \geq 0$, we have that

$$\sum_{\substack{Q \in \mathbb{P}(F_n) \\ Q|P \\ P \in R_k}} \deg Q = \begin{cases} (l-1)^{n-k} & \text{if } n < 2k + 1 \\ (l-1)^k & \text{if } n \geq 2k + 1. \end{cases}$$

Proof (i) For $k = 1$, it is clear from Figure 1. For $k \geq 2$, let $P \in R_k$. It follows from Eq. (3.1) (or see Figure 1) that $(x_0(P) = -b)$. Hence, by applying Abhyankar’s lemma [7, pp. 137] in Figure 3, we obtain the desired result.

(ii) For $k = 0$, we have $\#R_0 = l - 2$. For $k \geq 1$, as by (i) each place $(x_k = \alpha)$ is totally ramified in F_k , each has only one extension in F_k . Thus, the result follows.

(iii) Let $P \in R_k$ for some $k \geq 0$ and Q be a place of F_n lying above P , for some $n \geq k$. If $k = 0$, then by Lemma 3.2, P is totally ramified in F_n , and so (iii) holds. Now suppose that $k \geq 1$. Then it follows from Eq. (3.1) that

$$\begin{aligned} x_k(Q) &= x_k(P) = \alpha \quad \text{for some } \alpha \in \mathbb{F}_l^* \setminus \{-b\}, \\ x_i(Q) &= -b \quad \text{for all } i < k, \text{ and} \\ x_i(Q) &= 0 \quad \text{for all } k \leq n. \end{aligned}$$

By (ii), $\deg P = 1$. By Lemma 3.3(ii), for all $k \leq n \leq 2k$ the place P is unramified in F_n . Hence, by using fundamental equality [7, pp. 74] and Theorem 2.2(i),

$$\sum_{\substack{Q \in \mathbb{P}(F_n) \\ Q|P}} \deg Q = \sum_{\substack{Q \in \mathbb{P}(F_n) \\ Q|P}} f(Q|P) \deg P = [F_n : F_k] = (l - 1)^{n-k}.$$

Now suppose that $n \geq 2k + 1$. Let $R = Q \cap F_{2k}$. By applying Lemma 3.3 with $P'' := R$, we obtain that $e(Q|R) = (l - 1)^{n-2k} = [F_n : F_{2k}]$. That means that R is totally ramified in F_n for all $n \geq 2k + 1$, i.e. R has only one extension in F_n , which is Q and $\deg R = \deg Q$. Since P is unramified in F_{2k} , again by applying fundamental equality [7, pp. 74] and Theorem 2.2, we have that

$$\sum_{\substack{Q \in \mathbb{P}(F_n) \\ Q|P}} \deg Q = \sum_{\substack{R \in \mathbb{P}(F_{2k}) \\ R|P}} \deg R = \sum_{\substack{R \in \mathbb{P}(F_{2k}) \\ R|P}} f(R|P) \deg P = [F_{2k} : F_k] = (l - 1)^k.$$

□

Now we give the proof of Theorem 3.1. We first recall from [7, Definition 3.4.3] that the different of any finite separable extension of function fields F'/F is defined as follows:

$$\text{Diff}(F'/F) = \sum_{P \in \mathbb{P}(F)} \sum_{\substack{Q \in \mathbb{P}(F') \\ Q|P}} d(Q|P)Q.$$

Proof [Proof of Theorem 3.1] We know from Theorem 2.2(iii) that

$$R(\mathcal{F}) = \{P \in \mathbb{P}(F_0) : x_0(P) = \alpha \text{ for some } \alpha \in \mathbb{F}_l\}.$$

Moreover, since the tower \mathcal{F} is tame, for any $P \in \mathbb{P}(F_0)$ and $Q \in \mathbb{P}(F_n)$ with $Q|P$, by Dedekind’s different theorem [7, pp. 100] the different exponent of $Q|P$ is

$$d(Q|P) = e(Q|P) - 1.$$

Hence, the degree of the different of F_n/F_0 is

$$\deg \text{Diff}(F_n/F_0) = \sum_{P \in R(\mathcal{F})} \sum_{\substack{Q \in \mathbb{P}(F_n) \\ Q|P}} (e(Q|P) - 1) \deg Q. \tag{3.2}$$

By Lemma 3.2, all places P of F_0 with $x_0(P) \in \mathbb{F}_l \setminus \{-b\}$ are totally ramified in \mathcal{F} , and so for any $Q \in \mathbb{P}(F_n)$ with $Q|P$, we have that

$$e(Q|P) = [F_n : F_0] = (l - 1)^n. \tag{3.3}$$

Now let $Q \in \mathbb{P}(F_n)$ and $P = (x_0 = -b) \in \mathbb{P}(F_0)$ such that $Q|P$. Then by Lemma 3.3, we have the following situations:

(*) $x_n(Q) \in \mathbb{F}_l^*$ and $d(Q|P) = e(Q|P) - 1 = 0$,

(**) $x_n(Q) = 0$. In this case, there exists $1 \leq k < n$ such that at $P' := Q \cap F_k$, we have $x_k(P') = \alpha \in \mathbb{F}_l^* \setminus \{-b\}$. Hence, P' is in the set of R_k given in Lemma 3.4. Conversely, for any $P' \in R_k$, with $1 \leq k \leq n$, it follows from Eq. (3.1) that $P'| (x_0 = -b)$. By Lemma 3.3(ii), when $n < 2k + 1$, we have $d(Q|P) = e(Q|P) - 1 = 0$. When $n \geq 2k + 1$, by using Lemma 3.3(ii), we obtain that

$$\begin{aligned} d(Q|P) &= e(Q|P) - 1 = (l - 1)^{n-2k} - 1 \\ &= e(Q|P') - 1 = d(Q|P'). \end{aligned} \tag{3.4}$$

Now let

$$A := \sum_{\substack{P \in R(\mathcal{F}) \\ x_0(P) = -b}} \sum_{Q|P} d(Q|P) \deg Q.$$

Then by using Eq. (3.4), (*), (**), and Lemma 3.4, we get the following:

$$\begin{aligned} A &= \sum_{k=1}^{\lfloor \frac{n-1}{2} \rfloor} \sum_{\substack{P' \in R_k \\ Q|P'}} d(Q|P') \deg Q \\ &= \sum_{k=1}^{\lfloor \frac{n-1}{2} \rfloor} \#R_k ((l - 1)^{n-2k} - 1)(l - 1)^k \\ &= (l - 2) \left((l - 1)^n \sum_{k=0}^{\lfloor \frac{n-1}{2} \rfloor - 1} \frac{1}{(l - 1)^{k+1}} - \sum_{k=0}^{\lfloor \frac{n-1}{2} \rfloor - 1} (l - 1)^{k+1} \right) \\ &= (l - 2)(l - 1)^{n-1} \left(\frac{1}{(l - 1)^{\lfloor \frac{n-1}{2} \rfloor}} - 1 \right) \left(\frac{l - 1}{2 - l} \right) - \\ &\quad (l - 2)(l - 1) \left(\frac{(l - 1)^{\lfloor \frac{n-1}{2} \rfloor} - 1}{l - 2} \right) \\ &= -(l - 1)^{n - \lfloor \frac{n-1}{2} \rfloor} + (l - 1)^n - (l - 1)^{\lfloor \frac{n-1}{2} \rfloor + 1} + (l - 1). \end{aligned} \tag{3.5}$$

Now let Q be a place of F_n . By using Theorem 2.2(iii) and combining (3.2), (3.3), and (3.5), we obtain for all $n \geq 1$

$$\begin{aligned} \deg \text{Diff}(F_n/F_0) &= \sum_{\substack{P \in R(\mathcal{F}) \\ x_0(P) \in \mathbb{F}_l \setminus \{-b\}}} \sum_{Q|P} d(Q|P) \deg Q + \sum_{\substack{P \in R(\mathcal{F}) \\ x_0(P) = -b}} \sum_{Q|P} d(Q|P) \deg Q \\ &= (l-1)[(l-1)^n - 1] - (l-1)^{n - \lfloor \frac{n-1}{2} \rfloor} + (l-1)^n - \\ &\quad (l-1)^{\lfloor \frac{n-1}{2} \rfloor + 1} + (l-1) \\ &= l(l-1)^n - (l-1)^{n - \lfloor \frac{n-1}{2} \rfloor} - (l-1)^{\lfloor \frac{n-1}{2} \rfloor + 1} \\ &= \begin{cases} l(l-1)^n - l(l-1)^{n/2} & \text{if } n \equiv 0 \pmod{2} \\ l(l-1)^n - 2(l-1)^{(n+1)/2} & \text{if } n \equiv 1 \pmod{2}. \end{cases} \end{aligned}$$

Now by using the Hurwitz genus formula [7, pp.99] for the extension F_n/F_0 , the desired result follows:

$$\begin{aligned} 2g(F_n) - 2 &= [F_n : F_0](2g(F_0) - 2) + \deg \text{Diff}(F_n/F_0) \\ &= (l-1)^n(2g(F_0) - 2) + \deg \text{Diff}(F_n/F_0) \\ &= \begin{cases} (l-2)(l-1)^n - l(l-1)^{n/2} & \text{if } n \equiv 0 \pmod{2} \\ (l-2)(l-1)^n - 2(l-1)^{(n+1)/2} & \text{if } n \equiv 1 \pmod{2}. \end{cases} \end{aligned}$$

□

The following corollary is an immediate consequence of Theorem 3.1:

Corollary 3.5 *The genus of the tower \mathcal{F}/\mathbb{F}_q is*

$$\gamma(\mathcal{F}) = \frac{l-2}{2}.$$

Next we show that when $q = 2^k$ with $k \geq 2$ the limit of the tower \mathcal{F} over \mathbb{F}_q attains the Garcia and Stichtenoth lower bound given in Theorem 2.2(v).

Theorem 3.6 *Suppose that $r = 1$, i.e. l is a power of 2 and $q = l$. Then*

$$\lambda(\mathcal{F}) = \frac{2}{l-2}.$$

Proof We know that $\lambda(\mathcal{F}) = \nu(\mathcal{F})/\gamma(\mathcal{F})$. As $\gamma(\mathcal{F})$ is given in Corollary 3.5, it is enough to compute $\nu(\mathcal{F})$. For this, we need to estimate $N(F_n)$ for all $n \geq 0$. Since $q = l$ and each rational place of F_n/\mathbb{F}_q lies over a rational place of F_0/F_q , we have that

$$N(F_n) = \sum_{\substack{Q \in \mathbb{P}(F_n) \\ x_0(Q) \in \mathbb{F}_l \setminus \{-b\}}} 1 + \sum_{\substack{Q \in \mathbb{P}(F_n) \\ x_0(Q) = -b}} 1 + \sum_{\substack{Q \in \mathbb{P}(F_n) \\ x_0(Q) = \infty}} 1. \tag{3.6}$$

Let $P \in \mathbb{P}(F_0)$ be a rational place and $n \geq 1$. If P is totally ramified in F_n , then P has only one rational extension in F_n . If P splits completely in F_n , then P has $[F_n : F_0]$ rational extensions in F_n . Hence, by

Lemmas 3.2, 3.3, and 3.4 and Theorem 2.2(ii), for any $n, k \geq 1$ with $n \geq k$, we have

$$\sum_{\substack{Q \in \mathbb{P}(F_n) \\ x_0(Q) \in \mathbb{F}_l \setminus \{-b\}}} 1 = l - 1, \quad \sum_{\substack{Q \in \mathbb{P}(F_n) \\ x_0(Q) = \infty}} 1 = (l - 1)^n, \quad \text{and} \tag{3.7}$$

$$\sum_{\substack{Q \in \mathbb{P}(F_n) \\ x_0(Q) = -b}} 1 \leq \sum_{k=1}^{n-1} \sum_{P_k \in R_k} \sum_{\substack{Q \in \mathbb{P}(F_n) \\ Q|P_k}} 1 \leq B, \quad \text{where } B := \sum_{k=1}^{n-1} \sum_{P_k \in R_k} \sum_{\substack{Q \in \mathbb{P}(F_n) \\ Q|P_k}} \deg Q.$$

By using Lemma 3.4(iii), we obtain the following:

$$\begin{aligned} B &\leq \sum_{k=1}^{\lfloor \frac{n-1}{2} \rfloor} \#R_k \cdot (l - 1)^k + \sum_{k=\lfloor \frac{n-1}{2} \rfloor + 1}^{n-1} \#R_k \cdot (l - 1)^{n-k} \\ &= (l - 2) \left(\sum_{k=0}^{\lfloor \frac{n-1}{2} \rfloor - 1} (l - 1)^{k+1} + (l - 1)^n \sum_{k=\lfloor \frac{n-1}{2} \rfloor + 1}^n \frac{1}{(l - 1)^k} \right) \\ &= (l - 2)(l - 1) \left[\frac{(l - 1)^{\lfloor \frac{n-1}{2} \rfloor - 1} - 1}{l - 2} \right] + \\ &\quad (l - 2)(l - 1)^n \left[\frac{1}{(l - 1)^{n+1}} - \frac{1}{(l - 1)^{\lfloor \frac{n-1}{2} \rfloor + 1}} \right] \left(\frac{l - 1}{2 - l} \right) \\ &= (l - 1) \left[(l - 1)^{\lfloor \frac{n-1}{2} \rfloor} - 1 \right] - \\ &\quad (l - 1)^{n+1} \left[\frac{1}{(l - 1)^{n+1}} - \frac{1}{(l - 1)^{\lfloor \frac{n-1}{2} \rfloor + 1}} \right] \\ &= (l - 1)^{\lfloor \frac{n-1}{2} \rfloor + 1} - (l - 1) - 1 + (l - 1)^{n - \lfloor \frac{n-1}{2} \rfloor} \\ &= (l - 1)^{\lfloor \frac{n-1}{2} \rfloor + 1} + (l - 1)^{n - \lfloor \frac{n-1}{2} \rfloor} - l. \end{aligned} \tag{3.8}$$

Now by substituting each value of (3.7) and (3.8) for the sums involved in Eq. (3.6), the following follows:

$$(l - 1)^n + (l - 1) \leq N(F_n) \leq (l - 1)^n + (l - 1) + A_n,$$

where

$$A_n := \begin{cases} l(l - 1)^{n/2} - l & \text{if } n \equiv 0 \pmod{2} \\ 2(l - 1)^{(n+1)/2} - l & \text{if } n \equiv 1 \pmod{2}. \end{cases}$$

Hence, the splitting rate of \mathcal{F}/\mathbb{F}_q is

$$\nu(\mathcal{F}) = \lim_{n \rightarrow \infty} \frac{N(F_n)}{[F_n : F_0]} = 1. \tag{3.9}$$

Now by using Corollary 3.5 and (3.9) we obtain the desired result. \square

We here conjecture that the limit of the tower \mathcal{F} attains the Garcia and Stichtenoth lower bound for all $r \geq 1$.

References

- [1] Ballet S, Rolland R. Lower bounds on the class number of algebraic function fields defined over any finite field. *J Théor Nombres Bordeaux* 2012; 24: 505–540.
- [2] Garcia A, Stichtenoth H. A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound. *Invent Math* 1995; 121: 211–222.
- [3] Garcia A, Stichtenoth H, Rück HG. On tame towers over finite fields. *J Reine Angew Math* 2003; 557: 53–80.
- [4] Garcia A, Stichtenoth H, Thomas M. On towers and composita of towers of function fields over finite fields. *Finite Fields Th App* 1997; 3: 257–274.
- [5] Gerard VDG, Vlugt MVD. An asymptotically good tower of curves over the field with eight elements. *B Lond Math Soc* 2002; 34.03: 291–300.
- [6] Hess F, Stichtenoth H, Tutdere S. On invariants of towers of function fields over finite fields. *J Algebra Appl* 2013; 12 477–487.
- [7] Stichtenoth H. *Algebraic Function Fields and Codes*. 2nd ed. Berlin, Germany: Springer, 2009.
- [8] Tsfasman MA, Vladut SG, Zink T. Modular curves, Shimura curves and Goppa codes, better than the Varshamov-Gilbert bound. *Math Nachr* 1982; 109: 21–28.
- [9] Tutdere S. On the asymptotic theory of towers of function fields over finite fields. PhD, Sabancı University, İstanbul, Turkey, 2012.
- [10] Wulftange J. *Zahme Türme algebraischer Funktionenkörper*. PhD, Essen University, Essen, Germany, 2002.