Asymptotically good towers of function fields with small p-rank

Nurdagül Anbar[1], Henning Stichtenoth[1], Seher Tutdere[2]

[1]Sabancı University
MDBF, Orhanlı, Tuzla, 34956 İstanbul, Turkey
E-mail: nurdagulanbar2@gmail.com
E-mail: henning@sabanciuniv.edu
[2]Balıkesir University
Department of Mathematics, Altıeylül, 10145, Balıkesir, Turkey
E-mail: stutdere@gmail.com

Abstract

Over any quadratic finite field we construct function fields of large genus that have simultaneously many rational places, small p-rank, and many automorphisms.

keywords: towers of function fields, rational places, genus of a function field, automorphisms of function fields, p-rank
MSC[2010]: 11G20, 14G50, 14H05,

1 Introduction

Let $\mathbb{F}_q$ be the finite field of characteristic $p > 0$ and cardinality q, and let F be a function field over $\mathbb{F}_q$ with full constant field $\mathbb{F}_q$. We denote by $g(F)$ the genus and by $N(F)$ the number of rational places of $F/\mathbb{F}_q$. By a *tower of function fields* we mean an infinite sequence $\mathcal{F} = (F_i)_{i\geq 0}$ of function fields with full constant field $\mathbb{F}_q$ such that $F_0 \subseteq F_1 \subseteq F_2 \subseteq \ldots$, all extensions F_{i+1}/F_i are separable, and $g(F_i) \to \infty$ for $i \to \infty$. It is easy to see that the limit

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

exists, and it is called the *limit* of the tower [18, Section 7.2]. The Drinfeld–Vladut bound [20] implies that

$$0 \leq \lambda(\mathcal{F}) \leq \sqrt{q} - 1.$$

A tower $\mathcal{F}$ is called *asymptotically good* if $\lambda(\mathcal{F}) > 0$; otherwise, it is called *asymptotically bad*. Moreover, if $\lambda(\mathcal{F}) = \sqrt{q} - 1$, then $\mathcal{F}$ is called *asymptotically optimal*. Asymptotically good towers exist and they have been studied extensively, see [2, 3, 6, 7, 8, 10, 11, 12, 18] and the references therein. We remark that it is a non-trivial task to construct asymptotically good towers. In fact, most known examples of explicitly constructed towers are asymptotically bad. The reason is that $g(F_i)$ often increases too fast or $N(F_i)$ does not grow fast enough.

An important invariant of a function field $F/\mathbb{F}_q$ is its *p-rank* $s(F)$ (which is sometimes called the *Hasse–Witt invariant* of F), see [13, Section 6.7]. It is defined as follows: Let F' be the constant field extension of F with the algebraic closure $\bar{\mathbb{F}}_q$ of $\mathbb{F}_q$. The group of divisor classes of F' which are annihilated by p is a finite abelian group of exponent p, and $s(F)$ is defined as the dimension as a $\mathbb{F}_p$-vector space of this group. By [13, Theorem 6.96], the inequality $0 \le s(F) \le g(F)$ holds for every function field F over $\mathbb{F}_q$.

Another characterization of $s(F)$ is as follows. Let $L_F(t) = \sum_{i=0}^{2g(F)} a_i t^i \in \mathbb{Z}[t]$ denote the L-polynomial of $F/\mathbb{F}_q$, see [18, Chapter 5.1]. The coefficients a_i are divisible by q for $i = g(F)+1, \ldots, 2g(F)$. Let $\bar{L}(t) \in \mathbb{F}_p[t]$ be its reduction modulo p. Then $s(F)$ is equal to the degree of $\bar{L}(t)$, see [19]. This degree is 'in general' close to the genus $g(F)$, and $\deg(\bar{L}(t)) = g(F)$ if and only if the coefficient $a_{g(F)}$ is not divisible by p. In this sense, 'most' function fields are *ordinary*; i.e., $s(F) = g(F)$. We refer to [1] for the proof of the fact that there are 'few' curves of fixed genus g over $\mathbb{F}_q$ with p-rank less than g.

For a tower $\mathcal{F} = (F_i)_{i\ge 0}$ of function fields over $\mathbb{F}_q$, the quantity

$$\sigma(\mathcal{F}) := \liminf_{i\to\infty} s(F_i)/g(F_i)$$

is called the *asymptotic p-rank* of $\mathcal{F}$. Clearly we have the inequality

$$0 \le \sigma(\mathcal{F}) \le 1.$$

The asymptotic p-rank was introduced by Cramer et al. [9] to analyse the behaviour of various constructions related to multi-party computations and fast multiplication algorithms. According to their construction, it is desirable to have *asymptotically good towers $\mathcal{F}$ with $\sigma(\mathcal{F})$ as small as possible.* The aim of our paper is to construct such towers. By considering the above remarks, one may expect that for a 'general' tower of function fields, the asymptotic p-rank should be equal or close to 1.

We first recall some known results from the literature. The tower over a *quadratic* field $\mathbb{F}_q$ (i.e., q is a square) given by Garcia and Stichtenoth in [12] is asymptotically optimal and its asymptotic p-rank is $1/(\sqrt{q}+1)$, see [5, 9]. This is the smallest value of an asymptotic p-rank that has been hitherto observed among asymptotically good towers over $\mathbb{F}_q$. The asymptotic p-rank of some asymptotically good towers over a *cubic* field $\mathbb{F}_q$ (i.e., $q = p^{3a}$) has been determined in [2, 5], their p-rank values are close to $1/4$.

In Section 4 we will construct asymptotically good towers over quadratic fields whose asymptotic p-rank is significantly smaller than the asymptotic p-rank of the above-mentioned towers. More specifically, we will show in Theorem 4.3 that:

For any $\epsilon > 0$, there exists an asymptotically good tower $\mathcal{F}$ over $\mathbb{F}_q$ such that its asymptotic p-rank is $\sigma(\mathcal{F}) < \epsilon$.

We will also consider towers of function fields that have many automorphisms. Recall that an *automorphism* of a function field $F/\mathbb{F}_q$ is a field automorphism of F that fixes every element of $\mathbb{F}_q$. It is known that the automorphism group $\mathrm{Aut}(F)$ of $F/\mathbb{F}_q$ is always finite, see [13, Theorem 11.56]. By [15], function fields of fixed genus $g \geq 3$ having non-trivial automorphism groups are rare; i.e., in general $|\mathrm{Aut}(F)| = 1$ for function fields of fixed genus $g \geq 3$. For large classes of function fields (for instance if $\mathrm{Aut}(F)$ is abelian or if the order of $\mathrm{Aut}(F)$ is prime to p), there is a *linear* upper bound

$$|\mathrm{Aut}(F)| \leq A \cdot g(F)$$

with an absolute constant $A > 0$, see [14, 16]. A similar situation can be observed among the known examples of explicitly constructed towers. We will show in Section 4 (see Theorem 4.9) that over quadratic fields $\mathbb{F}_q$ the following holds:

For any $\epsilon > 0$, there exist a constant $B > 0$, depending on q, and an asymptotically good tower $\mathcal{F} = (F_i)_{i \geq 0}$ over $\mathbb{F}_q$ such that

$$\sigma(\mathcal{F}) < \epsilon \quad \textit{and} \quad |\mathrm{Aut}(F_i)| \geq B \cdot g(F_i) \ \ \textit{for all } i \geq 0.$$

In other words, there exist function fields over $\mathbb{F}_q$ of *large genus* which have simultaneously *many rational points, many automorphisms* and *small p-rank.*

2 Preliminaries

Let $E \supseteq F$ be a finite separable extension of function fields. Denote by $\mathbb{P}(F)$ the set of places of F. For a place $Q \in \mathbb{P}(E)$ lying above $P \in \mathbb{P}(F)$, we write $Q|P$ and denote by $e(Q|P)$ the ramification index and by $d(Q|P)$ the different exponent of $Q|P$. The genera of F and E are then related as follows, see [18, Theorem 3.4.13].

Lemma 2.1. *[Hurwitz genus formula] Let E/F be a finite separable extension of function fields over the same constant field $\mathbb{F}_q$. Then*

$$2g(E) - 2 = [E : F] \cdot (2g(F) - 2) + \sum_{P \in \mathbb{P}(F)} \sum_{Q \in \mathbb{P}(E),\, Q|P} d(Q|P) \cdot \deg Q \ .$$

For the p-ranks of F and E, such a formula does not hold in general. However, in the important special case where E/F is a Galois extension of degree p, one has the following formula, see [17, Theorem 2].

Lemma 2.2. *[Deuring–Shafarevich formula] Let E/F be a Galois extension of degree p of function fields over the same constant field $\mathbb{F}_q$. Then the p-ranks of F and E satisfy*

$$s(E) - 1 = p \cdot (s(F) - 1) + \sum_{P \in \mathbb{P}(F)} \sum_{Q \in \mathbb{P}(E),\, Q|P} (e(Q|P) - 1)) \cdot \deg Q \ .$$

We will need the following generalization of Lemma 2.2:

Lemma 2.3. *Let E/F be an extension of function fields of degree $[E : F] = p^m$ over the same constant field $\mathbb{F}_q$. Assume that there exist intermediate fields $F = F_0 \subseteq F_1 \subseteq \cdots F_{n-1} \subseteq F_n = E$ such that all extensions F_{i+1}/F_i are Galois. Then the p-ranks of F and E satisfy*

$$s(E) - 1 = [E : F] \cdot (s(F) - 1) + \sum_{P \in \mathbb{P}(F)} \sum_{Q \in \mathbb{P}(E),\, Q|P} (e(Q|P) - 1)) \cdot \deg Q \ .$$

Proof. We can refine the sequence $F = F_0 \subseteq F_1 \subseteq \cdots F_{n-1} \subseteq F_n = E$ such that all extensions F_{i+1}/F_i are Galois of degree p. Then the claim follows from Lemma 2.2 by induction. □

Let $b \geq 1$ be an integer. A separable extension E/F of function fields is called *b-bounded* if for every place $P \in \mathbb{P}(F)$ and every $Q \in \mathbb{P}(E)$ lying above P, the different exponent $d(Q|P)$ satisfies the equation

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

Remark 2.4. We remark that our definition of b-boundedness differs slightly from [3, 8], where the authors replace the condition "$d(Q|P) = b \cdot (e(Q|P) - 1)$" by "$d(Q|P) \leq b \cdot (e(Q|P) - 1)$".

A tower $\mathcal{F} = (F_i)_{i \geq 0}$ is called *b-bounded* if all extensions F_{i+1}/F_i are b-bounded, see [2, Section 3.3]. The property of being b-bounded is transitive as follows from the transitivity of ramification index and different exponent, see [18, Corollary 3.4.12]:

Lemma 2.5. *Let $F \subseteq E \subseteq H$ be separable extensions of function fields. If H/E and E/F are b-bounded, then H/F is also b-bounded.*

As most towers of function fields that we consider in this paper are p-towers, we give the definition of a *p-tower*.

Definition 2.6. A tower $\mathcal{F} = (F_i)_{i \geq 0}$ is called a *p-tower* over $\mathbb{F}_q$ if all extensions F_{i+1}/F_i are Galois and their degrees $[F_{i+1} : F_i]$ are powers of p.

We will need two more notions associated to a tower $\mathcal{F} = (F_i)_{i \geq 0}$. The sets of places

$$\mathrm{Split}\,(\mathcal{F}) = \{P \in \mathbb{P}(F_0) \mid \deg P = 1 \text{ and } P \text{ splits completely in } F_i/F_0 \text{ for all } i \geq 1\},$$

and

$$\mathrm{Ram}\,(\mathcal{F}) = \{P \in \mathbb{P}(F_0) \mid P \text{ is ramified in } F_i/F_0 \text{ for some } i \geq 1\}$$

are called the *splitting locus* and the *ramification locus* of $\mathcal{F}$, respectively. Note that the inequality $N(F_i) \geq [F_i : F_0] \cdot |\mathrm{Split}(\mathcal{F})|$ holds for all $i \geq 0$.

3 Composing a tower $\mathcal{B} = (B_i)_{i \geq 0}$ with an extension E/B_0

Starting from a given tower $\mathcal{B} = (B_i)_{i \geq 0}$ (called the *basic tower*), we will construct new towers by composing $\mathcal{B}$ with an extension E/B_0. In the next section we will specify the basic tower $\mathcal{B}$ and the field E to prove our main results. We assume that $\mathcal{B}$ and E satisfy the following conditions:

($B1$) $\mathcal{B}$ is an asymptotically good p-tower over $\mathbb{F}_q$.

($E1$) The extension E/B_0 is finite of degree m relatively prime to p, and $\mathbb{F}_q$ is the full constant field of E.

We set $E_i := E \cdot B_i$ for $i \geq 0$. It follows from ($B1$) and ($E1$) that $\mathcal{E} = E \cdot \mathcal{B} := (E_i)_{i \geq 0}$ is also a p-tower over $\mathbb{F}_q$.

Proposition 3.1. *Under the assumptions* $(B1)$ *and* $(E1)$*, the limits*

$$L_1(\mathcal{E}) = \lim_{i\to\infty} \frac{g(E_i)}{[E_i : E_0]}, \quad L_2(\mathcal{E}) = \lim_{i\to\infty} \frac{s(E_i)}{[E_i : E_0]} \quad \text{and} \quad L_3(\mathcal{E}) = \lim_{i\to\infty} \frac{N(E_i)}{[E_i : E_0]}$$

exist, and we have that

$$L_1(\mathcal{E}) > 0, \quad L_2(\mathcal{E}) \geq 0 \quad \text{and} \quad L_3(\mathcal{E}) \geq 0.$$

Proof. By [19, Lemma 7.2.3], the sequence $((g(E_i) - 1)/[E_i : E_0])_{i\geq 0}$ is monotonically non-decreasing. To prove that $L_1(\mathcal{E})$ exists, it suffices to show that this sequence is bounded from above. By Castelnuovo's Inequality [19, Theorem 3.11.3], we have

$$g(E_i) \leq g(E_0)[E_i : E_0] + mg(B_i) + ([E_i : E_0] - 1)(m - 1).$$

Then the fact that $[E_i : E_0] = [B_i : B_0]$ implies the following inequalities.

$$\begin{aligned} \frac{g(E_i)}{[E_i : E_0]} &\leq g(E_0) + m\frac{g(B_i)}{[B_i : B_0]} + \frac{[E_i : E_0] - 1}{[E_i : E_0]}(m - 1) \\ &\leq g(E_0) + m - 1 + m\frac{g(B_i)}{[B_i : B_0]} \end{aligned} \tag{3.1}$$

Since $\mathcal{B}$ is an asymptotically good tower, $g(B_i)/[B_i : B_0]$ is bounded above, see [19, Proposition 7.2.6]. Then we get the existence of $L_1(\mathcal{E})$ by Equation (3.1). Note that $g(E_i) > 0$ for all sufficiently large $i \geq 0$, i.e., $L_1(\mathcal{E}) > 0$.

By Lemma 2.3, we obtain that $(s(E_i) - 1)/[E_i : E_0] \leq (s(E_{i+1}) - 1)/[E_{i+1} : E_0]$ for all $i \geq 0$; i.e., the sequence $((s(E_i) - 1)/[E_i : E_0])_{i\geq 0}$ is monotonically non-decreasing. Also, by the fact $s(E_i) \leq g(E_i)$ we have

$$\frac{s(E_i) - 1}{[E_i : E_0]} \leq \frac{g(E_i)}{[E_i : E_0]},$$

hence the sequence is bounded above. Hence, it is convergent. Moreover, $L_3(\mathcal{E}) = \lim_{i\to\infty} \frac{N(E_i)}{[E_i:E_0]}$ exists by [19, Lemma 7.2.3] and $L_3(\mathcal{E}) \geq 0$. □

An immediate consequence of Proposition 3.1 is the following theorem:

Theorem 3.2. *Let* $\mathcal{E} = E \cdot \mathcal{B}$*, where* $\mathcal{B}$ *and* E *satisfy the properties* $(B1)$ *and* $(E1)$*. Then the limit and the asymptotic p-rank of* $\mathcal{E}$ *are given by*

$$\lambda(\mathcal{E}) = L_3(\mathcal{E})/L_1(\mathcal{E}) \quad \text{and} \quad \sigma(\mathcal{E}) = L_2(\mathcal{E})/L_1(\mathcal{E}).$$

We obtain more precise results on the asymptotic values $L_i(\mathcal{E})$ of the tower $\mathcal{E}$ under additional conditions. These assumptions are as follows:

$(B2)$ $\mathcal{B}$ is b-bounded for some $b \geq 1$.

$(B3)$ The ramification locus $\mathrm{Ram}(\mathcal{B})$ is finite and non-empty.

$(E2)$ Every place $P \in \mathrm{Ram}(\mathcal{B})$ is totally ramified in the extension E/B_0.

We remark that the existence of a totally ramified place in the extension E/B_0 implies that $\mathbb{F}_q$ is the full constant field of E.

Proposition 3.3. *With the above notation and assuming that* $(B1)$, $(B2)$, $(B3)$ *and* $(E1)$, $(E2)$ *hold, the following hold:*

(i) *Let $P \in \mathrm{Ram}(\mathcal{B})$ and $R \in \mathbb{P}(B_i)$ with $R|P$. Then R is totally ramified in E_i/B_i; i.e., R has exactly one extension Q in E_i, and* $\deg R = \deg Q$. *In particular, if* $\mathrm{Ram}(\mathcal{B}) = \{P_1, \ldots, P_r\}$ *then* $\mathrm{Ram}(\mathcal{E}) = \{Q_1, \ldots, Q_r\}$, *where Q_j is the unique extension of P_j in E_0.*

(ii) *The tower $\mathcal{E}$ is c-bounded, with $c = mb - m + 1$.*

Proof. The proof of item (i) is straightforward, hence we prove only item (ii). Let $Q \in \mathbb{P}(E_{i+1})$ with $i \geq 0$ that is ramified over E_i. We set $P := Q \cap E_i$, $Q_0 := Q \cap B_{i+1}$ and $P_0 := Q \cap B_i$. Then $Q_0|P_0$ is ramified, hence $P|P_0$ and $Q|Q_0$ are ramified with $e(P|P_0) = e(Q|Q_0) = m$ by (i). By considering the extensions $B_i \subseteq E_i \subseteq E_{i+1}$ and $B_i \subseteq B_{i+1} \subseteq E_{i+1}$, we apply the transitivity of the different exponents. Then the b-boundedness of the tower $\mathcal{B}$ yields

$$d(Q|P_0) = d(Q|P) + (m-1)e(Q|P) = (m-1) + mb(e(Q_0|P_0) - 1).$$

Observing that $e(Q|P) = e(Q_0|P_0)$, we obtain $d(Q|P) = (mb-m+1)(e(Q|P)-1)$, as desired. □

Proposition 3.4. *With the above notation and assuming that* $(B1)$, $(B2)$, $(B3)$ *and* $(E1)$, $(E2)$ *hold, we have for all* $i \geq 0$*:*

$$g(E_i)-1 = [B_i : B_0](g(E_0)-1) + \frac{mb-m+1}{b} \cdot \Big((g(B_i)-1) - [B_i : B_0](g(B_0)-1) \Big),$$

and

$$s(E_i) - 1 = [B_i : B_0](s(E_0) - 1) + \Big((s(B_i) - 1) - [B_i : B_0](s(B_0) - 1) \Big).$$

Proof. We set

$$\Delta_i := \sum_{P \in \mathbb{P}(B_0)} \sum_{Q \in \mathbb{P}(B_i),\, Q|P} (e(Q|P) - 1)) \cdot \deg Q.$$

Since B_i/B_0 is b-bounded, the degree of the different divisor of B_i/B_0 is equal to $b\Delta_i$. Then by the Hurwitz genus formula,

$$g(B_i) - 1 \quad = \quad [B_i : B_0](g(B_0) - 1) + \frac{b}{2} \cdot \Delta_i. \tag{3.2}$$

By Proposition 3.3.(i), we conclude that $R \in \mathbb{P}(E_i)$ is ramified in E_i/E_0 if and only if $R \cap B_i = Q$ is ramified in B_i/B_0. Moreover, the ramification indices are the same and $\deg R = \deg Q$. Therefore, by Proposition 3.3.(ii), the degree of the different divisor of E_i/E_0 is equal to $(mb-m+1)\Delta_i$. Then by the Hurwitz genus formula and the fact $[E_i : E_0] = [B_i : B_0]$, we have

$$g(E_i) - 1 \quad = \quad [B_i : B_0](g(E_0) - 1) + \frac{mb - m + 1}{2} \cdot \Delta_i. \tag{3.3}$$

Substituting Δ_i from Equation (3.2) into Equation (3.3), we get the first claim. The second claim of the proposition follows by the same argument, using Lemma 2.3. $\square$

4 Main results

In this section we assume that $q = \ell^2$ is a square, and we specify the basic tower $\mathcal{B}$ and the extension $E \supseteq B_0$. We take $\mathcal{B} := \mathcal{G} = (G_i)_{i \geq 0}$ as the optimal tower introduced by Garcia and Stichtenoth in [11].

4.1 Some properties of the tower by Garcia and Stichtenoth

The tower introduced by Garcia and Stichtenoth in [11] is defined as follows: $G_1 := \mathbb{F}_q(x_1)$ is a rational function field, $G_0 := \mathbb{F}_q(x_0)$ with $x_0 = x_1^\ell + x_1$, and for $i \geq 1$,

$$G_{i+1} = G_i(x_{i+1}) \quad \text{with} \quad x_{i+1}^\ell + x_{i+1} = \frac{x_i^\ell}{x_i^{\ell-1} + 1}.$$

Its properties that we need here, are:

$(GS1)$ $G_0 = \mathbb{F}_q(x_0)$ is a rational function field.

$(GS2)$ All extensions G_{i+1}/G_i are Galois p-extensions; i.e., $\mathcal{G}$ is a p-tower.

$(GS3)$ The ramification locus of $\mathcal{G}$ consists of the zero and the pole of x_0 in G_0 , hence $|\mathrm{Ram}(\mathcal{G})| = 2$ by [10, Lemma 3.3.(ii)].

$(GS4)$ $\mathcal{G}$ is 2-bounded by [10, Lemma 3.3.(ii) and 3.5.(iii)].

$(GS5)$ The splitting locus of $\mathcal{G}$ consists of the zeros of $x_0 - a$, $a \in \mathbb{F}_\ell^\times$, hence $|\mathrm{Split}(\mathcal{G})| = \ell - 1$ by [10, Lemma 3.9].

$(GS6)$ The tower $\mathcal{G}$ is optimal by [10, Theorem 3.1]; i.e., its limit is $\lambda(\mathcal{G}) = \ell - 1$.

$(GS7)$ $\lim\limits_{i\to\infty} g(G_i)/[G_i : G_0] = 1$ by [10, Remark 3.8], and hence by $(GS5)$ and $(GS6)$ $\lim\limits_{i\to\infty} N(G_i)/[G_i : G_0] = |\mathrm{Split}(\mathcal{G})| = \ell - 1$.

$(GS8)$ For a rational place $P \in \mathbb{P}(G_0) \setminus \mathrm{Split}(\mathcal{G})$, by $(GS7)$ one has

$$\lim_{i\to\infty} \frac{|\{Q \in \mathbb{P}(G_i)\,;\, Q \text{ is rational and } Q|P\}|}{[G_i : G_0]} = 0\,.$$

We will need one more property of the tower $\mathcal{G}$:

$(GS9)$ $\lim\limits_{i\to\infty} s(G_i)/[G_i : G_0] = 1$.

Proof of $(GS9)$. We use the quantity Δ_i as in the proof of Proposition 3.4. By Lemma 2.1, $(GS4)$ and $(GS7)$,

$$\lim_{i\to\infty} \Delta_i/[G_i : G_0] = \lim_{i\to\infty} g(G_i)/[G_i : G_0] + 1 = 2\,.$$

Then we obtain from $(GS2)$ and Lemma 2.3:

$$\lim_{i\to\infty} s(G_i)/[G_i : G_0] = -1 + 2 = 1\,.$$

□

An immediate consequence of $(GS7)$ and $(GS9)$ is that $\mathcal{G}$ is an *ordinary* tower; i.e., its asymptotic p-rank is $\sigma(\mathcal{G}) = 1$. This fact has already been observed in [5]. Note that the tower $\mathcal{G}$ satisfies $(B1)$ by $(GS2)$ and $(GS6)$, $(B2)$ by $(GS4)$ and $(B3)$ by $(GS3)$.

4.2 Compositum over the tower by Garcia and Stichtenoth and its Galois closure

Let $m \geq 1$ be an integer relatively prime to q. We consider the extension field $E \supseteq G_0$ defined as follows:

$$E := G_0(y) = \mathbb{F}_q(x_0, y) \quad \text{with} \quad y^m = x_0.$$

Note that E/G_0 is an extension of degree m, and the zero and the pole of x_0 are the only ramified places of G_0 in E, which are totally ramified. In particular, E satisfies the properties $(E1)$ and $(E2)$ by $(GS3)$. Observe also that $E = \mathbb{F}_q(y)$ is a rational function field.

Proposition 4.1. *Let $\mathcal{E} = E \cdot \mathcal{G} = (E_i)_{i\geq 0}$ be the composite of the function field E (as defined above) with the tower $\mathcal{G}$. Then:*
(i) $L_1(\mathcal{E}) = \lim_{i\to\infty} g(E_i)/[G_i : G_0] = m$,
(ii) $L_2(\mathcal{E}) = \lim_{i\to\infty} s(E_i)/[G_i : G_0] = 1$.

Proof. To prove item (i), we observe first that the function field $E = \mathbb{F}_q(x_0, y) = \mathbb{F}_q(y)$ has genus $g(E) = 0$. Now Proposition 3.4 and $(GS4)$, $(GS7)$ yield

$$\begin{aligned}\lim_{i\to\infty} \frac{g(E_i)}{[G_i : G_0]} &= g(E) - 1 + \frac{m+1}{2} \cdot \Big(\lim_{i\to\infty} \frac{g(G_i)}{[G_i : G_0]} - (g(G_0) - 1)\Big) \\ &= -1 + \frac{m+1}{2}(1+1) = m\,.\end{aligned}$$

(iii) We apply Proposition 3.4 and $(GS9)$ and get

$$\lim_{i\to\infty} \frac{s(E_i)}{[G_i : G_0]} = s(E) - 1 + \lim_{i\to\infty} \frac{s(G_i)}{[G_i : G_0]} - (s(G_0) - 1) = -1 + 1 + 1 = 1\,.$$

□

Proposition 4.2. *For the tower $\mathcal{E}$ as in Proposition 4.1, we have*

$$L_3(\mathcal{E}) = \lim_{i\to\infty} N(E_i)/[G_i : G_0] = (\ell - 1) \cdot \gcd(\ell + 1, m)\,.$$

Proof. In a rational function field $\mathbb{F}_q(z)$, we denote by $(z = a)$ the rational place which is the zero of the element $z - a$, for $a \in \mathbb{F}_q$. Let $P \in \mathbb{P}(E_0)$ be a rational place of $E_0 = \mathbb{F}_q(y)$ which lies over a place $(x_0 = a) \in \text{Split}(\mathcal{G})$. Then $P = (y = b)$ with $b \in \mathbb{F}_q$ and $b^m = a \in \mathbb{F}_\ell^\times$, by $(GS5)$. On the other hand, if $P \in \mathbb{P}(E_0)$ lies above a rational place $P_0 \in \mathbb{P}(G_0) \setminus \text{Split}(\mathcal{G})$, then

$$\lim_{i\to\infty} \frac{|\{Q \in \mathbb{P}(E_i)\,;\, Q \text{ is rational and } Q|P\}|}{[G_i : G_0]} = 0\,,$$

as follows from $(GS8)$. Therefore $\lim_{i\to\infty} N(E_i)/[G_i : G_0]$ is equal to the cardinality of the set

$$M := \{b \in \mathbb{F}_q \,|\, b^m \in \mathbb{F}_\ell^\times\}.$$

We observe that for an element $b \in \bar{\mathbb{F}}_q$,

$$b \in M \iff b^{q-1} = b^{m(\ell-1)} = 1 \iff b^{\gcd(q-1, m(\ell-1))} = 1\,.$$

Therefore, $|M| = \gcd(q-1, m(\ell-1)) = (\ell-1)\cdot\gcd((\ell+1), m)$, as desired. $\square$

Putting together the results of Proposition 4.1 and 4.2, we obtain our main result. We recall that $q = \ell^2$.

Theorem 4.3. *The limit and the asymptotic p-rank of the tower $\mathcal{E}$ as defined above, are*

$$\lambda(\mathcal{E}) = (\ell-1)\cdot\frac{\gcd(\ell+1, m)}{m} \quad\text{and}\quad \sigma(\mathcal{E}) = \frac{1}{m}\,.$$

Proof. We have $L_1(\mathcal{E}) = m$, $L_2(\mathcal{E}) = 1$ by Proposition 4.1 and $L_3(\mathcal{E}) = (\ell-1)\gcd(\ell+1, m)$ by Proposition 4.2. Then the result follows from Theorem 3.2. $\square$

Corollary 4.4. *For any divisor $m|(\ell+1)$ there exists an asymptotically optimal tower $\mathcal{E}$ over $\mathbb{F}_q$, whose asymptotic p-rank is $\sigma(\mathcal{E}) = 1/m$. In particular, for given $\epsilon > 0$ there exist a large enough even power $q = \ell^2$ of p and an asymptotically optimal tower $\mathcal{E}$ of function fields over $\mathbb{F}_q$ with $\sigma(\mathcal{E}) \le \epsilon$.*

Remark 4.5. Corollary 4.4 was already known in the case $m = \ell+1$, see [9].

Corollary 4.6. *For every $\epsilon > 0$ there exists an asymptotically good tower $\mathcal{E}$ over $\mathbb{F}_q$ whose asymptotic p-rank is less than ϵ. In other words, there is a constant $C > 0$ such that for infinitely many integers $g \in \mathbb{N}$ there exists a function field $F/\mathbb{F}_q$ of genus $g(F) = g$ that satisfies*

$$N(F) \ge C\cdot g(F) \text{ and } \; s(F) \le \epsilon\cdot g(F)\,.$$

We can choose $C = (\ell-1)\cdot M_{\ell,\epsilon}$, where

$$M_{\ell,\epsilon} = \max_m \{\gcd(\ell+1, m)/m\,;\, \gcd(m,\ell) = 1 \textit{ and } m > \epsilon^{-1}\}.$$

Remark 4.7. By the Drinfeld–Vladut bound we observe that $M_{\ell,\epsilon} \leq 1$. Note that for small ϵ, the constant C in our construction is also small. We do not know (but find it unlikely) if for every $\epsilon > 0$ there exist asymptotically *optimal* towers over a fixed constant field $\mathbb{F}_q$ whose asymptotic p-rank is less than ϵ.

Remark 4.8. It is easy to construct towers whose asymptotic p-rank is 0. For example, the tower $\mathcal{G} = (G_i)_{i\geq 0}$ defined as

$$G_0 = \mathbb{F}_q(x_0) \quad \text{and for } i \geq 0, \quad G_{i+1} = G_i(x_{i+1}) \text{ with } x_{i+1}^q + x_{i+1} = f(x_i),$$

where $f(x_i)$ is a polynomial of degree d relatively prime to q, has asymptotic p-rank 0. We do not know, however, if there exist *asymptotically good* towers whose asymptotic p-rank is 0.

The extensions E_{i+1}/E_i in the tower $\mathcal{E}$ above are Galois, but the extensions E_i/E_0 are not Galois, for all $i \geq 2$. However, a slight modification of our construction will produce a p-tower having that additional property. For convenience, we will call a tower $\mathcal{F} = (F_i)_{i\geq 0}$ a *Galois p-tower* if for all $i \geq 1$, the extension F_i/F_0 is a Galois p-extension.

Now we will use as the basic tower the Galois closure $\mathcal{G}^*$ of the Garcia-Stichtenoth tower $\mathcal{G}$ in [11]. It is defined as follows: $\mathcal{G}^* = (G_i^*)_{i\geq 0}$ where G_i^* is the Galois closure of G_i over G_0. This tower has all properties as listed in $(GS1)-(GS9)$ if we replace there the fields G_i by G_i^*, see [10]. Note that $\mathcal{G}^*$ satisfies $(B1)$, $(B2)$, $(B3)$, and E satisfies $(E1)$, $(E2)$. Then the composite tower $\mathcal{E}^* := E \cdot \mathcal{G}^*$ is a Galois p-tower which satisfies:

Theorem 4.9. *The limit and the asymptotic p-rank of the tower $\mathcal{E}^*$ are*

$$\lambda(\mathcal{E}^*) = (\ell - 1) \cdot \frac{\gcd(\ell + 1, m)}{m} \quad \text{and} \quad \sigma(\mathcal{E}^*) = \frac{1}{m}\,.$$

Moreover, the automorphism group of E_i^* over $\mathbb{F}_q$ has order

$$|\mathrm{Aut}(E_i^*)| \geq [E_i^* : E_0^*] \geq m^{-1} \cdot g(E_i^*)\,.$$

If m is a divisor of $(q-1)$, then $|\mathrm{Aut}(E_i^*)| \geq g(E_i^*)$.

Proof. The calculation of $L_1(\mathcal{E}^*)$, $L_2(\mathcal{E}^*)$ and $L_3(\mathcal{E}^*)$ is done in the same way as in Proposition 4.1 and 4.2. Then by Theorem 3.2 we obtain the desired result for $\lambda(\mathcal{E}^*)$ and $\sigma(\mathcal{E}^*)$.

The Galois group $\mathrm{Gal}(E_i^*/E_0^*)$ of the extension E_i^*/E_0^* is a subgroup of $\mathrm{Aut}(E_i^*)$, hence

$$|\mathrm{Aut}(E_i^*)| \geq |\mathrm{Gal}(E_i^*/E_0^*)| = [E_i^* : E_0^*].$$

Moreover, the inequality $g(E_i^*) \leq m[E_i^* : E_0^*]$ is shown as in Proposition 4.1.(i), which gives the desired result. Finally, if m is a divisor of $(q-1)$, then E/G_0^* is a Galois extension of degree m. Since the extensions fields E and G_i^* are Galois and linearly disjoint over G_0^*, their compositum E_i^* is also Galois over G_0^*, and

$$\mathrm{Gal}(E_i^*/G_0^*) \cong \mathrm{Gal}(E/G_0^*) \times \mathrm{Gal}(G_i^*/G_0^*).$$

Therefore, $|\mathrm{Aut}(E_i^*)| \geq m \cdot [G_i^* : G_0^*]$. Then the fact that $[G_i^* : G_0^*] = [E_i^* : E_0^*]$ gives the desired result. $\square$

Remark 4.10. The number of m-th roots of unity in $\mathbb{F}_q$ is equal to $d = \gcd(m, q-1)$. Note that for a m-th root of unity ζ the map $\tau_\zeta : E \mapsto E$ defined by $\tau_\zeta(y) = \zeta y$ is an automorphism of $E = E_0^*$. Since E_i^*/E_0^* is a Galois extension, there are $[E_i^* : E_0^*]$ distinct automorphisms of E_i^* whose restriction to E is equal to τ_ζ. That is, $|Aut(E_i^*)| \geq \gcd(m, q-1)[E_i^* : E_0^*]$.

Remark 4.11. The precise Galois groups $\mathrm{Gal}(\mathcal{G}_i^*/\mathcal{G}_0^*)$ have been computed in [4]. In particular, the extension degree $[\mathcal{G}_i^* : \mathcal{G}_0^*]$ is known, and so is $[E_i^* : E_0^*]$.

Acknowledgements

We are grateful to the reviewers for their valuable suggestions which helped to improve the paper substantially.

N. A. was supported by the Austrian Science Fund (FWF): Project F5505–N26 and Project F5511–N26, which is a part of the Special Research Program "Quasi-Monte Carlo Methods: Theory and Applications".

References

[1] J.D. Achter, R. Pries, Monodromy of the p-rank strata of the moduli space of curves, Int. Math. Res. Not. IMRN (2008) no. 15, Art. ID rnn053, 25 pp.

[2] N. Anbar, P. Beelen, N. Nguyen, A new tower meeting Zink's bound with good p-rank, Acta Arith. 177 (2017) no. 4, 347–374.

[3] A. Bassa, P. Beelen, A. Garcia, H. Stichtenoth, Towers of function fields over non-prime finite fields, Mosc. Math. J. 15 (1) (2015), 1–29.

[4] A. Bassa, P. Beelen, The Galois closure of Drinfeld modular towers, J. Number Theory 131 (3) (2011), 561–577.

[5] A. Bassa, P. Beelen, The Hasse-Witt invariant in some towers of function fields over finite fields, Bull. Braz. Math. Soc. (N.S.) 41 (2010) no. 4, 567–582.

[6] A. Bassa, A. Garcia, H. Stichtenoth, A new tower over cubic finite fields, Mosc. Math. J. 8 (3) (2008), 401–418.

[7] J. Bezerra, A. Garcia, H. Stichtenoth, An explicit tower of function fields over cubic finite fields and Zink's lower bound, J. Reine Angew. Math. 589 (2005), 159–199.

[8] N. Caro, A. Garcia, On a tower of Ihara and its limit, Acta Arith. 151 (2) (2012), 191–200.

[9] I. Cascudo, R. Cramer, C. Xing, Torsion limits and Riemann-Roch systems for function fields and applications, IEEE Trans. Inform. Theory 60 (7) (2014), 3871–3888.

[10] A. Garcia, H. Stichtenoth, On the Galois closure of towers. Recent trends in coding theory and its applications, 83–92, AMS/IP Stud. Adv. Math., 41, Amer. Math. Soc., Providence, RI, 2007.

[11] A. Garcia, H. Stichtenoth, On the asymptotic behaviour of some towers of function fields over finite fields, J. Number Theory 61 (2) (1996), 248–273.

[12] A. Garcia, H. Stichtenoth, A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound, Invent. Math. 121 (1) (1995), 211–222.

[13] J.W.P. Hirschfeld, G. Korchmaros, F. Torres, Algebraic curves over a finite field, Princeton University Press, 2013.

[14] S. Nakajima, On abelian automorphism groups of algebraic curves, J. London Math. Soc. (2) 36 (1987) no. 1, 23–32.

[15] H. Popp, The singularities of the moduli schemes of curves, J. Number Theory 1 (1969), 90–107.

[16] P. Roquette, Abschätzung der Automorphismenanzahl von Funktionenkörpern bei Primzahlcharakteristik, (German) Math. Z. 117 (1970), 157–163.

[17] M. Rosen, Some remarks on the p-rank of an algebraic curve, Arch. Math. (Basel) 41 (1983) no. 2, 143–146.

[18] H. Stichtenoth, Algebraic function fields and codes, 2nd edition, Graduate Texts in Mathematics, 254. Springer-Verlag, Berlin, 2009.

[19] H. Stichtenoth, Die Hasse-Witt-Invariante eines Kongruenzfunktionenkörpers, (German) Arch. Math. (Basel) 33 (1979) no. 4, 357–360.

[20] S.G. Vladut, V.G. Drinfeld, Number of points of an algebraic curve, (Russian) Funktsional. Anal. i Prilozhen. 17 (1983) no. 1, 68–69.