Asymptotically good towers of function fields with small p-rank

Nurdagül Anbar[1,2], Henning Stichtenoth[2], Seher Tutdere[3]

[1]Johannes Kepler University,

Altenbergerstrasse 69, 4040-Linz, Austria

E-mail: nurdagulanbar2@gmail.com

[2]Sabancı University,

MDBF, Orhanlı, Tuzla, 34956 İstanbul, Turkey

E-mail: henning@sabanciuniv.edu

[3]Gebze Technical University,

Department of Mathematics, 41400 Gebze, Kocaeli, 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, limit, p-rank
MSC[2010]: 14H05, 11G20, 14G50

1 Introduction

Let $\mathbb{F}_q$ be the finite field of characteristic $p > 0$ and cardinality q, where q is a power of p, 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 over $\mathbb{F}_q$ 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 [14]. The Drinfeld–Vladut bound states that

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

$\mathcal{F}$ is called *asymptotically good* if $\lambda(\mathcal{F}) > 0$, and *asymptotically optimal* if $\lambda(\mathcal{F}) = \sqrt{q} - 1$. The tower is *asymptotically bad* if $\lambda(\mathcal{F}) = 0$. Asymptotically good towers exist and they have been studied extensively, see [1, 3, 4, 5, 6, 8, 9, 10, 14] and the references therein. We note that it is a non-trivial task to construct asymptotically good towers, 'most' towers are bad.

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). It is defined as follows: Let $\bar{F}$ 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 degree zero and order p of $\bar{F}$ is a finite abelian group of exponent p, and $s(F)$ is defined as the rank of this group. It is well-known that the inequality $0 \leq s(F) \leq g(F)$ holds for every function field F over $\mathbb{F}_q$, and 'most' function fields are *ordinary*; i.e., $s(F) = g(F)$. For a tower $\mathcal{F} = (F_i)_{i \geq 0}$ 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*, or in short the *p-rank* of $\mathcal{F}$. Clearly we have the inequality

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

The asymptotic p-rank was introduced by Cramer et al. [7] 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. Observe however, since most function fields are ordinary, one expects that for a 'general' tower of function fields, the asymptotic p-rank should be 1.

First we recall known results from the literature. The Garcia–Stichtenoth tower over a *quadratic* field $\mathbb{F}_q$ (i.e., q is a square) in [10] is asymptotically optimal and its p-rank is $1/(\sqrt{q}+1)$, see [2, 7]. This is the smallest known p-rank of an asymptotically good tower. The p-rank of some asymptotically good towers over a *cubic* field $\mathbb{F}_q$ (i.e., $q = p^{3a}$) has been determined in [1, 2], it is close to $1/4$. In Section 3 below we will construct asymptotically good towers over quadratic fields whose p-rank is significantly less than the p-rank of the above-mentioned towers. More specifically, we show that for any $\epsilon > 0$, there exists an asymptotically good tower $\mathcal{F}$ over $\mathbb{F}_q$ such that its p-rank is $\sigma(\mathcal{F}) < \epsilon$.

We will also consider towers of function fields that have many automorphisms. Recall that the automorphism group $\mathrm{Aut}(F)$ of a function field $F/\mathbb{F}_q$ is always finite, and for a 'general' function field it is trivial; i.e., $|\mathrm{Aut}(F)| = 1$, see [12]. 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 [11, 13]. We will show (see Theorem 4.9.) that for every $\epsilon > 0$, there is a constant $B > 0$ and an asymptotically good tower $\mathcal{F} = (F_i)_{i \geq 0}$ over $\mathbb{F}_q$ (q a square) such that $\sigma(\mathcal{F}) < \epsilon$ and

$$|\mathrm{Aut}(F_i)| \geq B \cdot g(F_i)$$

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:

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 cyclic extension of degree p, one has:

Lemma 2.2 (Deuring–Shafarevich formula)**.** *Let E/F be a cyclic 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. $\square$

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

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

A tower $\mathcal{F} = (F_i)_{i \geq 0}$ is called b-bounded if all extensions F_{i+1}/F_i are b-bounded. The property of being b-bounded is transitive as follows from transitivity of ramification index and different exponent:

Lemma 2.4. *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.*

A tower $\mathcal{F} = (F_i)_{i \geq 0}$ is called a *p-tower* if all extensions F_{i+1}/F_i are Galois and their degrees $[F_{i+1} : F_i]$ are powers of p. Most towers of function fields that we consider in this paper, will be p-towers.

Lemma 2.5. *For an asymptotically good p-tower $\mathcal{F} = (F_i)_{i \geq 0}$, the sequence $(s(F_i)/g(F_i))_{i \geq 0}$ is convergent, hence the p-rank of $\mathcal{F}$ is*

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

Proof. We can assume w.l.o.g. that $g(F_i) > 0$ and $N(F_i) > 0$ for all i. We have

$$\frac{s(F_i)}{g(F_i)} = \frac{s(F_i) - 1}{N(F_i)} \cdot \frac{N(F_i)}{g(F_i)} + \frac{1}{g(F_i)}.$$

The sequence $(N(F_i)/g(F_i))_{i \geq 0}$ converges to $\lambda(\mathcal{F})$, and $1/g(F_i) \to 0$ as $i \to \infty$. The sequence $((s(F_i) - 1)/N(F_i))_{i \geq 0}$ is bounded from above as $(s(F_i) - 1)/N(F_i) \leq g(F_i)/N(F_i)$ and $\lim_{i \to \infty} g(F_i)/N(F_i) < \infty$ since the tower is asymptotically good. Moreover, it is monotonously increasing which follows easily from the inequalities $N(F_{i+1}) \leq [F_{i+1} : F_i] \cdot N(F_i)$ and $s(F_{i+1}) - 1 \geq [F_{i+1} : F_i] \cdot (s(F_i) - 1)$, see Lemma 2.3. Therefore, the sequence $((s(F_i) - 1)/N(F_i))_{i \geq 0}$ converges as well. This proves the lemma. □

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

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

are called the *splitting locus* and the *ramification locus* of $\mathcal{F}$, respectively. Note that $N(F_i) \geq [F_i : F_0] \cdot |\operatorname{Split}(\mathcal{F})|$ 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 $\mathcal{B}$ has the following properties:

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

$(B2)$ $\mathcal{B}$ is b-bounded.

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

The function field $E \supseteq B_0$ is supposed to satisfy:

$(E1)$ The extension E/B_0 is separable of degree $[E : B_0] = m$, and m is relatively prime to p.

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

The extensions E/B_0 and B_i/B_0 are linearly disjoint over B_0 for all $i \geq 0$. Setting $E_i := E \cdot B_i$ for $i \geq 0$, we obtain a tower $\mathcal{E} = E \cdot \mathcal{B} := (E_i)_{i\geq 0}$ over $\mathbb{F}_q$.

Proposition 3.1. *With the above notation, the following hold:*

(i) $\mathcal{E} = (E_i)_{i\geq 0}$ *is a p-tower.*

(ii) *For all $i \geq 0$, we have $[E_i : B_i] = m$ and $[E_{i+1} : E_i] = [B_{i+1} : B_i]$.*

(iii) *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* $\deg R = \deg Q$.

(iv) *Let $\mathrm{Ram}(\mathcal{B}) = \{P_1, \ldots, P_r\}$. Then $\mathrm{Ram}(\mathcal{E}) = \{Q_1, \ldots, Q_r\}$, where Q_j is the unique extension of P_j in E_j.*

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

Proof. The proofs of items (i) - (iv) are straightforward, hence we prove only item (v). 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 (iii). Transitivity of different exponents and b-boundedness of the tower $\mathcal{B}$ yield now

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

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

Proposition 3.2. *With the above notation, we have for all $i \geq 0$:*

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

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

Proof. We set

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

By the Hurwitz genus formula and Proposition 3.1.(v),

$$g(B_i) - 1 = [B_i : B_0](g(B_0) - 1) + \frac{b}{2} \cdot \Delta_i \text{ and } g(E_i) - 1 = [B_i : B_0](g(E_0) - 1) + \frac{mb - m + 1}{2} \cdot \Delta_i\,.$$

Substituting Δ_i from the first equation into the second one, we get the first claim. The second claim of the proposition follows by the same argument, using Lemma 2.3. □

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 Garcia–Stichtenoth tower, see [9]. It 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.

($GS3$) $\mathcal{G}$ is 2-bounded.

($GS4$) The ramification locus of $\mathcal{G}$ consists of the zero and the pole of x_0 in G_0 , hence $|\mathrm{Ram}(\mathcal{G})| = 2$.

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

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

($GS7$) $\lim_{i\to\infty} N(G_i)/[G_i : G_0] = |\mathrm{Split}(\mathcal{G})| = \ell - 1$ and $\lim_{i\to\infty} g(G_i)/[G_i : G_0] = 1$.

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

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

Proof of $(GS9)$. We use the quantity Δ_i as in the proof of Proposition 3.2. By Lemma 2.1, $(GS3)$ 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 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 [2].

The extension field $E \supseteq G_0$ is taken as follows:

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

Note that m is relatively prime to q, as in Section 3. It is obvious that $\mathcal{G}$ and E satisfy the conditions $(B1)-(B3)$ and $(E1), (E2)$ from Section 3. Observe also that $E = \mathbb{F}_q(y)$ is a rational function field.

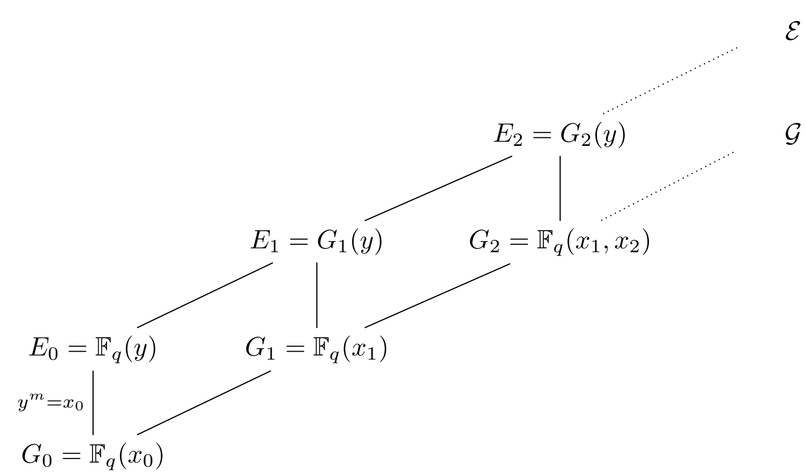

Figure 1: The towers $\mathcal{G}$ and $\mathcal{E}$

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) $[E_{i+1} : E_i] = [G_{i+1} : G_i]$ *for all* $i \geq 0$,

(ii) $\lim_{i\to\infty} g(E_i)/[G_i : G_0] = m$,

(iii) $\lim_{i\to\infty} s(E_i)/[G_i : G_0] = 1$, *Proof.* Item (i) is trivial. To prove item (ii), 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 3.2 and $(GS3), (GS7)$ yield

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

(iii) We apply Proposition 3.2 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*

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

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 $(x_0 = a) \in \mathrm{Split}(\mathcal{G})$. 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 $P_0 \in \mathbb{P}(G_0) \setminus \mathrm{Split}(\mathcal{G})$, 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. □

Putting together the results of Proposition 4.1 and 4.2, we obtain our main result:

Theorem 4.3. *($q = \ell^2$) 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. This follows from Proposition 4.1 and 4.2 since

$$\lambda(\mathcal{E}) = \frac{\lim_{i\to\infty} N(E_i)/[G_i : G_0]}{\lim_{i\to\infty} g(E_i)/[G_i : G_0]} \quad \text{and} \quad \sigma(\mathcal{E}) = \frac{\lim_{i\to\infty} s(E_i)/[G_i : G_0]}{\lim_{i\to\infty} g(E_i)/[G_i : G_0]}\,.$$

□

Corollary 4.4. *($q = \ell^2$) For any divisor $m|(\ell+1)$ there exists an asymptotically optimal tower $\mathcal{E}$ over $\mathbb{F}_q$, whose asymptotic p-rank is $\sigma(\mathcal{E}) = 1/m$.*

Corollary 4.5. *($q = \ell^2$) 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 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 that satisfies*

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

Remark 4.6. Corollary 4.4 was already known in the case $m = \ell + 1$, see [7].

Remark 4.7. 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 whose p-rank is less than ϵ.

Remark 4.8. It is easy to construct towers whose asymptotic p-rank is 0. We do not know, however, if there exist *asymptotically good* towers whose 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 $\mathcal{G}$. 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 [8]. The composite tower $\mathcal{E}^* := E \cdot \mathcal{G}^*$ is then a Galois p-tower which satisfies:

Theorem 4.9. *($q = \ell^2$) 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 $\lambda(\mathcal{E}^*)$ and $\sigma(E^*)$ is done in the same way as in Theorem 4.3. The inequality $g(E_i^*) \leq m[E_i^* : E_0^*]$ is shown as in Proposition 4.1.(ii). Finally, if m is a divisor of $(q-1)$, then the extension E_i^*/G_0^* is Galois of order $m \cdot [E_i^* : E_0^*]$. $\square$

5 Acknowledgment

Nurdagül Anbar 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] 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.

[2] 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.

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

[5] 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.

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

[7] 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.

[8] 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.

[9] 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.

[10] 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.

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

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

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

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