TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 372, Number 1, 1 July 2019, Pages 35–52
https://doi.org/10.1090/tran/7822
Article electronically published on March 26, 2019

THE ASYMPTOTIC BEHAVIOR OF AUTOMORPHISM GROUPS OF FUNCTION FIELDS OVER FINITE FIELDS

LIMING MA AND CHAOPING XING

Abstract. The purpose of this paper is to investigate the asymptotic behavior of automorphism groups of function fields when genus tends to infinity.

Motivated by applications in coding and cryptography, we consider the maximum size of abelian subgroups of the automorphism group $\mathrm{Aut}(F/\mathbb{F}_q)$ in terms of genus g_F for a function field F over a finite field $\mathbb{F}_q$. Although the whole group $\mathrm{Aut}(F/\mathbb{F}_q)$ could have size $\Omega({g_F}^4)$, the maximum size m_F of abelian subgroups of the automorphism group $\mathrm{Aut}(F/\mathbb{F}_q)$ is upper bounded by $4g_F+4$ for $g_F \geq 2$. In the present paper, we study the asymptotic behavior of m_F by defining $M_q = \limsup_{g_F\to\infty} \frac{m_F \cdot \log_q m_F}{g_F}$, where F runs through all function fields over $\mathbb{F}_q$. We show that M_q lies between 2 and 3 (resp., 4) for odd characteristic (resp., even characteristic). This means that m_F grows much more slowly than genus does asymptotically.

The second part of this paper is to study the maximum size b_F of subgroups of $\mathrm{Aut}(F/\mathbb{F}_q)$ whose order is coprime to q. The Hurwitz bound gives an upper bound $b_F \leq 84(g_F-1)$ for every function field $F/\mathbb{F}_q$ of genus $g_F \geq 2$. We investigate the asymptotic behavior of b_F by defining $B_q = \limsup_{g_F\to\infty} \frac{b_F}{g_F}$, where F runs through all function fields over $\mathbb{F}_q$. Although the Hurwitz bound shows $B_q \leq 84$, there are no lower bounds on B_q in the literature. One does not even know whether $B_q = 0$. For the first time, we show that $B_q \geq 2/3$ by explicitly constructing some towers of function fields in this paper.

1. Introduction

Let q be a prime power, and let $\mathbb{F}_q$ be the finite field with q elements. For a global function field $F/\mathbb{F}_q$, we denote by $\mathrm{Aut}(F/\mathbb{F}_q)$ the automorphism group of F over $\mathbb{F}_q$, that is,

$$\mathrm{Aut}(F/\mathbb{F}_q) = \{\sigma : F \to F | \sigma \text{ is an } \mathbb{F}_q\text{-automorphism of } F\}.$$

Due to demand from applications such as coding theory and cryptography [4,8,9, 15,22,25,26], there has been a lot of research on automorphism groups of univariate function fields over finite fields (i.e., global function fields) (see [7,11,12,14,16,24]). One of the problems with this topic is to look at the relation between the size of the automorphism group $\mathrm{Aut}(F/\mathbb{F}_q)$ and the genus g_F for a function field F over a finite field $\mathbb{F}_q$.

For a function field F over $\mathbb{F}_q$, the full constant field of F is defined to be the subfield of F whose elements are algebraic over $\mathbb{F}_q$. In this paper, we always mean that $\mathbb{F}_q$ is the full constant field whenever we write $F/\mathbb{F}_q$. For a function field

Received by the editors January 9, 2018.
2010 *Mathematics Subject Classification.* Primary 14H37, 11R58.
The first author was partially supported by the National Natural Science Foundation of China under Grant 11501493, the Shuangchuang Doctor Project of Jiangsu Province, and the Young Visiting Scholar Project of the China Scholarship Council.

$F/\mathbb{F}_q$ of genus $g_F \geq 2$, if $|\mathrm{Aut}(F/\mathbb{F}_q)| \geq 8g_F^3$, then F is isomorphic to one of the four exceptions: two hyperelliptic function fields, the Hermitian function field and the Suzuki function field [11]. In particular, for the Hermitian function field $H = \mathbb{F}_q(x, y)$ defined by $y^r + y = x^{r+1}$ with $q = r^2$, the automorphism group has size $r^3(r^2 - 1)(r^3 + 1)$. Thus, in the Hermitian function field case, one has $|\mathrm{Aut}(H/\mathbb{F}_q)| \geq 16g_H^4$.

A natural question involves how $|\mathrm{Aut}(F/\mathbb{F}_q)|$ behaves when g_F tends to infinity for a fixed q? For a fixed finite field $\mathbb{F}_q$, the genus g_F for any function field $F/\mathbb{F}_q$ in the above four classes of the exceptional function fields with $|\mathrm{Aut}(F/\mathbb{F}_q)| \geq 8g_F^3$ is upper bounded. This implies that, for a fixed q, one has

$$\limsup_{g_F \to \infty} \frac{|\mathrm{Aut}(F/\mathbb{F}_q)|}{{g_F}^3} \leq 8,$$

where F runs through all function fields over $\mathbb{F}_q$. This leads to the following open problem.

Open Problem 1. How does $|\mathrm{Aut}(F/\mathbb{F}_q)|$ behave when g_F tends to infinity for a fixed q? How does one properly define an asymptotic quantity of $|\mathrm{Aut}(F/\mathbb{F}_q)|$ in terms of genus g_F?

The second question refers to the growing speed of $|\mathrm{Aut}(F/\mathbb{F}_q)|$ in terms of genus g_F. For instance, we do not know if $|\mathrm{Aut}(F/\mathbb{F}_q)|$ grows linearly or quadratically in genus g_F.

On the other hand, for some applications in coding theory, cryptography, and combinatorics [4, 8, 9], one requires a large abelian (or even cyclic) subgroup of $\mathrm{Aut}(F/\mathbb{F}_q)$. This motives us to study the relation between the maximum size of abelian subgroups of the automorphism group $\mathrm{Aut}(F/\mathbb{F}_q)$ and the genus g_F for a function field F over a finite field $\mathbb{F}_q$. Let us provide a brief description of these applications.

(i) **Application to coding theory.** In [8], a class of codes, called *folded algebraic geometry codes* was proposed for the purpose of list decoding. To get a small list size, the authors applied the Chebotarev density theorem. One of the critical conditions for getting small list size is to have an automorphism of function field of large order. In other words, we need a global function field F over $\mathbb{F}_q$ whose automorphism group $\mathrm{Aut}(F/\mathbb{F}_q)$ contains a large cyclic subgroup.

(ii) **Application to cryptography.** Algebraic manipulation detection codes (AMD codes for short) have found wide applications in cryptography. In [4], a construction of AMD codes based on block codes with large transitive abelian groups was proposed. To construct such codes, one naturally thinks of algebraic geometry codes. If one makes use of the result given in [24], then the codes are transitive. Unfortunately, the automorphism groups of these codes are not abelian. Therefore, we have to look for function fields F over $\mathbb{F}_q$ whose automorphism group $\mathrm{Aut}(F/\mathbb{F}_q)$ contains a large abelian subgroup.

(iii) **Application to combinatorics.** Subspace design is a combinatorial structure that has found wide application in coding theory and computer science. In [9], Guruswami, Xing, and Yuan applied algebraic function fields over finite fields to construct such a combinatorial structure. One of the key points is to have an automorphism of large order to produce a nonzero

Moore determinant. Therefore, to have a subspace design with good parameters via this construction, we require a global function field F over $\mathbb{F}_q$ whose automorphism group $\mathrm{Aut}(F/\mathbb{F}_q)$ contains a large cyclic subgroup. Now based on Theorem 3.6, we conclude that the result in [9] cannot be improved unless a different approach is found.

For a function field $F/\mathbb{F}_q$, we define the quantity

$$m_F = \max\{|\mathcal{G}| : \mathcal{G} \text{ is an abelian subgroup of } \mathrm{Aut}(F/\mathbb{F}_q)\}.$$

Although $|\mathrm{Aut}(F/\mathbb{F}_q)|$ can be as large as $16{g_F}^4$, the quantity m_F is much smaller. In fact, it was proved in [12, Theorem 11.79] that m_F is at most linear in g_F. More precisely we have that, for any function field F with genus $g_F \geq 2$, one has

$$m_F \leq \begin{cases} 4g_F + 4 & \text{for } \mathrm{char}(\mathbb{F}_q) \neq 2, \\ 4g_F + 2 & \text{for } \mathrm{char}(\mathbb{F}_q) = 2. \end{cases}$$

For the Hermitian function field defined above, we have $m_F \geq q - 1 \geq 2g_F$ [6]. This implies that m_F can indeed be linear in g_F. But the question is how m_F behaves asymptotically as g_F tends to infinity. Can m_F grow linearly with g_F when $g_F \to \infty$? Our result shows that m_F grows much more slowly than g_F. In fact, in this paper, we show that g_F grows at least as fast as $\Omega(m_F \log m_F)$ asymptotically. Thus, to study the asymptotic behavior of m_F as g_F tends to infinity, we define the asymptotic quantity

$$M_q = \limsup_{g_F \to \infty} \frac{m_F \cdot \log_q m_F}{g_F}$$

for every prime power q. We will see later that M_q is a positive constant. The main purpose of the first part of this paper is to find some reasonable lower and upper bounds on M_q.

The second part of this paper is to study the maximum size b_F of subgroups of $\mathrm{Aut}(F/\mathbb{F}_q)$ whose order is coprime to q, i.e.,

$$b_F = \max\{|\mathcal{G}| : \mathcal{G} \leq \mathrm{Aut}(F/\mathbb{F}_q) \text{ and } \gcd(|\mathcal{G}|, q) = 1\}.$$

The Hurwitz bound gives an upper bound $b_F \leq 84(g_F - 1)$ for every function field $F/\mathbb{F}_q$ of genus $g_F \geq 2$ [12,13]. The Hermitian function field H gives $b_H \geq q - 1$ [6]. However, in this case, both b_H and g_H depend on q. Therefore, the Hermitian function field does not provide any information on the asymptotic behavior of b_F. In this paper, we show that, over a fixed q, b_F can grow linearly in g_F. To prove our result, we introduce the following asymptotic quantity:

$$B_q = \limsup_{g_F \to \infty} \frac{b_F}{g_F},$$

where F runs through all function fields over $\mathbb{F}_q$. It follows from the Hurwitz bound that $B_q \leq 84$. As far as we know, there are no lower bounds on B_q in the literature. One does not even know whether $B_q = 0$. In this paper, we show that $B_q \geq 2/3$ by explicitly constructing some towers of function fields. This means that b_F can grow linearly with g_F when $g_F \to \infty$.

The paper is organized as follows. In section 2, we will introduce some preliminaries on function fields including Hilbert's ramification theory, the conductor, cyclotomic function fields, ray class fields, and the Chebotarev density theorem. Section 3 is devoted to proving the lower and upper bounds on M_q. In section 4,

we prove a lower bound on B_q by explicitly constructing two towers of function fields.

2. Preliminaries

Let $F/\mathbb{F}_q$ be a global function field of genus $g_F \geq 2$. For a subgroup $\mathcal{G}$ of the automorphism group of $F/\mathbb{F}_q$, denote by $F^{\mathcal{G}}$ the fixed subfield of F with respect to $\mathcal{G}$, that is,

$$F^{\mathcal{G}} = \{z \in F | \sigma(z) = z \text{ for any } \sigma \in \mathcal{G}\}.$$

Then $F/F^{\mathcal{G}}$ is a Galois extension with the Galois group $\mathrm{Gal}(F/F^{\mathcal{G}}) = \mathcal{G}$.

2.1. **Hilbert's ramification theory.**

The Hurwitz genus formula yields

$$2g_F - 2 = |\mathcal{G}| \cdot (2g(F^{\mathcal{G}}) - 2) + \deg \mathrm{Diff}(F/F^{\mathcal{G}}),$$

where $\mathrm{Diff}(F/F^{\mathcal{G}})$ stands for the different of the extension $F/F^{\mathcal{G}}$ (see [23, Theorem 3.4.13]).

Let $\mathbb{P}_F$ denote the set of places of F. For a place $P \in \mathbb{P}_F$ and a place Q with $Q = P \cap F^{\mathcal{G}}$ being the restriction of P to $F^{\mathcal{G}}$, we denote by $d_P(F/F^{\mathcal{G}})$, $e_P(F/F^{\mathcal{G}})$ (resp., $d(P|Q)$ and $e(P|Q)$) the different exponent (resp., ramification index of $P|Q$). Then the different of $F/F^{\mathcal{G}}$ is given by

$$\mathrm{Diff}(F/F^{\mathcal{G}}) = \sum_{P \in \mathbb{P}_F} d_P(F/F^{\mathcal{G}})P.$$

If $P|Q$ is unramified or tamely ramified, then $d_P(F/F^{\mathcal{G}}) = e_P(F/F^{\mathcal{G}}) - 1$ by Dedekind's different theorem [23, Theorem 3.5.1]. However, if $P|Q$ is wildly ramified, that is, if $e_P(F/F^{\mathcal{G}})$ is divisible by $\mathrm{char}(\mathbb{F}_q)$, then it is more complicated to calculate the different exponent $d_P(F/F^{\mathcal{G}})$. One way to find the different exponent $d_P(F/F^{\mathcal{G}})$ is through ramification groups and Hilbert's different theorem.

The ith ramification group $\mathcal{G}_i(P)$ of $P|Q$ for each $i \geq -1$ is defined by

$$\mathcal{G}_i(P) = \{\sigma \in \mathcal{G} | v_P(\sigma(z) - z) \geq i + 1 \text{ for all } z \in \mathcal{O}_P\},$$

where $\mathcal{O}_P$ stands for the integral ring of P in F and v_P is the normalized discrete valuation of F corresponding to the place P. If $P|Q$ is wildly ramified, then the different exponent $d_P(F/F^{\mathcal{G}})$ is

$$d_P(F/F^{\mathcal{G}}) = \sum_{i=0}^{\infty} \Big(|\mathcal{G}_i(P)| - 1\Big)$$

by Hilbert's different theorem [23, Theorem 3.8.7]. Let $a_P(F/F^{\mathcal{G}})$ be the least nonnegative integer l such that the ramification groups $\mathcal{G}_i(P)$ are trivial for all $i \geq l$. Then we have

$$d_P(F/F^{\mathcal{G}}) = \sum_{i=0}^{a_P(F/F^{\mathcal{G}})-1} \Big(|\mathcal{G}_i(P)| - 1\Big) \geq a_P(F/F^{\mathcal{G}}).$$

2.2. **Conductor.** For a real number x, we extend the above definition of ramification groups to real numbers $x \geq -1$ by putting $\mathcal{G}_x(P) = \mathcal{G}_{\lceil x \rceil}(P)$, where $\lceil x \rceil$ is the least integer $\geq x$. Let g_x be the order of the xth ramification group $\mathcal{G}_x(P)$. Define the function $\varphi(x)$ for $x \geq -1$ by putting

$$\varphi(x) = \int_0^x \frac{1}{[\mathcal{G}_0(P) : \mathcal{G}_t(P)]} dt,$$

where $[\mathcal{G}_0(P) : \mathcal{G}_t(P)] = [\mathcal{G}_t(P) : \mathcal{G}_0(P)]^{-1}$ if $t \leq 0$. Explicitly, we have

$$\varphi(x) = \frac{1}{g_0}\Big(g_1 + g_2 + \cdots + g_{\lfloor x \rfloor} + (x - \lfloor x \rfloor) g_{\lfloor x \rfloor + 1}\Big)$$

for $x > 0$, and $\varphi(x) = x$ for $-1 \leq x \leq 0$. Then the function φ is continuous, piecewise linear, strictly monotone increasing, and concave on $[-1, \infty)$ (see [1, Chapter XI.2]).

Now we define the function ψ to be the inverse function of φ, and we define the vth upper index ramification group by

$$\mathcal{G}^v(P) := \mathcal{G}_{\psi(v)}(P).$$

Then we have $\mathcal{G}^{-1}(P) = \mathcal{G}_{-1}(P)$, $\mathcal{G}^0(P) = \mathcal{G}_0(P)$, and $\mathcal{G}^v(P) = \{\mathrm{id}\}$ for sufficiently large v.

The conductor exponent $c_P(F/F^{\mathcal{G}})$ can be equivalently defined to be the least nonnegative integer k such that the upper index ramification group $\mathcal{G}^v(P)$ is trivial for all $v \geq k$ (see [18, Definition 3.3.3 and Theorem 3.8.10]). Moreover, we have the following relations:

$$c_P(F/F^{\mathcal{G}}) = \frac{d_P(F/F^{\mathcal{G}}) + a_P(F/F^{\mathcal{G}})}{e_P(F/F^{\mathcal{G}})} \leq 2 \cdot \frac{d_P(F/F^{\mathcal{G}})}{e_P(F/F^{\mathcal{G}})}. \tag{1}$$

It is well known that $c_P(F/F^{\mathcal{G}}) = 0$ if and only if P is unramified in $F/F^{\mathcal{G}}$, $c_P(F/F^{\mathcal{G}}) = 1$ if and only if P is tamely ramified in $F/F^{\mathcal{G}}$, and $c_P(F/F^{\mathcal{G}}) \geq 2$ if and only if P is wildly ramified in $F/F^{\mathcal{G}}$ (see [19, Theorem 2.3.4]).

Define the conductor of $F/F^{\mathcal{G}}$ by

$$\mathrm{Cond}(F/F^{\mathcal{G}}) = \sum_{P \in \mathbb{P}_F} c_P(F/F^{\mathcal{G}}) P.$$

It is clear that the conductor of $F/F^{\mathcal{G}}$ measures the ramification of the extension $F/F^{\mathcal{G}}$.

2.3. **Cyclotomic function fields.** In this subsection, we briefly review some of the fundamental notions and results of cyclotomic function fields. The theory of cyclotomic function fields was developed in the language of function fields by Hayes (see [10, 19]).

Let q be a prime power. Let x be an indeterminate over $\mathbb{F}_q$, let $R = \mathbb{F}_q[x]$ be the polynomial ring, let $k = \mathbb{F}_q(x)$ be the quotient field of R, and let k^{ac} be the algebraic closure of k. Let φ be the endomorphism given by

$$\varphi(z) = z^q + xz$$

for all $z \in k^{\mathrm{ac}}$. Define a ring homomorphism

$$R \to \mathrm{End}_{\mathbb{F}_q}(k^{\mathrm{ac}}), \qquad f(x) \mapsto f(\varphi).$$

Then the $\mathbb{F}_q$-vector space of k^{ac} is made into an R-module by introducing the following action of R on k^{ac}—namely,

$$z^{f(x)} = f(\varphi)(z)$$

for all $f(x) \in R$ and $z \in k^{\mathrm{ac}}$. For a nonzero polynomial $M \in R$, we consider the set of M-torsion points of k^{ac} defined by

$$\Lambda_M = \{z \in F^{\mathrm{ac}} | z^M = 0\}.$$

In fact, z^M is a separable polynomial of degree q^d, where $d = \deg(M)$. The cyclotomic function field over k with modulus M is defined by the subfield of k^{ac} generated over k by all elements of Λ_M, and it is denoted by $k(\Lambda_M)$. In particular, we list the following facts.

Proposition 2.1. *Let P be a monic irreducible polynomial of degree d in R, and let n be a positive integer. Then the following hold:*

(i) $[k(\Lambda_{P^n}) : k] = \phi(P^n)$, *where $\phi(P^n)$ is the Euler function of P^n, i.e., $\phi(P^n) = q^{(n-1)d}(q^d - 1)$.*

(ii) $\mathrm{Gal}(k(\Lambda_{P^n})/k) \cong (\mathbb{F}_q[x]/(P^n))^*$. *The Galois automorphism σ_f associated with $\overline{f} \in (\mathbb{F}_q[x]/(P^n))^*$ is determined by $\sigma_f(\lambda) = \lambda^f$ for $\lambda \in \Lambda_{P^n}$.*

(iii) *The zero place of P in k, also denoted by P, is totally ramified in $k(\Lambda_{P^n})$ with different exponent $d_P(k(\Lambda_{P^n})/k) = n(q^d - 1)q^{d(n-1)} - q^{d(n-1)}$. All other finite places of k are unramified in $k(\Lambda_{P^n})/k$.*

(iv) *The infinite place ∞ of k splits into $\phi(P^n)/(q-1)$ places of $k(\Lambda_{P^n})$, and the ramification index $e_\infty(k(\Lambda_{P^n})/k)$ is equal to $q-1$. In particular, $\mathbb{F}_q$ is the full constant field of $k(\Lambda_{P^n})$.*

(v) *The genus of $k(\Lambda_{P^n})$ is given by*

$$2g(k(\Lambda_{P^n})) - 2 = q^{d(n-1)}\Big[(qdn - dn - q)\frac{q^d - 1}{q-1} - d\Big].$$

2.4. **Ray class fields.** Let $E/\mathbb{F}_q$ be a global function field. Let $\mathrm{Div}^0(E)$ be the subgroup of the divisor group $\mathrm{Div}(E)$ that consists of all divisors of E of degree 0. The principal divisor group $\mathrm{Princ}(E) = \{\mathrm{div}(x) : x \in E^*\}$ is a subgroup of $\mathrm{Div}^0(E)$. The factor group $\mathrm{Cl}(E) := \mathrm{Div}^0(E)/\mathrm{Princ}(E)$ is called the divisor class group of degree 0 of E, and the cardinality of $\mathrm{Cl}(E)$ is called the divisor class number of E, which is denoted by h_E.

We fix a place ∞ of $E/\mathbb{F}_q$ of degree t. Denote by S_∞ the set $\mathbb{P}_E \setminus \{\infty\}$. Let A be the holomorphy ring $\mathcal{O}_{S_\infty}$, i.e.,

$$A = \{x \in E : \ v_Q(x) \geq 0 \text{ for all } Q \neq \infty\}.$$

Let Fr_∞ and Princ_∞ denote the fractional S_∞-ideal group and principal S_∞-ideal group of A, respectively. Then the fractional ideal class group $\mathrm{Cl}(A) := \mathrm{Fr}_\infty/\mathrm{Princ}_\infty$ of A is a finite abelian group with cardinality $h(A) = t \cdot h_E$ [20].

Let $D = \sum_Q v_Q(D)Q$ be a positive divisor of E with $\infty \notin \mathrm{supp}(D)$. For $x \in E^*$, $x \equiv 1 (\mathrm{mod}\ D)$ means that x satisfies the following condition:

$$v_Q(x-1) \geq v_Q(D) \qquad \text{for each } Q \in \mathrm{supp}(D).$$

Let $\mathrm{Fr}_{D,\infty}$ be the subgroup of Fr_∞ consisting of the S_∞-ideals that are relatively prime to D, that is,

$$\mathrm{Fr}_{D,\infty} = \{I \in \mathrm{Fr}_\infty : \ v_Q(I) = 0 \text{ for all } Q \in \mathrm{supp}(D)\}.$$

Define the subgroup $\mathrm{Princ}_{D,\infty}$ of $\mathrm{Fr}_{D,\infty}$ by

$$\mathrm{Princ}_{D,\infty} = \{(xA) : \ x \in E^*, x \equiv 1 (\mathrm{mod}\ D)\}.$$

The factor group $\mathrm{Fr}_{D,\infty}/\mathrm{Princ}_{D,\infty}$ is called the S_∞-ray class group modulo D. It is a finite group and is denoted by $\mathrm{Cl}_D(A)$. If $D = 0$, then $\mathrm{Cl}_D(A) = \mathrm{Cl}(A)$.

The S_∞-ray class field modulo D, denoted by E_∞^D, is constructed as a finite abelian extension of E corresponding to a certain open subgroup of the idèle class group of E with finite index in which the Galois group is isomorphic to $\mathrm{Cl}_D(A)$ (see [19, section 2.5]). The ray class field E_∞^D is the largest finite abelian extension F of E such that the place ∞ splits completely in F/E and the conductor divisor $\mathrm{Cond}(F/E) \leq D$. The degree and genus formula of the ray class field E_∞^D can be found from [2]. For a positive divisor $D = \sum_{j=1}^s c_j Q_j$, we denote by $\phi(D)$ the Euler function of D, i.e., $\phi(D) = \prod_{j=1}^s (q^{\deg(Q_j)} - 1) q^{(c_j-1)\deg(Q_j)}$.

Proposition 2.2 (See [2]). *Let ∞ be a place of E of degree $t > 0$. Let $D = \sum_{j=1}^s c_j Q_j$ be a positive divisor of E with $\infty \notin \mathrm{supp}(D)$. Let h_E and g_E be the class number and the genus of E, respectively. Then we have as follows:*

(1) $[E_\infty^D : E] = \frac{1}{q-1} \cdot h_E \cdot t \cdot \phi(D)$.

(2) *The genus of E_∞^D is*

$$g(E_\infty^D) = 1 + \frac{h_E}{2q-2}\big[\phi(D)(2g_E - 2 + \deg(D)) - w\big],$$

where $w = [\phi(D)/\phi(Q_1) - q - 2] \cdot \deg(Q_1)$ if D is the multiple of a single place Q_1, and $w = \sum_{j=1}^s \phi(D)\deg(Q_j)/\phi(Q_j)$ otherwise.

2.5. **Chebotarev density theorem.** Let F/E be a Galois extension of degree m of global function fields over the same full constant field $\mathbb{F}_q$. For a place P of F lying over Q of E, let $[\frac{F/E}{P}]$ be the Frobenius automorphism of P over Q. Then, for any automorphism $\sigma \in \mathrm{Gal}(F/E)$, the Frobenius automorphism of $\sigma(P)$ is $\sigma[\frac{F/E}{P}]\sigma^{-1}$. The conjugacy class

$$\Big\{\sigma\big[\frac{F/E}{P}\big]\sigma^{-1} : \sigma \in \mathrm{Gal}(F/E)\Big\}$$

is determined by Q. Hence, we denote this conjugacy class by $[\frac{F/E}{Q}]$. The Chebotarev density theorem, in many different forms, gives an equidistribution result for the occurrence of conjugacy classes as the Frobenius class of places. An example of such a theorem is [21, Theorem 9.13B].

Theorem 2.3 (Chebotarev density theorem). *Let F/E be a finite Galois extension of global function fields, and let $\mathcal{C}$ be a conjugacy class in* $\mathrm{Gal}(F/E)$. *Let U_E denote the set of places of E that are unramified in F. Then, for every positive integer $k \geq 1$, one has*

$$\left|\left\{Q \in U_E : \ [\frac{F/E}{Q}] = \mathcal{C},\ \deg(Q) = k\right\}\right| = \frac{|\mathcal{C}|}{[F:E]} \times \frac{q^k}{k} + O\left(\frac{q^{k/2}}{k}\right).$$

The above Chebotarev density theorem tells us the asymptotic behavior of how places of E split in F. For our purposes, we need an explicit version of the Chebotarev density theorem. Let x be a separating transcendent element of E over $\mathbb{F}_q$. Let $d = [E : \mathbb{F}_q(x)]$. For a conjugacy class $\mathcal{C}$ of $\mathrm{Gal}(F/E)$, let $N_k(F/E, \mathcal{C})$ denote the number of places Q of degree k in E which are unramified in both F/E and

$E/\mathbb{F}_q(x)$ such that $[\frac{F/E}{Q}] = \mathcal{C}$. Then the following result holds true from [5, Proposition 6.4.8], [17], or from [8, Theorem 3.7].

Proposition 2.4. *Notations are given as above. Then one has*

$$\left|N_k(F/E,\mathcal{C}) - \frac{|\mathcal{C}|}{km}q^k\right| \le \frac{2|\mathcal{C}|}{km}(m+g_F)q^{k/2} + m(2g_E+1)q^{k/4} + g_F + dm.$$

3. Asymptotic behavior of abelian subgroups of automorphism groups

The main result of this section is to show that M_q is between 2 and 3 for odd characteristic (or 4 for even characteristic).

3.1. **Finding a suitable ray class field.** Let $F/\mathbb{F}_q$ be a global function field of genus $g_F \ge 2$, and let $\mathcal{G}$ be an abelian subgroup of $\mathrm{Aut}(F/\mathbb{F}_q)$ with $m_F = |\mathcal{G}|$. The main purpose of this subsection is to show that F is contained in the ray class group $\left(F^{\mathcal{G}}\right)^D_\infty$ for some lower-degree place ∞ and lower-degree positive divisor D. The idea works as follows. Assume that there exists a place ∞ of $F^{\mathcal{G}}$ such that ∞ splits completely in $F/F^{\mathcal{G}}$. Let D be the conductor divisor of $F/F^{\mathcal{G}}$; then F is a subfield of $\left(F^{\mathcal{G}}\right)^D_\infty$ from the conductor theorem [19, Theorem 2.5.4]. Hence, we need to find a place ∞ of $F^{\mathcal{G}}$ that splits completely in $F/F^{\mathcal{G}}$. This can be done via the Chebotarev density theorem.

For convenience, we denote by E the function field $F^{\mathcal{G}}$.

Proposition 3.1. *Put $t = \lceil 6\log_q g_F + 18\rceil$. Then there exists a place ∞ of degree t of E such that ∞ splits completely in F/E.*

Proof. For any place $P \in \mathbb{P}_E$ and each integer $k \ge 2g_E$, there exists an element $x \in E$ with pole divisor $(x)_\infty = k\cdot P$ from Riemann's theorem (see [23, Proposition 1.6.6]). Hence, we can find a separating transcendence element x of $E/\mathbb{F}_q$ with $d = [E:\mathbb{F}_q(x)] = \ell\cdot t$ for some positive integer $\ell \le 2g_E+1$ (note that if $2g_E$ is divisible by the characteristic, we choose $\ell = 2g_E+1$; otherwise we let $\ell = 2g_E$).

Let $\mathcal{C}$ be the conjugacy class containing the identity automorphism of F/E. Then it is clear that it is now sufficient to prove

$$N_t(F/E,\mathcal{C}) \ge 1.$$

By Proposition 2.4, we have the following inequality:

$$N_t(F/E,\mathcal{C}) \ge \frac{1}{m_F t}q^t - \left(\frac{2}{m_F t}(m_F+g_F)q^{t/2} + m_F(2g_E+1)q^{t/4} + g_F + dm_F\right).$$

Thus, we need to prove that the right-hand side of the above inequality is positive.

First, we note that we have (i) $m_F = [F:E] \le 4g_F+4$ (note that $\mathcal{G}$ is an abelian subgroup of $\mathrm{Aut}(F/\mathbb{F}_q)$), (ii) $g_E \le g_F$, and (iii) $d = \ell t \le (2g_E+1)t \le (2g_F+1)t$. Thus, we have

$$\frac{2}{m_F t}(m_F+g_F)q^{t/2} \le \frac{2}{m_F t}\left(4g_F+4+g_F\right)q^{t/2} \le \frac{1}{4}\cdot\frac{1}{m_F t}q^t,$$

$$m_F(2g_E+1)q^{t/4} \le (4g_F+4)(2g_F+1)q^{t/4} \le \frac{1}{4}\cdot\frac{1}{(4g_F+4)t}q^t \le \frac{1}{4}\cdot\frac{1}{m_F t}q^t,$$

$$g_F < \frac{1}{4}\cdot\frac{1}{(4g_F+4)t}q^t \le \frac{1}{4}\cdot\frac{1}{m_F t}q^t,$$

and

$$dm_F \le (2g_F+1)t(4g_F+4) \le \frac{1}{4}\cdot\frac{1}{(4g_F+4)t}q^t \le \frac{1}{4}\cdot\frac{1}{m_F t}q^t.$$

This completes the proof. □

3.2. **Bounds on M_q.** Again, we assume that $F/\mathbb{F}_q$ is a function field of genus $g_F \ge 2$, and we let $\mathcal{G}$ be an abelian subgroup of $\mathrm{Aut}(F/\mathbb{F}_q)$ with $|\mathcal{G}| = m_F$. Put $E = F^{\mathcal{G}}$. By Proposition 3.1, there exists a place ∞ of E with degree $t = \lceil 6\log_q g_F + 18\rceil$. Let the effective divisor $D = \sum_{i=1}^{s} c_i Q_i$ be the conductor of F/E. Then F is a subfield of E_∞^D. Moreover, we have

$$[E_\infty^D : E] = h_E \cdot t \cdot \frac{1}{q-1}\cdot\prod_{i=1}^{s}(q^{\deg(Q_i)}-1)q^{(c_i-1)\deg(Q_i)}.$$

First, we provide an upper bound for the order m_F in terms of g_F and the conductor.

Lemma 3.2. *Let $\mathcal{G}$ be an abelian subgroup of $\mathrm{Aut}(F/\mathbb{F}_q)$ with $|\mathcal{G}| = m_F$. Put $E = F^{\mathcal{G}}$. Let the divisor $D = \sum_{i=1}^{s} c_i Q_i$ be the conductor of F/E. Put $t = \lceil 6\log_q g_F + 18\rceil$. Then*

$$\log_q m_F \le \log_q t + 3g_E + \sum_{i=1}^{s} c_i \deg(Q_i).$$

Proof. First, by the Hasse–Weil theorem, we have an upper bound on the class number h_E (see [23, Theorems 5.1.15 and 5.2.1])

$$h_E \le (1+\sqrt{q})^{2g_E}.$$

Since F is a subfield of E_∞^D, we have $[F:E]$ dividing $[E_\infty^D : E]$; that is,

$$m_F | h_E \cdot t \cdot \frac{1}{q-1}\cdot\prod_{i=1}^{s}(q^{\deg(Q_i)}-1)q^{(c_i-1)\deg(Q_i)} \le t(1+\sqrt{q})^{2g_E} q^{\sum_{i=1}^{s} c_i\deg(Q_i)}.$$

Hence, we obtain

$$\log_q m_F \le \log_q t + 2g_E\log_q(1+\sqrt{q}) + \sum_{i=1}^{s} c_i\deg(Q_i) \le \log_q t + 3g_E + \sum_{i=1}^{s} c_i\deg(Q_i).$$

The proof is completed. □

Lemma 3.2 gives a relation between m_F and the conductor. This relation can be turned into a relation between m_F and g_F, as shown below.

Proposition 3.3. *Let $F/\mathbb{F}_q$ be a global function field. Put $t = \lceil 6\log_q g_F + 18\rceil$. Then we have*

$$g_F \ge \frac{1}{4}m_F\log_q m_F - \frac{1}{4}m_F\log_q t - m_F + 1.$$

Proof. Let $\mathcal{G}$ be an abelian subgroup of $\mathrm{Aut}(F/\mathbb{F}_q)$ with $|\mathcal{G}| = m_F$. Let the divisor $D = \sum_{i=1}^{s} c_i Q_i$ be the conductor of F/E. The Hurwitz genus formula [23, Theorem 3.4.13] yields

$$2g_F - 2 = m_F\cdot(2g_E-2) + \sum_{i=1}^{s}\sum_{P|Q_i} d(P|Q_i)\deg(P).$$

As $d(P|Q_i)$, $f(P|Q_i)$, and $e(P|Q_i)$ depend only on Q_i, we may denote $d(P|Q_i)$, $f(P|Q_i)$, and $e(P|Q_i)$ by $d(Q_i)$, $f(Q_i)$, and $e(Q_i)$, respectively. First, we have

$$\begin{aligned}\sum_{P|Q_i} d(Q_i)\deg(P) &= \sum_{P|Q_i} d(Q_i)f(Q_i)\deg(Q_i)\\ &= \frac{d(Q_i)}{e(Q_i)}\deg(Q_i)\sum_{P|Q_i} e(Q_i)f(Q_i) = \frac{d(Q_i)}{e(Q_i)}\deg(Q_i)m_F.\end{aligned}$$

The last equality holds from the fundamental equality (see [23, Theorem 3.1.11]). Thus,

$$2g_F - 2 = m_F \cdot (2g_E - 2) + m_F \cdot \sum_{i=1}^{s} \frac{d(Q_i)}{e(Q_i)}\deg(Q_i).$$

Hence, we obtain

$$\begin{aligned}\frac{2g_F-2}{m_F} &= 2g_E - 2 + \sum_{i=1}^{s} \frac{d(Q_i)}{e(Q_i)}\deg(Q_i)\\ &\geq 2g_E - 2 + \frac{1}{2}\sum_{i=1}^{s} c_i\deg(Q_i)\\ &= \frac{3}{2}g_E + \frac{1}{2}\sum_{i=1}^{s} c_i\deg(Q_i) + \frac{1}{2}g_E - 2\\ &\geq \frac{1}{2}\log_q m_F - \frac{1}{2}\log_q t - 2.\end{aligned}$$

The first inequality follows from equation (1) in subsection 2.2, and the last inequality follows from Lemma 3.2. This completes the proof. □

Let us give a lower bound by considering the cyclotomic function fields.

Example 1. Let F be the cyclotomic function field $\mathbb{F}_q(x)(\Lambda_P)$, where P is an irreducible polynomial of degree d in $\mathbb{F}_q[x]$. The Galois group of $F/\mathbb{F}_q(x)$ is a cyclic group of order $q^d - 1$. Then the maximum size m_F of abelian subgroups of the automorphism group $\mathrm{Aut}(F/\mathbb{F}_q)$ is $m_F \geq q^d - 1$. By the Hurwitz genus formula and Proposition 2.1, the genus of F is

$$2g_F - 2 = (q^d - 1)(-2) + (q^d - 2)d + \frac{q-2}{q-1}(q^d - 1).$$

Hence, this gives a lower bound on M_q:

$$M_q \geq \lim_{d\to\infty} \frac{m_F \cdot \log_q m_F}{g_F} = 2.$$

The above example provides a lower bound on M_q for the case in which $|\mathcal{G}|$ is coprime to the characteristic. The next example gives the same lower bound on M_q for the case in which $|\mathcal{G}|$ is divisible by the characteristic.

Example 2. Let F_n be the cyclotomic function field $\mathbb{F}_q(x)(\Lambda_{P^n})$, where P is an irreducible polynomial of degree d in $\mathbb{F}_q[x]$ and $n \geq 2$. The Galois group of $F_n/\mathbb{F}_q(x)$ is an abelian group of order $(q^d-1)q^{d(n-1)}$. Then the maximum size m_{F_n} of abelian

subgroups of the automorphism group $\mathrm{Aut}(F_n/\mathbb{F}_q)$ is $m_{F_n} \geq (q^d-1)q^{(n-1)d}$. By the Hurwitz genus formula and Proposition 2.1, the genus of F_n is

$$2g_{F_n}-2 = (q^d-1)q^{d(n-1)}(-2)+\left[n(q^d-1)q^{d(n-1)}-q^{d(n-1)}\right]d+\frac{q-2}{q-1}(q^d-1)q^{d(n-1)}.$$

Hence, this gives a lower bound on M_q:

$$M_q \geq \lim_{n\to\infty} \frac{m_{F_n}\cdot \log_q m_{F_n}}{g_{F_n}} = 2.$$

Theorem 3.4. *For every prime power q, one has*

$$2 \leq M_q \leq 4.$$

Proof. The lower bound $M_q \geq 2$ is given in Examples 1 and 2. We now prove the upper bound.

Let $\{F/\mathbb{F}_q\}$ be a family of function fields with $g_F \to \infty$ and $M_q = \lim_{g_F\to\infty} \frac{m_F \log_q m_F}{g_F}$. By Examples 1 and 2, one has the result that, for sufficiently large g_F, $\frac{m_F \log_q m_F}{g_F} \geq M_q/2 \geq 1$, i.e., $g_F \leq m_F \log_q m_F$.

Without loss of generality, we may assume that $g_F \geq 2$ for every function field F in this family. By Proposition 3.3, we have

$$\begin{aligned} g_F &\geq \frac{1}{4}m_F \log_q m_F - \frac{1}{4}m_F \log_q t - m_F + 1 \\ &\geq \frac{1}{4}m_F \log_q m_F - \frac{1}{4}m_F \log_q(6\log_q g_F + 18) - m_F + 1 \\ &\geq \frac{1}{4}m_F \log_q m_F - \frac{1}{4}m_F \log_q(6\log_q(m_F \log_q m_F) + 18) - m_F + 1. \end{aligned}$$

Dividing both sides of the above inequality by $m_F \log_q m_F$ and taking limits, one obtains $\lim_{g_F\to\infty} \frac{g_F}{m_F \log_q m_F} \geq \frac{1}{4}$. The desired result follows. □

The upper bound given in the above theorem holds for both even and odd characteristics. However, for odd characteristic, we can refine the proof of Proposition 3.3 by better estimating the different exponent. Let us prove a lemma first.

Lemma 3.5. *Let F/E be a finite abelian extension of global function fields, and let Q be a place of E with conductor exponent $c = c_Q(F/E) \geq 2$. Let $e = bp^w$ be the ramification index of Q in the extension F/E, where p is the characteristic of F, $p \nmid b$ and w is a positive integer. Then the different exponent $d_Q(F/E)$ of Q in F/E has a lower bound*

$$d_Q(F/E) \geq cbp^w - 1 - b - (c-2)bp^{w-1}.$$

Proof. Let P be a place of F lying over Q. Let g_i be the order of $\mathcal{G}_i(P)$, and let a be the least nonnegative integer k such that $\mathcal{G}_i(P)$ are trivial for all $i \geq k$. As the different exponent $d(P|Q)$ of $P|Q$ does not depend on the choice of P, we denote $d(P|Q)$ by $d_Q(F/E)$. Then the different exponent $d = d_Q(F/E)$ of Q in F/E is calculated by

$$d = \sum_{i=0}^{a-1}(g_i - 1)$$

from Hilbert's different theorem [23, Theorem 3.8.7]. The ramification theory of the Galois extension yields $g_0 = e = bp^w$ and $g_1 = p^w$ [23, Proposition 3.8.5]. Let

n_j be the number of integers $i \geq 1$ with $g_i = p^{w-j+1}$ for $1 \leq j \leq w$. Furthermore, we have

$$a = 1 + \sum_{j=1}^{w} n_j, \qquad d = ce - a = ce - 1 - \sum_{j=1}^{w} n_j.$$

The Hasse–Arf theorem'[19, Proposition 2.3.3] shows that $g_0 | \sum_{i=1}^{n_1} g_i = n_1 p^w$ since $\mathcal{G}_{n_1}(P) \neq \mathcal{G}_{n_1+1}(P)$. It follows that $b | n_1$ and $n_1 \geq b$. For $c \geq 2$, we have

$$\begin{aligned} ce = d + a &= \sum_{i=0}^{a-1} g_i = g_0 + \sum_{j=1}^{w} n_j p^{w-j+1} \\ &= e + b \cdot p^w + (n_1 - b)p^w + \sum_{j=2}^{w} n_j p^{w-j+1} \\ &\geq 2e + (n_1 - b)p + \sum_{j=2}^{w} n_j p = 2e - bp + \sum_{j=1}^{w} n_j p. \end{aligned}$$

It is clear that $b + (c-2)bp^{w-1} \geq \sum_{j=1}^{w} n_j$ from the above inequality and $e = bp^w$. Hence, the different exponent $d_Q(F/E)$ has a lower bound

$$d_Q(F/E) = d = ce - 1 - \sum_{j=1}^{w} n_j \geq cbp^w - 1 - b - (c-2)bp^{w-1}.$$

The proof is complete. □

Theorem 3.6. *Assume that the characteristic p of $\mathbb{F}_q$ is odd. Let $F/\mathbb{F}_q$ be a global function field. Put $t = \lceil 6 \log_q g_F + 18 \rceil$. Then we have*

$$g_F \geq \frac{1}{3} m_F \log_q m_F - \frac{1}{3} m_F \log_q t - m_F + 1.$$

As a consequence, we have $M_q \leq 3$.

Proof. We use the same notations as in the proof of Proposition 3.3. Let the divisor $D = \sum_{i=1}^{r} Q_i + \sum_{j=r+1}^{s} c_j Q_j$, with $c_j \geq 2$, be the conductor of F/E. Then the Hurwitz genus formula yields

$$\frac{2g_F - 2}{m_F} = 2g_E - 2 + \sum_{i=1}^{s} \frac{d(Q_i)}{e(Q_i)} \deg(Q_i).$$

Suppose that there are exactly r_0 places of E with ramification index 2. Without loss of generality, we can assume that

$$\frac{d(Q_i)}{e(Q_i)} = 1 - \frac{1}{e(Q_i)} = \frac{1}{2}$$

for $1 \leq i \leq r_0$. For other tamely ramified places Q_i with $r_0 + 1 \leq i \leq r$, we have

$$\frac{d(Q_i)}{e(Q_i)} = 1 - \frac{1}{e(Q_i)} \geq \frac{2}{3}.$$

For the wildly ramified places Q_j with ramification index $e(Q_j) = b_j p^{w_j}$, the following inequality,

$$\frac{d(Q_j)}{e(Q_j)} \geq \frac{c_j b_j p^{w_j} - 1 - b_j - (c_j - 2)p^{w_j - 1}}{b_j p^{w_j}} \geq \frac{2}{3} c_j,$$

holds true for each $r + 1 \leq j \leq s$ from Lemma 3.5 and $p \geq 3$.

Since the extension F/E is abelian, we have

$$m_F|h_E\cdot t\cdot\prod_{i=1}^{s}e(Q_i)\le q^{2g_E}\cdot t\cdot 2^{r_0}\cdot\prod_{i=r_0+1}^{r}(q^{\deg(Q_i)}-1)\cdot\prod_{j=r+1}^{s}(q^{\deg(Q_j)}-1)q^{(c_j-1)\deg(Q_j)}.$$

Hence, we have

$$\log_q m_F-\log_q t\le 2g_E+r_0\log_q 2+\sum_{i=r_0+1}^{r}\deg(Q_i)+\sum_{j=r+1}^{s}c_j\deg(Q_j).$$

It follows that

$$\begin{aligned}\frac{2g_F-2}{m_F}&\ge 2g_E-2+\frac{1}{2}\sum_{i=1}^{r_0}\deg(Q_i)+\frac{2}{3}\sum_{i=r_0+1}^{r}\deg(Q_i)+\frac{2}{3}\sum_{j=r+1}^{s}c_j\deg(Q_j)\\&\ge\frac{2}{3}\Big[2g_E+r_0\log_q 2+\sum_{i=r_0+1}^{r}\deg(Q_i)+\sum_{j=r+1}^{s}c_j\deg(Q_j)\Big]\\&\quad+\frac{2g_E}{3}-2+\frac{1}{2}\sum_{i=1}^{r_0}\deg(Q_i)-\frac{2}{3}r_0\log_q 2\\&\ge\frac{2}{3}\log_q m_F-\frac{2}{3}\log_q t+\frac{2g_E}{3}-2+\frac{r_0}{6}\big(3-4\log_q 2\big)\\&\ge\frac{2}{3}\log_q m_F-\frac{2}{3}\log_q t-2.\end{aligned}$$

Hence, we obtain

$$g_F\ge\frac{1}{3}m_F\log_q m_F-\frac{1}{3}m_F\log_q t-m_F+1.$$

The desired result for $M_q\le 3$ follows. □

4. Asymptotic behavior of subgroups whose order is coprime to q

The main purpose of this section is to provide a linear lower bound by constructing some tame towers of function fields which are recursively defined over $\mathbb{F}_q$.

4.1. **Towers of function fields.** First, let us introduce some basic definitions and results of towers of function fields. For more results on towers of function fields, please refer to [3, 23, 24]. A tower of function fields over $\mathbb{F}_q$ is an infinite sequence $\mathcal{F}=(F_0,F_1,F_2,\cdots)$ of function fields $F_n/\mathbb{F}_q$ with the following properties:

(i) $F_0\subsetneq F_1\subsetneq\cdots\subsetneq F_n\subsetneq F_{n+1}\cdots$.
(ii) The extension F_{n+1}/F_n is finite and separable for each $n\ge 0$.
(iii) The genera satisfy $g_{F_n}\to\infty$ for $n\to\infty$.

We say that the tower $\mathcal{F}=(F_0,F_1,F_2,\cdots)$ is tame if every place of F_0 is unramified or tamely ramified in the extension F_n/F_0 for any $n\ge 1$.

Definition 4.1. Let $\mathcal{F}=(F_0,F_1,F_2,\cdots)$ be an infinite sequence of function fields over $\mathbb{F}_q$, and let $f(T),h(T)\in\mathbb{F}_q(T)$ be two separable rational functions with $\deg(f)\ge 2$ (i.e., $\deg(f)=-v_{P_\infty}(f)$, where v_{P_∞} is the normalized discrete valuation at the infinite place). We say that the sequence $\mathcal{F}$ can be described recursively by the equation

$$f(Y)=h(X)$$

if there are elements y_n for all $n\ge 0$ such that the following hold true:

(1) $F_0 = \mathbb{F}_q(y_0)$, where y_0 is transcendental over $\mathbb{F}_q$;
(2) $F_{n+1} = F_n(y_{n+1})$, where $f(y_{n+1}) = h(y_n)$ for every $n \geq 0$;
(3) $[F_{n+1} : F_n] = \deg(f)$ for every $n \geq 0$.

We define the corresponding basic function field F of the sequence as

$$F := \mathbb{F}_q(x, y) \qquad \text{with } f(y) = h(x).$$

Definition 4.2. Let $\mathcal{F} = (F_0, F_1, F_2, \cdots)$ be a tower over $\mathbb{F}_q$.

(1) The genus $\gamma(\mathcal{F}/F_0)$ of $\mathcal{F}$ over F_0 is defined by

$$\gamma(\mathcal{F}/F_0) = \lim_{n\to\infty} \frac{g_{F_n}}{[F_n : F_0]}.$$

(2) The ramification locus of $\mathcal{F}$ over F_0 is defined by

$$\mathrm{Ram}(\mathcal{F}/F_0) = \{P \in \mathbb{P}_{F_0} |\ P \text{ is ramified in } F_n/F_0 \text{ for some } n \geq 1\}.$$

Let $\mathcal{F} = (F_0, F_1, F_2, \cdots)$ be a tame tower of function fields over $\mathbb{F}_q$. Assume that $\mathrm{Ram}(\mathcal{F}/F_0)$ is finite. For each place $P \in \mathrm{Ram}(\mathcal{F}/F_0)$ and every place $Q \in \mathbb{P}_{F_n}$ lying over P, the different exponent $d(Q|P) = e(Q|P) - 1$ since the tower $\mathcal{F}$ is tame. Then the genus $\gamma(\mathcal{F}/F_0)$ is finite and bounded by

$$\gamma(\mathcal{F}/F_0) \leq g_{F_0} - 1 + \frac{1}{2} \sum_{P\in \mathrm{Ram}(\mathcal{F}/F_0)} \deg P$$

from the Hurwitz genus formula (see [23, Theorem 7.2.10]).

In the case of a finite ramification locus, the ramification divisor of $\mathcal{F}/F_0$ is defined by

$$R(\mathcal{F}/F_0) = \sum_{P\in \mathrm{Ram}(\mathcal{F}/F_0)} P.$$

Let L be an algebraic extension of K. Then we can consider the constant field extension $\mathcal{F}L = (F_0L, F_1L, F_2L, \ldots, F_iL, \cdots)$ of the tower $\mathcal{F}$ by L. The following proposition provides a useful criterion for the finiteness of the ramification locus of recursive towers [23, Remark 7.2.22 and Proposition 7.2.23].

Proposition 4.3. *Let $\mathcal{F} = (F_0, F_1, F_2, \cdots)$ be a recursive tower over the finite field $\mathbb{F}_q$ defined by the equation $f(Y) = h(X)$. We denote by F the basic function field of $\mathcal{F}$. Let L be a finite extension of $\mathbb{F}_q$ such that all places of $L(x)$ which ramify in the extension $FL/L(x)$ are rational. Hence, the set*

$$\Lambda_0 := \{x(P) | P \in \mathbb{P}_{L(x)} \text{ is ramified in } FL/L(x)\}$$

is contained in $L \cup \{\infty\}$. Suppose that there exists a finite subset $\Lambda \supseteq \Lambda_0$ of $L \cup \{\infty\}$ such that any solution $\alpha \in \overline{\mathbb{F}_q} \cup \{\infty\}$ of the equation $h(\alpha) = f(\beta)$, for every $\beta \in \Lambda$, is still in Λ. Then the ramification locus $\mathrm{Ram}(\mathcal{F}L/F_0L)$ is finite and

$$\mathrm{Ram}(\mathcal{F}L/F_0L) \subseteq \{P \in \mathbb{P}_{F_0L} |\ y_0(P) \in \Lambda\}.$$

Furthermore, $\mathrm{Ram}(\mathcal{F}/F_0)$ is finite and $\deg R(\mathcal{F}/F_0) = \deg R(\mathcal{F}L/F_0L)$.

4.2. **Constructions of tame towers.** In this subsection, we will provide a lower bound $B_q \geq 2/3$ by explicitly constructing two tame towers of function fields.

Proposition 4.4. *Assume that* $\mathrm{char}(\mathbb{F}_q) \neq 3$. *The infinite sequence* $\mathcal{F} = (F_0, F_1, F_2, \cdots)$ *which is recursively defined over* $\mathbb{F}_q$ *by the equation*

$$Y^3 = \frac{X^2 + X + 1}{3X}$$

is a tame tower of function fields over $\mathbb{F}_q$.

Proof. First, note that $F_{n+1} = F_n(y_{n+1})$ with $y_{n+1}^3 = (y_n^2 + y_n + 1)/(3y_n)$; hence, $[F_{n+1} : F_n] \leq 3$. Since $\mathrm{char}(\mathbb{F}_q) \neq 3$, it follows that F_{n+1}/F_n is separable.

The goal is to find places $P_n \in \mathbb{P}_{F_n}$ and $P_{n+1} \in \mathbb{P}_{F_{n+1}}$ with $P_{n+1}|P_n$ such that $e(P_{n+1}|P_n) = 3$. We proceed as follows. Let $P_0 \in \mathbb{P}_{F_0}$ be the unique pole of y_0 in $F_0 = \mathbb{F}_q(y_0)$, and let $P_1 \in \mathbb{P}_{F_1}$ lie over P_0. From the equation $y_1^3 = (y_0^2 + y_0 + 1)/(3y_0)$, we obtain

$$3v_{P_1}(y_1) = v_{P_1}(y_1^3) = e(P_1|P_0)v_{P_0}\Big(\frac{y_0^2 + y_0 + 1}{3y_0}\Big) = e(P_1|P_0) \cdot (-1).$$

Hence, $e(P_1|P_0) = 3$ and $v_{P_1}(y_1) = -1$. Similarly, from the equation $y_2^3 = (y_1^2 + y_1 + 1)/(3y_1)$, there exists a place $P_2 \in \mathbb{P}_{F_2}$ with $P_2|P_1$ such that $e(P_2|P_1) = 3$ and $v_{P_2}(y_2) = -1$. By iterating this process, we obtain $P_{n+1} \in \mathbb{P}_{F_{n+1}}$ with $P_{n+1}|P_n$ such that $e(P_{n+1}|P_n) = 3$ and $v_{P_{n+1}}(y_{n+1}) = -1$ for all $n \geq 0$. Therefore, $[F_{n+1} : F_n] = e(P_{n+1}|P_n) = 3$. It follows that F_{n+1} and F_n have the same full constant field $\mathbb{F}_q$ since constant field extensions are unramified (see [23, Proposition 7.2.15]). Hence, conditions (i) and (ii) for a tower have been showed.

From the theory of Kummer extension [23, Proposition 3.7.3], exactly the following places of F_0 are ramified in F_1/F_0: the zero and the pole of y_0, the two zeros of $y_0^2+y_0+1$ or a place of degree 2, depending on the factorization of $y_0^2+y_0+1$ in $\mathbb{F}_q[y_0]$. The Hurwitz genus formula for F_1/F_0 yields $2g_{F_1} - 2 = 3 \times (2g_{F_0} - 2) + 4 \times (3 - 1)$. Hence, $g_{F_1} = 2$.

As $F_i \subsetneq F_{i+1}$, we have

$$2g_{F_{i+1}} - 2 \geq [F_{i+1} : F_i](2g_{F_i} - 2) \geq 2(2g_{F_i} - 2) = 4g_{F_i} - 4.$$

Thus, if $g_{F_i} \geq 2$, we have $2g_{F_{i+1}} \geq 4g_{F_i} - 2 \geq 3g_{F_i}$, i.e., $g_{F_{i+1}} \geq 3g_{F_i}/2 > g_{F_i}$. This implies that the genus g_{F_i} strictly increases for $i \geq 1$. Condition (iii) for a tower of function fields is satisfied. □

Theorem 4.5. *Assume that* $\mathrm{char}(\mathbb{F}_q) \neq 3$. *Let* $\mathcal{F} = (F_0, F_1, \cdots)$ *be a recursive tower defined by the equation*

$$Y^3 = \frac{X^2 + X + 1}{3X}$$

over the finite field $\mathbb{F}_q$. *Let* E_n *be the Galois closure of* F_n *over* F_0. *Then*

$$B_q \geq \limsup_{n\to\infty} \frac{|\mathrm{Gal}(E_n/F_0)|}{g_{E_n}} \geq \frac{2}{3}.$$

Proof. First, let us choose a finite field $L \supseteq \mathbb{F}_q$ such that L contains an element w of order 3. Note that if $3|(q-1)$, then we can choose $L = \mathbb{F}_q$; otherwise we let $L = \mathbb{F}_{q^2}$. From the theory of the Kummer extension, all ramified places in $FL/L(x)$

are exactly the rational places P_0, P_w, P_{w^2}, and P_∞, that is, $\Lambda_0 = \{0, w, w^2, \infty\}$. Now let us consider the set

$$\Lambda = \{0, w, w^2, \infty, 1\} \subseteq L \cup \{\infty\},$$

which satisfies the condition of Proposition 4.3. In fact, it remains to show that any solution $\alpha \in \overline{\mathbb{F}_q} \cup \{\infty\}$ of the equation

$$\frac{\alpha^2 + \alpha + 1}{3\alpha} = \beta^3$$

for every $\beta \in \Lambda$ is still in Λ. This can be verified easily as follows:

- if $\beta = \infty$, then $\alpha = \infty$ or $\alpha = 0$;
- if $\beta = 0$, then $\alpha = w$ or $\alpha = w^2$;
- if $\beta = 1, w,$ or w^2, then $\alpha = 1$.

Hence, it has been shown that the ramification locus

$$\mathrm{Ram}(\mathcal{F}L/F_0L) \subseteq \{P \in \mathbb{P}_{F_0L} | y_0(P) \in \Lambda\} = \{P_0, P_w, P_{w^2}, P_1, P_\infty\}$$

from Proposition 4.3.

Let E_n be the Galois closure of F_n over F_0. In fact, E_n is the compositum of the fields $\sigma(F_n)$, where σ runs through all embeddings $\sigma : F_n \to \overline{F_0}$ (note that $\overline{F_0} \supseteq F_0$ is the algebraic closure of F_0). If P is unramified in F_n/F_0, then P is unramified in E_n/F_0 from an immediate consequence of Abhyankar's lemma (see [23, Corollary 3.9.3]). As P is tamely ramified in F_n/F_0, it is also tamely ramified in $\sigma(F_n)/F_0$. Hence, P is tamely ramified in E_n/F_0 from Abhyankar's lemma [23, Theorem 3.9.1]. Let $\mathcal{E} = (F_0, E_1, \ldots, E_n, \cdots)$ be the Galois closure of the tower $\mathcal{F}$. Then the tower $\mathcal{E}$ is tame and $\mathrm{Ram}(\mathcal{E}/F_0) = \mathrm{Ram}(\mathcal{F}/F_0)$.

The genus $\gamma(\mathcal{E}/F_0)$ of $\mathcal{E}$ over F_0 is

$$\begin{aligned}
\gamma(\mathcal{E}/F_0) &\leq g_{F_0} - 1 + \frac{1}{2} \sum_{P \in \mathrm{Ram}(\mathcal{E}/F_0)} \deg(P) \\
&= g_{F_0} - 1 + \frac{1}{2} \sum_{P \in \mathrm{Ram}(\mathcal{F}/F_0)} \deg(P) \\
&= g_{F_0} - 1 + \frac{1}{2} \sum_{P \in \mathrm{Ram}(\mathcal{F}L/F_0L)} \deg(P) \\
&\leq \frac{3}{2}.
\end{aligned}$$

The first inequality follows from [23, Proposition 7.2.10] and the second equality follows from Proposition 4.3. Let b_{E_n} be the maximum size of subgroups of $\mathrm{Aut}(E_n/\mathbb{F}_q)$ whose order is coprime to q. The Galois group of E_n/F_0 is a subgroup of $\mathrm{Aut}(E_n/\mathbb{F}_q)$. It follows that

$$b_{E_n} \geq |\mathrm{Gal}(E_n/F_0)| = [E_n : F_0].$$

Hence, we obtain

$$B_q \geq \limsup_{n\to\infty} \frac{b_{E_n}}{g_{E_n}} \geq \limsup_{n\to\infty} \frac{[E_n : F_0]}{g_{E_n}} = \frac{1}{\gamma(\mathcal{E}/F_0)} \geq \frac{2}{3}. \qquad \square$$

Theorem 4.6. *Assume that* $\mathrm{char}(\mathbb{F}_q) \neq 2$. *Let* $\mathcal{F} = (F_0, F_1, \cdots)$ *be a recursive tower defined by the equation*

$$Y^4 = \frac{X^2+1}{2X}$$

over the finite field $\mathbb{F}_q$. *Let* E_n *be the Galois closure of* F_n *over* F_0. *Then we have*

$$B_q \geq \limsup_{n\to\infty} \frac{|\mathrm{Gal}(E_n/F_0)|}{g_{E_n}} \geq \frac{2}{3}.$$

Proof. It is easy to verify that $\Lambda_0 = \{0, i, -i, \infty\}$ and $\Lambda = \{0, i, -i, \infty, 1\}$ satisfy the conditions of Proposition 4.3. The rest of the proof uses similar arguments to those in Proposition 4.4 and Theorem 4.5. The details are omitted. □

References

[1] E. Artin and J. Tate, *Class field theory*, American Mathematical Society, Providence, RI, 2009.

[2] R. Auer, *Ray class fields of global function fields with many rational places*, Acta Arith. **95** (2000), no. 2, 97–122, DOI 10.4064/aa-95-2-97-122. MR1785410

[3] P. Beelen, A. Garcia, and H. Stichtenoth, *Towards a classification of recursive towers of function fields over finite fields*, Finite Fields Appl. **12** (2006), no. 1, 56–77, DOI 10.1016/j.ffa.2005.01.004. MR2190187

[4] R. Cramer, C. Padró, and C. Xing, *Optimal algebraic manipulation detection codes in the constant-error model*, Theory of cryptography. Part I, Lecture Notes in Comput. Sci., vol. 9014, Springer, Heidelberg, 2015, pp. 481–501, DOI 10.1007/978-3-662-46494-6_20. MR3346238

[5] M. D. Fried and M. Jarden, *Field arithmetic*, 3rd ed., Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge, A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], vol. 11, Springer-Verlag, Berlin, 2008. MR2445111

[6] A. Garcia, H. Stichtenoth, and C.-P. Xing, *On subfields of the Hermitian function field*, Compositio Math. **120** (2000), no. 2, 137–170, DOI 10.1023/A:1001736016924. MR1739176

[7] M. Giulietti and G. Korchmáros, *Algebraic curves with many automorphisms*, arXiv:1702.08812 (2017).

[8] V. Guruswami and C. Xing, *Optimal rate algebraic list decoding using narrow ray class fields*, J. Combin. Theory Ser. A **129** (2015), 160–183, DOI 10.1016/j.jcta.2014.09.003. MR3275120

[9] V. Guruswami, C. Xing, and C. Yuan, *Subspace designs based on algebraic function fields*, Trans. Amer. Math. Soc. **370** (2018), no. 12, 8757–8775, DOI 10.1090/tran/7369. MR3864394

[10] D. R. Hayes, *Explicit class field theory for rational function fields*, Trans. Amer. Math. Soc. **189** (1974), 77–91, DOI 10.2307/1996848. MR0330106

[11] H.-W. Henn, *Funktionenkörper mit grosser Automorphismengruppe* (German), J. Reine Angew. Math. **302** (1978), 96–115, DOI 10.1515/crll.1978.302.96. MR511696

[12] J. W. P. Hirschfeld, G. Korchmáros, and F. Torres, *Algebraic curves over a finite field*, Princeton Series in Applied Mathematics, Princeton University Press, Princeton, NJ, 2008. MR2386879

[13] A. Hurwitz, *Ueber algebraische Gebilde mit eindeutigen Transformationen in sich* (German), Math. Ann. **41** (1892), no. 3, 403–442, DOI 10.1007/BF01443420. MR1510753

[14] G. Korchmáros and M. Montanucci, *Ordinary algebraic curves with many automorphisms in positive characteristic*, arXiv:1610.05252 (2016).

[15] G. Korchmáros and P. Speziali, *Hermitian codes with automorphism group isomorphic to* $\mathrm{PGL}(2, q)$ *with* q *odd*, Finite Fields Appl. **44** (2017), 1–17, DOI 10.1016/j.ffa.2016.11.003. MR3583742

[16] L. Ma, C. Xing, and S. L. Yeo, *On automorphism groups of cyclotomic function fields over finite fields*, J. Number Theory **169** (2016), 406–419, DOI 10.1016/j.jnt.2016.05.026. MR3531248

[17] V. Kumar Murty and J. Scherk, *Effective versions of the Chebotarev density theorem for function fields* (English, with English and French summaries), C. R. Acad. Sci. Paris Sér. I Math. **319** (1994), no. 6, 523–528. MR1298275

[18] J. Neukirch, *Class field theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 280, Springer-Verlag, Berlin, 1986. MR819231
[19] H. Niederreiter and C. Xing, *Rational points on curves over finite fields: Theory and applications*, London Mathematical Society Lecture Note Series, vol. 285, Cambridge University Press, Cambridge, England, 2001. MR1837382
[20] M. Rosen, *S-units and S-class group in algebraic function fields*, J. Algebra **26** (1973), 98–108, DOI 10.1016/0021-8693(73)90036-7. MR0327777
[21] M. Rosen, *Number theory in function fields*, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002. MR1876657
[22] H. Stichtenoth, *On automorphisms of geometric Goppa codes*, J. Algebra **130** (1990), no. 1, 113–121, DOI 10.1016/0021-8693(90)90104-V. MR1045740
[23] H. Stichtenoth, *Algebraic function fields and codes*, 2nd ed., Graduate Texts in Mathematics, vol. 254, Springer-Verlag, Berlin, 2009. MR2464941
[24] H. Stichtenoth, *Transitive and self-dual codes attaining the Tsfasman-Vlăduţ-Zink bound*, IEEE Trans. Inform. Theory **52** (2006), no. 5, 2218–2224, DOI 10.1109/TIT.2006.872986. MR2234479
[25] S. Wesemeyer, *On the automorphism group of various Goppa codes*, IEEE Trans. Inform. Theory **44** (1998), no. 2, 630–643, DOI 10.1109/18.661509. MR1607734
[26] C. Xing, *On automorphism groups of the Hermitian codes*, IEEE Trans. Inform. Theory **41** (1995), no. 6, 1629–1635, DOI 10.1109/18.476234. Special issue on algebraic geometry codes. MR1391020

School of Mathematical Sciences, Yangzhou University, Yangzhou 225002, People's Republic of China
Email address: lmma@yzu.edu.cn

Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore 637371
Email address: xingcp@ntu.edu.sg