On subfields of the Hermitian function field involving the involution automorphism

Ma, Liming; Xing, Chaoping

2018

Ma, L., & Xing, C. (2019). On subfields of the Hermitian function field involving the involution automorphism. Journal of Number Theory, 198, 293-317. doi:10.1016/j.jnt.2018.10.014

https://hdl.handle.net/10356/139361

https://doi.org/10.1016/j.jnt.2018.10.014

ON SUBFIELDS OF THE HERMITIAN FUNCTION FIELDS INVOLVING THE INVOLUTION AUTOMORPHISM

LIMING MA AND CHAOPING XING

Abstract. A function field over a finite field is called maximal if it achieves the Hasse-Weil bound. Finding possible genera that maximal function fields achieve has both theoretical interest and practical applications to coding theory and other topics. As a subfield of a maximal function field is also maximal, one way to find maximal function fields is to find all subfields of a maximal function field. Due to the large automorphism group of the Hermitian function field, it is natural to find as many subfields of the Hermitian function field as possible. In literature, most of papers studied subfields fixed by subgroups of the decomposition group at one point (usually the point at infinity). This is because it becomes much more complicated to study the subfield fixed by a subgroup that is not contained in the decomposition group at one point. In this paper, we study subfields of the Hermitian function field fixed by subgroups that are not contained in the decomposition group of any point except the cyclic subgroups. It turns out that some new maximal function fields are found.

1. Introduction

Let $\mathbb{F}_\ell$ be a finite field with ℓ elements and $F/\mathbb{F}_\ell$ be an algebraic function field of one variable with the full constant field $\mathbb{F}_\ell$ with genus g. If the number of rational places of F attains the Hasse-Weil bound

$$N(F) \leq \ell + 1 + 2g\sqrt{\ell},$$

then F is said to be *maximal*. It follows that F could be maximal only if either g is zero or ℓ is a square.

The most important example of maximal function field is the Hermitian function field $H/\mathbb{F}_\ell$ with $\ell = q^2$, where q is a prime power. The Hermitian function field H over $\mathbb{F}_{q^2}$ is defined by the equation

$$y^q + y = x^{q+1}$$

with $H = \mathbb{F}_{q^2}(x, y)$.

The set of rational places of H consists of the infinite place P_∞ which is the unique common pole of x and y and $P_{\alpha,\beta}$ which is the unique common zero of $x - \alpha$ and $y - \beta$ for each $(\alpha, \beta) \in \mathbb{F}_{q^2}^2$ satisfying $\beta^q + \beta = \alpha^{q+1}$. Thus, it has $q^3 + 1$ rational places in total. The genus of the Hermitian function field is $(q^2 - q)/2$. Furthermore, the Hermitian function field is the unique maximal function field of genus $(q^2 - q)/2$ over

The first author is partially supported by the National Natural Science Foundation of China under Grant 11501493 and the State Scholarship Fund of China Scholarship Council.

the finite field $\mathbb{F}_{q^2}$ (see [13]). The automorphism group $\mathcal{A}$ of the Hermitian function field is defined by

$$\mathcal{A} = \mathrm{Aut}(H/\mathbb{F}_{q^2}) = \{\sigma : H \mapsto H | \sigma \text{ is a } \mathbb{F}_{q^2}\text{-automorphism of } H\}.$$

This automorphism group is extremely large and isomorphic to the projective unitary group $\mathrm{PGU}(3, q^2)$ with order $q^3(q^2-1)(q^3+1)$ (see [14]). The decomposition group $\mathcal{A}(P_\infty)$ of the infinite place is equal to

$$\{\sigma \in \mathcal{A} : \ \sigma(P_\infty) = P_\infty\} = \{\sigma = [a, b, c] : \ (a, b, c) \in \mathbb{F}_{q^2}^* \times \mathbb{F}_{q^2} \times \mathbb{F}_{q^2}, c^q + c = b^{q+1}\},$$

where $\sigma = [a, b, c]$ is the automorphism defined by

$$\begin{cases} \sigma(x) = ax + b, \\ \sigma(y) = a^{q+1}y + ab^q x + c. \end{cases}$$

Thus, the order of $\mathcal{A}(P_\infty)$ is $q^3(q^2-1)$. Apart from the automorphisms of $\mathcal{A}(P_\infty)$, there is an *involution* automorphism, denoted by ω, given by

$$\omega(x) = \frac{x}{y}, \qquad \omega(y) = \frac{1}{y}.$$

The order of ω is 2. Then the full automorphism group of H is generated by $\mathcal{A}(P_\infty)$ and ω, i.e., $\mathcal{A} = \langle \mathcal{A}(P_\infty), \omega \rangle$.

For a maximal function field $F/\mathbb{F}_{q^2}$, any function field E with $\mathbb{F}_{q^2} \subsetneq E \subseteq F$ is maximal as well (see [10]). Hence, one can construct a large number of maximal function fields by considering the fixed subfields with respect to some subgroups of the automorphism group $\mathcal{A}$ of the Hermitian function fields (see [1, 2, 3, 4, 5, 6, 7, 8, 9, 11, 12, 16]).

The goal of this article to find out possible genera which are achieved by maximal function fields. One natural way to realize this goal is to find as many subfields of H as possible. This is equivalent to finding as many subgroups of $\mathcal{A}$ as possible. The subfields of the Hermitian function fields considered in the literature are usually those fixed by subgroups of the decomposition group $\mathcal{A}(P_\infty)$ except for [7] where the subgroup is generated by ω and the subgroup $\{\sigma = [a, 0, 0] : \ a \in \mathbb{F}_{q^2}^*\}$ and the characteristic of $\mathbb{F}_{q^2}$ is odd, etc. In particular, it was showed in [2] that we can obtain all the genera of maximal function fields from the fixed subfields of the subgroups of the $\mathcal{A}(P_\infty)$ for the odd characteristic case. In this article, we consider various subgroups of $\mathcal{A}$ that involve both the decomposition group $\mathcal{A}(P_\infty)$ and the involution automorphism ω. It would be exciting to find all subgroups of $\mathcal{A}$ and genera of corresponding subfields. The current article moves one step forward by considering the involution automorphism ω. Most of the subgroups discussed in this paper are not contained in the decomposition group at any point except the cyclic subgroup. Thus, the subfields of the Hermitian function field obtained in this paper are new despite some genera of these subfields have already been found in literature.

We summarize genera obtained in this paper in Tables I and II. In particular, we get some new genera that are not achievable by subgroups of the decomposition group $\mathcal{A}(P_\infty)$. The genera in Table 1 (i)-(iii) and Table 2 (ii) have not be found in literature, while the rest of the genera given in Tables 1 and 2 can be found in [4, 7].

TABLE 1. Genera for even characteristic

No.	Conditions on parameter	Genera	References
(i)	$d=(m,q+1), \tilde{d}=(m,q-1)$	$[q^2-q+m-(d-1)(q-1)-\tilde{d}(q+1)]/(4m)$	Thm 3.2
(ii)	$m\|(q-1)$	$(q^2-q-mq)/(4m)$	Thm 4.1
(iii)	$m\|(q+1)$	$(q^2-q-mq+2m-2)/(4m)$	Thm 4.2
(iv)	$m\|(q^2-1), d=(m,q+1)$	$(q-1)(q+1-d)/(2m)$	Thm 5.1

TABLE 2. Genera for odd characteristic

No.	Conditions on parameter	Genera	References
(i)	$3\nmid(q+1), m\|(q+1)$, m is odd	$1+(q^2-q-2)/(2m)$	Thm 4.3
(ii)	$3\nmid(q+1), 4\|m\|(q+1), q\equiv 3 (\mathrm{mod}\ 8)$	$1+(q^2-4q-5)/(2m)$	Thm 4.3
(iii)	$3\nmid(q+1), m\|(q+1)$ and (i), (ii) are not satisfied	$1+(q^2-2q-3)/(2m)$	Thm 4.3
(iv)	$m\|2(q-1)$, m is odd	$(q^2-q)/(2m)$	Thm 4.5
(v)	$4\|m\|2(q-1), q\equiv 3 (\mathrm{mod}\ 4)$	$(q^2-4q+3)/2m$	Thm 4.5
(vi)	$m\|2(q-1)$ and No. (iv), (v) are not satisfied	$(q^2-2q+1)/(2m)$	Thm 4.5
(vii)	$m\|(q+1)$	$(q-1)(q+1-m)/(2m)$	Thm 5.3
(viii)	$m\|2(q+1), m\nmid(q+1)$	$(q-1)(q+1-\frac{m}{2})/(2m)$	Thm 5.3

2. PRELIMINARY

Let $\mathcal{G}$ be a subgroup of the automorphism group $\mathcal{A}$ and let $H^{\mathcal{G}}$ be the fixed subfield of the Hermitian function field H with respect to $\mathcal{G}$, i.e.,

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

Then $H/H^{\mathcal{G}}$ is a Galois extension of algebraic function fields with the Galois group $\mathcal{G}=\mathrm{Gal}(H/H^{\mathcal{G}})$. The Hurwitz genus formula yields

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

where $\mathrm{Diff}(H/H^{\mathcal{G}})$ is the different of the extension $H/H^{\mathcal{G}}$.

Let P be a place of H and let $Q=P\cap H^{\mathcal{G}}$ be the restriction of P to $H^{\mathcal{G}}$. We denote by $d(P)=d(P|Q)$, $e(P)=e(P|Q)$ the different exponent and ramification index of $P|Q$, respectively. Then the different of $H/H^{\mathcal{G}}$ is given by

$$\mathrm{Diff}(H/H^{\mathcal{G}})=\sum_{P\in H} d(P)P.$$

If $P|Q$ is unramified or tamely ramified, then $d(P)=e(P)-1$ by Dedekind's Different Theorem [15, Theorem 3.5.1]. The i-th 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 v_P is the normalized discrete valuation of H corresponding to the place P. If $P|Q$ is wildly ramified, that is, $e(P)$ is divisible by $\mathrm{char}(\mathbb{F}_{q^2})$, then the different exponent $d(P)$ is

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

by Hilbert's Different Theorem [15, Theorem 3.8.7].

It has been showed that any ramified place $P \in \mathbb{P}_H$ in the extension $H/H^{\mathcal{G}}$ must be a rational place or a place of degree three (see [7, Proposition 2.2]). Furthermore, a place of degree three of H in the extension $H/H^{\mathcal{G}}$ is unramified or tamely ramified, and has ramification index being a divisor of q^2-q+1. In particular, assume that $H/H^{\mathcal{G}}$ is tamely ramified and all places of degree 3 of H are unramified in $H/H^{\mathcal{G}}$. If P is tamely ramified, then

$$d(P) = e(P) - 1 = \#\{\sigma \in \mathcal{G} \setminus \{1\} : \ \sigma(P) = P\}.$$

Let $N(\sigma)$ be the number of rational places stabilized by the automorphism σ, that is,

$$N(\sigma) = \#\{P \in \mathbb{P}_H : \ \deg(P) = 1 \text{ and } \sigma(P) = P\}.$$

Hence, the degree of the different of $H/H^{\mathcal{G}}$ is

$$\deg(\mathrm{Diff}(H/H^{\mathcal{G}})) = \sum_{P \in \mathbb{P}_H, \deg P = 1} (e(P) - 1) = \sum_{1 \neq \sigma \in \mathcal{G}} N(\sigma).$$

3. The fixed subfields of $\langle [a,0,0], \omega \rangle$ in even characteristic

In this section, we consider the group $\mathcal{C}$ which is generated by the automorphisms ϵ and ω, where

$$\epsilon(x) = ax, \quad \epsilon(y) = a^{q+1}y \quad \text{and} \quad \omega(x) = x/y, \quad \omega(y) = 1/y.$$

Here a is a primitive (q^2-1)-th root of unity. This subgroup was first discussed in [7] where only odd characteristic was considered. The reason why the even characteristic was not considered is that the extension is wildly ramified in the case of even characteristic. Thus, we consider only the even characteristic case in this section.

Any $\sigma \in \mathcal{C}$ must be in the form ϵ^i or $\omega\epsilon^i$ for some $0 \leq i \leq q^2-2$, since $\epsilon\omega = \omega\epsilon^{-q}$. Hence, $\mathrm{ord}(\mathcal{C}) = 2(q^2-1)$. The automorphisms in $\mathcal{C}$ can be given explicitly in the following form

$$\epsilon^i(x) = a^i x, \quad \epsilon^i(y) = a^{i(q+1)}y \quad \text{and} \quad \omega\epsilon^i(x) = \frac{a^i x}{y}, \quad \omega\epsilon^i(y) = \frac{a^{i(q+1)}}{y}$$

for $0 \leq i \leq q^2-2$. In order to obtain the genus of the fixed subfield from the Hurwitz genus formula, we need to calculate the different exponent for each ramified place in the extension $H/H^{\mathcal{C}}$.

Proposition 3.1. *Assume that char$(\mathbb{F}_{q^2}) = 2$. Let H be the Hermitian function field over $\mathbb{F}_{q^2}$ and let $\mathcal{C}$ be the group generated by the ϵ and ω. Then the different of the extension $H/H^{\mathcal{C}}$ is*

$$\mathrm{Diff}(H/H^{\mathcal{C}}) = (q^2-2)P_\infty + (q^2-2)P_{0,0} + (3q+2)\sum_{\beta \in \mathbb{F}_q^*} P_{0,\beta}.$$

Proof. First let us calculate the different exponent of each rational place of H. For the infinity place P_∞,

$$\sigma(P_\infty) = P_\infty \Leftrightarrow \sigma \in \mathcal{A}(P_\infty) \cap \mathcal{C} = \langle \epsilon \rangle.$$

Then the order of the decomposition group of P_∞ in $H/H^{\mathcal{C}}$ is $|\mathcal{G}_0(P_\infty)| = q^2-1$. Hence, the different exponent of P_∞ in $H/H^{\mathcal{C}}$ is $d(P_\infty) = e(P_\infty) - 1 = q^2 - 2$.

For the place $P_{0,0}$, it is easy to see that $\epsilon^i(P_{0,0}) = P_{0,0}$ and $\omega\epsilon^i(P_{0,0}) = P_\infty$ for any $0 \le i \le q^2-2$. Hence, $|\mathcal{G}_0(P_{0,0})| = q^2 - 1$ and the different exponent of $P_{0,0}$ in $H/H^{\mathcal{C}}$ is also $d(P_{0,0}) = q^2 - 2$.

For a place $P_{0,\beta}$ with $\beta^q + \beta = 0$ and $\beta \neq 0$,

$$\epsilon^i(P_{0,\beta}) = P_{0,\beta} \Leftrightarrow a^{i(q+1)}\beta = \beta \Leftrightarrow (q-1)|i.$$

Moreover, x is a prime element of $P_{0,\beta}$ and for $i = (q-1)k$ with $0 < k \le q$,

$$v_{P_{0,\beta}}(\epsilon^i(x) - x) = v_{P_{0,\beta}}(a^i x - x) = v_{P_{0,\beta}}((a^i - 1)x) = 1.$$

On the other hand,

$$\omega\epsilon^i(P_{0,\beta}) = P_{0,\beta} \Leftrightarrow a^{i(q+1)}/\beta = \beta \Leftrightarrow a^{i(q+1)} = \beta^2.$$

Then there are exactly $q+1$ automorphisms $\omega\epsilon^i$ such that $\omega\epsilon^i(P_{0,\beta}) = P_{0,\beta}$. If β runs through all elements of $\mathbb{F}_q^*$, then the solutions i runs through the set of positive integers between 0 and q^2-2. For such an integer i satisfying with $\omega\epsilon^i(P_{0,\beta}) = P_{0,\beta}$, we have

$$v_{P_{0,\beta}}\Big(\omega\epsilon^i(x) - x\Big) = v_{P_{0,\beta}}\Big(\frac{a^i x}{y} - x\Big) = v_{P_{0,\beta}}\Big(\frac{y - a^i}{y}x\Big) = \begin{cases} q+2 & \text{if } \beta = a^i, \\ 1 & \text{otherwise.} \end{cases}$$

The last equation holds true since the place $P_{0,\beta}$ is the unique common zero of x and $y - \beta$, i.e., $v_{P_{0,\beta}}(x) = 1$ and $v_{P_{0,\beta}}(y - \beta) = q + 1$ which is obtained from the defining equation $y^q + y = x^{q+1}$ and the Strict Triangle Inequality. Hence, $|\mathcal{G}_0(P_{0,\beta})| = 2q + 2$, $|\mathcal{G}_1(P_{0,\beta})| = |\mathcal{G}_2(P_{0,\beta})| = \cdots = |\mathcal{G}_{q+1}(P_{0,\beta})| = 2$ and $|\mathcal{G}_{q+2}(P_{0,\beta})| = 1$. By Hilbert's Different Theorem, the different exponent of $P_{0,\beta}$ is

$$d(P_{0,\beta}) = \sum_{i=0}^{+\infty} \Big(|\mathcal{G}_i(P_{0,\beta})| - 1\Big) = 3q + 2.$$

For a place $P_{\alpha,\beta}$ with $\beta^q + \beta = \alpha^{q+1}$ and $\alpha \neq 0$,

$$\epsilon^i(P_{\alpha,\beta}) = P_{\alpha,\beta} \Leftrightarrow a^i\alpha = \alpha,\ a^{i(q+1)}\beta = \beta \Leftrightarrow i = 0.$$

On the other hand,

$$\omega\epsilon^i(P_{\alpha,\beta}) = P_{\alpha,\beta} \Leftrightarrow \frac{a^i\alpha}{\beta} = \alpha,\ \frac{a^{i(q+1)}}{\beta} = \beta \Leftrightarrow \beta = a^i,\ \beta^2 = a^{i(q+1)}.$$

Then $\beta \in \mathbb{F}_q$ which is a contradiction to $\beta^q + \beta = \alpha^{q+1} \neq 0$. Hence, $|\mathcal{G}_0(P_{\alpha,\beta})| = 1$ and the different exponent of $P_{\alpha,\beta}$ is $d(P_{\alpha,\beta}) = 0$.

By the Hurwitz genus formula, we have

$$q^2 - q - 2 \ge 2(q^2-1)[2g(H^{\mathcal{C}}) - 2] + (q^2-2) + (q^2-2) + (3q+2)(q-1).$$

It follows that $g(H^{\mathcal{C}}) \le 0$. The genus of any function field must be a non-negative integer. Hence, $g(H^{\mathcal{C}}) = 0$ and all places of degree three of H are unramified in $H/H^{\mathcal{C}}$. This proposition follows immediately. □

Theorem 3.2. *Assume that* $char(\mathbb{F}_{q^2}) = 2$. *Let* m *be a divisor of* q^2-1 *and let* $b \in \mathbb{F}_{q^2}^*$ *be an element of order* m. *Consider the group* $\mathcal{G} = \langle \lambda, \omega \rangle$ *which is generated by the automorphism* λ *and* ω, *where*

$$\lambda(x) = bx, \quad \lambda(y) = b^{q+1}y \quad \textit{and} \quad \omega(x) = \frac{x}{y}, \quad \omega(y) = \frac{1}{y}.$$

Let $d = \gcd(m, q+1), \tilde{d} = \gcd(m, q-1)$. *Then the genus of the fixed field* $H^{\mathcal{G}}$ *is*

$$g(H^{\mathcal{G}}) = \frac{q^2 - q + m - (d-1)(q-1) - \tilde{d}(q+1)}{4m}.$$

Proof. The order of the group $\mathcal{G}$ is $2m$, and it consists of all automorphisms with the form

$$\sigma_c(x) = cx, \quad \sigma_c(y) = c^{q+1}y, \quad c^m = 1$$

and

$$\tau_c(x) = \frac{cx}{y}, \quad \tau_c(y) = \frac{c^{q+1}}{y}, \quad c^m = 1.$$

We only need to calculate the different exponents for P_∞ and $P_{0,\beta}$ with $\beta \in \mathbb{F}_q$ in the extension $H/H^{\mathcal{G}}$ from Proposition 3.1.

For the infinity place P_∞, we have $\sigma(P_\infty) = P_\infty \Leftrightarrow \sigma \in \mathcal{A}(P_\infty) \cap \mathcal{G} = \langle \lambda \rangle$. This implies that $|\mathcal{G}_0(P_\infty)| = m$. Hence, the different exponent of P_∞ is $d(P_\infty) = m - 1$.

For the place $P_{0,0}$, we also have $\sigma(P_{0,0}) = P_{0,0} \Leftrightarrow \sigma \in \mathcal{A}(P_\infty) \cap \mathcal{G} = \langle \lambda \rangle$. Thus, $|\mathcal{G}_0(P_{0,0})| = m$ and $d(P_{0,0}) = m - 1$.

For a place $P_{0,\beta}$ with $\beta^q + \beta = 0$ and $\beta \neq 0$, we have

$$\sigma_c(P_{0,\beta}) = P_{0,\beta} \Leftrightarrow c^{q+1} = 1 \text{ and } c^m = 1.$$

Then there are exactly $d = \gcd(m, q+1)$ automorphisms σ_c such that $\sigma_c(P_{0,\beta}) = P_{0,\beta}$. Furthermore, $v_{P_{0,\beta}}(\sigma_c(x) - x) = 1$ for $c \neq 1$. On the other hand,

$$\tau_c(P_{0,\beta}) = P_{0,\beta} \Leftrightarrow c^{q+1} = \beta^2, \quad \beta^q + \beta = 0 \quad \text{and} \quad c^m = 1.$$

For each fixed element $\beta \in \mathbb{F}_q^*$, let $N(\beta)$ denote the number of elements $c \in \mathbb{F}_{q^2}^*$ satisfy $c^{q+1} = \beta^2$ and $c^m = 1$. Then we obtain $\sum_{\beta \in \mathbb{F}_q^*} N(\beta) = m$. Furthermore, we have

$$v_{P_{0,\beta}}\Big(\tau_c(x) - x\Big) = v_{P_{0,\beta}}\Big(\frac{cx}{y} - x\Big) = v_{P_{0,\beta}}\Big(\frac{y-c}{y}x\Big) = \begin{cases} q+2 & \text{if } c = \beta, \\ 1 & \text{otherwise.} \end{cases}$$

If $c = \beta$, then $\beta^{q-1} = 1$ and $\beta^m = 1$. Then there are exactly $\tilde{d} = \gcd(m, q-1)$ elements $\beta \in \mathbb{F}_q^*$ such that the place $P_{0,\beta}$ is wildly ramified in $H/H^{\mathcal{G}}$. For such a wildly ramified place $P_{0,\beta}$, the orders of the higher ramification groups are $|\mathcal{G}_i(P_{0,\beta})| = 2$ for $1 \leq i \leq q+1$ and $|\mathcal{G}_{q+2}(P_{0,\beta})| = 1$. Hence,

$$\sum_{\beta \in \mathbb{F}_q^*} |\mathcal{G}_0(P_{0,\beta})| = d(q-1) + m, \quad \sum_{\beta \in \mathbb{F}_q^*} (|\mathcal{G}_i(P_{0,\beta})| - 1) = \tilde{d}$$

for each $1 \le i \le q+1$ and $|\mathcal{G}_{q+2}(P_{0,\beta})| = 1$ for any $\beta \in \mathbb{F}_q^*$. Hence, the sum of different exponents for all the places $P_{0,\beta}$ with $\beta \in \mathbb{F}_q^*$ is

$$\sum_{\beta \in \mathbb{F}_q^*} d(P_{0,\beta}) = (d-1)(q-1) + m + \tilde{d}(q+1)$$

by Hilbert's Different Theorem.

For other places P, we have $d(P) = 0$. Hence, the degree of the different of $H/H^{\mathcal{G}}$ is

$$\deg(\mathrm{Diff}(H/H^{\mathcal{G}})) = m - 1 + m - 1 + (d-1)(q-1) + m + \tilde{d}(q+1).$$

The Hurwitz genus formula for $H/H^{\mathcal{G}}$ yields

$$q^2 - q - 2 = 2m \cdot [2g(H^{\mathcal{G}}) - 2] + \deg(\mathrm{Diff}(H/H^{\mathcal{G}})).$$

Hence, this theorem follows immediately. □

Corollary 3.3. *Assume that* $char(\mathbb{F}_{q^2}) = 2$ *and* H *is the Hermitian function field over the finite field* $\mathbb{F}_{q^2}$.

(1) *For any divisor* m *of* $q-1$, *there is a subfield* $E \subseteq H$ *of genus*

$$g(E) = \frac{q^2 - q - mq}{4m}.$$

(2) *For any divisor* m *of* $q+1$, *there is a subfield* $E \subseteq H$ *of genus*

$$g(E) = \frac{q^2 - q - mq + 2m - 2}{4m}.$$

Proof. Let $\mathcal{G}$ be the group which is defined in Theorem 3.2.

(1) If $m|(q-1)$, then $d = \gcd(m, q+1) = 1$ and $\tilde{d} = \gcd(m, q-1) = m$. By Theorem 3.2, the genus of the fixed field $E = H^{\mathcal{G}}$ is

$$g(E) = \frac{q^2 - q - mq}{4m}.$$

(2) If $m|(q+1)$, then $d = \gcd(m, q+1) = m$ and $\tilde{d} = \gcd(m, q-1) = 1$. By Theorem 3.2, the genus of the fixed field $E = H^{\mathcal{G}}$ is

$$g(E) = \frac{q^2 - q - mq + 2m - 2}{4m}.$$

This completes the proof. □

4. The fixed fields of subgroups of $\langle [1, 0, c], \omega \rangle$

In this section, we consider another group generated by the automorphisms ω and τ, where τ is given by $\tau(x) = x$, $\tau(y) = y + c$ for some $c \in \mathbb{F}_{q^2}$ satisfying $c^q + c = 0$. Let $\sigma = \tau\omega$, then

$$\sigma(x) = \frac{x}{y+c}, \quad \sigma(y) = \frac{1}{y+c}.$$

The automorphism σ^i can be given in the following form

$$\sigma^i(x) = \frac{x}{u_i y + v_i}, \quad \sigma^i(y) = \frac{u_{i-1} y + v_{i-1}}{u_i y + v_i},$$

where u_i, v_i satisfy the recursive relations $u_i = v_{i-1}$, $v_i = cv_{i-1} + u_{i-1}$ with the initial values $u_0 = v_{-1} = 0$ and $v_0 = u_{-1} = 1$. Then it can be calculated that

$$v_n = \sum_{i=0}^{[\frac{n}{2}]} \binom{n-i}{i} c^{n-2i}.$$

However, it is difficult to find the order of σ by using the above formula of v_n. Hence, we rewrite the above recursive relations in the matrix representation

$$\begin{pmatrix} v_i \\ v_{i-1} \end{pmatrix} = \begin{pmatrix} c & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} v_{i-1} \\ v_{i-2} \end{pmatrix}.$$

Let C be the matrix $\begin{pmatrix} c & 1 \\ 1 & 0 \end{pmatrix}$. Then

$$\begin{pmatrix} v_i \\ v_{i-1} \end{pmatrix} = C^i \begin{pmatrix} v_0 \\ v_{-1} \end{pmatrix} = C^i \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

The characteristic polynomial of the matrix C is

$$\det(xI_2 - C) = \begin{vmatrix} x-c & -1 \\ -1 & x \end{vmatrix} = x^2 - cx - 1.$$

Since the product of the two eigenvalues is -1, we may assume that the two eigenvalues are $x_1 = \delta$ and $x_2 = -\delta^{-1}$. Then we have

$$c = x_1 + x_2 = \delta - \delta^{-1}.$$

By the identity $c^q + c = 0$, we have

$$c^q + c = 0 \Leftrightarrow \left(\delta - \frac{1}{\delta}\right)^q + \left(\delta - \frac{1}{\delta}\right) = 0 \Leftrightarrow (\delta^{q+1} - 1)(\delta^{q-1} + 1) = 0.$$

Hence, $\delta^{q+1} = 1$ or $\delta^{q-1} = -1$.

It is easy to calculate that the vector $\vec{p_1} = (\delta, 1)^T$ is an eigenvector of the eigenvalue $x_1 = \delta$ and the vector $\vec{p_2} = (-1, \delta)^T$ is an eigenvector of the eigenvalue $x_2 = -\delta^{-1}$. If $x_1 \neq x_2$, that is, $\delta^2 \neq -1$, then the matrix $P = \begin{pmatrix} \delta & -1 \\ 1 & \delta \end{pmatrix}$ is invertible and its inverse is given by

$$P^{-1} = \frac{1}{\delta^2 + 1} \begin{pmatrix} \delta & 1 \\ -1 & \delta \end{pmatrix}.$$

Hence, the matrix C can be diagonalized to its eigenvalue matrix $\Lambda = \begin{pmatrix} \delta & 0 \\ 0 & -\delta^{-1} \end{pmatrix}$, that is, $P^{-1}CP = \Lambda$. Then

$$\begin{aligned} C^i &= (P\Lambda P^{-1})^i = P\Lambda^i P^{-1} \\ &= \frac{1}{\delta^2+1} \begin{pmatrix} \delta & -1 \\ 1 & \delta \end{pmatrix} \cdot \begin{pmatrix} \delta & 0 \\ 0 & -\delta^{-1} \end{pmatrix}^i \cdot \begin{pmatrix} \delta & 1 \\ -1 & \delta \end{pmatrix} \\ &= \frac{1}{\delta^2+1} \begin{pmatrix} \delta^{i+2} + (-\delta)^{-i} & \delta^{i+1} + (-\delta)^{-i+1} \\ \delta^{i+1} + (-\delta)^{-i+1} & \delta^i + (-\delta)^{-i+2} \end{pmatrix} \end{aligned} \tag{1}$$

Hence, v_i can also be given by the following formula

$$v_i = \frac{\delta^{i+2} + (-\delta)^{-i}}{\delta^2 + 1}.$$

Then the order of the automorphism σ can be determined as follows. Note that

$$\sigma^i = 1 \Leftrightarrow \begin{pmatrix} v_i \\ v_{i-1} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \Leftrightarrow C^i \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \Leftrightarrow C^i = \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}.$$

If $\delta^{i+1} + (-\delta)^{-i+1} = 0$, that is, $\delta^{2i} = (-1)^i$, then $\delta^{i+2} + (-\delta)^{-i} = \delta^i + (-\delta)^{-i+2}$. Hence,

$$\sigma^i = 1 \Leftrightarrow C^i = I_2 \Leftrightarrow \begin{pmatrix} \delta & 0 \\ 0 & -\delta^{-1} \end{pmatrix}^i = I_2 \Leftrightarrow \delta^i = 1 \text{ and } (-1)^i = 1.$$

If $\delta^2 = -1$, then the matrix C cannot be diagonalized.

4.1. **Even characteristic.** In the even characteristic case, we have $c = \delta + \delta^{-1}$ and

$$c^q + c = 0 \Leftrightarrow (\delta^{q-1} - 1)(\delta^{q+1} - 1) = 0 \Leftrightarrow \delta^{q-1} = 1 \text{ or } \delta^{q+1} = 1.$$

If $\delta^2 = -1$, then $\delta = 1$ and $c = 0$. Hence, τ is the identity automorphism. So we can assume δ as an element in $\mathbb{F}_{q^2}$ with an order n which is $q - 1 > 1$ or $q + 1$ in this subsection.

Now we need to determine the group structure of the group $\mathcal{D}$ generated by the two automorphisms τ and ω. Firstly, let us determine the order of the automorphism $\sigma = \tau \cdot \omega$. Note that

$$\sigma^i = 1 \Leftrightarrow v_{i-1} = 0 \text{ and } v_i = 1.$$

It has been showed that

$$v_i = \frac{1}{c}\Big(\delta^{i+1} + \frac{1}{\delta^{i+1}}\Big),$$

then $v_{i-1} = 0 \Leftrightarrow \delta^i + \delta^{-i} = 0 \Leftrightarrow \delta^{2i} = 1 \Leftrightarrow \delta^i = 1 \Leftrightarrow \mathrm{ord}(\delta)|i$. Moreover, if $\mathrm{ord}(\delta)|i$, then $v_i = 1$. Hence, the order of the automorphism σ is the same as the order of δ. Secondly, it can be directly verified that $\omega\sigma = \sigma^{n-1}\omega$. Hence,

$$\mathcal{D} = \langle \tau, \omega \rangle = \langle \omega, \sigma | \omega^2 = 1, \sigma^n = 1, \omega\sigma = \sigma^{n-1}\omega \rangle,$$

i.e., $\mathcal{D}$ is isomorphic to the Dihedral group D_n of order $2n$.

Now we need to consider the ramification in the Galois extension $H/H^{\mathcal{D}}$. Firstly, we consider the automorphism σ^i for $1 \le i \le n-1$, then $v_{i-1} \neq 0$ and $\sigma^i(P_\infty) \neq P_\infty$. For any rational place $P_{\alpha,\beta} \in \mathbb{P}_H$,

$$\sigma(P_{\alpha,\beta}) = P_{\alpha,\beta} \Leftrightarrow \frac{\alpha}{v_{i-1}\beta + v_i} = \alpha, \quad \frac{v_{i-2}\beta + v_{i-1}}{v_{i-1}\beta + v_i} = \beta, \quad \beta^q + \beta = \alpha^{q+1}.$$

If $\alpha \neq 0$, then $v_{i-1}\beta + v_i = 1$. Since $c^q + c = 0$, we have $c \in \mathbb{F}_q$ and $v_i \in \mathbb{F}_q$ which follows from the formula of v_i in the variable c. Then $\beta \in \mathbb{F}_q$ which contradicts to the third equation $\beta^q + \beta = \alpha^{q+1} \neq 0$. Hence, $\alpha = 0$ and $\beta \in \mathbb{F}_q$. From the second equation,

$$v_{i-2}\beta + v_{i-1} = v_{i-1}\beta^2 + v_i\beta \Rightarrow v_{i-1}(\beta^2 + c\beta + 1) = 0 \Rightarrow \beta^2 + c\beta + 1 = 0.$$

Then there are two roots $\beta = \delta$ and $\beta = \delta^{-1}$.
If $n = q - 1$, then $\delta^q + \delta = 0$ and $(\delta^{-1})^q + \delta^{-1} = 0$. Hence, the two places $P_{0,\delta}$ and $P_{0,\delta^{-1}}$ are stabilized by the automorphism σ^i. Furthermore,

$$v_{P_{0,\delta}}\Big(\sigma^i(x) - x\Big) = v_{P_{0,\delta}}\Big(\frac{x}{v_{i-1}y + v_i} - x\Big) = v_{P_{0,\delta}}\Big(\frac{v_{i-1}y + v_i + 1}{v_{i-1}y + v_i}x\Big) = 1,$$

since $v_{i-1}\delta + v_i + 1 = 1 + \delta^{-i} \neq 0$.
If $n = q+1$, then $\delta^q + \delta \neq 0$ and $(\delta^{-1})^q + \delta^{-1} \neq 0$ which contradict to $\alpha = 0$ in the third equation. Hence, $P_{\alpha,\beta}$ can't be stabilized by the automorphism σ^i for any $1 \leq i \leq q$.

Secondly, we consider the automorphism $\sigma^i\omega$ for $0 \leq i \leq n-1$,

$$\sigma^i\omega(x) = \frac{x}{v_{i-2}y + v_{i-1}}, \quad \sigma^i\omega(y) = \frac{v_{i-1}y + v_i}{v_{i-2}y + v_{i-1}}.$$

The order of the automorphism $\sigma^i\omega$ is 2, since $\omega\sigma = \sigma^{n-1}\omega$. For $i = 0$, we know $\omega(P_{0,0}) = P_\infty$. If $\beta \neq 0$, then

$$\omega(P_{\alpha,\beta}) = P_{\alpha,\beta} \Leftrightarrow \frac{\alpha}{\beta} = \alpha, \quad \frac{1}{\beta} = \beta, \quad \beta^q + \beta = \alpha^{q+1}.$$

Hence, $P_{0,1}$ is the unique rational place stabilized by the automorphism ω. Furthermore,

$$v_{P_{0,1}}\Big(\omega(x) - x\Big) = v_{P_{0,1}}\Big(\frac{x}{y} - x\Big) = v_{P_{0,1}}\Big(\frac{y+1}{y}x\Big) = q + 2.$$

For $i = 1$, then $\sigma\omega = \tau$, i.e., $\tau(x) = x,\ \tau(y) = y + c$. Hence, P_∞ is the unique rational place stabilized by the automorphism τ and

$$v_{P_\infty}\Big(\tau(\frac{x}{y}) - \frac{x}{y}\Big) = v_{P_\infty}\Big(\frac{x}{y+c} - \frac{x}{y}\Big) = v_{P_\infty}\Big(\frac{cx}{y(y+c)}\Big) = q + 2.$$

For $2 \leq i \leq n-1$, then $v_{i-2} \neq 0$ and $\sigma^i\omega(P_\infty) \neq P_\infty$. For the place $P_{\alpha,\beta} \in \mathbb{P}_H$,

$$\sigma^i\omega(P_{\alpha,\beta}) = P_{\alpha,\beta} \Leftrightarrow \frac{\alpha}{v_{i-2}\beta + v_{i-1}} = \alpha, \quad \frac{v_{i-1}\beta + v_i}{v_{i-2}\beta + v_{i-1}} = \beta, \quad \beta^q + \beta = \alpha^{q+1}.$$

If $\alpha \neq 0$, then $v_{i-2}\beta + v_{i-1} = 1$. Since $c \in \mathbb{F}_q$, we know $v_{i-2}, v_{i-1} \in \mathbb{F}_q$. It follows that $\beta \in \mathbb{F}_q$ which contradicts to the third equation $\beta^q + \beta = \alpha^{q+1} \neq 0$. Hence, $\alpha = 0$, $\beta \in \mathbb{F}_q$ and

$$v_{i-1}\beta + v_i = v_{i-2}\beta^2 + v_{i-1}\beta \Leftrightarrow \beta^2 = \frac{v_i}{v_{i-2}}.$$

Moreover, it is easy to verify that v_i/v_{i-2} are pairwise distinct elements in $\mathbb{F}_q$ for $2 \leq i \leq n-1$. Hence, the place P_{0,β_i} with $\beta_i = (\frac{v_i}{v_{i-2}})^{\frac{q}{2}}$ is the unique rational place stabilized by $\sigma^i\omega$. Furthermore,

$$v_{P_{0,\beta_i}}\Big(\sigma^i\omega(x) - x\Big) = v_{P_{0,\beta_i}}\Big(\frac{x}{v_{i-2}y + v_{i-1}} - x\Big) = v_{P_{0,\beta_i}}\Big(\frac{v_{i-2}y + v_{i-1} + 1}{v_{i-2}y + v_{i-1}}x\Big) = q + 2.$$

The last equation holds true, since $v_{i-2}\beta_i + v_{i-1} + 1 = 0 \Leftrightarrow v_{i-2}^2{\beta_i}^2 + v_{i-1}^2 + 1 = 0 \Leftrightarrow v_{i-2}v_i + v_{i-1}^2 = 1$ which can be obtained from the formula of v_i in the variable δ.

Theorem 4.1. *Let H be the Hermitian function field over $\mathbb{F}_{q^2}$ with even characteristic, let m be a divisor of $q-1$ and let $\mathcal{G}$ be the subgroup $\langle \omega, \sigma^{\frac{q-1}{m}} \rangle$ of $\mathcal{D}$. Then the genus of the fixed field $H^{\mathcal{G}}$ is*

$$g(H^{\mathcal{G}}) = \frac{q^2-q-mq}{4m}.$$

Proof. The ramification groups of P_∞ in $H/H^{\mathcal{G}}$ are given by

$$\mathcal{G}_0(P_\infty) = \mathcal{G}_1(P_\infty) = \cdots = \mathcal{G}_{q+1}(P_\infty) = \langle \tau \rangle \text{ and } \mathcal{G}_{q+2}(P_\infty) = \{id\}.$$

Hence, the different exponent of P_∞ in $H/H^{\mathcal{G}}$ is

$$d(P_\infty) = \sum_{i=0}^{+\infty} (|\mathcal{G}_i(P_\infty)| - 1) = q+2.$$

It is easy to verify that $v_i/v_{i-2} \neq \delta^2$ or δ^{-2}, that is to say, $P_{0,\beta_i} \neq P_{0,\delta}$ or $P_{0,\delta^{-1}}$ for $2 \leq i \leq q-2$. Then the different exponents of $P_{0,1}$ and P_{0,β_i} for $2 \leq i \leq q-2$ are also

$$d(P_{0,1}) = d(P_{0,\beta_i}) = q+2.$$

The decomposition groups of $P_{0,\delta}$ and $P_{0,\delta^{-1}}$ are $\langle \sigma \rangle$ which is a group of order $q-1$. Hence, the different exponents of $P_{0,\delta}$ and $P_{0,\delta^{-1}}$ are

$$d(P_{0,\delta}) = d(P_{0,\delta^{-1}}) = q-2.$$

By the Hurwitz genus formula, we have

$$q^2-q-2 \geq 2(q-1)[2g(H^{\mathcal{D}})-2] + 2\cdot(q-2) + (q-1)\cdot(q+2).$$

Hence, $g(H^{\mathcal{D}}) = 0$ and all places of degree three of H are unramified in $H/H^{\mathcal{D}}$. The order of the subgroup $\mathcal{G}$ is $2m$. Then this theorem follows from the Hurwitz genus formula

$$q^2-q-2 = 2m\cdot[2g(H^{\mathcal{G}})-2] + 2\cdot(m-1) + m\cdot(q+2).$$

□

Theorem 4.2. *Let H be the Hermitian function field over $\mathbb{F}_{q^2}$ with even characteristic, let m be a divisor of $q+1$ and let $\mathcal{G}$ be the subgroup $\langle \omega, \sigma^{\frac{q+1}{m}} \rangle$ of $\mathcal{D}$. Then the genus of the fixed field $H^{\mathcal{G}}$ is*

$$g(H^{\mathcal{G}}) = \frac{q^2-q-mq+2m-2}{4m}.$$

Proof. The different exponents of the rational places P_∞ and $P_{0,\beta}$ with $\beta \in \mathbb{F}_q$ in the extension $H/H^{\mathcal{D}}$ are

$$d(P_\infty) = d(P_{0,\beta}) = q+2.$$

By the Hurwitz genus formula, we have

$$q^2-q-2 \geq 2(q+1)[2g(H^{\mathcal{D}})-2] + (q+1)\cdot(q+2).$$

Hence, $g(H^{\mathcal{D}}) = 0$ and all places of degree three of H are unramified in $H/H^{\mathcal{D}}$. The order of the subgroup $\mathcal{G}$ is $2m$. Then this theorem follows from the Hurwitz genus formula

$$q^2-q-2 = 2m\cdot[2g(H^{\mathcal{G}})-2] + m\cdot(q+2).$$

□

In this sub-subsection, we choose δ with the maximal order $q-1$ or $q+1$ satisfying $c^q+c=0$. However, the order of δ may just be a positive divisor of $q-1$ or $q+1$. Here are some examples, such as the order of δ is 3 which divides $q-1$ in Example 1 and the order of δ is 5 in Example 2. Since the calculations are similar to the Theorem 4.1 and 4.2, we omit the details.

Example 1. *Let $\mathcal{G}$ be the group generated by the automorphisms τ and ω which are given by $\tau(x)=x,\ \tau(y)=y+1$ and $\omega(x)=x/y,\ \omega(y)=1/y$. If $q=2^{2k}$, then the genus of the fixed subfield $H^{\mathcal{G}}$ is*

$$g(H^{\mathcal{G}})=\frac{q^2-4q}{12}.$$

Example 2. *Let $\mathcal{G}$ be the group generated by the automorphisms ω and τ which is given by $\tau(x)=x,\ \tau(y)=y+c$ with $c^2+c+1=0$ and $c^q+c=0$. If $q=4^{2k}$, then the genus of the fixed subfield $H^{\mathcal{G}}$ is*

$$g(H^{\mathcal{G}})=\frac{q^2-6q}{20}.$$

Otherwise, the genus of the fixed subfield $H^{\mathcal{G}}$ is

$$g(H^{\mathcal{G}})=\frac{q^2-6q+8}{20}.$$

4.2. **Odd characteristic.** In the odd characteristic case, we obtain $c=\delta-\delta^{-1}$ and

$$c^q+c=0\Leftrightarrow(\delta^{q+1}-1)(\delta^{q-1}+1)=0\Leftrightarrow\delta^{q+1}=1 \text{ or } \delta^{q-1}=-1.$$

Hence, we can fix δ as an element in $\mathbb{F}_{q^2}$ with an order n which is $q+1$ or $2(q-1)$ in this subsection. If $\delta^2=-1$, then $\mathrm{ord}(\delta)=4$. Hence, we also assume that $q\neq 3$ in this subsection for simplicity.

The automorphism σ^i is given by

$$\sigma^i(x)=\frac{x}{v_{i-1}y+v_i},\quad \sigma^i(y)=\frac{v_{i-2}y+v_{i-1}}{v_{i-1}y+v_i}.$$

We have shown that $\sigma^i=1\Leftrightarrow\delta^i=1$ and $(-1)^i=1$. Hence, the order of the automorphism σ is the same as the order of δ. Let $\mathcal{D}$ be the group generated by the automorphism σ. Then the Galois extension $H/H^{\mathcal{D}}$ is tamely ramified.

4.2.1. *ord*$(\delta)=q+1$. The order the automorphism σ is $q+1$. We assume that $3\nmid(q+1)$ in this sub-subsection. As $\gcd(q+1,q^2-q+1)=\gcd(q+1,3)=1$, then all places of degree 3 in H are unramified in $H/H^{\mathcal{D}}$.

For the infinite place P_∞ and $1\leq i\leq q$,

$$\sigma^i(P_\infty)=P_\infty\Leftrightarrow v_{i-1}=0\Leftrightarrow\delta^{i+1}+(-1)^{i-1}\delta^{-i+1}=0\Leftrightarrow\delta^{2i}=(-1)^i.$$

If i is even, then $\delta^{2i}=1\Leftrightarrow 2i=q+1\Leftrightarrow i=(q+1)/2$ is even $\Leftrightarrow q\equiv 3(\mathrm{mod}4)$. Otherwise, $\delta^{2i}=-1\Leftrightarrow 2i=(q+1)/2$ or $3(q+1)/2\Leftrightarrow i=(q+1)/4$ or $3(q+1)/4$ is odd $\Leftrightarrow q\equiv 3(\mathrm{mod}8)$.

For any rational place $P_{\alpha,\beta} \in \mathbb{P}_H$ and $1 \le i \le q$,

$$\sigma^i(P_{\alpha,\beta}) = P_{\alpha,\beta} \Leftrightarrow \frac{\alpha}{v_{i-1}\beta + v_i} = \alpha, \quad \frac{v_{i-2}\beta + v_{i-1}}{v_{i-1}\beta + v_i} = \beta, \quad \beta^q + \beta = \alpha^{q+1}.$$

Case 1: $\alpha \neq 0$.
From the first equation, we have $v_{i-1}\beta + v_i = 1$. If $v_{i-1} = 0$, then $v_i = 1$. It follows that $\mathrm{ord}(\sigma)|i$ which is impossible for $1 \le i \le q$. Hence, $v_{i-1} \neq 0$ and this implies that $v_{i-2}\beta + v_{i-1} = v_{i-1}\beta^2 + v_i\beta \Leftrightarrow v_{i-1}(\beta^2 + c\beta - 1) = 0 \Leftrightarrow \beta^2 + c\beta - 1 = 0$. There are two solutions $\beta = -\delta$ or $\beta = \delta^{-1}$.
Substitute $\beta = -\delta$ into the first equation, then we have $-v_{i-1}\delta + v_i = (-1)^i\delta^{-i}$. If $q \equiv 1(\mathrm{mod}4)$, then $-v_{i-1}\delta + v_i = 1 \Leftrightarrow \delta^i = (-1)^i \Leftrightarrow i = (q+1)/2$. Furthermore, $\alpha^{q+1} = (-\delta)^q + (-\delta) = -(\delta^q + \delta) \neq 0$. Hence, the $q+1$ places $P_{\alpha,-\delta}$ with $\alpha^{q+1} = -(\delta^q + \delta)$ are stabilized by the automorphism $\sigma^{\frac{q+1}{2}}$. If $q \equiv 3(\mathrm{mod}4)$, then $-v_{i-1}\delta + v_i = (-1)^i\delta^{-i} \neq 1$. Substitute $\beta = \delta^{-1}$ into the first equation similarly, then we have $v_{i-1}\delta^{-1} + v_i = \delta^i \neq 1$. Hence, the place $P_{\alpha,\delta^{-1}}$ can't be stabilized by the automorphism σ^i.
Case 2: $\alpha = 0$.
In this case, we have $\beta^q + \beta = 0$ and $v_{i-2}\beta + v_{i-1} = v_{i-1}\beta^2 + v_i\beta \Leftrightarrow v_{i-1}(\beta^2 + c\beta - 1) = 0$. If $v_{i-1} = 0$, then $\sigma^i(P_{0,\beta}) = P_{0,\beta}$ for any β with $\beta^q + \beta = 0$.
If $v_{i-1} \neq 0$, then $\beta^2 + c\beta - 1 = 0$. Hence, $\beta = -\delta$ or $\beta = \delta^{-1}$. Furthermore, $(-\delta)^q + (-\delta) = -\delta^q - \delta \neq 0$ and $(\delta^{-1})^q + \delta^{-1} \neq 0$ if $\delta^4 \neq 1$, that is, $q \neq 3$. Hence, the place $P_{0,\beta}$ can't be stabilized by the automorphism σ^i with $v_{i-1} \neq 0$.

If $q \equiv 1(\mathrm{mod}\ 4)$, then $v_{i-1} \neq 0$ for every $1 \le i \le q$. Hence,

$$\mathrm{Diff}(H/H^{\mathcal{D}}) = \sum_{\alpha^{q+1} = -\delta^q - \delta} P_{\alpha,\delta}.$$

If $q \equiv 7(\mathrm{mod}\ 8)$, then $v_{\frac{q+1}{2}-1} = 0$. Then the places P_∞ and $P_{0,\beta}$ with $\beta^q + \beta = 0$ are stabilized by the automorphism $\sigma^{\frac{q+1}{2}}$. Hence,

$$\mathrm{Diff}(H/H^{\mathcal{D}}) = P_\infty + \sum_{\beta^q + \beta = 0} P_{0,\beta}.$$

If $q \equiv 3(\mathrm{mod}\ 8)$, then $v_{\frac{q+1}{4}-1}, v_{\frac{q+1}{2}-1}$ and $v_{\frac{3(q+1)}{4}-1}$ are equal to 0. Then the places P_∞ and $P_{0,\beta}$ with $\beta^q + \beta = 0$ are stabilized by the automorphisms $\sigma^{\frac{q+1}{4}}, \sigma^{\frac{q+1}{2}}$ and $\sigma^{\frac{3(q+1)}{4}}$. Hence,

$$\mathrm{Diff}(H/H^{\mathcal{D}}) = 3P_\infty + 3\sum_{\beta^q + \beta = 0} P_{0,\beta}.$$

Theorem 4.3. *Let H be the Hermitian function field over $\mathbb{F}_{q^2}$ with odd characteristic. Assume that $3 \nmid (q+1)$. Let m be a positive divisor of $q+1$ and let $\mathcal{G}$ be the group generated by the automorphism $\sigma^{\frac{q+1}{m}}$. Then the genus of the fixed field $H^{\mathcal{G}}$ is*

$$g(H^{\mathcal{G}}) = \begin{cases} 1 + (q^2 - q - 2)/2m & \text{if } m \text{ is odd,} \\ 1 + (q^2 - 4q - 5)/2m & \text{if } 4|m \text{ and } q \equiv 3(\mathrm{mod}\ 8), \\ 1 + (q^2 - 2q - 3)/2m & \text{otherwise.} \end{cases}$$

Proof. It is easy to check that $\sigma^{\frac{q+1}{2}} \in \mathcal{G} \Leftrightarrow m$ is even. If $q \equiv 1(\text{mod } 4)$ or $q \equiv 7(\text{mod } 8)$, then

$$q^2 - q - 2 = m[2g(H^{\mathcal{G}}) - 2] + \begin{cases} q+1 & \text{if m is even,} \\ 0 & \text{if m is odd.} \end{cases}$$

If $q \equiv 3(\text{mod } 8)$, then the automorphisms $\sigma^{\frac{q+1}{4}}, \sigma^{\frac{3(q+1)}{4}} \in \mathcal{G} \Leftrightarrow 4|m$. This theorem follows from the Hurwitz genus formula,

$$q^2 - q - 2 = m[2g(H^{\mathcal{G}}) - 2] + \begin{cases} 0 & \text{if m is odd,} \\ 3(q+1) & \text{if } 4|m, \\ q+1 & \text{otherwise.} \end{cases}$$

□

Remark 4.4. *We assume that* $3 \nmid (q+1)$ *in Theorem 4.3, since all places of degree* 3 *of* H *are unramified in the extension* $H/H^{\mathcal{G}}$ *under this assumption. In fact, we can't determine whether the places of degree* 3 *of* H *are ramified in* $H/H^{\mathcal{G}}$ *or not in the case of* $3|(q+1)$. *The similar case occurs in Theorem 5.4 as well.*

4.2.2. *ord*$(\delta) = 2(q-1)$. If $\text{ord}(\delta) = 2(q-1)$, then the order of the automorphism σ is $2(q-1)$. As $\gcd(2q-2, q^2-q+1) = 1$, all places of degree 3 of H are unramified in $H/H^{\mathcal{D}}$.

For the infinite place P_∞ and $1 \le i \le 2q-3$,,

$$\sigma^i(P_\infty) = P_\infty \Leftrightarrow v_{i-1} = 0 \Leftrightarrow \delta^{i+1} + (-1)^{i-1}\delta^{-i+1} = 0 \Leftrightarrow \delta^{2i} = (-1)^i.$$

If i is even, then $\delta^{2i} = 1 \Leftrightarrow i = q-1$. If i is odd, then $\delta^{2i} = -1 \Leftrightarrow 2i = q-1$ or $3(q-1) \Leftrightarrow i = (q-1)/2$ or $3(q-1)/2$ is odd $\Leftrightarrow q \equiv 3(\text{mod}4)$.

For the place $P_{\alpha,\beta}$ and $1 \le i \le 2q-3$,

$$\sigma^i(P_{\alpha,\beta}) = P_{\alpha,\beta} \Leftrightarrow \frac{\alpha}{v_{i-1}\beta + v_i} = \alpha, \quad \frac{v_{i-2}\beta + v_{i-1}}{v_{i-1}\beta + v_i} = \beta, \quad \beta^q + \beta = \alpha^{q+1}.$$

If $\alpha \neq 0$, then $v_{i-1}\beta + v_i = 1$. Suppose that $v_{i-1} = 0$, then $v_i = 1$. It follows that $\text{ord}(\sigma)|i$ which is impossible for $1 \le i \le 2q-3$. Hence, $v_{i-1} \neq 0$ and $\beta^2 + c\beta - 1 = 0$. There are two solutions $\beta = -\delta$ or $\beta = \delta^{-1}$. It is easy to check that $v_{i-1}\beta + v_i = -v_{i-1}\delta + v_i = (-1)^i\delta^{-i} \neq 1$, since $\delta^{q-1} = -1 \neq (-1)^{q-1}$. Moreover, $v_{i-1}\delta^{-1} + v_i = \delta^i \neq 1$. Hence, $\sigma^i(P_{\alpha,\beta}) \neq P_{\alpha,\beta}$ for $\alpha \neq 0$.
Otherwise, $\beta^q + \beta = 0$ and

$$v_{i-2}\beta + v_{i-1} = v_{i-1}\beta^2 + v_i\beta \Leftrightarrow v_{i-1}(\beta^2 + c\beta - 1) = 0.$$

If $v_{i-1} = 0$, then the places $P_{0,\beta}$ with $\beta^q + \beta = 0$ are stabilized by σ^i. Otherwise, $\beta^2 + c\beta - 1 = 0$ has two solutions $\beta = -\delta$ of $\beta = \delta^{-1}$. It is easy to check that $(-\delta)^q + (-\delta) = -(\delta^q + \delta) = 0$ and $(\delta^{-1})^q + (\delta^{-1}) = 0$, since $\delta^{q-1} = -1$. Hence, the two places $P_{0,-\delta}$ and $P_{0,\delta^{-1}}$ are stabilized by the automorphism σ^i with $v_{i-1} \neq 0$.

If $q \equiv 1(\text{mod } 4)$, then the places P_∞ and $P_{0,\beta}$ with $\beta^q + \beta = 0$ are stabilized by the automorphism σ^{q-1}. Hence, the different of $H/H^{\mathcal{D}}$ is

$$\text{Diff}(H/H^{\mathcal{D}}) = P_\infty + \sum_{\beta^q+\beta=0} P_{0,\beta} + (2q-4)(P_{0,-\delta} + P_{0,\delta^{-1}}).$$

If $q \equiv 3 (\mathrm{mod}\ 4)$, then the places P_∞ and $P_{0,\beta}$ with $\beta^q + \beta = 0$ are stabilized by the automorphism $\sigma^{\frac{q-1}{2}}$, σ^{q-1} and $\sigma^{\frac{3(q-1)}{2}}$. Hence, the different of $H/H^{\mathcal{D}}$ is

$$\mathrm{Diff}(H/H^{\mathcal{D}}) = 3P_\infty + 3\sum_{\beta^q+\beta=0} P_{0,\beta} + (2q-6)(P_{0,-\delta} + P_{0,\delta^{-1}}).$$

Theorem 4.5. *Let H be the Hermitian function field over $\mathbb{F}_{q^2}$ with odd characteristic, let m be a positive divisor of $2(q-1)$ and let $\mathcal{G}$ be the group generated by the automorphism $\sigma^{\frac{2(q-1)}{m}}$. Then the genus of the fixed field $H^{\mathcal{G}}$ is*

$$g(H^{\mathcal{G}}) = \begin{cases} (q^2-q)/2m & \text{if } m \text{ is odd,} \\ (q^2-4q+3)/2m & \text{if } 4|m \text{ and } q \equiv 3 (\mathit{mod}\ 4), \\ (q^2-2q+1)/2m & \text{otherwise.} \end{cases}$$

Proof. It is easy to check that $\sigma^{q-1} \in \mathcal{G} \Leftrightarrow m$ is even. If $q \equiv 1 (\mathrm{mod}\ 4)$, then

$$q^2-q-2 = m[2g(H^{\mathcal{G}})-2] + \begin{cases} q+1+2(m-2) & \text{if } m \text{ is even,} \\ 2(m-1) & \text{if } m \text{ is odd.} \end{cases}$$

If $q \equiv 3 (\mathrm{mod}\ 4)$, then the automorphisms $\sigma^{\frac{q-1}{2}}, \sigma^{\frac{3(q-1)}{2}} \in \mathcal{G} \Leftrightarrow 4|m$. This theorem follows from the Hurwitz genus formula,

$$q^2-q-2 = m[2g(H^{\mathcal{G}})-2] + \begin{cases} 2(m-1) & \text{if } m \text{ is odd,} \\ 3(q+1)+2(m-4) & \text{if } 4|m, \\ q+1+2(m-2) & \text{otherwise.} \end{cases}$$

□

5. The fixed subfields of subgroups of $\langle [a,0,c], \omega \rangle$

Let τ be an automorphism of the Hermitian function field H over $\mathbb{F}_{q^2}$ with the form

$$\tau(x) = ax, \quad \tau(y) = a^{q+1}y + c$$

where $c^q + c = 0$ and a is a (q^2-1)-th primitive element of the finite field $\mathbb{F}_{q^2}$. Let $\sigma = \tau\omega$, then

$$\sigma(x) = \frac{ax}{a^{q+1}y + c}, \quad \sigma(y) = \frac{1}{a^{q+1}y + c}.$$

The automorphism σ^i can be given in the following form

$$\sigma^i(x) = \frac{a^i x}{u_i y + v_i}, \quad \sigma^i(y) = \frac{u_{i-1}y + v_{i-1}}{u_i y + v_i}$$

where u_i, v_i satisfy the recursive relations $u_i = a^{q+1}v_{i-1}$, $v_i = cv_{i-1} + u_{i-1}$ with the initial values $u_0 = v_{-1} = 0$, $v_0 = 1$. The above recursive relations can be rewritten in the matrix representation

$$\begin{pmatrix} v_i \\ v_{i-1} \end{pmatrix} = \begin{pmatrix} c & a^{q+1} \\ 1 & 0 \end{pmatrix} \begin{pmatrix} v_{i-1} \\ v_{i-2} \end{pmatrix}.$$

Let $C = \begin{pmatrix} c & a^{q+1} \\ 1 & 0 \end{pmatrix}$. Then the characteristic polynomial of the matrix C is

$$\det(xI_2 - C) = \begin{vmatrix} x-c & -a^{q+1} \\ -1 & x \end{vmatrix} = x^2 - cx - a^{q+1}.$$

Assume that the two eigenvalues are $x_1 = \delta$ and $x_2 = -\frac{a^{q+1}}{\delta}$. Then we have

$$c = \delta - \frac{a^{q+1}}{\delta}.$$

By the identity $c^q + c = 0$, we have

$$c^q + c = 0 \Leftrightarrow (\delta - \frac{a^{q+1}}{\delta})^q + (\delta - \frac{a^{q+1}}{\delta}) = 0 \Leftrightarrow (\delta^{q+1} - a^{q+1})(\delta^{q-1} + 1) = 0.$$

Hence, $\delta^{q+1} = a^{q+1}$ or $\delta^{q-1} = -1$.

If $\delta^2 \neq -a^{q+1}$, then there exists an invertible matrix $P = \begin{pmatrix} \delta & -a^{q+1} \\ 1 & \delta \end{pmatrix}$ such that C is similar to the diagonal matrix $\Lambda = \begin{pmatrix} \delta & 0 \\ 0 & -\frac{a^{q+1}}{\delta} \end{pmatrix}$, that is, $P^{-1}CP = \Lambda$. Then we can calculate that

$$\begin{aligned} C^i &= (P\Lambda P^{-1})^i = P\Lambda^i P^{-1} \\ &= \frac{1}{\delta^2 + a^{q+1}} \begin{pmatrix} \delta & -a^{q+1} \\ 1 & \delta \end{pmatrix} \cdot \begin{pmatrix} \delta & 0 \\ 0 & -\frac{a^{q+1}}{\delta} \end{pmatrix}^i \cdot \begin{pmatrix} \delta & a^{q+1} \\ -1 & \delta \end{pmatrix} \qquad (2) \\ &= \frac{1}{\delta^2 + a^{q+1}} \begin{pmatrix} \delta^{i+2} + (-\delta)^{-i} a^{(i+1)(q+1)} & a^{q+1}\delta^{i+1} + (-\delta)^{-i+1} a^{(i+1)(q+1)} \\ \delta^{i+1} + (-\delta)^{-i+1} a^{i(q+1)} & a^{q+1}\delta^i + (-\delta)^{-i+2} a^{i(q+1)} \end{pmatrix}. \end{aligned}$$

Hence, v_i can be given by the following formula

$$v_i = \frac{\delta^{i+2} + (-\delta)^{-i} a^{(i+1)(q+1)}}{\delta^2 + a^{q+1}}.$$

5.1. **Even characteristic.** In the even characteristic case, $c = \delta + a^{q+1}\delta^{-1}$ and

$$c^q + c = 0 \Leftrightarrow \delta^{q-1} = 1 \text{ or } \delta^{q+1} = a^{q+1}.$$

Hence, we can fix δ as an element in $\mathbb{F}_{q^2}$ with order n, which is $q-1$ or q^2-1.

5.1.1. *ord*$(\delta) = q-1$. If $\mathrm{ord}(\delta) = q-1$, then we can assume that $\delta = a^{q+1}$ in this sub-subsection. Firstly let us determine the order of the automorphism σ. Note that

$$\sigma^i = 1 \Leftrightarrow v_{i-1} = 0 \text{ and } v_i = a^i.$$

It is easy to calculate that $v_{i-1} = 0 \Leftrightarrow \delta^{2i} = a^{(q+1)i} \Leftrightarrow q-1 | i$. If $i = (q-1)k$ for some k, then

$$v_{(q-1)k} = a^{(q-1)k} \Leftrightarrow \frac{\delta^{(q-1)k+2} + \delta^{(1-q)k} a^{((q-1)k+1)(q+1)}}{\delta^2 + a^{q+1}} = a^{(q-1)k} = 1 \Leftrightarrow q+1 | k.$$

Hence, the order of σ is $\mathrm{ord}(\sigma) = q^2 - 1$.

Now we consider the fixed subfield with respect to the cyclic group $\mathcal{D}$ generated by the automorphism σ. For the infinity place P_∞ and $1 \le i \le q^2-2$, we have $\sigma^i(P_\infty) = P_\infty \Leftrightarrow v_{i-1} = 0$. For $1 \le i \le q^2-2$, we have $\sigma^i(P_{\alpha,\beta}) = (P_{\alpha,\beta})$ if and only if

$$\frac{a^i\alpha}{a^{q+1}v_{i-1}\beta + v_i} = \alpha, \quad \frac{a^{q+1}v_{i-2}\beta + v_{i-1}}{a^{q+1}v_{i-1}\beta + v_i} = \beta, \quad \beta^q + \beta = \alpha^{q+1}.$$

Case 1: $\alpha \neq 0$.
We have $a^{q+1}v_{i-1}\beta + v_i = a^i$. Assume that $v_{i-1} = 0$, then $v_i = a^i$. It follows that $\sigma^i = 1$ which is impossible. Hence, $v_{i-1} \neq 0$ and

$$\frac{a^{q+1}v_{i-2}\beta + v_{i-1}}{a^{q+1}v_{i-1}\beta + v_i} = \beta \Rightarrow v_{i-1}(a^{q+1}\beta^2 + c\beta + 1) = 0 \Rightarrow (a^{q+1}\beta + \delta)(\beta + \frac{1}{\delta}) = 1.$$

Thus there are two solutions $\beta = \delta^{-1}$ and $\beta = a^{-(q+1)}\delta$. It is easy to calculate that

$$a^{q+1}v_{i-1}\beta + v_i = \begin{cases} \delta^i & \text{if } \beta = \delta^{-1}, \\ 1 & \text{if } \beta = a^{-(q+1)}\delta. \end{cases}$$

It is easy to check that $a^{q+1}v_{i-1}\beta + v_i \neq a^i$. Therefore, the place $P_{\alpha,\beta}$ with $\alpha \neq 0$ can't be stabilized by the automorphism σ^i for $1 \le i \le q^2-2$.
Case 2: $\alpha = 0$.
It follows that $v_{i-1}(a^{q+1}\beta^2 + c\beta + 1) = 0$ and $\beta^q + \beta = 0$. If $v_{i-1} = 0$, then $i = (q-1)k$ for $1 \le k \le q$. For each k, the places $P_{0,\beta}$ with $\beta^q + \beta = 0$ and P_∞ are stabilized by the automorphism σ^i. Hence, the number of the rational places stabilized by the automorphism σ^i is $N(\sigma^i) = q+1$.
If $v_{i-1} \neq 0$, then $\beta = \delta^{-1}$ or $\beta = a^{-(q+1)}\delta$. Moreover, it can be calculated directly that

$$(\frac{1}{\delta})^q + \frac{1}{\delta} = \frac{\delta^{q-1}+1}{\delta^q} = 0 \text{ and } (a^{-(q+1)}\delta)^q + a^{-(q+1)}\delta = a^{-(q+1)}(\delta^q + \delta) = 0.$$

Hence, the places $P_{0,\delta^{-1}}$ and $P_{0,a^{-(q+1)}\delta}$ are stabilized by the automorphism σ^i with $v_{i-1} \neq 0$, that is, $N(\sigma^i) = 2$. By the Hurwitz genus formula,

$$q^2 - q - 2 \ge (q^2-1)[2g(H^{\mathcal{D}}) - 2] + (q+1)q + 2(q^2 - 2 - q).$$

Hence, the genus of the fixed subfield is $g(H^{\mathcal{D}}) = 0$ and all places of degree 3 of H are unramified in $H/H^{\mathcal{D}}$.

Theorem 5.1. *Let H be the Hermitian function field over $\mathbb{F}_{q^2}$ with even characteristic, let m be a positive divisor of q^2-1 and let $\mathcal{G}$ be the group generated by the automorphism $\sigma^{\frac{q^2-1}{m}}$ with $d = \gcd(m, q+1)$. Then the genus of the fixed field $H^{\mathcal{G}}$ is*

$$g(H^{\mathcal{G}}) = \frac{(q-1)(q+1-d)}{2m}.$$

Proof. It is easy to check that the number of automorphisms in the intersection of $\mathcal{G}$ and $\langle \sigma^{q-1} \rangle$ is $d = \gcd(m, q+1)$. Hence, this theorem follows immediately from the Hurwitz genus formula

$$q^2 - q - 2 = m[2g(H^{\mathcal{G}}) - 2] + (q+1)(d-1) + 2(m-d).$$

□

5.1.2. $\delta^{q+1} = a^{q+1}$. If $\delta^{q+1} = a^{q+1}$, then we can assume that $\delta = a$ in this sub-subsection. Hence, $c = \delta + \delta^q$ and

$$v_i = \frac{\delta^{i+1} + \delta^{q(i+1)}}{\delta + \delta^q}.$$

Now we can determine the order of σ, since $\sigma^i = 1 \Leftrightarrow v_{i-1} = 0$ and $v_i = a^i$. It is easy to see that $v_{i-1} = 0 \Leftrightarrow \delta^i + \delta^{qi} = 0 \Leftrightarrow \delta^{i(q-1)} = 1 \Leftrightarrow q+1 | i$. For $i = (q+1)k$, we have

$$v_i = a^i \Leftrightarrow \frac{\delta^{(q+1)k+1} + \delta^{q((q+1)k+1)}}{\delta + \delta^q} = \delta^{(q+1)k} = a^{(q+1)k}.$$

Hence, $\mathrm{ord}(\sigma) = q+1$.

Then we consider the fixed subfield with respect to the cyclic group $\mathcal{D}$ generated by the automorphism σ. For $1 \le i \le q$, we know $v_{i-1} \neq 0$ and $\sigma^i(P_\infty) \neq P_\infty$. Moreover, $\sigma^i(P_{\alpha,\beta}) = P_{\alpha,\beta}$ if and only if

$$\frac{a^i\alpha}{a^{q+1}v_{i-1}\beta + v_i} = \alpha, \quad \frac{a^{q+1}v_{i-2}\beta + v_{i-1}}{a^{q+1}v_{i-1}\beta + v_i} = \beta, \quad \beta^q + \beta = \alpha^{q+1}.$$

It follows from the second equation that $a^{q+1}\beta^2 + c\beta + 1 = 0$. Hence,

$$\beta = \delta^{-1} \text{ or } \beta = \delta^{-q}.$$

If $\beta = \delta^{-1}$, then $a^{q+1}v_{i-1}\beta + v_i = a^{q+1}v_{i-1}\delta^{-1} + v_i = \delta^i = a^i$ and $(\delta^{-1})^q + \delta^{-1} = \delta^{-(q+1)}(\delta^q + \delta) \neq 0$.
If $\beta = \delta^{-q}$, then $a^{q+1}v_{i-1}\beta + v_i = a^{q+1}v_{i-1}\delta^{-q} + v_i = \delta^{iq} \neq a^i$ and $(\delta^{-q})^q + \delta^{-q} = \delta^{-(q+1)}(\delta^q + \delta) \neq 0$.
Thus the places $P_{\alpha,\delta^{-1}}$ with $\alpha^{q+1} = \delta^{-q} + \delta^{-1}$ are stabilized by the automorphism σ^i. Hence, $N(\sigma^i) = q+1$ for $1 \le i \le q$. By the Hurwitz genus formula,

$$q^2 - q - 2 \ge (q+1)[2g(H^{\mathcal{D}}) - 2] + q(q+1).$$

Hence, the genus of the fixed subfield is $g(H^{\mathcal{D}}) = 0$ and all places of degree 3 of H are unramified in $H/H^{\mathcal{D}}$.

Theorem 5.2. *Let H be the Hermitian function field over $\mathbb{F}_{q^2}$ with even characteristic, let m be a positive divisor of $q+1$ and let $\mathcal{G}$ be the group generated by the automorphism $\sigma^{\frac{q+1}{m}}$. Then the genus of the fixed field $H^{\mathcal{G}}$ is*

$$g(H^{\mathcal{G}}) = \frac{(q-1)(q+1-m)}{2m}.$$

Proof. This theorem follows from the Hurwitz genus formula

$$q^2 - q - 2 = m[2g(H^{\mathcal{G}}) - 2] + (m-1)(q+1).$$

□

5.2. **Odd characteristic.** In the odd characteristic case, $c = \delta - a^{q+1}\delta^{-1}$ and

$$c^q + c = 0 \Leftrightarrow \delta^{q+1} = a^{q+1} \text{ or } \delta^{q-1} = -1.$$

5.2.1. $\delta^{q-1} = -1$. If $\delta^{q-1} = -1$, then we assume that $\delta = a^{\frac{q+1}{2}}$ and $\mathrm{ord}(\delta) = 2(q-1)$ in this sub-subsection. It can be calculated directly that

$$v_{i-1} = 0 \Leftrightarrow \delta^{i+1} + (-1)^{i-1}\frac{a^{(q+1)i}}{\delta^{i-1}} = 0 \Leftrightarrow \delta^{2i} = (-1)^i a^{(q+1)i} \Leftrightarrow 2|i.$$

For the even integer i,

$$v_i = a^i \Leftrightarrow \delta^{i+2} + (-1)^i\frac{a^{(i+1)(q+1)}}{\delta^i} = a^i(\delta^2 + a^{q+1}) \Leftrightarrow \delta^i = a^i \Leftrightarrow 2(q+1)|i.$$

Hence, $\mathrm{ord}(\sigma) = 2(q+1)$.

Now we consider the cyclic group $\mathcal{D}$ generated by the automorphism σ. For the infinity place P_∞ and $1 \le i \le 2q+1$, we have $\sigma^i(P_\infty) = P_\infty \Leftrightarrow v_{i-1} = 0$. For $1 \le i \le 2q+1$, we have $\sigma^i(P_{\alpha,\beta}) = P_{\alpha,\beta}$ if and only if

$$\frac{a^i\alpha}{a^{q+1}v_{i-1}\beta + v_i} = \alpha, \quad \frac{a^{q+1}v_{i-2}\beta + v_{i-1}}{a^{q+1}v_{i-1}\beta + v_i} = \beta, \quad \beta^q + \beta = \alpha^{q+1}.$$

Case 1: $\alpha \neq 0$**.**
In this case, $a^{q+1}v_{i-1}\beta + v_i = a^i$. Assume that $v_{i-1} = 0$, then $v_i = a^i$. It follows that $\sigma^i = 1$ which is impossible for $1 \le i \le 2q+1$. Hence, $v_{i-1} \neq 0$ and

$$v_{i-1}(a^{q+1}\beta^2 + c\beta - 1) = 0 \Rightarrow (a^{q+1}\beta + \delta)(\beta - \delta^{-1}) = 0 \Rightarrow \beta = -a^{-(q+1)}\delta \text{ or } \beta = \delta^{-1}$$

from the second equation. It is easy to check that

$$a^{q+1}v_{i-1}\beta + v_i = \begin{cases} \delta^i & \text{if } \beta = \delta^{-1}, \\ (-\delta)^i & \text{if } \beta = -a^{-(q+1)}\delta. \end{cases}$$

It can be verified directly that $a^{q+1}v_{i-1}\beta + v_i \neq a^i$. Hence, the places $P_{\alpha,\beta}$ with $\alpha \neq 0$ can't be stabilized by the automorphism σ^i for $1 \le i \le 2q+1$.
Case 2: $\alpha = 0$**.**
From the second equation, we have

$$v_{i-1}(a^{q+1}\beta^2 + c\beta - 1) = 0.$$

If $v_{i-1} = 0$, then the places $P_{0,\beta}$ with $\beta^q + \beta = 0$ and P_∞ are stabilized by the automorphism σ^i. Hence, $N(\sigma^i) = q+1$ for each even integer i.
If $v_{i-1} \neq 0$, that is, i is odd, then $a^{q+1}\beta^2 + c\beta - 1 = 0$. Hence, $\beta = \delta^{-1}$ or $\beta = -a^{-(q+1)}\delta$. It follows that $\beta^q + \beta = 0$, since $\delta^{q-1} = -1$. Hence, the places $P_{0,\delta^{-1}}$ and $P_{0,-a^{-(q+1)}\delta}$ are stabilized by the automorphisms σ^i, that is, $N(\sigma^i) = 2$ for each odd integer i. By the Hurwitz genus formula,

$$q^2 - q - 2 \ge 2(q+1)[2g(H^{\mathcal{D}}) - 2] + (q+1)q + 2(q+1).$$

Hence, the genus of fixed subfield is $g(H^{\mathcal{D}}) = 0$ and all places of degree 3 of H are unramified in $H/H^{\mathcal{D}}$.

Theorem 5.3. *Let H be the Hermitian function field over $\mathbb{F}_{q^2}$ with odd characteristic, let m be a positive divisor of $2(q+1)$ and let $\mathcal{G}$ be the group generated by the*

automorphism $\sigma^{\frac{2(q+1)}{m}}$. *If* $m|q+1$, *then the genus of the fixed field* $H^{\mathcal{G}}$ *is*

$$g(H^{\mathcal{G}}) = \frac{(q-1)(q+1-m)}{2m}.$$

Otherwise, the genus of the fixed field $H^{\mathcal{G}}$ *is*

$$g(H^{\mathcal{G}}) = \frac{(q-1)(q+1-\frac{m}{2})}{2m}.$$

Proof. If $m|q+1$, then $\frac{2(q+1)}{m}$ is even. By the Hurwitz genus formula,

$$q^2-q-2 = m[2g(H^{\mathcal{G}})-2] + (q+1)(m-1).$$

If $m \nmid q+1$, then $\frac{2(q+1)}{m}$ is odd. By the Hurwitz genus formula,

$$q^2-q-2 = m[2g(H^{\mathcal{G}})-2] + (q+1)(\frac{m}{2}-1) + 2\cdot\frac{m}{2}.$$

This theorem follows immediately. □

5.2.2. $\delta^{q+1} = a^{q+1}$. If $\delta^{q+1} = a^{q+1}$, then we assume that $\delta = a$ in this sub-subsection. Firstly let us determine the order of the automorphism σ. Note that $\sigma^i = 1 \Leftrightarrow v_{i-1} = 0$ and $v_i = a^i$. It can be calculated that

$$v_{i-1} = 0 \Leftrightarrow \delta^{i+1} + (-1)^{i-1}\frac{a^{i(q+1)}}{\delta^{i-1}} = 0 \Leftrightarrow \delta^{2i} = (-1)^i a^{i(q+1)} \Leftrightarrow a^{(q-1)i} = (-1)^i.$$

If $q \equiv 1(\mathrm{mod}4)$, then $v_{i-1} = 0 \Leftrightarrow \frac{q+1}{2}|i$. It is easy to verify that $v_{\frac{q+1}{2}} = a^{\frac{q+1}{2}}$. Hence, the order of σ is

$$\mathrm{ord}(\sigma) = (q+1)/2.$$

If $q \equiv 3(\mathrm{mod}4)$, then $v_{i-1} = 0 \Leftrightarrow q+1|i$. It is easy to verify that $v_{q+1} = a^{q+1}$. Hence, the order of σ is

$$\mathrm{ord}(\sigma) = q+1.$$

Let $\mathcal{D}$ be the cyclic group generated by the automorphism σ. Here we assume that $3 \nmid (q+1)$, then all places of degree 3 of H are unramified in $H/H^{\mathcal{D}}$. For $1 \le i \le \mathrm{ord}(\sigma)-1$, then $v_{i-1} \neq 0$ and $\sigma^i(P_\infty) \neq P_\infty$. Hence, $\sigma^i(P_{\alpha,\beta}) = P_{\alpha,\beta}$ if and only if

$$\frac{a^i\alpha}{a^{q+1}v_{i-1}\beta + v_i} = \alpha, \quad \frac{a^{q+1}v_{i-2}\beta + v_{i-1}}{a^{q+1}v_{i-1}\beta + v_i} = \beta, \quad \beta^q + \beta = \alpha^{q+1}.$$

It is easy to see that $a^{q+1}\beta^2 + c\beta - 1 = 0$, since $v_{i-1} \neq 0$. It follows that

$$\beta = \delta^{-1} \text{ or } \beta = -a^{-(q+1)}\delta.$$

If $\beta = \delta^{-1}$, then $a^{q+1}v_{i-1}\beta + v_i = \delta^i = a^i$ and $\beta^q + \beta = \delta^{-q} + \delta^{-1} = \delta^{-q-1}(\delta^q + \delta) \neq 0$.
If $\beta = -a^{-(q+1)}\delta$, then $a^{q+1}v_{i-1}\beta + v_i = -\delta v_{i-1} + v_i = (-1)^i a^{iq} \neq a^i$ and $\beta^q + \beta = -a^{-(q+1)}(\delta^q + \delta) \neq 0$.
Thus the places $P_{\alpha,\delta^{-1}}$ with $\alpha^{q+1} = \delta^{-q} + \delta^{-1}$ are stabilized by the automorphism σ^i. Hence, $N(\sigma^i) = q+1$ for $1 \le i \le \mathrm{ord}(\sigma)-1$. By the Hurwitz genus formula,

$$q^2-q-2 = \mathrm{ord}(\sigma)\cdot[2g(H^{\mathcal{D}})-2] + (\mathrm{ord}(\sigma)-1)(q+1).$$

Hence, the genus of the fixed subfield is

$$g(H^{\mathcal{D}}) = \begin{cases} (q-1)/2 & \text{if } q \equiv 1 (\text{mod } 4) \\ 0 & \text{if } q \equiv 3 (\text{mod } 4). \end{cases}$$

Theorem 5.4. *Let H be the Hermitian function field over $\mathbb{F}_{q^2}$ with odd characteristic. Assume that $3 \nmid (q+1)$. Let m be a positive divisor of $ord(\sigma)$ and let $\mathcal{G}$ be a subgroup of $\mathcal{D}$ with order m. Then the genus of the fixed field of $H^{\mathcal{G}}$ is*

$$g(H^{\mathcal{G}}) = \frac{(q-1)(q+1-m)}{2m}.$$

Proof. This theorem follows from the Hurwitz genus formula

$$q^2 - q - 2 = m[2g(H^{\mathcal{G}}) - 2] + (m-1)(q+1).$$

□

Remark 5.5. *The places of degree 3 of H may be ramified only if $q \equiv 1 (mod\ 4)$ and $3|(q+1)$ hold true at the same time. Hence, we can only assume that $q \not\equiv 5 (mod\ 12)$ in Theorem 5.4 by the Chinese Remainder Theorem.*

References

[1] M. Abdon and L. Quoos, *On the genera of subfields of the Hermitian function field*, Finite Fields Appl. **10**(2004), 271–284.

[2] A. Bassa, L.M. Ma, C.P. Xing and S.L. Yeo, *Towards a characterization of subfields of the Deligne–Lusztig function fields*, Journal of Combinatorial Theory, Series A **120**(2013), 1351–1371.

[3] A. Cossidente and G. Korchmáros, *On curves covered by the Hermitian curves*, J. Algebra **216**(1999), 56–76.

[4] A. Cossidente, G. Korchmáros and F. Torres, *Curves of large genus covered by the Hermitian curve*, Comm. Algebra **28**(2000), 4707–4728.

[5] R. Fuhrmann, A. Garcia and F. Torres, *On maximal curves*, J. Number Theory **67**(1997), 29–51.

[6] R. Fuhrmann and F. Torres, *The genus of curves over finite fields with many rational points*, Manuscripta Math. **89**(1996), 103–106.

[7] A. Garcia, H. Stichtenoth and C.P. Xing, *On subfields of the Hermitian function fields*, Compositio Mathematica **120**(2000), 137–170.

[8] M. Giuliette and G. Korchmáros, *A new family of maximal curves over a finite field*, Math. Ann. **343**(2009), 229–245.

[9] J.W.P. Hirschfeld, G. Korchmáros and F. Torres, *Algebraic Curves over a Finite Field*, Princeton Series in Applied Mathematics, Princeton University Press, 2008.

[10] G. Lachaud, *Sommes d'Eisenstein et nombre de points de certaines courbes algébriques sur les corps finis*, C. R. Acad. Sci. Paris Ser. I **305**(1987), 729–732.

[11] L.M. Ma, C.P. Xing and S.L. Yeo, *On automorphism groups of cyclotomic function fields over finite fields*, J. Number Theory **169**(2016), 406–419.

[12] H. Niederreiter and C.P. Xing, *Rational points on curves over finite fields: Theory and Applications*, LMS **285**, Cambridge, 2001.

[13] H.-G. Rück and H. Stichtenoth, *A characterization of Hermitian function fields over finite fields*, J. Reine Angew. Math. **457**(1994), 185–188.

[14] H. Stichtenoth, *Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik, Teil I and Teil II*, Arch. Math. **24**(1973), 524–544 and 615–631.

[15] H. Stichtenoch, *Algebraic Function Fields and Codes*, Grad. Texts in Math. **254**, Springer–Verlag, 2009.

[16] C.P. Xing and H. Stichtenoth, *The genus of maximal function fields over finite fields*, Manuscript Math. **86**(1995), 217–224.

School of Mathematical Sciences, Yangzhou University, Yangzhou China 225002
E-mail address: lmma@yzu.edu.cn

Division of Mathematical Sciences, School of Physical & Mathematical Sciences, Nanyang Technological University, Singapore 637371
E-mail address: xingcp@ntu.edu.sg