J. Korean Math. Soc. **52** (2015), No. 2, pp. 225–237
http://dx.doi.org/10.4134/JKMS.2015.52.2.225

ON SUBFIELDS OF GK AND GENERALIZED GK FUNCTION FIELDS

Yusuf Danisman and Mehmet Ozdemir

Abstract. In this article, we show that many of the genera that Giulietti and Fanali obtained from subfields of the GK curve can be obtained by using similar techniques used by Garcia, Stichtenoth and Xing. In the meantime, we obtain some new genera from the subfields of GK and generalized GK function fields.

1. Introduction

Let F/K be an algebraic function field of genus g with constant field K where K is a finite field and $N(F)$ be the number of rational places of F. By Hasse-Weil Theorem [13, Theorem 5.2.3], the number of rational places of F/K is bounded by

$$\mid N(F) - (|K| + 1) \mid \leq 2\sqrt{|K|}g. \tag{1}$$

A function field is called maximal if its number of rational places attains the upper bound in the above inequality. Obviously, maximal function fields which are not rational can only exist over finite fields of square cardinality. The most well-known example of a maximal function field is the Hermitian function field $\mathcal{H} = \mathbb{F}_{q^2}(x, y)$, where $\mathbb{F}_{q^2}$ is the finite field with q^2 elements. $\mathcal{H}$ is defined by the equation

$$x^q + x = y^{q+1} \tag{2}$$

and, $\mathcal{H}$ has the genus

$$\frac{q(q-1)}{2}, \tag{3}$$

which is the maximum possible genus of all maximal function fields over $\mathbb{F}_{q^2}$. In fact, $\mathcal{H}$ is the unique maximal function field, up to isomorphism, with this genus [10].

Received October 22, 2013; Revised November 3, 2014.
2010 *Mathematics Subject Classification.* 14H05.
Key words and phrases. algebraic curves, function field, automorphism group.

One of the interesting questions about maximal function fields is their genus spectrum. In fact, the main problem is to describe the following set:

$$M(q^2) := \{g \geq 0 \mid \text{there exists a maximal function field } F/\mathbb{F}_{q^2} \text{ with genus } g\}.$$

In this regard, it is important to find new maximal function fields of various genera over a fixed finite field. One of the main tools in describing a new maximal function field of different genus is to consider the subfields of a given maximal function field. The automorphism group of a maximal function field is of special interest due to its importance for finding the corresponding subfields as Serre's result states that every subfield of a maximal function field is maximal [9]. The Hermitian function field has a large automorphism group with respect to its genus [11, 12], so it is an important source of generating new maximal function fields. Indeed, all known examples of maximal function fields had been shown to be subfields of the Hermitian function field before a new maximal function field, the GK function field, was constructed by Giulietti-Korchmáros. The GK function field is defined over $\mathbb{F}_{q^6}$ with the following defining equations:

$$x^q + x = y^{q+1}, \tag{4}$$

$$y^{q^2} - y = z^{\frac{q^3+1}{q+1}}. \tag{5}$$

The GK function field is not a subfield of the Hermitian function field for $q > 2$ [7], and it is later generalized to a family of maximal function fields, the generalized GK function field [5]. For any odd integer $n \geq 3$, the generalized GK function fields $\mathcal{C}_n$ are the family of function fields defined over $\mathbb{F}_{q^{2n}}$ by the following equations:

$$x^q + x = y^{q+1}, \tag{6}$$

$$y^{q^2} - y = z^{\frac{q^n+1}{q+1}}. \tag{7}$$

The equation ([5]) also defines a maximal function field [1]. So, $\mathcal{C}_n$ can be considered as the compositum of two maximal function field. The member of $\mathcal{C}_n$ for $n = 3$ obviously coincides with the GK function field. The genus $g(\mathcal{C}_n)$ and the number of rational places $N(\mathcal{C}_n)$ of $\mathcal{C}_n$ are given as

$$g(\mathcal{C}_n) = \frac{(q-1)(q^{n+1} + q^n - q^2)}{2}, \quad N(\mathcal{C}_n) = q^{2n+2} - q^{n+3} + q^{n+2} + 1. \tag{8}$$

It is not known yet whether the members of this family for $n \geq 5$ are subfields of the Hermitian function field or not. However, it is known that Hermitian function field is not Galois cover of them [3].

A large class of subfields of the Hermitian function field was described in [6] by considering the fixed fields of certain subgroups of the automorphism group of the Hermitian function field. Later, these results were improved in [2].

The automorphism group of the GK function field and the generalized GK function field are also known [7, 8]. Some subfields of the GK function field are described in [4], and some new genera are obtained by a strong group-theoretic arguments. Here, we construct some subgroups of GK and generalized GK function field with similar techniques that were used in [2, 6], and we get some new genera as well as many of the genera that were obtained in [4].

In the next section, we describe automorphism group of the GK and the generalized GK function fields. As mentioned above, we henceforth denote the GK function field by $\mathcal{C}_3$ and the finite field $\mathbb{F}_{q^{2n}}$ by K unless stated otherwise in the sequel. In Sections 3 and 4, we compute the genera of the fixed fields of certain subgroups, where K is a field of odd characteristic.

2. Automorphisms of $\mathcal{C}_n$

Let G be the automorphism group of $\mathcal{C}_n$ and P_∞ be the common pole of x, y, and z in $\mathcal{C}_n$. Then, for $n \geq 3$ the group

$$G(P_\infty) = \{\sigma \in G \mid \sigma(P_\infty) = P_\infty\}, \tag{9}$$

consists of the automorphisms of the following form [8]:

$$\sigma(x) = \gamma^{q^n+1}x + \gamma^m \beta^q y + \alpha,\ \sigma(y) = \gamma^m y + \beta,\ \sigma(z) = \gamma z, \tag{10}$$

where γ is a $(q^n+1)(q-1)$-th root of unity, $m = \frac{q^n+1}{q+1}$, and $\beta \in \mathbb{F}_{q^2}$ with $\alpha^q + \alpha = \beta^{q+1}$. Hence, the order of $G(P_\infty)$ is $q^3(q-1)(q^n+1)$.

Each automorphism in $G(P_\infty)$ can be represented by a triple $[\gamma, \beta, \alpha]$, and the group structure of $G(P_\infty)$ is as follows:

$$\begin{aligned}[]
[\gamma_1, \beta_1, \alpha_1] \cdot [\gamma_2, \beta_2, \alpha_2] &= [\gamma_1\gamma_2, \gamma_2^m \beta_1 + \beta_2, \gamma_2^{q^n+1}\alpha_1 + \gamma_2^m \beta_2^q \beta_1 + \alpha_2],\\
id &= [1, 0, 0],\\
[\gamma, \beta, \alpha]^{-1} &= [\gamma^{-1}, -\gamma^{-m}\beta, \gamma^{-(q^n+1)}\alpha^q].
\end{aligned}$$

The map $w : \mathcal{C}_3 \mapsto \mathcal{C}_3$ defined by

$$w(x) = \frac{1}{x}, \qquad w(z) = \frac{z}{x} \tag{11}$$

is an automorphism of the GK function field $\mathcal{C}_3$. By [8], we have

(i) $G = G(P_\infty)$ for $n \geq 5$,
(ii) $G = \langle w, G(P_\infty)\rangle$ for $n = 3$.

3. Genus computation for the fixed fields of the subgroups of $G(P_\infty)$

In this section, we show how to compute the genera of the fixed fields of the subgroups of $G(P_\infty)$, where K is a field of odd characteristic.

Lemma 3.1. *The fixed field of* $G(P_\infty)$ *is* $K(z^{(q-1)(q^n+1)})$ *for* $n \geq 3$.

Proof. Since $\gamma^{(q-1)(q^n+1)} = 1$ we have $\sigma(z^{(q-1)(q^n+1)}) = (\gamma z)^{(q-1)(q^n+1)} = z^{(q-1)(q^n+1)}$ for any $\sigma \in G(P_\infty)$. Besides, it can be seen from the defining equations of $\mathcal{C}_n$ that $|\mathcal{C}_n : K(z^{(q-1)(q^n+1)})| = |K(x, y, z) : K(y, z)| \cdot |K(y, z) :$

$K(z)| = qq^2(q-1)(q^n+1) = q^3(q-1)(q^n+1)$, which is equal to cardinality of $|G(P_\infty)|$. Hence, it follows that $K(z^{(q-1)(q^n+1)})$ is the fixed field of $G(P_\infty)$. □

Lemma 3.2. *Let $\theta = z^{(q-1)(q^n+1)}$. Then, for $n \geq 3$ the ramified places of $K(\theta)$ in the extension $\mathcal{C}_n/K(\theta)$ are $(\theta = \infty)$ and $(\theta = 0)$.*

Proof. Let R_∞ be the unique place of $\mathcal{H}$ lying below P_∞. Let A denote the set of automorphisms of $\mathcal{H}$ and

$$A(R_\infty) = \{\sigma \in A \mid \sigma(R_\infty) = R_\infty\}. \tag{12}$$

By [8], we have

$$A(R_\infty) = \{\sigma|_{\mathcal{H}} \mid \sigma \in G(P_\infty)\}. \tag{13}$$

So, the fixed field of the group $A(R_\infty)$ in $\mathcal{H}$ is the same as the fixed field of $G(P_\infty)$ in $\mathcal{C}_n$. The only ramified places of $K(\theta)$ in the extension $\mathcal{H}/K(\theta)$ are $(\theta = 0)$ and $(\theta = \infty)$, and all the places lying above $(\theta = 0)$ in $\mathcal{H}$ are the places R_{ab} for $x = a \in \mathbb{F}_{q^2}$ and $y = b$ with $a^q + a = b^{q+1}$ [6]. The fact that all these places with R_∞ in $\mathcal{H}$ are the only places of $\mathcal{H}$ that are ramified in $\mathcal{C}_n/\mathcal{H}$ completes our proof. □

All the ramified places of $\mathcal{C}_n$ except for P_∞ are tamely ramified in the extension $\mathcal{C}_n/K(\theta)$ as all the places of $\mathcal{H}$ except for R_∞ in $\mathcal{H}/K(\theta)$ are tamely ramified and $|\mathcal{C}_n : \mathcal{H}| = \frac{q^n+1}{q+1}$. The number of these places is q^3, and each of these places is uniquely determined by some values $a, b \in \mathbb{F}_{q^2}$ with $a^q + a = b^{q+1}$. We will denote these places by P_{ab0}. Let U be a subgroup of $G(P_\infty)$ and $\mathcal{C}_n^U$ its fixed field. By Hurwitz Genus Formula, we have

$$(q-1)(q^{n+1} + q^n - q^2) - 2 = |U|(2g(\mathcal{C}_n^U) - 2) + \deg \operatorname{Diff}(\mathcal{C}_n \backslash \mathcal{C}_n^U). \tag{14}$$

We need to compute $\deg \operatorname{Diff}(\mathcal{C}_n \backslash \mathcal{C}_n^U)$. We have,

$$\begin{aligned} \deg \operatorname{Diff}(\mathcal{C}_n \backslash \mathcal{C}_n^U) &= d(P_\infty) + \sum_{a \in \mathbb{F}_{q^2}} d(P_{ab0}) \\ &= d(P_\infty) + \sum_{a \in \mathbb{F}_{q^2}} [e(P_{ab0}) - 1] \\ &= d(P_\infty) + \sum_{a \in \mathbb{F}_{q^2}} |\{\sigma \in U - \{Id\} : \sigma(P_{ab0}) = P_{ab0}\}| \\ &= d(P_\infty) + \sum_{\sigma \in U - \{Id\}} N(\sigma), \end{aligned} \tag{15}$$

where $N(\sigma) = |\{(a,b) : a^q + a = b^{q+1},\, \sigma(P_{ab0}) = P_{ab0}\}|$.

Since P_∞ is totally ramified in the extension $\mathcal{C}_n/\mathcal{C}_n^U$ we have

$$d(P_\infty) = \sum_{1 \neq \sigma \in U} v_{P_\infty}[\sigma(\tau) - \tau], \tag{16}$$

where τ is a prime element for P_∞. Since $\tau = \frac{z^{q^n-3}}{x}$ is a prime element of P_∞ we have

$$v_{P_\infty}(\sigma(\tau)-\tau) = \begin{cases} \frac{q^n+1}{q+1}+1 & \gamma = 1,\ \beta \neq 0 \\ q^n+2 & \gamma = 1,\ \beta = 0 \\ 1 & \text{else.} \end{cases} \tag{17}$$

Lemma 3.3. *Let $\sigma = [\gamma, \beta, \alpha] \in G(P_\infty)$. Then*

$$N(\sigma) = \begin{cases} q^3 & \textit{if} \quad \gamma^m = 1,\ \alpha = 0,\ \beta = 0 \\ q & \textit{if} \quad \gamma^m \neq 1,\ \gamma^{q^n+1} = 1,\ \alpha = \frac{\gamma^m\beta^{q+1}}{\gamma^m-1} \\ 1 & \textit{if} \quad \gamma^{q^n+1} \neq 1 \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. We have

$$\begin{aligned} \sigma(P_{ab0}) = P_{ab0} \quad &\Leftrightarrow \quad \sigma(x-a),\ \sigma(y-b),\ \sigma(z) \in P_{abo} \\ &\Leftrightarrow \quad \gamma^{q^n+1}x + \gamma^m\beta^q y + \alpha - a,\ \gamma^m y + \beta - b,\ \gamma z \in P_{abo} \\ &\Leftrightarrow \quad \gamma^{q^n+1}(x-a) + \gamma^{q^n+1}a + \gamma^m\beta^q(y-b) + \gamma^m\beta^q b + \alpha - a, \\ &\qquad \gamma^m(y-b) + \gamma^m b + \beta - b \in P_{abo} \\ &\Leftrightarrow \quad \gamma^{q^n+1}a + \gamma^m\beta^q b + \alpha - a,\ \gamma^m b + \beta - b \in P_{abo} \\ &\Leftrightarrow \quad [\gamma^{q^n+1}-1]a + \gamma^m\beta^q b + \alpha = 0,\ [\gamma^m - 1]b + \beta = 0. \end{aligned}$$

We now need to do computations case by case.

Case 1: If $\gamma^m = 1 \Rightarrow \beta = 0$, then $\alpha = 0$. Since, there is no condition on a and b we get $N(\sigma) = q^3$.

Case 2: If $\gamma^m \neq 1$ and $\gamma^{q^n+1} = 1$, then $b = -\frac{\beta}{\gamma^m-1}$. Hence $-\gamma^m\beta^q\frac{\beta}{\gamma^m-1} + \alpha = 0$ and $\alpha = \frac{\gamma^m\beta^{q+1}}{\gamma^m-1}$. So, we get $N(\sigma) = q$ as there is no condition on a.

Case 3: If $\gamma^{q^n+1} \neq 1$, then $b = -\frac{\beta}{\gamma^m-1}$ and $a = -\frac{\gamma^m\beta^q b+\alpha}{\gamma^{q^n+1}-1}$. So, we get $N(\sigma) = 1$. □

3.1. Example 1: A subgroup of $G(P_\infty)$

We will now construct a certain type of subgroups of $G(P_\infty)$. Before this, we fix the following notations.

$q = p^h$ for some prime number p and positive integer h,
$m = \frac{q^n+1}{q+1}$,
t is a divisor of $(q-1)(q^n+1)$,
$d = \gcd(t, q^n+1)$,
$s = \min\{r \geq 1 : p^r \equiv 1 \mod (\frac{t}{d})\}$,
u_1 and u_2 are integers with $0 \leq u_1, u_2 \leq h$, $s|u_1$ and $s|u_2$.

Lemma 3.4. $\mathbb{F}_{p^s} \subseteq \mathbb{F}_q$.

Proof. $(q-1)(q^n+1) = tk$ for some $k \in \mathbb{Z}$, which implies $(q-1)(q^n+1)/d \equiv 0 \mod t/d$. So, we have $q-1 \equiv 0 \mod t/d$ and hence $s \leq h$. We can write $h = sa+b$ for some $a, b \in \mathbb{Z}$ with $b < s$ and hence $p^b = p^h/p^{sa} \equiv 1 \mod t/d$. The minimality of s gives that b is zero, and this implies $s|h$. □

Lemma 3.5. *There is a u_1/s dimensional $\mathbb{F}_{p^s}$ subspace of $\mathbb{F}_q$.*

Proof. This is an immediate result of Lemma 3.4. □

Let W_1 be a u_1/s dimensional $\mathbb{F}_{p^s}$ subspace of $\mathbb{F}_q$. Then we have $|W_1| = p^{u_1}$.

Lemma 3.6. *Let L be the set of automorphisms of the following form:*

$$\sigma = \begin{cases} z \to \gamma z \\ y \to \gamma^m y + \beta \\ x \to \gamma^{q^n+1}x + \gamma^m \beta^q y + \frac{\beta^{q+1}}{2}, \end{cases}$$

where $\beta \in W_1$ and γ is a t-th root of unity. Then, L is a subgroup of $G(P_\infty)$.

Proof. Any $\sigma \in L$ is obviously an automorphism of $G(P_\infty)$ as $\beta^{(q+1)q} = \beta^{(q+1)}$. So, it is enough to check that L is closed under composition. Let $\sigma_1 = [\gamma_1, \beta_1, \frac{\beta_1^{q+1}}{2}]$ and $\sigma_2 = [\gamma_2, \beta_2, \frac{\beta_2^{q+1}}{2}]$. Then,

$$\sigma_1\sigma_2 = [\gamma_1\gamma_2, \gamma_2^m\beta_1 + \beta_2, \gamma^{q^n+1}\frac{\beta_1^{q+1}}{2} + \gamma_2^m\beta_2^q\beta_1 + \frac{\beta_2^{q+1}}{2}].$$

We have

$$(\gamma_2^m\beta_1 + \beta_2)^{q+1} = \gamma_2^{(q+1)m}\beta_1^{(q+1)} + 2\gamma_2^{qm}\beta_1\beta_2 + \beta_2^{q+1}.$$

Since $p^s - 1 \equiv 0 \mod t/d$ we have $p^s - 1 = kt/d$ for some integer k. So, $(\gamma_2^m)^{p^s-1} = (\gamma_2^m)^{kt/d} = (\gamma_2^t)^{km/d} = 1$ implying $\gamma_2^m \in F_{p^s}$. We also have $\beta \in F_q$. Thus,

$$\frac{(\gamma_2^m\beta_1 + \beta_2)^{q+1}}{2} = \gamma^{q^n+1}\frac{\beta_1^{q+1}}{2} + \gamma_2^m\beta_2^q\beta_1 + \frac{\beta_2^{q+1}}{2}.$$

This completes our proof. □

Now, we construct another type of subgroup of $G(P_\infty)$. For this, we need to prove some lemmas.

Lemma 3.7. *Let $V = \{x \in \mathbb{F}_{q^2} : x^q + x = 0\}$. Then V has a $\mathbb{F}_{p^s}$ subspace of dimension u_2/s.*

Proof. V is a one dimensional $\mathbb{F}_q$ vector space as well as a h/s dimensional $\mathbb{F}_{p^s}$ space. So, it has a subspace of dimension u_2/s. □

Let W_2 be a subspace V given in Lemma 3.7. Then $|W_2| = p^{u_2}$.

Lemma 3.8. *Let J be the set of automorphisms of the following form:*

$$\sigma = \begin{cases} z \to z \\ y \to y \\ x \to x + \alpha, \end{cases}$$

where $\alpha \in W_2$. Then, J is a subgroup of $\mathrm{Aut}_K(\mathcal{C}_n)$.

Proof. It is obvious from Lemma 3.7. □

Lemma 3.9. *$J \rtimes L$ is well defined.*

Proof. i) The intersection of J and L is obviously identity. Let $[\gamma^m, \beta, \frac{\beta^{q+1}}{2}] \in L$ and $[1, 0, \alpha] \in J$. Then we have

$$[\gamma^m, \beta, \frac{\beta^{q+1}}{2}][1, 0, \alpha][\gamma^m, \beta, \frac{\beta^{q+1}}{2}]^{-1} = [1, 0, \frac{\alpha}{\gamma^{q^n+1}}].$$

Since $p^s - 1 \equiv 0 \mod t$ we have $p^s - 1 = kt$ for some integer. So, it turns out that $(\gamma^{q^n+1})^{p^s-1} = (\gamma^{q^n+1})^{k\frac{t}{d}} = (\gamma^t)^{k\frac{q^n+1}{d}} = 1$. So, $[1, 0, \frac{\alpha}{\gamma^{q^n+1}}] \in J$, and this implies L normalizes J. □

Let $U = J \rtimes L$. Then U consists of the automorphisms of the following form:

$$\begin{cases} z \to \gamma z \\ y \to \gamma^m y + \beta \\ x \to \gamma^{q^n+1} x + \gamma^m \beta^q y + \frac{\beta^{q+1}}{2} + \alpha, \end{cases}$$

where $\gamma^t = 1$, $\beta \in W_1$, $\alpha \in W_2$. Hence, $|U| = tp^{u_1}p^{u_2}$. We need to calculate different of the fixed field of U in order to calculate the genus of its fixed field.

Lemma 3.10. *The different exponent of P_∞ in the extension $\mathcal{C}_n/\mathcal{C}_n^U$ is*

$$d(P_\infty) = (m+1)(p^{u_1} - 1)p^{u_2} + (q^n + 2)(p^{u_2} - 1) + (t-1)p^{u_1+u_2}. \tag{18}$$

Proof. By the equations (16) and (17), we have

$$\begin{aligned} d(P_\infty) &= \sum_{1 \neq \sigma \in U} v_{P_\infty}[\sigma(t) - t] \\ &= (m+1)(p^{u_1} - 1)p^{u_2} + (q^n + 2)(p^{u_2} - 1) + 1(tp^{u_1}p^{u_2} - p^{u_1}p^{u_2}). \end{aligned}$$ □

Proposition 3.11. *The degree of $\mathrm{Diff}(\mathcal{C}_n/\mathcal{C}_n^U)$ is*

$$\begin{aligned} \deg \mathrm{Diff}(\mathcal{C}_n/\mathcal{C}_n^U) = {} & (m+1)(p^{u_1} - 1)p^{u_2} + (q^n + 2)(p^{u_2} - 1) + (t-1)p^{u_1+u_2} \\ & + q^3[\gcd(t, m) - 1] + q[\gcd(t, q^n + 1) - \gcd(t, m)]p^{u_1} \\ & + [t - \gcd(t, q^n + 1)]p^{u_1+u_2}. \end{aligned}$$

Proof. From (15), we have $\deg \operatorname{Diff}(\mathcal{C}_n \backslash \mathcal{C}_n^U) = d(P_\infty) + \sum_{\sigma \in U-\{1\}} N(\sigma)$. The proof follows from Lemma 3.3, Lemma 3.10 and the calculation of the cardinalities of the following sets

$$|\{\sigma : \gamma^m = 1, \beta = 0, \alpha = 0\}| = \gcd(t, m),$$
$$|\{\sigma : \gamma^m \neq 1, \gamma^{q^n+1} = 1, \alpha = \frac{\gamma^m \beta^{q+1}}{\gamma^m - 1}\}| = (\gcd(t, q^n+1) - \gcd(t, m))p^{u_1},$$
$$|\{\sigma : \gamma^{q^n+1} \neq 1\}| = tp^{u_1+u_2} - \gcd(t, q^n+1)p^{u_1+u_2}. \qquad \square$$

We now state the main theorem of this section.

Theorem 3.12. *The genus of $\mathcal{C}_n^U$ is given*

$$\begin{aligned} g(\mathcal{C}_n^U) = \frac{1}{2|U|} \big\{ &(q-1)(q^{n+1} + q^n - q^2) - 2 - [(m+1)(p^{u_1} - 1)p^{u_2} \\ &+ (q^n + 2)(p^{u_2} - 1) + (t-1)p^{u_1+u_2} \\ &+ q^3(\gcd(t, m) - 1) + q(\gcd(t, q^n+1) - \gcd(t, m))p^{u_1} \\ &+ (t - \gcd(t, q^n+1))p^{u_1+u_2}] \big\} + 2|U|. \end{aligned}$$

Proof. Follows from (14) and the proposition above. □

3.2. Example 2: A subgroup of G for $n = 3$

In this section, we will extend Theorem 5.4 in [6]. Let γ be a $(q-1)(q^3+1)$-th root of unity. We consider the following automorphisms

$$(19) \qquad \epsilon = \begin{cases} z \to \gamma z \\ y \to \gamma^m y \\ x \to \gamma^{q^3+1} x \end{cases} \quad \text{and} \quad \omega = \begin{cases} z \to z/x \\ y \to y/x \\ x \to 1/x. \end{cases}$$

Let U be the group generated by these automorphisms. Then, we have $|U| = 2(q-1)(q^3+1)$.

Lemma 3.13. $\mathcal{C}_3^U = K(x^{(q-1)} + x^{-(q-1)})$.

Proof. It follows from the fact that $[K(x) : K(x^{(q-1)} + x^{-(q-1)})] = 2(q-1)$. □

Note that all the places in the extension $K(x^{(q-1)}) \backslash K(x^{(q-1)} + x^{-(q-1)})$ are unramified, and the only ramified places in $K(x) \backslash K(x^{(q-1)})$ are $(x = \infty)$ and $(x = 0)$. So, there is no ramified place in the extension $\mathcal{C}_3 \backslash \mathcal{X}_3^U$ apart from the places P_∞ and P_{ab0}.

The automorphisms in U are in the form

$$(20) \qquad \sigma = \begin{cases} z \to \gamma z \\ y \to \gamma^m y \\ x \to \gamma^{q^3+1} x \end{cases} \quad \text{and} \quad \tau = \begin{cases} z \to \gamma z/x \\ y \to \gamma^m y/x \\ x \to \gamma^{q^3+1}/x. \end{cases}$$

We can now state the following lemma.

Lemma 3.14. *Let σ and τ be given as above. Then*

$$N(\sigma) = \begin{cases} q^3+1 & \gamma^m = 1,\ \alpha=\beta=0 \\ q+1 & \gamma^m \neq 1,\ \gamma^{q^n+1} = 1 \\ 2 & \gamma^{q^3+1} \neq 1 \\ 0 & \textit{otherwise}, \end{cases}$$

and

$$N(\tau) = \begin{cases} q+1 & \gamma^m \in F_q \\ 0 & \gamma^m \notin F_q,\ \gamma^{(q^3+1)(q-1)/2} = 1 \\ 2 & \gamma^{(q^3+1)(q-1)/2} = -1. \end{cases}$$

Proof. Calculation of $N(\sigma)$ is the direct result of Lemma 3.3. For the second part, we first note that the places P_∞ and P_{000} do contribute to $N(\tau)$. So, we have to count the pairs $(a,b) \in (F_{q^2})^\times \times F_{q^2}$ such that $P_{ab0} \in N(\tau)$. We have

$$\begin{aligned} \tau(P_{ab0}) = P_{ab0} \quad & \Leftrightarrow \quad \tau(x-a), \tau(y-b), \tau(z) \in P_{ab0} \\ & \Leftrightarrow \quad \gamma^{q^3+1}/x - a, \\ & \qquad \gamma^m y/x - b, \gamma z/x \in P_{ab0} \\ & \Leftrightarrow \quad \gamma^{q^3+1}/x - \gamma^{q^3+1}/a + \gamma^{q^3+1}/a - a, \\ & \qquad \gamma^m y/x - \gamma^m b/a + \gamma^m b/a - b, \gamma z/x \in P_{ab0} \\ & \Leftrightarrow \quad \frac{\gamma^{q^3+1}}{ax}(a-x) - \frac{1}{a}(\gamma^{q^3+1} - a^2), \\ & \qquad \frac{\gamma^m}{ax}(ya - bx) + \frac{b}{a}(\gamma^m - a) \in P_{ab0} \\ & \Leftrightarrow \quad \frac{\gamma^{q^3+1}}{ax}(a-x) - \frac{1}{a}(\gamma^{q^3+1} - a^2), \\ & \qquad \frac{\gamma^m}{ax}[(a(y-b) + b(a-x))] + \frac{b}{a}(\gamma^m - a) \in P_{ab0} \\ & \Leftrightarrow \quad (\gamma^{q^3+1} - a^2), b(\gamma^m - a) \in P_{ab0} \\ & \Leftrightarrow \quad \gamma^{q^3+1} - a^2 = 0 \text{ and } b(\gamma^m - a) = 0. \end{aligned}$$

Hence, we need to count the pairs $(a,b) \in (F_{q^2})^\times \times F_{q^2}$ such that $\gamma^{q^3+1} = a^2$ and $b(\gamma^m - a) = 0$. We do the calculations case by case.

Case 1: $\gamma^m \in F_q$.

If $\gamma^m \in F_q$, then $a^2 = \gamma^{q^3+1} = \gamma^{m(q+1)} = \gamma^{m(q-1)}\gamma^{2m} = \gamma^{2m}$. Hence, we get $a = \pm\gamma^m$. If $a = -\gamma^m \in F_q$, then we have $-2\gamma^m = b^{q+1}$ as $a^q + a = b^{q+1}$. So, for $b \neq 0$ it turns out that $\gamma^m = a$, which is contradiction. Therefore, we have $\gamma^m = a$ $b^{q+1} = 2\gamma^m$.

Case 2: $\gamma^m \notin F_q$ and $\gamma^{m(q^2-1)/2} = 1$.

In this case, we have $a^{q-1} = \gamma^{(q^3+1)(q-1)/2}$=1 and hence $a \in F_q$. This implies $\gamma^m \neq a$ and $b = 0$ and hence $a = 0$. So, we get a contradiction.

Case 3: $\gamma^m \notin F_q$ and $\gamma^{m(q^2-1)/2} = -1$.

In this case, we have $a^{q-1} = -1$ and $a^q = -a$ and hence $b = 0$ and $a = \pm\gamma^{(q^3+1)/2}$. □

Theorem 3.15. *Let t be a divisor of $(q^3+1)(q-1)$ and γ be primitive n-th root of unity. The genus of the subgroup U generated by ϵ and ω defined as in* (19) *is*

$$\begin{aligned} g(\mathcal{C}_n^U) = \big((q^3+1)(q^2-2) - \{(q^3+1)[d_1-1] + (q+1)[d_2-d_1] + 2[t-d_2] \\ + (q+1)d_3 + 2[t-d_4]\} + 4t\big)/4t, \end{aligned}$$

where $d_1 = \gcd(t,m)$, $d_2 = \gcd(t,q^3+1)$, $d_3 = \gcd(m(q-1),t)$ and $d_4 = \gcd(t,(q^3+1)(q-1)/2)$.

Proof. Note that all the places of U are tamely ramified in the extension $\mathcal{C}_n/\mathcal{C}_n^U$ as $|U| = 2t$ and t is a divisor of $(q-1)(q^3+1)$. U consists of elements of the form σ and τ given in (20). By Lemma 3.14, we have

$$\begin{aligned} \sum_{\gamma^t=1,\gamma\neq 1} N(\sigma_\gamma) = (q^3+1)[\gcd(t,m)-1] + (q+1)[\gcd(t,q^3+1) - \gcd(t,m)] \\ + 2[t - \gcd(t,q^3+1)], \end{aligned}$$

and

$$\sum_{\gamma^t=1} N(\tau_\gamma) = (q+1)\gcd(m(q-1),t) + 2[t - \gcd(t,(q^3+1)(q-1)/2)].$$

By Hurwitz-genus formula, we get the desired result. □

3.3. Example 3: A subgroup of G for $n = 3$

We now extend the Example 5.6 in [6]. Let t be a divisor of $(q-1)(q^3+1)$ and $d = \gcd((q-1)(q^3+1),(q^3-1)t)$. Let t_1 be a divisor of d and α_o be an element of order t_1. Let J be the subgroup of G which consists of the elements of the form

$$\sigma_\gamma = \begin{cases} z \to \gamma z \\ y \to \gamma^m y \\ x \to \gamma^{q^3+1} x, \end{cases}$$

where γ is a t'th root of unity. We also define the following automorphism

$$\rho = \begin{cases} z \to \alpha_o z/x \\ y \to \alpha_o^m y/x \\ x \to \alpha_o^{q^3+1} 1/x. \end{cases}$$

Lemma 3.16. *The group $U = J \cup \rho J$ is a subgroup of G for $n = 3$.*

Proof. Since

$$\rho^2 = \begin{cases} z \to \alpha_o^2/\alpha_o^{q^3+1} z \\ y \to (\alpha_o^2/\alpha_o^{q^3+1})^m y \\ x \to (\alpha_o^2/\alpha_o^{q^3+1})^{q^3+1} x \end{cases} \quad \text{and} \quad \sigma_\gamma \circ \rho = \begin{cases} z \to (\gamma\alpha_o/(\gamma\alpha_o)^{q^3+1}) z/x \\ y \to (\gamma\alpha_o/(\gamma\alpha_o)^{q^3+1})^m y/x \\ x \to (\gamma\alpha_o/(\gamma\alpha_o)^{q^3+1})^{q^3+1} 1/x \end{cases}$$

we see that ρ^2 and $\sigma_\gamma \circ \rho$ are in $\mathcal{G}$. □

Theorem 3.17. *Let U be the subgroup constructed in Lemma 3.16. Then, we have*

$$g(\mathcal{X}^U) = \big((q^3+1)(q^2-2) - \{(q^3+1)[d_1-1] + (q+1)[d_2-d_1] + 2[t-d_2] + (q+1)\delta_1 + 2\delta_2\} + 4t\big)/4t,$$

where

$$d_1 = \gcd(t,m),\ d_2 = \gcd(t, q^3+1),\ d_3 = \gcd(m(q-1), t),$$

$$d_4 = \gcd(t, (q^3+1)(q-1)/2),\ \delta_1 = \begin{cases} d_3 & \frac{t_2}{\gcd(t_2, m(q-1))} \mid \frac{t}{d_3} \\ 0 & else \end{cases} \quad \textit{and}$$

$$\delta_2 = \begin{cases} t - d_4 & \frac{t_2}{\gcd(t_2,(q^3+1)(q-1)/2)} \mid \frac{t}{d_4} \\ t & else \end{cases}.$$

Proof. All the places of U in $\mathcal{C}_n/\mathcal{C}_n^U$ are tamely ramified as $|U| = 2t$. U consists of elements of the form

$$\sigma_\gamma = \begin{cases} z \to \gamma z \\ y \to \gamma^m y \\ x \to \gamma^{q^3+1} x \end{cases} \quad \text{and} \quad \tau_\gamma = \begin{cases} z \to (\gamma\alpha_o) z/x \\ y \to (\gamma\alpha_o)^m y/x \\ x \to (\gamma\alpha_o)^{q^3+1} 1/x. \end{cases}$$

By Lemma 3.14, we have

$$\sum_{\gamma^t=1, \gamma\neq 1} N(\sigma_\gamma) = (q^3+1)[\gcd(t,m)-1] + (q+1)[\gcd(t,q^3+1) - \gcd(t,m)] + 2[t - \gcd(t,q^3+1)].$$

For the elements of the second type, we first consider

$$\{\gamma : (\gamma\alpha_o)^{m(q-1)} = 1\} = \{\gamma : \gamma^{m(q-1)} = \alpha_o^{-m(q-1)}\}. \tag{21}$$

The image of the group $\langle \gamma^{m(q-1)} \rangle$ under the homomorphism $\alpha : x \to x^{m(q-1)}$ is the unique subgroup of the group generated by primitive $(q-1)(q^n+1)$-th root of unity, and its order is t/d_3. So, if the order of $(\alpha_o)^{-m(q-1)}$ does not divide t/d_3, then the set in (21) would be empty. The kernel of α consists of the elements of order d_3.

Now we consider the set

$$|\{\gamma : (\gamma\alpha_o)^{(q^3+1)(q-1)/2} = 1\}| = |\{\gamma : (\gamma)^{(q^3+1)(q-1)/2} = (\alpha_o)^{(q^3+1)(q-1)/2}\}. \tag{22}$$

The image of $\langle \gamma^{(q^3+1)(q-1)/2} \rangle$ under the homomorphism $x \to x^{(q^3+1)(q-1)/2}$ is the unique subgroup of order t/d_4 of the group generated by primitive $(q-1)(q^n+1)$'th root of unity. Hence if the order of $(\alpha_o)^{(q^3+1)(q-1)/2}$ does not divide t/d_4, then the set in (22) is empty. The kernel of the map $x \to x^{(q^3+1)(q-1)/2}$ in $\langle \gamma^{m(q-1)} \rangle$ consists of the elements of order d_4. □

Remark 3.18. By Theorem 3.12 and Theorem 3.17, we can construct the maximal function fields over the finite fields of the cardinalities 5^6, 5^{10}, 3^{10} and 3^{18} with the following genera which are new up to [2], [4], [6], [8]:

$\mathbb{F}_{5^6}$	: 146	Theorem 3.12
$\mathbb{F}_{5^{10}}$	: $1820, 2080, 3120, 3640, 4681, 7282, 9362, 12482, 18724$	Theorem 3.12
$\mathbb{F}_{3^{10}}$	: 481	Theorem 3.12
$\mathbb{F}_{3^{18}}$	: $45, 91, 145, 289, 579, 645, 1057, 1755, 2547, 3511, 5617, 6552, 12300, 39361$	Theorem 3.12
$\mathbb{F}_{3^{18}}$	: $505, 1311, 255535$	Theorem 3.17

Remark 3.19. One can use Theorem 3.12, Theorem 3.15 and Theorem 3.17 to construct maximal function fields over the finite field with the cardinality 5^6 with the genera that were obtained in [4]:

$9, 14, 21, 38, 70, 76, 86, 140, 220, 282, 362, 442, 724$	Theorem 3.12
$9, 27, 37, 73, 76, 109, 180, 220, 361, 724$	Theorem 3.15
$9, 27, 37, 38, 73, 76, 109, 180, 220, 361, 362, 724$	Theorem 3.17

References

[1] M. Abdon, J. Bezerra, and L. Quoos, *Further examples of maximal curves*, J. Pure Appl. Algebra **213** (2009), no. 6, 1192–1196.

[2] M. Abdon and L. Quoos, *On the genera of subfields of the Hermitian function field*, Finite Fields Appl. **10** (2004), no. 3, 271–284.

[3] I. Duursma and K.-H. Mak, *On maximal curves which are not Galois subcovers of the Hermitian curve*, Bull. Braz. Math. Soc. (N.S.) **43** (2012), no. 3, 453–465.

[4] S. Fanali and M. Giulietti, *Quotient curves of the GK curve*, Adv. Geom. **12** (2012), no. 2, 239–268.

[5] A. Garcia, C. Güneri, and H. Stichtenoth, *A generalization of the Giulietti-Korchmáros maximal curve*, Adv. Geom. **10** (2010), no. 3, 427–434.

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

[7] M. Giulietti and G. Korchmáros, *A new family of maximal curves over a finite field*, Math. Ann. **343** (2009), no. 1, 229–245.

[8] C. Güneri, M. Özdemir, and H. Stichtenoth, *The automorphism group of the generalized Giulietti-Korchmáros function field*, Adv. Geom. **13** (2013), no. 2, 369–380.

[9] G. Lachaud, *Sommes d'Eisenstein et nombre de points de certaines courbes algébriques sur les corps finis*, C. R. Acad. Sci. Paris Sér. I Math. **305** (1987), no. 16, 729–732.

[10] H. G. Ruck and H. Stichtenoth, *Characterization of Hermitian function fields over finite fields*, J. Reine Angew. Math. **457** (1994), 185–188.

[11] H. Stichtenoth, *Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. I*, Arch. Math. **24** (1973), 527–544.

[12] ———, *Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. II*, Arch. Math. **24** (1973), 615–631.

[13] ———, *Algebraic Function Fields and Codes*, Springer-Verlag, Berlin, 2009.

Yusuf Danisman
Elementary Mathematics Education
Mevlana University
Konya, Turkey
E-mail address: ydanisman@mevlana.edu.tr

Mehmet Ozdemir
Elementary Mathematics Education
Mevlana University
Konya, Turkey
E-mail address: mozdemir@mevlana.edu.tr