DTU Library

A complete characterization of Galois subfields of the generalized Giulietti–Korchmáros function field

Anbar, Nurdagül; Bassa, Alp; Beelen, Peter

Link back to DTU Orbit

A complete characterization of Galois subfields of the generalized Giulietti–Korchmáros function field

Nurdagül Anbar [a], Alp Bassa [b], Peter Beelen [a,*]

[a] *Technical University of Denmark, Department of Applied Mathematics and Computer Science, Matematiktorvet 303B, 2800 Kgs. Lyngby, Denmark*
[b] *Boğaziçi University, Faculty of Arts and Sciences, Department of Mathematics, 34342 Bebek, İstanbul, Turkey*

A R T I C L E   I N F O

A B S T R A C T

We give a complete characterization of all Galois subfields of the generalized Giulietti–Korchmáros function fields $\mathcal{C}_n/\mathbb{F}_{q^{2n}}$ for $n \geq 5$. Calculating the genera of the corresponding fixed fields, we find new additions to the list of known genera of maximal function fields.

© 2017 Elsevier Inc. All rights reserved.

---

* Corresponding author.
E-mail addresses: nurdagulanbar2@gmail.com (N. Anbar), alp.bassa@boun.edu.tr (A. Bassa), pabe@dtu.dk (P. Beelen).

1. Introduction

Let F be a function field of genus $g(F)$ over the finite field $\mathbb{F}_\ell$ with ℓ elements. The Hasse–Weil theorem gives the following upper bound for the number of rational places $N(F)$ of F:

$$N(F) \le \ell + 1 + 2g(F)\sqrt{\ell} \ .$$

Function fields attaining this bound are called maximal, and have played a central role in the theory of function fields over finite fields (or equivalently curves over finite fields).

An important example of maximal function fields is the Hermitian function field $\mathcal{H}$ over the finite field $\mathbb{F}_{q^2}$, where q is a power of a prime p. It is given by $\mathcal{H} = \mathbb{F}_{q^2}(x, y)$ with

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

It has genus $q(q-1)/2$ (in fact the largest possible genus for a maximal function field over $\mathbb{F}_{q^2}$) and a large automorphism group $A \cong \mathrm{P}GU(3, q)$. By a theorem of Serre (see [14]) a subfield of a maximal function field is itself also maximal, provided it is a function field over the same field of constants. Studying such subfields of the Hermitian function field leads to many new examples of maximal function fields. One way to construct such subfields is by taking fixed fields of subgroups of A (see among others [1,2,8] and the references in [7]). Since all maximal subgroups of A are known, interest has been diverted into studying subgroups of the various maximal subgroups. The maximal subgroup $A(P_\infty)$ fixing the unique pole P_∞ of x, together with an involution generates the whole automorphism group A. A complete characterization of all subgroups of $A(P_\infty)$ and the genera of the corresponding fixed fields has been given in [2].

For a long time, all known maximal function fields were subfields of the Hermitian function field. This led to the question whether any maximal function fields could be embedded as subfields in the Hermitian function field. Giulietti and Korchmáros [10] introduced a new family of maximal function fields (GK function fields) over finite fields $\mathbb{F}_{q^6}$, which are not subfields of the Hermitian function field over the corresponding field for $q > 2$. The GK function field is given by $\mathcal{C} = \mathbb{F}_{q^6}(x, y, z)$ with

$$x^q + x = y^{q+1} \quad \text{and} \quad z^{(q^3+1)/(q+1)} = y \sum_{i=0}^{q}(-1)^{i+1}x^{i(q-1)} \ .$$

The GK function field was generalized in [9] to a family of maximal function fields over finite fields $\mathbb{F}_{q^{2n}}$ with n odd. The generalized GK (GGK) function field, also known as the Garcia–Güneri–Stichtenoth function field, is given by $\mathcal{C}_n = \mathbb{F}_{q^{2n}}(x, y, z)$ with

$$x^q + x = y^{q+1} \quad \text{and} \quad z^{(q^n+1)/(q+1)} = y^{q^2} - y \ .$$

For convenience we will in the remainder of this article write $m = (q^n + 1)/(q + 1)$. One recovers the Hermitian function field $\mathcal{H}$ for $n = 1$, and the GK function field $\mathcal{C}$ for $n = 3$, since

$$\sum_{i=0}^{q}(-1)^{i+1}x^{i(q-1)} = -1 + x^{q-1}\sum_{j=0}^{q-1}(-1)^j x^{j(q-1)} = -1 + x^{q-1}(x^{q-1} + 1)^{q-1}$$

$$= -1 + \left(y^{q+1}\right)^{q-1}.$$

Note that the GGK function field contains a constant field extension of the Hermitian function field $\mathcal{H}$ over $\mathbb{F}_{q^2}$ as a subfield. The GGK function fields are not Galois subfields of the Hermitian function fields ([5,11]).

The automorphism groups of the GGK function fields were determined in [12,13]. In particular, it was shown that for $n > 3$ any automorphism of $\mathcal{C}_n$ restricts to an automorphism of $\mathcal{H}$ fixing P_∞. We use this together with the characterization in [2] to characterize all subgroups of the automorphism group of $\mathcal{C}_n$ for $n > 3$. For $n = 3$ the automorphisms of $\mathcal{C}_n$ do not restrict necessarily to an automorphism of $\mathcal{H}$ fixing P_∞, but we obtain a characterization of a large class of subgroups. Adapting an approach from [8] in a similar way as in [3], we obtain an explicit expression for the genus of the fixed field of these characterized subgroups. This leads to new additions to the list of known genera of maximal function fields.

2. Results about the Hermitian function field

We denote by $\mathcal{H}$ the Hermitian function field over $\mathbb{F}_{q^2}$. It can be given as $\mathcal{H} = \mathbb{F}_{q^2}(x, y)$ with $x^q + x = y^{q+1}$. The functions x and y have exactly one pole at a place, which we denote by P_∞. As is well known $\mathcal{H}$ has a large automorphism group A isomorphic to $\mathrm{PGU}(3, q)$. We denote by $A(P_\infty)$ the stabilizer of P_∞. For $a \in \mathbb{F}_{q^2}^*$, $b \in \mathbb{F}_{q^2}$ and any $c \in \mathbb{F}_{q^2}$ satisfying $c^q + c = b^{q+1}$, an automorphism $\sigma \in A(P_\infty)$ can be described by the equations

$$\sigma(x) = a^{q+1}x + ab^q y + c \quad \text{and} \quad \sigma(y) = ay + b .$$

Instead of σ, we write $[a, b, c]$ for this automorphism. Then $A(P_\infty)$ is given by

$$A(P_\infty) = \{[a, b, c] \mid a \in \mathbb{F}_{q^2}^*, b, c \in \mathbb{F}_{q^2} \text{ where } c^q + c = b^{q+1}\} . \tag{1}$$

The group law is given by

$$[a', b', c'] \circ [a, b, c] = [a'a, ab' + b, a^{q+1}c' + ab^q b' + c].$$

Following [2], for a given subgroup $H \leq A(P_\infty)$, we define the map $\phi : H \to \mathbb{F}_{q^2}^*$ such that $[a, b, c] \mapsto a$. We denote by U_H the kernel $\ker \phi$ and by H_1 the image $\mathrm{im}\phi$ of ϕ. Then

$U_H = \{[1, b, c] \in H\}$ is the unique p-Sylow subgroup of H, where p is the characteristic of $\mathbb{F}_{q^2}$. Further, define $\psi : U_H \to \mathbb{F}_{q^2}$ such that $[1, b, c] \mapsto b$. Let $H_2 = \operatorname{im}\psi$ and $H_3 = \ker \psi$. For convenience, we write $h_1 := \#H_1$ and $h_w := \#U_H$. Note that we have $\#H = h_1 h_w$, and $h_w = \#H_2\#H_3$.

In [2] it was described precisely which triples (H_1, H_2, H_3) up to conjugation can arise as H varies over all subgroups of $A(P_\infty)$. It will be convenient for a subset $S \subset \mathbb{F}_{q^2}$ and integer $i \geq 0$ to denote by $\mathbb{F}_p(S^i)$ the field obtained from $\mathbb{F}_p$ by adjoining all ith powers of elements from S. Then, we have the following theorem.

Theorem 2.1 *(Theorem 3.6 [2]). For each subgroup $H \leq A(P_\infty)$ up to conjugation we have the following:*

(i) H_1 *is a cyclic subgroup of $\mathbb{F}_{q^2}^*$.*
(ii) $H_2 \subset \mathbb{F}_{q^2}$ *is a vector space over $\mathbb{F}_p(H_1)$.*
(iii) $H_3 \subset \{c \in \mathbb{F}_{q^2} \mid c^q + c = 0\}$ *is a vector space over $\mathbb{F}_p(H_1^{q+1})$ containing W, where*
$W = \{b_1 b_2^q - b_2 b_1^q \mid b_1, b_2 \in H_2\}$ *if p is odd and $W = \{b^{q+1} \mid b \in H_2\}$ if $p = 2$.*

Conversely, for any H_1, H_2, H_3 satisfying (i), (ii) and (iii) there exists a subgroup $H \leq A(P_\infty)$ giving rise to this triple.

Given the triple (H_1, H_2, H_3) the genus of the fixed field of H can be determined in terms of $h_1, \#H_2$ and $\#H_3$, see [8]. Theorem 2.1 characterizes all possible subgroups $H \leq A(P_\infty)$ up to conjugation, but to make this result algorithmic one needs to be able to compute all possibilities for $(h_1, \#H_2, \#H_3)$ in a fast way. In [2] for a given odd q all possible values of $h_1, \#H_2$ and $\#H_3$ have been determined explicitly, while for even q many (but possibly not all) possibilities were listed. In this algorithmic sense, the case $q = 2$ is not completely settled.

3. Subgroups of the automorphism group of the GGK function field

The GKK function field $\mathcal{C}_n$ introduced in [9] is maximal over $\mathbb{F}_{q^{2n}}$ and has genus $g(\mathcal{C}_n) = (q - 1)(q^{n+1} + q^n - q^2)/2$. The function z has a unique pole in $\mathcal{C}_n$, which we denote by Q_∞. As mentioned previously $\mathcal{C}_1 = \mathcal{H}$, the Hermitian function field, and $\mathcal{C}_3 = \mathcal{C}$, the GK function field.

The automorphism group $B := \operatorname{Aut}(\mathcal{C}_n)$ of $\mathcal{C}_n$ has been determined in [12,13]. The stabilizer of Q_∞, which we will denote by $B(Q_\infty)$, is in most cases equal to the entire automorphism group. More precisely, we have

$$[B : B(Q_\infty)] = \begin{cases} q^3 + 1 & \text{if } n \leq 3 \\ 1 & \text{if } n \geq 5 \end{cases} \tag{2}$$

Note that for $n = 1$, we simply have $Q_\infty = P_\infty$ and $B(Q_\infty) = A(P_\infty)$. For general odd n, the group $B(Q_\infty)$ can be described explicitly. All automorphisms $\sigma \in B(Q_\infty)$ can be

obtained in the following way: for $a \in \mathbb{F}_{q^2}^*$, $b, c \in \mathbb{F}_{q^2}$ and $d \in \mathbb{F}_{q^{2n}}$, such that $c^q + c = b^{q+1}$ and $d^m = a$, define

$$\sigma(x) = a^{q+1}x + ab^qy + c, \quad \sigma(y) = ay + b \quad \text{and} \quad \sigma(z) = dz \ .$$

It will be convenient to write $[a, b, c, d]$ for σ. Then we have

$$B(Q_\infty) = \{[a, b, c, d] \mid a \in \mathbb{F}_{q^2}^*, b, c \in \mathbb{F}_{q^2}, d \in \mathbb{F}_{q^{2n}} \ \text{ where } \ c^q + c = b^{q+1} \ \text{ and } \ d^m = a\} \ . \tag{3}$$

Note that for any $a \in \mathbb{F}_{q^2}^*$, the equation $d^m = a$ has m distinct solutions in $\mathbb{F}_{q^{2n}}$. We obtain that $\#B(Q_\infty) = mq^3(q^2 - 1)$. The group law is easily seen to be

$$[a', b', c', d'] \circ [a, b, c, d] = [a'a, ab' + b, a^{q+1}c' + ab^q b' + c, d'd] \tag{4}$$

It is clear from Equations (1) and (3) that the map

$$\pi : B(Q_\infty) \to A(P_\infty) \ \text{ defined by } \ \pi([a, b, c, d]) = [a, b, c]$$

is a surjective group homomorphism. Note that the GGK function field over $\mathbb{F}_{q^{2n}}$ contains the Hermitian function field over $\mathbb{F}_{q^2}$ as a subfield. Then the map π corresponds to restricting automorphisms of the GGK function field to this subfield.

For any $[a, b, c, d] \in B(Q_\infty)$, we have

$$d^{(q^n+1)(q-1)} = d^{m(q^2-1)} = a^{q^2-1} = 1 \ .$$

Hence $d \in \mu$, where $\mu \leq \mathbb{F}_{q^{2n}}^*$ is the multiplicative group of $(q^n + 1)(q - 1)$th roots of unity.
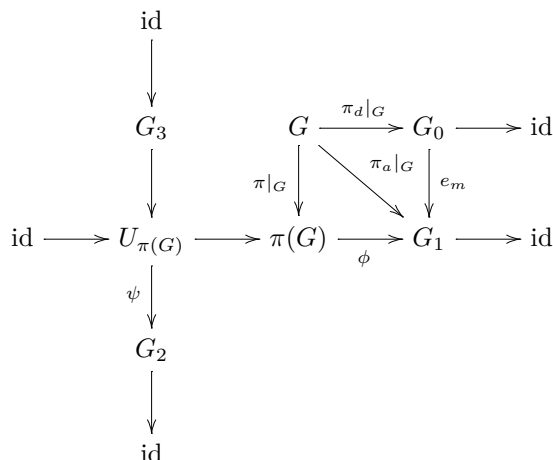
Definition 3.1. Write $\pi_d : B(Q_\infty) \to \mu$ for the map given by $\pi_d([a, b, c, d]) := d$. Then for any $G \subset B(Q_\infty)$, we define $G_0 := \pi_d(G) \subset \mu$ and $g_0 := \#G_0$. Similarly, write $\pi_a : B(Q_\infty) \to \mathbb{F}_{q^2}^*$ for the map given by $\pi_a([a, b, c, d]) := a$. Then we define $G_1 := \pi_a(G)$ and $g_1 := \#G_1$.

Note that π_d and π_a are group homomorphisms, and that $\pi_a = e_m \circ \pi_d$, where e_m is the mth power map. We denote by $\pi|_G$, $\pi_a|_G$ and $\pi_d|_G$ the restriction to G of the maps π, π_a and π_d respectively. The map π can be used to associate objects to a subgroup $G \leq B(Q_\infty)$. Indeed, writing $H = \pi(G) \leq A(P_\infty)$, we can construct the triple (H_1, H_2, H_3) from the previous section. To stress the dependency on G, we will write (G_1, G_2, G_3) instead. At first sight this gives a problem, since the notation G_1 was already used in Definition 3.1. However, a direct computation shows that

$$e_m \circ \pi_d|_G = \pi_a|_G = \phi \circ \pi|_G,$$

with $\phi : \pi(G) \to \mathbb{F}_{q^2}^*$ given by $\phi([a, b, c]) = a$, just as in the previous section. Therefore the two definitions for G_1 actually give rise to the same group. Analogously to the Hermitian function field case, we also define $g_w := \# \ker(\pi_d|_G)$.

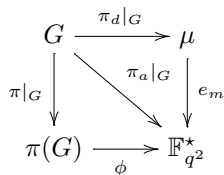The situation is as depicted in the following picture.

$$
\begin{array}{ccccccc}
 & \text{id} & & & & & \\
 & \downarrow & & & & & \\
 & G_3 & & G & \xrightarrow{\pi_d|_G} & G_0 \longrightarrow \text{id} \\
 & \downarrow & & \pi|_G \downarrow & \pi_a|_G \searrow & \downarrow e_m & \\
\text{id} \longrightarrow & U_{\pi(G)} & \longrightarrow & \pi(G) & \xrightarrow{\phi} & G_1 \longrightarrow \text{id} \\
 & \psi \downarrow & & & & & \\
 & G_2 & & & & & \\
 & \downarrow & & & & & \\
 & \text{id} & & & & &
\end{array}
$$

With this notation, we obtain the following lemma.

Lemma 3.2. *Let $G \leq B(Q_\infty)$ be a subgroup. Then we have*

(i) $\#G = g_0 g_w$,
(ii) $\#\pi(G) = g_1 g_w$.

Proof. The different maps and groups are depicted in the following commutative diagram.

$$
\begin{array}{ccc}
G & \xrightarrow{\pi_d|_G} & \mu \\
\pi|_G \downarrow & \pi_a|_G \searrow & \downarrow e_m \\
\pi(G) & \xrightarrow{\phi} & \mathbb{F}_{q^2}^\star
\end{array}
$$

Considering the map $\pi_d|_G$, we deduce

$$\#G = (\#\mathrm{im}\pi_d|_G) \cdot (\# \ker \pi_d|_G) = \#G_0 \cdot g_w = g_0 g_w \ .$$

Note that $\ker \pi_d|_G = \{[1, b, c, 1] \in G\}$ and $\ker \phi = \{[1, b, c] \in \pi(G)\}$. Hence $\# \ker \phi = \# \ker \pi_d|_G = g_w$. Therefore

$$\#\pi(G) = (\#\phi(\pi(G))) \cdot (\# \ker \phi) = \#\pi_a(G) \cdot g_w = g_1 g_w \ . \qquad \square$$

Also we can deduce the following relation between g_0 and g_1.

Lemma 3.3. *Let $G \leq B(Q_\infty)$ be given. Then*

$$G_1 = G_0^m \quad and \quad g_1 = \frac{g_0}{\gcd(g_0, m)} \ .$$

Proof. The identity $e_m \circ \pi_d|_G = \pi_a|_G$, together with the fact that $d^m = a$, implies that $G_1 = \pi_a(G) = (e_m \circ \pi_d)(G) = G_0^m$. Since G_0 is a subgroup of the cyclic group μ, it is itself cyclic of order g_0. Therefore the kernel of the mth power map from G_0 to G_0^m has cardinality $\gcd(g_0, m)$. This implies $\#G_0^m = \#G_0 / \gcd(g_0, m)$, which proves the claim. $\quad \square$

Remark 3.4. Using the previous two lemmas we see that $\# \ker \pi|_G = \#G/\#\pi(G) = \gcd(g_0, m)$.

We now describe the subgroups of $B(Q_\infty)$ in terms of subgroups of $A(P_\infty)$ and of μ. Recall that μ is the subgroup of $\mathbb{F}_{q^{2n}}^*$ consisting of the $m(q^2 - 1)$th roots of unity.

Theorem 3.5. *Let Σ be the set of pairs (H, M) such that $H \leq A(P_\infty)$, $M \leq \mu$ and $M^m = \phi(H)$ and let Ξ for any $G \leq B(Q_\infty)$ be defined as $\Xi(G) = (\pi(G), \pi_d(G))$. Then the map Ξ gives a bijection between the set of subgroups of $B(Q_\infty)$ and Σ.*

Proof. Note that Lemma 3.3 implies that $\Xi(G) \in \Sigma$. First we show surjectivity of Ξ. Let $H \leq A(P_\infty)$ and $M \leq \mu$ be subgroups with $M^m = \phi(H)$. Then we claim that $G := \pi^{-1}(H) \cap \pi_d^{-1}(M)$ has the property that $\Xi(G) = (H, M)$. In other words, we need to show that

$$\pi(\pi^{-1}(H) \cap \pi_d^{-1}(M)) = H \text{ and } \pi_d(\pi^{-1}(H) \cap \pi_d^{-1}(M)) = M.$$

It is clear that $\pi(\pi^{-1}(H) \cap \pi_d^{-1}(M)) \subset \pi(\pi^{-1}(H)) = H$ and $\pi_d(\pi^{-1}(H) \cap \pi_d^{-1}(M)) \subset \pi_d(\pi_d^{-1}(M)) = M$. On the other hand, using that $M^m = \phi(H)$, we see that for any $[a, b, c] \in H$ there exists $d \in M$ such that $d^m = a$. This implies $[a, b, c, d] \in \pi^{-1}(H) \cap \pi_d^{-1}(M)$, whence $[a, b, c] \in \pi(\pi^{-1}(H) \cap \pi_d^{-1}(M))$. Similarly for any $d \in M$ there exists $[a, b, c] \in H$ such that $a = d^m$. Then $[d^m, b, c, d] \in \pi^{-1}(H) \cap \pi_d^{-1}(M)$ and hence $d \in \pi_d(\pi^{-1}(H) \cap \pi_d^{-1}(M))$. This shows that Ξ is surjective.

Now we show that Ξ is injective. Let $G \leq B(Q_\infty)$ be chosen arbitrarily. By definition we have $\Xi(G) = (\pi(G), \pi_d(G))$. The proof of the surjectivity of Ξ implies that the subgroup $\pi^{-1}(\pi(G)) \cap \pi_d^{-1}(\pi_d(G))$ has the same image as G under Ξ. To show injectivity, it is enough to show that

$$G = \pi^{-1}(\pi(G)) \cap \pi_d^{-1}(\pi_d(G)). \tag{5}$$

Indeed, if $\Xi(G) = \Xi(\tilde{G})$, then Equation (5) would imply that

$$G = \pi^{-1}(\pi(G)) \cap \pi_d^{-1}(\pi_d(G)) = \pi^{-1}(\pi(\tilde{G})) \cap \pi_d^{-1}(\pi_d(\tilde{G})) = \tilde{G},$$

where the middle equality uses $\Xi(G) = \Xi(\tilde{G})$ and the first (resp. last) equality uses Equation (5) for the subgroup G (resp. $\tilde{G}$). Now we prove Equation (5) itself.

It is easy to see that $G \subset \pi^{-1}(\pi(G))$ and $G \subset \pi_d^{-1}(\pi_d(G))$, implying that $G \subset \pi^{-1}(\pi(G)) \cap \pi_d^{-1}(\pi_d(G))$. What is left is to show the reverse inclusion. Let $g \in \pi^{-1}(\pi(G)) \cap \pi_d^{-1}(\pi_d(G))$ and write $g = [a, b, c, d]$. Since in particular $g \in \pi^{-1}(\pi(G))$, there exists $\tilde{d}$ such that $[a, b, c, \tilde{d}] \in G$. Since $G \subset \pi^{-1}(\pi(G)) \cap \pi_d^{-1}(\pi_d(G))$, we see that

$$[a, b, c, d] \circ [a, b, c, \tilde{d}]^{-1} = [1, 0, 0, d\tilde{d}^{-1}] \in \pi^{-1}(\pi(G)) \cap \pi_d^{-1}(\pi_d(G)). \tag{6}$$

Then Equation (6) implies that

$$g \in G \quad \text{if and only if} \quad [1, 0, 0, d\tilde{d}^{-1}] \in G. \tag{7}$$

Since $[1, 0, 0, d\tilde{d}^{-1}] \in \pi^{-1}(\pi(G)) \cap \pi_d^{-1}(\pi_d(G))$, in particular $[1, 0, 0, d\tilde{d}^{-1}] \in \pi_d^{-1}(\pi_d(G))$, implying that there exist $\tilde{b}$ and $\tilde{c}$ such that $[1, \tilde{b}, \tilde{c}, d\tilde{d}^{-1}] \in G$.

Now note that by Equation (4)

$$[1, \tilde{b}, \tilde{c}, d\tilde{d}^{-1}]^p = [1, 0, c', (d\tilde{d}^{-1})^p]$$

for a certain c' and hence

$$[1, \tilde{b}, \tilde{c}, d\tilde{d}^{-1}]^{p^2} = [1, 0, 0, (d\tilde{d}^{-1})^{p^2}].$$

Since $d\tilde{d}^{-1} \in \mathbb{F}_{q^{2n}}$, this implies that $[1, 0, 0, d\tilde{d}^{-1}] = [1, 0, 0, (d\tilde{d}^{-1})^{q^{2n}}] = [1, \tilde{b}, \tilde{c}, d\tilde{d}^{-1}]^{q^{2n}} \in G$. By Equation (7), we conclude that $g \in G$ as desired. This shows that Equation (5) holds, and thus completes the proof of the theorem. $\quad\square$

Combining Theorems 2.1 and 3.5, we deduce the following characterization of all subgroups $G \leq B(Q_\infty)$.

Theorem 3.6. *For a subgroup $G \leq B(Q_\infty)$, let G_0, G_2 and G_3 be as above. Then up to conjugation we have the following:*

(i) *G_0 is a cyclic subgroup of μ, the group of $m(q^2 - 1)$th roots of unity in $\mathbb{F}_{q^{2n}}^*$.*
(ii) *$G_2 \subset \mathbb{F}_{q^2}$ is a vector space over $\mathbb{F}_p(G_0^m)$.*
(iii) *$G_3 \subset \{c \in \mathbb{F}_{q^2} \mid c^q + c = 0\}$ is a vector space over $\mathbb{F}_p(G_0^{q^n+1})$ containing W, where $W = \{b_1 b_2^q - b_2 b_1^q \mid b_1, b_2 \in G_2\}$ if p is odd and $W = G_2^{q+1} = \{b^{q+1} \mid b \in G_2\}$ if $p = 2$.*

Conversely, for any G_0, G_2, G_3 satisfying (i), (ii) and (iii) there exists a subgroup $G \leq B(Q_\infty)$ giving rise to this triple.

Remark 3.7. For $n \geq 5$ every automorphism of $\mathcal{C}_n$ fixes Q_∞, so we have $B = B(Q_\infty)$ (see Equation (2)). Hence in this case Theorem 3.6 characterizes all subgroups of the automorphism group of the GGK function field.

4. Genus computation

Let $G \leq B(Q_\infty)$ be a subgroup. We denote the fixed field of G by $\mathcal{C}_n^G$. The aim of this section is to compute the genus of $\mathcal{C}_n^G$. As above, we let $G_0 = \pi_d(G)$, $G_1 = \pi_a(G)$, $U_{\pi(G)} = \ker \phi$, $G_2 = \psi(U_{\pi(G)})$ and $G_3 = \ker \psi$. Moreover, $g_0 = \#G_0$, $g_1 = \#G_1$, $g_w = \#U_{\pi(G)} = \#G_2\#G_3$ and $\#G = g_0 g_w$.

We will adapt the approach in [8] to calculate genera of Galois subfields of the GGK function field. A similar approach has been used in [3]. However since the genus formulas have not been worked out in full generality (it is assumed that the characteristic is odd in [3]), we do so below.

The fixed field of $B(Q_\infty)$ is $\mathbb{F}_{q^{2n}}(t)$, where $t = z^{(q-1)(q^n+1)}$. Let us recall some details about the extension $\mathcal{C}_n/\mathbb{F}_{q^{2n}}(t)$ and its ramification structure:

- $(t = 0)$ and $(t = \infty)$ are the only places ramified in the extension $\mathcal{C}_n/\mathbb{F}_{q^{2n}}(t)$
- $(t = \infty)$ is totally ramified in the extension $\mathcal{C}_n/\mathbb{F}_{q^{2n}}(t)$. The unique place of $\mathcal{C}_n$ lying over $(t = \infty)$ was denoted by Q_∞, and its restriction to $\mathbb{F}_{q^{2n}}(x, y)$ by P_∞. Note that this is a slight abuse of notation, since P_∞ previously denoted the restriction of Q_∞ to $\mathbb{F}_{q^2}(x, y)$. However, in both cases the place denotes the unique common pole of x and y. A uniformizing element at Q_∞ is given by $\tau = \frac{z^{q^n-3}}{x}$.
- $(t = 0)$ is tamely ramified in $\mathbb{F}_{q^{2n}}(x, y)/\mathbb{F}_{q^{2n}}(t)$ with ramification index $q^2 - 1$. The q^3 places of $\mathbb{F}_{q^{2n}}(x, y)$ lying above $(t = 0)$ are uniquely characterized by the value of x and y at those places, and hence will be denoted as

$$\{ P_{\alpha\beta} \mid \alpha, \beta \in \mathbb{F}_{q^2}, \alpha^q + \alpha = \beta^{q+1} \} .$$

Each place $P_{\alpha\beta}$ is totally ramified in the extension $\mathcal{C}_n/\mathbb{F}_{q^{2n}}(x, y)$, and we denote the unique place of $\mathcal{C}_n$ lying over it by $Q_{\alpha\beta}$.

As shown in [3] for odd characteristic, the degree of the different divisor of the extension $\mathcal{C}_n/\mathcal{C}_n^G$ is given by

$$\deg \text{Diff}(\mathcal{C}_n/\mathcal{C}_n^G) = \sum_{\text{id} \neq g \in G} v_{Q_\infty}(g(\tau) - \tau) + \sum_{\text{id} \neq g \in G} N(g) , \tag{8}$$

where v_{Q_∞} is the valuation corresponding to the place Q_∞, $\tau = z^{q^n-3}/x$ a uniformizing element at Q_∞, and

$$N(g) := \#\{Q_{\alpha\beta} \mid g(Q_{\alpha\beta}) = Q_{\alpha\beta}\} \ .$$

However, the proof given in [3] for Equation (8) carries over directly to the even characteristic. Since $Q_{\alpha\beta}|P_{\alpha\beta}$ is totally ramified in $\mathcal{C}_n/\mathbb{F}_{q^{2n}}(x,y)$, we have the following conclusion.

Lemma 4.1.

$$N(g) = \#\{P_{\alpha\beta} \mid \pi(g)(P_{\alpha\beta}) = P_{\alpha\beta}\} \ .$$

As a consequence of Lemma 4.1 and [8, Lemma 4.2] we obtain the following description of $N(g)$ in terms of the order $\mathrm{ord}(\pi(g))$ of $\pi(g)$ in $A(P_\infty)$.

Theorem 4.2. *Let $g \in B(Q_\infty)$. We have*

$$N(g) = \begin{cases} 0 & \text{if } p \mid \mathrm{ord}(\pi(g)), \\ q^3 & \text{if } \pi(g) = \mathrm{id}, \\ q & \text{if } \mathrm{ord}(\pi(g)) \mid (q+1), \\ 1 & \text{otherwise.} \end{cases}$$

In [8, Lemma 4.3] the number of elements in a subgroup H of $A(P_\infty)$ of various orders coprime to p have been calculated. Since $\pi|_G : G \to A(P_\infty)$ is a group homomorphism with kernel of size $\gcd(g_0, m)$ (see Remark 3.4), we obtain the following:

Lemma 4.3. *Let G be a subgroup of $B(Q_\infty)$, and $a \in G_1$ an element of order of order $s > 1$. The number of elements $g \in G$ of the form $[a, \star, \star, \star]$ such that $\pi(g)$ has order s if given by*

- $\gcd(g_0, m)g_w$ *if $s \nmid (q+1)$,*
- $\gcd(g_0, m)\#G_2$ *if $s \mid (q+1)$.*

Now we can calculate the expressions appearing in Equation (8) for the degree of the different in the extension $\mathcal{C}_n/\mathcal{C}_n^G$.

Proposition 4.4. *Let $\delta_1 = \gcd(g_0, m)$, $\delta_2 = \gcd(g_0, q^n + 1)$ and $\tau = z^{q^n - 3}/x$. Then we have the following equalities.*

1. $\displaystyle\sum_{\mathrm{id} \neq g \in G} v_{Q_\infty}(g(\tau) - \tau) = (m + g_0)g_w + (q^n + 1 - m)\#G_3 - (q^n + 2);$

2. $\displaystyle\sum_{\mathrm{id} \neq g \in G} N(g) = q(\delta_2 - \delta_1)\#G_2 + (g_0 - \delta_2)g_w + q^3(\delta_1 - 1).$

Proof.

1. As was shown in [5], for an element $g = [a, b, c, d]$, which is different from id, we have

$$v_{Q_\infty}(g(\tau) - \tau) = \begin{cases} m + 1 & \text{if } d = 1, b \neq 0, \\ q^n + 2 & \text{if } d = 1, b = 0, \\ 1 & \text{otherwise.} \end{cases}$$

   The number of elements in $G\backslash\{\text{id}\}$ with $d = 1$ and $b \neq 0$ (respectively $b = 0$) is given by $g_w - \#G_3$ (respectively $\#G_3 - 1$). This leaves $\#G - g_w = g_0 g_w - g_w$ elements for the third case.

2. Since G_1 is a cyclic group of order g_1, there are exactly $\gcd(g_1, q + 1) - 1$ elements in $G_1\backslash\{1\}$ of order dividing $q + 1$. The remaining $(g_1 - \gcd(g_1, q + 1))$ elements in $G_1\backslash\{1\}$ have order not dividing $q + 1$. The number of elements g in $G\backslash\{\text{id}\}$ such that $\pi(g) = [1, 0, 0]$ equals $\# \ker \pi|_G - 1 = \delta_1 - 1$. Then by using the facts that $g_1 = g_0/\delta_1$ and $\gcd(g_1, q+1) = \delta_2/\delta_1$, we obtain the desired result from Theorem 4.2 and Lemma 4.3. $\square$

Using the Riemann–Hurwitz genus formula for the extension $\mathcal{C}_n/\mathcal{C}_n^G$, we obtain the following expression for the genus of $\mathcal{C}_n^G$.

Theorem 4.5. *For $G \leq B(Q_\infty)$, let $\delta_1 = \gcd(g_0, m)$ and $\delta_2 = \gcd(g_0, q^n + 1)$. Then we have*

$$g(\mathcal{C}_n^G) = \frac{q^2(q^n + 1) - q^3 \delta_1 - q(\delta_2 - \delta_1)\#G_2 + (\delta_2 - m)g_w - (q^n + 1 - m)\#G_3}{2\#G}.$$

Remark 4.6. *For $n = 1$ we have $m = \delta_1 = 1$, $g_0 = g_1$ and $\delta_2 = \gcd(g_1, q + 1)$, and we obtain*

$$g(\mathcal{H}^G) = \frac{q - \#G_3}{2\#G}(q - (\delta_2 - 1)\#G_2),$$

as in [8, Thm 4.4].

Combining possible values for $g_1, \#G_2, \#G_3$ as given in [2] with Theorem 4.5 we can obtain many genera of maximal function fields. For several of these, no maximal function field of this genus was previously known to the best of our knowledge. We compared our results with the genera of maximal function fields given in [1–4,6,8,12]. Some of the new genera for small values of n and q are as follows.

$\mathbb{F}_{q^{2n}}$	new genera
$\mathbb{F}_{2^{12}}$	18
$\mathbb{F}_{2^{18}}$	37, 45, 82, 99, 189, 207, 244, 406, 840, 1708
$\mathbb{F}_{2^{20}}$	52, 502, 2552
$\mathbb{F}_{3^{12}}$	16400, 17437, 52456
$\mathbb{F}_{3^{14}}$	1365, 2731, 4369, 8739
$\mathbb{F}_{3^{18}}$	49, 330, 2065, 27280, 39388, 47775, 54532, 54588, 78736, 78816, 95466, 95550, 109092, 118201, 157512, 190932, 236281, 236523, 354640, 472683, 708916, 709644, 1062856, 1418196, 1534612, 1860033, 2125740, 3069264, 3720066, 4605241, 9210603, 13817128, 27634620
$\mathbb{F}_{5^{6}}$	99, 285
$\mathbb{F}_{5^{10}}$	24186, 37450, 64492
$\mathbb{F}_{5^{12}}$	124804, 1874462, 2539056, 3124904, 7617168, 9374712

Acknowledgments

References

[1] M. Abdón, L. Quoos, On the genera of subfields of the Hermitian function field, Finite Fields Appl. 10 (2004) 271–284.
[2] A. Bassa, L. Ma, C. Xing, S.L. Yeo, Towards a characterization of subfields of the Deligne–Lusztig function fields, J. Comb. Theory, Ser. A 120 (7) (2013) 1351–1371.
[3] Y. Danışman, M. Özdemir, On subfields of GK and generalized GK function fields, J. Korean Math. Soc. 52 (2) (2015) 225–237.
[4] Y. Danışman, M. Özdemir, On the genus spectrum of maximal curves over finite fields, J. Discrete Math. Sci. Cryptogr. 18 (5) (2015) 513–529.
[5] I. Duursma, K.-H. Mak, On maximal curves which are not Galois subcovers of the Hermitian curve, Bull. Braz. Math. Soc. 43 (3) (2012) 453–465.
[6] S. Fanali, M. Giulietti, Quotient curves of the GK curve, Adv. Geom. 12 (2) (2012) 239–268.
[7] J.W.P. Hirschfeld, G. Korchmáros, F. Torres, Algebraic Curves Over a Finite Field, Princeton University Press, 2008.
[8] A. Garcia, H. Stichtenoth, C. Xing, On subfields of the Hermitian function field, Compos. Math. 120 (2) (2000) 137–170.

 [9] A. Garcia, C. Güneri, H. Stichtenoth, A generalization of the Giulietti–Korchmáros maximal curve, Adv. Geom. 10 (3) (2010) 427–434.
[10] M. Giulietti, G. Korchmáros, A new family of maximal curves over a finite field, Math. Ann. 343 (2009) 229–245.
[11] M. Giulietti, M. Montanucci, G. Zini, On maximal curves that are not quotients of the Hermitian curve, Finite Fields Appl. 41 (2016) 72–88.
[12] C. Güneri, M. Özdemir, H. Stichtenoth, The automorphism group of the generalized Giulietti–Korchmáros function field, Adv. Geom. 13 (2013) 369–380.
[13] R. Guralnick, B. Malmskog, R. Pries, The automorphism group of a family of maximal curves, J. Algebra 361 (2012) 92–116.
[14] 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 (16) (1987) 729–732.