On subfields of the second generalization of the GK maximal function field

Beelen, Peter ; Montanucci, Maria

Published in:
Finite Fields and Their Applications

Link to article, DOI:
http://arxiv.org/abs/1811.00049
10.1016/j.ffa.2020.101669

Publication date:
2020

Document Version
Early version, also known as pre-print

On subfields of the second generalization of the GK maximal function field

Peter Beelen and Maria Montanucci

Abstract

The second generalized GK function fields K_n are a recently found family of maximal function fields over the finite field with q^{2n} elements, where q is a prime power and $n \geq 1$ an odd integer. In this paper we construct many new maximal function fields by determining various Galois subfields of K_n. In case $\gcd(q+1, n) = 1$ and either q is even or $q \equiv 1 \pmod 4$, we find a complete list of Galois subfields of K_n. Our construction adds several previously unknown genera to the genus spectrum of maximal curves.

AMS: 11G20, 14H25, 14H37

Keywords: second generalized Giulietti–Korchmáros function fields, maximal function fields, genus spectrum of maximal curves.

1 Introduction

A function field F defined over a finite field with square cardinality is called maximal, if the Hasse–Weil bound is attained. More precisely, for a function field F of genus $g(F)$ over the finite field $\mathbb{F}_{Q^2}$ with Q^2 elements, the Hasse–Weil bound states that:

$$N(F) \leq Q^2 + 1 + 2g(F)Q,$$

where $N(F)$ denotes the number of rational places $N(F)$ of F. For a maximal function field it then holds that $N(F) \leq Q^2 + 1 + 2g(F)Q$.

An important example of a maximal function field is the Hermitian function field H over the finite field $\mathbb{F}_{q^2}$. It can for example be defined as follows: $H = \mathbb{F}_{q^2}(x, y)$ with $y^{q+1} = x^{q+1} - 1$. The Hermitian curve 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 isomorphic to $\mathrm{PGU}(3, q)$. Since a subfield of a maximal function field with the same field of constants is maximal by a theorem of Serre [18], computing fixed fields of H of a subgroup of $\mathrm{PGU}(3, q)$ have given rise to many examples of maximal function fields. Since all maximal subgroups of $\mathrm{PGU}(3, q)$ are known, subgroups of these and the corresponding fixed fields have been studied in various papers, see for example [1, 3, 10, 22]. One such maximal subgroup arises by considering the stabilizer of a rational place of H. This maximal subgroup, its subgroups and the corresponding fixed field of H have for example been studied in [3, 10]. Another maximal subgroup of $\mathrm{PGU}(3, q)$, which we will denote by M_ℓ, arises by considering the stabilizer of a chord ℓ. A full description of the subgroups of this group was given in [6] for even q and in [23] for $q \equiv 1 \pmod 4$. Many genera of maximal function fields have been obtained in this way, adding to the understanding of the genus spectrum of maximal curves. For $q \equiv 3 \pmod 4$ a complete list of subgroups is not known.

In [11] Giulietti and Korchmáros [11] 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 $q > 2$. Therefore considering subfields of the GK function field, can give rise to new genera of maximal function fields. Such examples were found in for example [8]. Later, 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. These maximal function fields are often called the Garcia–Güneri–Stichtenoth (GGS) function fields. All subgroups of the automorphism groups of these fields were classified in [2], but before that several subfields were already determined in [15].

Recently a second generalization of the GK function field was discovered [4]. As for the GGS function field, for each odd n a maximal function field K_n was found with constant field $\mathbb{F}_{q^{2n}}$. Though the genus of K_n is equal to the corresponding GGS function field, their automorphism groups are different. A preliminary study in [4] already revealed that new genera of maximal function fields can be obtained by considering fixed fields of subgroups of $\mathrm{Aut}(K_n)$. The current article expands upon these results and is the analogue of [2] for the second generalization K_n of the GK function field. We are mainly interested in the cases that q is even or $q \equiv 1 \pmod q$, since otherwise not even a complete list of subgroups of M_ℓ is known. With this restriction, we construct many subgroups of the automorphism group of K_n. If additionally $\gcd(q+1, n) = 1$, the list is complete.

2 The curve $\mathcal{X}_n$ and its automorphism group

Throughout this paper p is a prime, $q = p^h$ with $h \geq 1$ and $n \geq 1$ is odd. Let $\mathbb{K}$ be the algebraic closure of $\mathbb{F}_{q^{2n}}$. We denote with $\mathcal{X}_n \subset \mathbb{P}^3$ the algebraic curve defined by the following affine equations

$$\mathcal{X}_n : \begin{cases} Y^{q+1} = X^{q+1} - 1 \\ Z^m = Y \dfrac{X^{q^2} - X}{X^{q+1} - 1} \end{cases},$$

where $m := (q^n + 1)/(q + 1)$. Further, let $K_n = \mathbb{K}(x, y, z)$ with $y^{q+1} = x^{q+1} - 1$ and $z^m = y(x^{q^2} - x)/(x^{q+1} - 1)$ be the function field of $\mathcal{X}_n$ over $\mathbb{K}$. The Hermitian curve $\mathcal{H}_q \subset \mathbb{P}^2$ defined by the affine equation $Y^{q+1} = X^{q+1} - 1$, gives rise to the subfield $H := \mathbb{K}(x, y)$ of K_n.

The curve $\mathcal{X}_n$ and its function field K_n were constructed and studied in [4], where it was shown that $\mathcal{X}_n$ is a maximal curve when considered over the finite field $\mathbb{F}_{q^{2n}}$. Moreover, the full automorphism group of K_n, and hence $\mathcal{X}_n$, was determined in [4]. More precisely, it was shown there that

$$Aut(K_n) = \{\alpha_{a,b,\xi} \mid a^{q+1} - c^{q+1} = 1,\, \xi^{q^n+1} = 1\},$$

with $\alpha_{a,b,\xi}$ acting on $x, y, z \in K_n$ as follows:

$$\begin{pmatrix} \alpha_{a,b,\xi}(x) \\ \alpha_{a,b,\xi}(y) \\ \alpha_{a,b,\xi}(z) \end{pmatrix} := \begin{pmatrix} a & c^q\xi^m & 0 \\ c & a^q\xi^m & 0 \\ 0 & 0 & \xi \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix}.$$

In particular, we have $|Aut(K_n)| = q(q^2-1)(q^n+1)$. Denote by O the set of q^3+1 places of K_n corresponding to the $\mathbb{F}_{q^2}$-rational points of $\mathcal{X}_n$. The group $Aut(K_n)$ acts on O in two orbits. One orbit, which we denote by O_1, is formed by the $q + 1$ places $R^1_\infty, \ldots, R^{q+1}_\infty$ of K_n, centered at the $q + 1$ points at infinity of $\mathcal{X}_n$. We denote the other orbit $O \setminus O_1$ with O_2. Denoting by $Aut(K_n)_P$ the subgroup of automorphisms fixing a

place P of K_n, we see from the Orbit Stabilizer Theorem that $|Aut(K_n)_P| = q(q^2-1)m$ for every $P \in O_1$, while $|Aut(K_n)_P| = q^n+1$ for every $P \in O_2$. From [17, Theorem 11.49], we deduce that for $P \in O_1$ we have $Aut(\mathcal{X}_n)_P \cong E_q \rtimes C_{(q^2-1)m}$, where E_q is an elementary abelian group of order q while $C_{(q^2-1)m}$ is cyclic of order $(q^2-1)m$. Similarly for $P \in O_2$, we have $Aut(\mathcal{X}_n)_P \cong C_{q^n+1}$ is cyclic. The orbits O_1 and O_2 are the only two short orbits of $Aut(K_n)$.

Any automorphism of K_n gives rise to an automorphism of H by restriction. Hence we have a group homomorphism $\pi : Aut(K_n) \to Aut(H)$. The restriction $\pi(\alpha_{a,b,\xi}) \in Aut(H)$ will be denoted by β_{a,b,ξ^m}. Note that β_{a,b,ξ^m} only depends on a, b and ξ^m, justifying the notation. Note that $M_\ell := \pi(Aut(K_n))$ is a maximal subgroup of $Aut(H) \cong \mathrm{PGU}(3,q)$ of cardinality $(q^3-q)(q+1)$. The notation M_ℓ is motivated by the fact that this group consists exactly of those elements of $\mathrm{PGU}(3,q)$ that stabilize the line ℓ defined by $T = 0$ when using the homogeneous coordinates $(X : Y : T)$ for $\mathbb{P}^2$. We use several subgroups of $Aut(K_n)$ very frequently in the sequel; see [4] for more details. First of all, define $S_\ell := \{\alpha_{a,b,1} \mid a^{q+1} - c^{q+1} = 1\}$. It is a normal subgroup of $Aut(K_n)$ of cardinality $q^3 - q$ isomorphic to $\mathrm{SL}(2,q)$. Since $\pi(S_\ell) \cong S_\ell$, we may identify these groups. Therefore, with slight abuse of notation we will denote them both by S_ℓ. In this way, group S_ℓ can be interpreted as a normal subgroup of M_ℓ of index $q+1$. A further subgroup that we will use frequently, is $C_m := \ker \pi = \{\alpha_{1,0,\xi} \mid \xi^m = 1\}$. Since $C_m = \ker \pi$, we have $Aut(K_n)/C_m \cong M_\ell$. Note that C_m is a central subgroup of $Aut(K_n)$ as well as a cyclic group of order m. As a result, the subgroup of $Aut(K_n)$ generated by S_ℓ and C_m can be written as a direct product $S_\ell \times C_m$. Also note that any non-trivial element from C_m fixes all q^3+1 places of K_n, corresponding to the $\mathbb{F}_{q^2}$-rational points of $\mathcal{X}_n$. Moreover, the fixed field of C_m is precisely the function field H. The group $Aut(K_n)$ also contains a cyclic group C_{q^n+1} of order q^n+1, namely $C_{q^n+1} = \{\alpha_{1,0,\xi} \mid \xi^{q^n+1} = 1.\}$ Note that $C_{q^n+1} \cap S_\ell = \{\alpha_{1,0,1}\}$. Since S_ℓ can be seen as a normal subgroup of $Aut(K_n)$, this gives rise to the following semidirect product description: $Aut(K_n) \cong S_\ell \rtimes C_{q^n+1}$.

Given a subgroup $L \subset Aut(K_n)$, we obtain by restriction a subgroup $\pi(L)$ of $Aut(H)$. To easy the notation, we write $\bar{L} := \pi(L)$. From the Second Isomorphism Theorem, we obtain that $\bar{L} \cong L/(L \cap \ker \pi) \cong LC_m/C_m$. In the sequel, we will write $L_m := L \cap C_m$. In particular, we have $|L| = |\bar{L}| \cdot |L_m|$. As a first result, we relate the genera of the fixed field of a subgroup $L \subset Aut(K_n)$ with that of the subgroup $\bar{L} \subset Aut(H)$. This relation will give the first step in reducing the classification of the genera of Galois subfields of K_n to that of the genera of Galois subfields of H containing the fixed field of M_ℓ. For a subgroup $L \subset Aut(K_n)$, we denote with K_n^L its fixed field and similarly $H^{\bar{L}}$ denotes the fixed field of $\bar{L} \subset M_\ell$. Further a subgroup of $Aut(K_n)$ or M_ℓ is called tame, if it has order relatively prime to q.

Theorem 2.1. *Let $L \subset Aut(K_n)$ be a subgroup and write $L_m = L \cap C_m$ and $\bar{L} = \pi(L)$. Further assume that the set O of q^3+1 places corresponding to $\mathcal{X}_n(\mathbb{F}_{q^2})$ is partitioned in N orbits under the action of L. Then*

$$2g_L - 2 = \frac{m}{|L_m|}(2g_{\bar{L}} - 2) + N\left(\frac{m}{|L_m|} - 1\right),$$

where g_L (resp. $g_{\bar{L}}$) denotes the genus of K_n^L (resp. $H^{\bar{L}}$). In case $\bar{L}$ is tame, we have

$$g_L = g_{\bar{L}} + \frac{(q^2-1)(q+1)(m/|L_m|-1)}{2|\bar{L}|}.$$

Proof. First of all note that any place of $H^{\bar{L}}$ ramified in the extension $K_n/H^{\bar{L}}$ needs to lie below a place in O, since O_1 and O_2 are the only short orbits of $Aut(K_n)$. Moreover, since $H = K_n^{C_m}$, the fixed field of C_m, we see that $H^{\bar{L}} = K_n^{LC_m}$. Therefore, the extension $K_n^L/H^{\bar{L}}$ is a Galois extension with cyclic Galois group $LC_m/L \cong C_m/L_m$. Since any element of C_m fixes all places in O, any place of $H^{\bar{L}}$ lying below a place in O is totally ramified in the extension $K_n^L/H^{\bar{L}}$. Hence the number of places of $H^{\bar{L}}$ that ramify in the extension

$K_n/H^{\bar{L}}$ is equal to N. Since the extension degree $[K_n : H^{\bar{L}}] = m/|L_m|$ is tame, the Riemann-Hurwitz theorem implies the first part of the theorem.

Now suppose that $\bar{L}$ is a tame subgroup. Let $\bar{O}$ denote the set of places of H corresponding to the $\mathbb{F}_{q^2}$-rational points of H_q. The above proof implies in particular that the places in $O = O_1 \cup O_2$ are totally ramified in K_n/H. This implies that the action of the subgroup L on O is equivalent to the one of $\bar{L}$ on $\bar{O}$. In particular, the number of orbits in $\bar{O}$ under the action of $\bar{L}$ is the same as N, the number of orbits in O under the action of L. For a given place P of H denote its restriction to $H^{\bar{L}}$ with $P_{\bar{L}}$. Moreover, let $e(P|P_{\bar{L}})$ denote the ramification index of P in the extension $H/H^{\bar{L}}$. Then we have

$$\sum_{P\in\bar{O}} e(P|P_{\bar{L}}) = \sum_{P_{\bar{L}}} \sum_{P|P_{\bar{L}}} e(P|P_{\bar{L}}) = \sum_{P_{\bar{L}}} [H : H^{\bar{L}}] = N \cdot |\bar{L}|.$$

Here the summation $\sum_{P_{\bar{L}}}$ is over all places $P_{\bar{L}}$ of $H^{\bar{L}}$ lying below a place in $\bar{O}$. On the other hand, since $\bar{L}$ is tame, the Riemann-Hurwitz theorem applied to the extension $H/H^{\bar{L}}$ implies that

$$\sum_{P\in\bar{O}} e(P|P_{\bar{L}}) = |O| + \sum_{P\in O} e(P|P_{\bar{L}}) - 1 = |O| + q^2 - q - 2 - |\bar{L}|(2g_{\bar{L}} - 2).$$

Here we used that H has genus $q(q-1)/2$. Combining these expressions and using that $|O| = q^3 + 1$, we can express N in terms of q, $|\bar{L}|$ and $g_{\bar{L}}$. Substituting this expression in the formula given in the first part of the theorem, we obtain the desired result. □

Remark 2.2. *The proof of Theorem 2.1 implies that N can be computed given only $\bar{L}$, since N is equal to the number of orbits in $\bar{O}$, the set of places of H corresponding to the $\mathbb{F}_{q^2}$-rational points of $\mathcal{H}_q$, under the action of $\bar{L}$. Note that the group M_ℓ acts on the places of H with two short orbits $\bar{O}_1$ and $\bar{O}_2$ given by the places lying below those in O_1 and O_2 respectively.*

The above remark shows that once a group $\bar{L} \subset M_\ell$ is given, the number of orbits N can be determined. The only data from L that is needed in order to compute g_L is that cardinality of $L_m = L \cap C_m$. Our strategy in the classification of all possible genera g_L is to classify all possible genera $g_{\bar{L}}$ and number of orbits N for subgroups $\bar{L} \subset M_\ell$, and then to study what the possibilities for $|L_m|$ are for a given $\bar{L} \subset M_\ell$. In order to do this, we study certain subgroups of L. We first define two maps used to analyze the situation.

Definition 2.3. *For a divisor k of $q^n + 1$, let $\mu_k \subset \mathbb{F}_{q^{2n}}^*$ denote the multiplicative cyclic subgroup of $\mathbb{F}_{q^{2n}}^*$ of order k. Define $\rho : Aut(K_n) \to \mu_{q^n+1}$ by $\rho(\alpha_{a,b,\xi}) = \xi$. Similarly define $\bar{\rho} : Aut(H) \to \mu_{q+1}$ by $\bar{\rho}(\beta_{a,b,\zeta}) = \zeta$.*

Lemma 2.4. *Let a subgroup $L \subset Aut(K_n)$ be given and write $L_0 := \rho(L)$, $L_1 := L \cap (S_\ell \times C_m)$ and $\bar{L} := \pi(L)$. Then the following hold:*

1. $\bar{\rho}(\bar{L}) = L_0^m$,
2. $\bar{L} \cap S_\ell = \pi(L_1)$,
3. $\rho(L_1) = L_0 \cap \mu_m$.

Proof. To prove the first item, note that $\bar{\rho}(\pi(\alpha_{a,b,\xi})) = \xi^m = \rho(\alpha_{a,b,\xi})^m$. Since $\bar{L} = \pi(L)$, this implies that $\bar{\rho}(\bar{L}) = L_0^m$. The second item follows, first observe that $\pi(L \cap (S_\ell \times C_m)) = \pi(L) \cap S_\ell$, since $\pi(S_\ell \times C_m) = S_\ell$ and $\pi^{-1}(S_\ell) = S_\ell \times C_m$. This implies that $\pi(L_1) = \pi(L \cap (S_\ell \times C_m)) = \pi(L) \cap S_\ell = \bar{L} \cap S_\ell$, proving the second item of the lemma. Finally, if $\alpha_{a,b,\xi} \in L_1$, then $\xi^m = 1$, since $L_1 \subset S_\ell \times C_m$. Hence $\rho(L_1) \subseteq L_0 \cap \mu_m$. On the other hand, if $\xi \in L_0 \cap \mu_m$, then there exists $\alpha_{a,b,\xi} \in L$ such that $\xi^m = 1$. By definition, this implies that $\alpha_{a,b,\xi} \in L_1$. Hence $\rho(L_1) \supseteq L_0 \cap \mu_m$. □

The point of this lemma is that a group L gives rise to a triple of groups $(L_0, L_1, \bar{L})$, with certain properties that at least partially determine L. The following theorem gives a partial converse.

Theorem 2.5. *Let $L_0 \subset \mu_{q^n+1}$, $L_1 \subset S_\ell \times C_m$ and $\bar{L} \subset M_\ell$ be groups satisfying $\bar{\rho}(\bar{L}) = L_0^m$, $\bar{L} \cap S_\ell = \pi(L_1)$, and $\rho(L_1) = L_0 \cap \mu_m$. Moreover, assume that $L_1 \cap C_m = \{\alpha_{1,0,\xi} \mid \xi \in L_0 \cap \mu_m\}$. Then there exists a subgroup $L \subset Aut(K_n)$ such that $\rho(L) = L_0$, $L \cap (S_\ell \times C_m) = L_1$, and $\pi(L) = \bar{L}$.*

Proof. Let a triple $(L_0, L_1, \bar{L})$ with the indicated properties be given and denote with η a generator of the cyclic group L_0. Then $\zeta := \eta^m$ is a generator of L_0^m. Further define $s := |L_0^m|$. Since $\bar{\rho}(\bar{L}) = L_0^m$, for each integer i, there exists an element $g_i \in Aut(K_n)$ such that $\pi(g_i) \in \bar{L}$ and $\bar{\rho}(\pi(g_i)) = \zeta^i$. We set $g_0 = \alpha_{1,0,1}$ to be the identify element of $Aut(K_n)$. Now consider the set

$$L := \cup_{i=0}^{s-1} g_i L_1 \subseteq Aut(K_n).$$

First of all, we claim that L is a subgroup of $Aut(K_n)$. Indeed, choose two elements from L, say $g_i l_1$ and $g_j l_2$, where $l_1, l_2 \in L_1$. Further choose an integer k such that $0 \leq k < s$ and $i - j \equiv k \pmod{s}$. To show that L is a group, all we need to show is that the element $g := g_k^{-1}(g_i l_1)(g_j l_2)^{-1}$ is an element of L_1, since then $(g_i l_1)(g_j l_2)^{-1} \in g_k L_1 \subseteq L$. Now note that $\pi(g) \in \bar{L}$, since $\pi(L_1) \subseteq \bar{L}$ and $\pi(g_i), \pi(g_j), \pi(g_k) \in \bar{L}$. On the other hand by choice of k, $\bar{\rho}(\pi(g)) = \zeta^{i-j-k} = 1$, with together with the previous implies that $\pi(g) \in \bar{L} \cap S_\ell$. Since $\bar{L} \cap S_\ell \subseteq \pi(L_1)$, we see that there exists $h \in L_1$ such that $\pi(g) = \pi(h)$, implying that $gh^{-1} \in \ker \pi = C_m$ and hence that $gh^{-1} = \alpha_{1,0,\xi}$ for some $\xi \in \mu_m$. On the other hand, $\xi = \rho(gh^{-1}) = \eta^{i-j-k}\rho(l_1 l_2^{-1} h^{-1}) \in L_0$. Combined with the previous and the assumption that $L_1 \cap C_m = \{\alpha_{1,0,\xi} \mid \xi \in L_0 \cap \mu_m\}$, we see that $gh^{-1} \in L_1$. Since by construction $h \in L_1$, this implies that $g \in L_1$ just as we wanted to show. This concludes the proof of the claim that L is a subgroup of $Aut(K_n)$.

It is clear by construction that $\rho(L) \subseteq L_0$, since $\rho(g_i) = \eta^i \in L_0$ and $\rho(L_1) \subseteq L_0$. Moreover, since $\rho(g_1) = \eta$ is a generator of L_0, we see that $\rho(L) = L_0$. Now we show that $L \cap (S_\ell \times C_m) = L_1$. It is trivial to see that the inclusion $L \cap (S_\ell \times C_m) \supseteq L_1$ holds. Now suppose that $g_i l_1 \in L \cap (S_\ell \times C_m)$, where g_i is as in the previous and $l_1 \in L_1$. If $g_i l_1 \in S_l \times C_m$, then $\bar{\rho}(\pi(g_i l_1)) = 1$, but on the other hand $\bar{\rho}(\pi(g_i l_1)) = \zeta^i$. Since $0 \leq i < s$ and ζ has order s, this implies that $i = 0$. But then $g_i l_1 = l_1 \in L_1$, which is what we wanted to show. Finally we prove that $\pi(L) = \bar{L}$. From the construction of L it is clear that $\pi(L) \subset \bar{L}$ and that $\pi(L) = \cup_{i=0}^{s-1} \pi(g_i)\pi(L_1) = \cup_{i=0}^{s-1} \pi(g_i)(\bar{L} \cap S_\ell)$. Since $\bar{\rho}(\pi(g_i)) = \zeta^i$, we have $|\pi(L)| = s \cdot |\bar{L} \cap S_\ell|$. On the other hand, the map $\bar{\rho}$ restricted to $\bar{L}$ has image L_0^m and kernel precisely $\bar{L} \cap S_\ell$. Therefore, we obtain $|\bar{L}| = s|\bar{L} \cap S_\ell|$. This implies $\bar{L} = \pi(L)$. ∎

Corollary 2.6. *Let $L_0 \subset \mu_{q^n+1}$ be a subgroup of cardinality r such that L_0^m is a group of cardinality s. Then $r = s \cdot \gcd(r, m)$. Moreover, let $\bar{L} \subset M_\ell$ be a group satisfying $\bar{\rho}(\bar{L}) = L_0^m$, then there exists a subgroup $L \subseteq M_\ell$ such that $\pi(L) = \bar{L}$, $\rho(L) = L_0$, and $|L \cap C_m| = \gcd(r, m)$.*

Proof. It is easy to see that if L_0 is a cyclic group of order m, then L_0^m has cardinality $m/\gcd(r, m)$. This proves the first statement. Since S_ℓ can be interpreted as a subgroup of $Aut(K_n)$, the same is true for $\bar{L} \cap S_\ell$. Also the group $L_0 \cap \mu_m$ can be interpreted as a subgroup of $Aut(K_n)$ by identifying $\xi \in L_0 \cap \mu_m$ with $\alpha_{1,0,\xi}$. With these identifications in mind, define $L_1 := (\bar{L} \cap S_\ell) \times (L_0 \cap \mu_m) \subset S_\ell \times C_m$. Clearly $\bar{L} \cap S_\ell = \pi(L_1)$, and $\rho(L_1) = L_0 \cap \mu_m$. Moreover, $|L \cap C_m| = |L_1 \cap C_m| = |L_0 \cap \mu_m| = |L_0|/|L_0^m| = \gcd(r, m)$ by the first part. Theorem 2.5 can therefore be applied. ∎

In general, for a subgroup L of $Aut(K_n)$, $L_m = L \cap C_m = L_1 \cap C_m$ can be thought of as a subgroup of $L_0 \cap \mu_m$, but it need not be the whole group. For the group L constructed in the proof of Theorem 2.5, we have $L_m \cong L_0 \cap \mu_m$. Other groups L giving rise to the triple may exist such that L_m and $L_0 \cap \mu_m$ do

not have the same cardinality. In view of Theorem 2.1, the cardinality of L_m is important when calculating possible genera g_L of the fixed field of L and the groups constructed in Theorem 2.5 may not give rise to a complete list of possible genera g_L. However, as we will show now in some cases all genera will already be obtained using the groups constructed in Theorem 2.5.

Corollary 2.7. *Let $\bar{L} \subset M_\ell$ be a subgroup and write $s := |\bar{\rho}(\bar{L})|$. Further, let $L \subset Aut(K_n)$ be a subgroup such that $\pi(L) = \bar{L}$ and write $L_m = L \cap C_m$. If $\gcd(s, m/|L_m|) = 1$, then there exists a subgroup $\tilde{L} \subseteq Aut(K_n)$ constructed using Theorem 2.5 such that $g_L = g_{\tilde{L}}$.*

Proof. Theorem 2.1 implies that the genus of g_L depends on data involving $\bar{L}$, but otherwise only on the cardinality of L_m. Now for $\tilde{L}_1 := (\bar{L} \cap S_\ell) \times L_m \subset S_\ell \times C_m$, we have $|\rho(\tilde{L}_1)| = |L_m|$. Let $L_0 \subseteq \mu_{q^n+1}$ be the cyclic subgroup of order $r := s \cdot |L_m|$. Then $\gcd(r, m) = |L_m|$, since by assumption $\gcd(s, m/|L_m|) = 1$ and hence $|L_0^m| = s$. Applying Corollary 2.6 we obtain a group $\tilde{L}$ with the property that $\pi(\tilde{L}) = \bar{L}$, $\rho(\tilde{L}) = L_0$, and $\tilde{L} \cap C_m = L_m$. Hence $g_L = g_{\tilde{L}}$ by Theorem 2.1, which is what we wanted to show. □

Note that the condition $\gcd(s, m/|L_m|) = 1$ is automatically satisfied in case $\gcd(m, q+1) = 1$, since s divides $q+1$. Hence we can classify all possible genera g_L in terms of subgroups $\bar{L}$ of M_ℓ if $\gcd(n, q+1) = 1$. If this condition is not satisfied, we obtain many, but potentially not all, possible genera g_L. In the next section, we now turn our attention to a description of subgroups of M_ℓ when q is even or $q \equiv 1 \pmod 4$ as well as their combinatorial dates needed to apply Theorem 2.1.

3 Some preliminary results on M_ℓ and $\mathrm{PGU}(3, q)$

The Hermitian curve $\mathcal{H}_q$ can be seen as the set of points $P = (X : Y : Z)$ in $\mathbb{P}^2$ satisfying $Y^{q+1} = X^{q+1} - Z^{q+1}$, that is, as the set of isotropic points of $\mathbb{P}^2 = \mathbb{P}^2(\mathbb{K})$, where $\mathbb{K} = \bar{\mathbb{F}}_{q^2}$, with respect to the unitary polarity defined by the Hermitian form $Y^{q+1} - X^{q+1} + Z^{q+1}$.

In particular, given a point $P = (a : b : c)$ in $\mathbb{P}^2$ then its polar line ℓ with respect to $\mathcal{H}_q$ is defined as $\ell : -a^q X + b^q Y + c^q Z = 0$. If $P \in \mathcal{H}_q$ then ℓ is the tangent line of $\mathcal{H}_q$ at P, otherwise $P \notin \ell$ and ℓ is $(q+1)$-secant line at $\mathcal{H}_q$. The couple (P, ℓ) is called a pole-polar pair (with respect to $\mathcal{H}_q$.

Using this geometrical point of view, the following lemma describes how an element in $\mathrm{PGU}(3, q)$ of a given order acts on $\mathbb{P}^2$, and in particular on $\mathcal{H}_q$. This can be obtained using the usual terminology of collineations of projective planes. In particular, a linear collineation σ of $\mathbb{P}^2$ is a (P, ℓ)-*perspectivity* if σ preserves each line through the point P (the *center* of σ), and fixes each point on the line ℓ (the *axis* of σ). A (P, ℓ)-perspectivity is either an *elation* or a *homology* according to $P \in \ell$ or $P \notin \ell$, respectively. A (P, ℓ)-perspectivity is in $PGL(3, q^2)$ if and only if its center and its axis are in $\mathbb{P}^2(\mathbb{F}_{q^2})$.

Lemma 3.1. ([21, Lemma 2.2]) *For a nontrivial element $\sigma \in \mathrm{PGU}(3, q)$, one of the following cases holds.*

(A) $\mathrm{ord}(\sigma) \mid (q+1)$ *and σ is a homology, whose center P is a point of $\mathbb{P}^2(\mathbb{F}_{q^2}) \setminus \mathcal{H}_q$ and whose axis ℓ is a chord of $\mathcal{H}_q(\mathbb{F}_{q^2})$ such that (P, ℓ) is a pole-polar pair.*

(B) $p \nmid \mathrm{ord}(\sigma)$ *and σ fixes the vertices P_1, P_2, P_3 of a non-degenerate triangle $T \subset \mathbb{P}^2(\mathbb{F}_{q^6})$.*

- *(B1)* $\mathrm{ord}(\sigma) \mid (q+1)$, *$P_1, P_2, P_3 \in \mathbb{P}^2(\mathbb{F}_{q^2}) \setminus \mathcal{H}_q$, and T is self-polar.*
- *(B2)* $\mathrm{ord}(\sigma) \mid (q^2-1)$, $\mathrm{ord} \nmid (q+1)$, *$P_1 \in \mathbb{P}^2(\mathbb{F}_{q^2}) \setminus \mathcal{H}_q$, and $P_2, P_3 \in \mathcal{H}_q(\mathbb{F}_{q^2})$.*
- *(B3)* $\mathrm{ord}(\sigma) \mid (q^2-q+1)$, *and $P_1, P_2, P_3 \in \mathcal{H}_q(\mathbb{F}_{q^6}) \setminus \mathcal{H}_q(\mathbb{F}_{q^2})$.*

(C) $\mathrm{ord}(\sigma) = p$ *and* σ *is an elation, whose center* P *is a point of* $\mathcal{H}_q(\mathbb{F}_{q^2})$ *and whose axis* ℓ *is tangent to* $\mathcal{H}_q$ *at* P *such that* (P, ℓ) *is a pole-polar pair.*

(D) either $\mathrm{ord}(\sigma) = p$ *with* $p \neq 2$, *or* $\mathrm{ord}(\sigma) = 4$ *with* $p = 2$; σ *fixes a point* $P \in \mathcal{H}_q(\mathbb{F}_{q^2})$ *and a line* ℓ *which is tangent to* $\mathcal{H}_q$ *at* P, *such that* (P, ℓ) *is a pole-polar pair.*

(E) $\mathrm{ord}(\sigma) = p \cdot d$, *where* $1 \neq d \mid (q+1)$; σ *fixes two points* $P \in \mathcal{H}_q(\mathbb{F}_{q^2})$ *and* $Q \in \mathbb{P}^2(\mathbb{F}_{q^2}) \setminus \mathcal{H}_q$; σ *fixes the line* PQ *which is the tangent to* $\mathcal{H}_q$ *at* P, *and another line through* P *which is the polar of* Q.

In the following we will refer to an element $\sigma \in \mathrm{PGU}(3, q)$ to be of type (A), (B), (C), (D) or (E) as in Lemma 3.1.

Let P be the point with homogeneous coordinates $(0 : 0 : 1)$ and let $\ell : Z = 0$ be the polar line of P. The maximal subgroup M_ℓ of $\mathrm{PGU}(3, q)$ fixing P (equivalently ℓ) has order $q(q^2-1)(q+1)$ and it is given by the following matrix representation

$$M_\ell = \left\{ \begin{pmatrix} a & \tau c^q & 0 \\ c & \tau a^q & 0 \\ 0 & 0 & 1 \end{pmatrix} : a, c, \tau \in \mathbb{F}_{q^2},\ a^{q+1} - c^{q+1} = 1,\ \tau^{q+1} = 1 \right\}.$$

An element $\sigma \in M_\ell$ will be identified with the triple $[a, c, \tau]$, see [4].

The group M_ℓ has a normal subgroup of index $q+1$ given by

$$S_\ell = \left\{ \begin{pmatrix} a & c^q & 0 \\ c & a^q & 0 \\ 0 & 0 & 1 \end{pmatrix} : a, c \in \mathbb{F}_{q^2},\ a^{q+1} - c^{q+1} = 1 \right\} \cong \mathrm{SL}(2, q).$$

The center of M_ℓ is given by

$$Z = Z(M_\ell) = \langle \alpha \rangle,\ \text{where } \alpha = \begin{pmatrix} \epsilon & 0 & 0 \\ 0 & \epsilon & 0 \\ 0 & 0 & 1 \end{pmatrix} = [\epsilon, 0, \epsilon^2],\ \text{and } \epsilon^{q+1} = 1 \text{ primitive.}$$

Remark 3.2. *Note that* Z *fixes* $\bar{O}_1$ *pointwise. Indeed, if* $\bar{P}_1 = (a : b : 0) \in \ell$ *then* $\alpha(\bar{P}_1) = (\epsilon a : \epsilon b : 0) = \bar{P}_1$. *Furthermore,* M_ℓ *does not contain elements of type (B3) and (D) since the do not fix any point in* $\mathbb{P}^2(\mathbb{F}_{q^2}) \setminus \mathcal{H}_q$. *If* $\sigma \in M_\ell$ *fixes a point* $R \in \bar{O}_2$ *then* α *is of type (A).*

If $p = 2$ the group M_ℓ is isomorphic to $\mathrm{SL}(2, q) \times Z$ since $S_\ell \cap Z$ is trivial, see [6]. If p is odd then $S_\ell \cap Z = \langle [-1, 0, 1] \rangle$. If q is odd then M_ℓ can be written as $S_\ell \rtimes C_{q+1}$ where C_{q+1} is generated by an element of type (A) whose center is an $\mathbb{F}_{q^2}$-rational point $Q \in \ell \setminus \mathcal{H}_q$, see [22]. If $q \equiv 1 \pmod 4$ then defining Z_1 to be the subgroup of Z of order $(q+1)/2$, then $Z_1 \cap S_\ell$ is trivial and $\langle S_\ell, Z_1 \rangle = S_\ell \times Z_1$.

The complete list of subgroups of M_ℓ up to isomorphism is known for $p = 2$ and $q \equiv 1 \pmod q$, see [6] and [23] respectively. Since later, we will need these groups for a case by case analysis, we list them in the following two lemmas. A group C_e will denote a cyclic group of order e. In the first of the two next lemmas, the groups C_w can always be seen as a subgroup of Z.

Lemma 3.3. [6] *Let* $p = 2$ *and* $q = 2^h$ *where* $h \geq 1$ *and let* w *be an arbitrary divisor of* $q+1$. *The following is the complete list of subgroups of* M_ℓ *up to isomorphism.*

1. $E_{2^f} \times C_w$, *where* $f \leq h$, E_{2^f} *is elementary abelian of order* 2^f;

2. $\mathrm{SL}(2,2) \times C_w$ *where either* h *is even or* $3 \nmid w$*;*

3. $(C_{3^k} \rtimes C_2) \times C_{w/3^k}$*, where* h *is odd and* $3^k || w$*;*

4. $\mathrm{SL}(2,2^f) \times C_w$*, where* $f > 1$ *and* $f \mid h$*;*

5. $D_{2t} \times C_w$ *where* D_{2t} *is a dihedral group of order* $2t$ *with* $t \mid (q-1)$*;*

6. $\mathbf{A}_5 \times C_w$ *and* h *is even;*

7. $\mathbf{A}_4 \times C_w$ *and* h *is even;*

8. $(E_{2^f} \rtimes C_d) \times C_w$*, where* $f \leq h$*,* E_{2^f} *is elementary abelian of order* 2^f *and* C_d *is cyclic of order* d *where* $d \mid \gcd(2^f - 1, q-1)$*;*

9. $C_d \times C_w$*, where* $d \mid (q-1)$*;*

10. *groups fixing a self-polar triangle* $T = \{P_1, P_2, P_3\} \subseteq \mathbb{P}^2(\mathbb{F}_{q^2}) \setminus \mathcal{H}_q(\mathbb{F}_{q^2})$ *fixing* $P = P_1$ *and acting transitively on* $T \setminus \{P_1\}$*;*

11. *groups fixing a self-polar triangle* $T = \{P_1, P_2, P_3\} \subseteq \mathbb{P}^2(\mathbb{F}_{q^2}) \setminus \mathcal{H}_q(\mathbb{F}_{q^2})$*, with* $P = P_1$ *pointwise.*

Furthermore, if $\bar{L} \leq M_\ell$ *is a subgroup of type 1-9 then* $\bar{L} \cap Z$ *is isomorphic to* C_w*.*

In the next lemma we list the subgroups of M_ℓ in case $q \equiv 1 \pmod 4$. The mentiond groups C_w can be identified with subgroups of Z_1.

Lemma 3.4. [23] *Let* p *an odd prime,* $q = p^h$ *with* $h \geq 1$*,* $q \equiv 1 \pmod 4$ *and let* w *be an arbitrary divisor of* $(q+1)/2$*. The following is the complete list of subgroups of* M_ℓ *up to isomorphism.*

1. $\mathrm{SL}(2,5) \times C_w$*, when* $q^2 \equiv 1 \pmod 5$*;*

2. $G_{48} \times C_w$ *when* $p \geq 5$*,* $8 \mid (q-1)$ *and* G_{48} *has order* 48*;*

3. $\mathrm{SL}(2,3) \times C_w$ *when* $p \geq 5$ *and* $3 \nmid w$*;*

4. $(Q_8 \rtimes C_{3^k}) \times C_{w/3^{k-1}}$ *where* $p \geq 5$*,* $k \geq 2$*,* $3^{k-1} || w$*, and* Q_8 *is the quaternion group of order* 8*;*

5. C_d *of order* $d \mid (q^2-1)$ *with* $d \nmid (q+1)$*;*

6. $Dic_d \times C_w$ *where* $Dic_d = \langle \delta, \epsilon \mid \delta^{2d} = 1, \epsilon^2 = \delta^d,\ \epsilon^{-1}\delta\epsilon = \delta^{-1} \rangle$ *is a dicyclic group of order* $4d$ *and* $1 < d \mid (q-1)/2$*;*

7. $\mathrm{SL}(2,p^k) \times C_w$ *where* $k \mid h$*;*

8. $\mathrm{TL}(2,p^k) \times C_w$ *where* $k \mid h$ *and* h/k *is even;*

9. $(\mathrm{SL}(2,3) \rtimes C_2) \times C_w \cong SmallGroup(48,29) \times C_w$ *where* $p \geq 5$ *and* $8 \nmid (q-1)$*;*

10. $D_{2d} \times C_w$ *where* D_{2d} *is a dihedral group of order* $2d$ *with* $2 < d \mid (q-1)$*;*

11. $\hat{Dic}_m \times C_w$ *where* $\hat{Dic}_m = Dic_m \rtimes C_2 = \langle \alpha, \xi \mid \alpha^{4m} = 1, \alpha^{2m} = \xi^2, \xi^{-1}\alpha\xi = \alpha^{2m-1} \rangle$ *has order* $8m$ *and* $m \mid (q-1)/2$ *but* $m \nmid (q-1)/4$*;*

12. $\mathrm{SU}^{\pm}(2,p^k)\times C_w \cong (\mathrm{SL}(2,p^k)\rtimes C_2)\times C_w$, *where* $k \mid h$ *and* h/k *is odd;*

13. *groups fixing a self-polar triangle* $T=\{P_1,P_2,P_3\}\subseteq \mathbb{P}^2(\mathbb{F}_{q^2})\setminus \mathcal{H}_q(\mathbb{F}_{q^2})$, *with* $P=P_1$ *pointwise;*

14. *groups fixing a self-polar triangle* $T=\{P_1,P_2,P_3\}\subseteq \mathbb{P}^2(\mathbb{F}_{q^2})\setminus \mathcal{H}_q(\mathbb{F}_{q^2})$ *fixing* $P=P_1$ *and acting transitively on* $T\setminus\{P_1\}$*;*

15. *groups fixing a point* $R\in \mathcal{H}_q(\mathbb{F}_{q^2})\cap \ell$.

Furthermore if $\bar{L}\leq M_\ell$ *is a subgroup of type 1-12 or of type 15 then* $\bar{L}\cap Z_1$ *is isomorphic to* C_w.

With these preliminaries in place, we proceed by analyzing the cases q even and $q\equiv 1 \pmod 4$ in the following two sections.

4 The case q even: determination of the number of orbits N

Let $q=2^h$ with $h\geq 1$. The genus of $\mathcal{H}_q/\bar{L}$ with $\bar{L}\leq M_\ell$ was computed in [6, Section 4]. However, in case the characteristic divides the order of $\bar{L}$, we also need to know the number N of $\bar{L}$-orbits in $\bar{O}_1\cup\bar{O}_2$ before being able to apply Theorem 2.1. By revisiting the genus computations in [6, Section 4], we achieve this in the current section. We will denote with N_i the number of orbits of $\bar{L}$ in its action on $\bar{O}_i$ with $i=1,2$, so that $N=N_1+N_2$. In the following $\bar{L}_Z$ will denote $\bar{L}\cap Z$ and $w=|\bar{L}_Z|$.

We now proceed with a case-by-case analysis for $\bar{L}$ according to Lemma 3.3. Note that if $\bar{L}$ is a group of order coprime with p then we only need to know $g_{\bar{L}}$ in order to compute N according to Theorem 2.1. Therefore, we will not address Cases 9 and 11 from Lemma 3.3 in this section.

Lemma 4.1. *Let* $L\leq Aut(\mathcal{X}_n)$ *and let* $\pi(L)=\bar{L}=E_{2^f}\times C_w$, *where* $f\leq h$, E_{2^f} *is elementary abelian of order* 2^f *and* $C_w=\bar{L}_Z$. *Then*

$$g_{\bar{L}}=\frac{(q+1)(q-w-2^f)+w(2^f+1)}{2^{f+1}w},$$

and

$$N=\frac{q}{2^f}+1+\frac{q}{2^f}\cdot\frac{q^2-1}{w}.$$

Proof. The computation of $g_{\bar{L}}$ was given in [6, Proposition 4.4]. By Lemma 3.1 (C) $\bar{L}$ fixes exactly one point $\bar{P}_1\in\bar{O}_1$, $\bar{L}_Z=C_w$ fixes $\bar{O}_1$ pointwise from Remark 3.2 and every other element in $\bar{L}$ has exactly $\bar{P}_1$ as its unique fixed point from Lemma 3.1 (E). This implies that $\bar{L}$ has an orbit of length 1 in $\bar{O}_1$ and from the Orbit Stabilizer Theorem it acts on $\bar{O}_1\setminus\{\bar{P}_1\}$ with orbits of length 2^f, as $|\bar{L}_{\bar{Q}}|=|\bar{L}_Z|$ and $2^f=|\bar{L}|/|\bar{L}_Z|$ for every $\bar{Q}\in\bar{O}_1\setminus\{\bar{P}_1\}$. Also $\bar{L}$ acts with long orbits on $\bar{O}_2$ since no elements in $\bar{L}$ fix points in $\bar{O}_2$. This shows that $N_1=1+\frac{(q+1)-1}{2^f}=\frac{q}{2^f}+1$, while $N_2=\frac{|\bar{O}_2|}{|\bar{L}|}=\frac{q^3-q}{2^f|\bar{L}_Z|}=\frac{q}{2^f}\cdot\frac{q^2-1}{w}$. ∎

Lemma 4.2. *Let* $L\leq Aut(\mathcal{X}_n)$ *and let* $\bar{L}=\mathrm{SL}(2,2)\times C_w$ *where* $C_w=\bar{L}_Z$ *and either* h *is even or* $3\nmid w$. *Then*

$$g_{\bar{L}}=\begin{cases}\dfrac{q^2-wq-3q+4w-4}{12w}, & \text{if } h \text{ is even,}\\[2ex] \dfrac{(q+1)(q-w-4)+9w}{12w}, & \text{otherwise.}\end{cases}\quad\text{and}\quad N=\begin{cases}\dfrac{q+8}{6}+\dfrac{q}{2}\cdot\dfrac{q-1}{3}\cdot\dfrac{q+1}{w}, & \text{if } h \text{ is even,}\\[2ex] \dfrac{q+4}{6}+\dfrac{q^3-q}{6w}, & \text{otherwise.}\end{cases}$$

Let $\bar{L} = (C_{3^k} \rtimes C_2) \times C_{w/3^k}$, where $k \geq 1$, $C_w = \bar{L}_Z$, h is odd and $3^k || w$. Then,

$$g_{\bar{L}} = \frac{(q+1)(q-w-8)+9w}{12w}, \quad \text{and} \quad N = \frac{q+4}{6} + \frac{(q+1)(q^2-q-2)}{w} + \frac{q+1}{w}.$$

Proof. From [6, Proposition 4.2] subgroups $\bar{L}$ of types 2 and 3 in Lemma 3.3 are exactly those for which $\bar{L}/(\bar{L} \cap Z) \cong \mathrm{SL}(2,2)$. The genus $g_{\bar{L}}$ was already computed in [6, Proposition 4.2] and the action of $\bar{L}$ on $\bar{O}_1 \cup \bar{O}_2$ can be deduced from its computation. In fact, from the proof of [6, Proposition 4.2],

- If h is even, that is, $3 \mid (q-1)$ then $\bar{L}$ acts on the two fixed points of its unique subgroup D of order 3 which is of type (B2) from Lemma 3.1. Also these points are in $\bar{O}_1$ since they are points of ℓ. The 3 involutions of $\bar{L}$ each fix a point of $\bar{O}_1$. since these involutions do not commute with the elements of order 3 in D these points are mutually distinct.

  Thus $\bar{L}/\bar{L}_Z = \mathrm{SL}(2,2)$ acts with orbits of length 6 on the remaining points of $\bar{O}_1$. In this way we get that $N_1 = 2 + \frac{(q+1)-3-2}{6} = \frac{q+8}{6}$. Since $\bar{L}$ contains no elements fixing a point in $\bar{O}_2$ we get also that $N_2 = \frac{q^3-q}{|\bar{L}|} = \frac{q}{2} \cdot \frac{q-1}{3} \cdot \frac{q+1}{w}$.

- Let h be odd and $3 \mid |\bar{L}_Z|$. The three involutions of $\bar{L}$ each fix a point in $\bar{O}_1$, while the stabilizer in $\bar{L}$ of one of the remaining points in $\bar{O}_1$ is $\bar{L}_Z$ since now D is generated by an element of type (B1). Hence $N_1 = 1 + \frac{(q+1)-3}{6} = \frac{q+4}{6}$. As recalled, the two elements of order 3 in $\bar{L}$ are of type $(B1)$ and hence fix pointwise a self-polar triangle T having ℓ as a side. From the proof of [6, Proposition 4.2], $\bar{L}$ contains 2 other subgroups of order 3 and hence a further 4 elements of order 3 which turn out to be of type (A). Each of the subgroups of order 3 fix a different side of T. Also, these sides are both different from ℓ. This implies that $\bar{O}_2$ contains a set of $2(q+1)$ points, the points of intersection of the two sides of T with $\mathcal{H}_q$, on which $\bar{L}$ acts with stabilizer of order 3, and hence with orbits of length $2|\bar{L}_Z|$. Moreover from [6, Proposition 4.2] $\bar{L}$ acts with long orbits on the remaining $q^3 - q - 2(q+1)$ points of $\bar{O}_2$. This shows that $N_2 = \frac{2(q+1)}{2|\bar{L}_Z|} + \frac{q^3-q-2(q+1)}{|\bar{L}|} = \frac{q+1}{w} + \frac{(q+1)(q^2-q-2)}{6w}$.

- Let h be odd and $3 \nmid |\bar{L}_Z|$. As before, the three involutions of $\bar{L}$ fixes exactly 3 distinct points which are in $\bar{O}_1$, while the stabilizer in $\bar{L}$ of one of the remaining points in $\bar{O}_1$ is $\bar{L}_Z$. Hence $N_1 = 1 + \frac{(q+1)-3}{6} = \frac{q+4}{6}$. The difference in this case is that from the proof of [6, Proposition 4.2] no elements in $\bar{L}$ fix a point in $\bar{O}_2$, implying that $N_2 = \frac{q^3-q}{6|\bar{L}_Z|} = \frac{q^3-q}{6w}$.

□

Lemma 4.3. *Let $L \leq Aut(\mathcal{X}_n)$ and let $\bar{L} = \mathrm{SL}(2,2^f) \times C_w$ with $C_w = \bar{L}_Z$, $f \mid h$ and $f > 1$. Then*

$$g_{\bar{L}} = \frac{(q+1)\left[q - w - 2^f(2^f-1)\gcd(2^f+1,w) - 2^f\right] + (2^f+1)w(2^{2f}-2^f+1)}{2^{f+1}(2^f+1)(2^f-1)w},$$

if h/f is odd, while

$$g_{\bar{L}} = \frac{(q+1)(q-2^{2f}-w) - w(2\cdot 2^{3f} - 2^{2f} - 2\cdot 2^f - 1)}{2^{f+1}(2^f+1)(2^f-1)w} + 1,$$

if h/f is even. Also,

$$N = \begin{cases} 1 + \dfrac{q-2^f}{2^f(2^{2f}-1)} + \dfrac{(q+1)\gcd(w,2^f+1)}{(2^f+1)w} + \dfrac{q+1}{w}\cdot\dfrac{q(q-1)-2^f(2^f-1)}{2^f(2^f-1)(2^f+1)}, & \text{if } h/f \text{ is odd,} \\ 2 + \dfrac{q-2^{2f}}{2^f(2^{2f}-1)} + \dfrac{q}{2^f}\cdot\dfrac{q-1}{2^{2f}-1}\cdot\dfrac{q+1}{w}, & \text{if } h/f \text{ is even.} \end{cases}$$

Proof. The genus $g_{\bar{L}}$ was computed in [6, Proposition 4.9] and according to its computation we can determine the action of $\bar{L}$ on $\bar{O}_1 \cup \bar{O}_2$ according to h/f odd or h/f even.

- Let h/f be odd. Then 2^f+1 divides $q+1$. Since $\mathrm{SL}(2,2^f)$ contains exactly 2^f+1 Sylow 2-subgroups, it has an orbit of length 2^f+1 on $\bar{O}_1$ given by the corresponding fixed points. The other elements in $\mathrm{SL}(2,2^f)$ have no fixed points on $\bar{O}_1 \cup \bar{O}_2$ and hence $\bar{L}$ acts with orbits of length $2^f(2^{2f}-1)$ on the remaining $(q+1)-(2^f+1) = q-2^f$ points in $\bar{O}_1$. Since 2^f+1 divides $q+1$ it might be that $\gcd(2^f+1, |\bar{L}_Z|)$ is not trivial. From [6, Proposition 4.9] if this would happen then $\bar{O}_2$ would contain a subset of $2^f(2^f-1)(q+1)$ points whose stabilizer in $\bar{L}$ has order $\gcd(2^f+1,|\bar{L}_Z|)$. Hence on these points $\bar{L}$ would act with orbits of length $|\bar{L}|/\gcd(2^f+1,|\bar{L}_Z|)$. Also $\bar{L}$ acts with long orbits on the remaining $q^3-q-2^f(2^f-1)(q+1)$ points in $\bar{O}_2$. Hence $N_1 = 1 + \frac{q-2^f}{2^f(2^{2f}-1)}$, and $N_2 = \frac{\gcd(2^f+1,|\bar{L}_Z|)2^f(2^f-1)(q+1)}{|\bar{L}|} + \frac{(q^3-q)-2^f(2^f-1)(q+1)}{|\bar{L}|} = \frac{(q+1)\gcd(w,2^f+1)}{(2^f+1)w} + \frac{q+1}{w}\cdot\frac{q(q-1)-2^f(2^f-1)}{2^f(2^f-1)(2^f+1)}$.
- Let h/f be even. Then $2^{2f}-1$ divides $q-1$ and hence all the elements of odd order in $\mathrm{SL}(2,2^f)$ are of type (B2) from Lemma 3.1. Since $\mathrm{SL}(2,2^f)$ contains exactly 2^f+1 Sylow 2-subgroups, it has an orbit of length 2^f+1 on $\bar{O}_1$ given by the corresponding fixed points. The elements of order 2^f+1 fix two points on $\bar{O}_1$, and hence from the Orbit Stabilizer Theorem $\bar{O}_1$ contains also a set of $2^f(2^f-1)$ points whose stabilizer has order 2^f+1. Also $\bar{L}$ acts semiregularly on $\bar{O}_2$ and with orbits of length $2^f(2^{2f}-1)$ on the remaining $(q+1)-(2^f+1)-2^f(2^f-1)$ points of $\bar{O}_1$. Thus, $N_1 = 2 + \frac{q-2^{2f}}{2^f(2^{2f}-1)}$, and $N_2 = \frac{q^3-q}{|\bar{L}|} = \frac{q}{2^f}\cdot\frac{q-1}{2^{2f}-1}\cdot\frac{q+1}{w}$.

□

Lemma 4.4. *Let $L \leq Aut(\mathcal{X}_n)$ and let $\bar{L} = D_{2t} \times C_w$ where D_{2t} is a dihedral group of order $2t$ with $t \mid (q-1)$ and $C_w = \bar{L}_Z$. Then*

$$g_{\bar{L}} = \frac{q^2-qw-qt+wt+w-t-1}{4tw} \quad \text{and} \quad N = \frac{q-1+3t}{2t} + \frac{q}{2}\cdot\frac{q-1}{t}\cdot\frac{q+1}{w}.$$

Proof. The genus $g_{\bar{L}}$ was already computed in [6, Proposition 4.5]. Furthermore, $\bar{L}/\bar{L}_Z$ has an orbit of length 2 given by the two fixed points on ℓ of its unique cyclic subgroup of order t, which is of type (B2) from Lemma 3.1. Since $\bar{L}$ contains exactly t involutions, and $\bar{L}$ acts transitively on the set of its involutions, $\bar{L}/\bar{L}_Z$ has another orbit in $\bar{O}_1$ of length t given by their fixed points. In the set of the remaining points in $\bar{O}_1$, $\bar{L}/\bar{L}_Z$ acts with orbits of length $2t$. Hence $N_1 = 2 + \frac{(q+1)-2-t}{2t} = \frac{q-1+3t}{2t}$. Since $\bar{L}$ acts semiregularly on $\bar{O}_2$ we have $N_2 = \frac{q^3-q}{|\bar{L}|} = \frac{q^3-q}{2t|\bar{L}_Z|} = \frac{q}{2}\cdot\frac{q-1}{t}\cdot\frac{q+1}{w}$. □

Lemma 4.5. *Let h be even and let $L \leq Aut(\mathcal{X}_n)$ and let $\bar{L} = \mathbf{A}_5 \times C_w$, where $C_w = \bar{L}_Z$ and h is even. Then*

$$g_{\bar{L}} = \frac{(q+1)(q-w-16)+65w-48\delta}{120w}, \quad \textit{where} \quad \delta = \begin{cases} w, & \textit{if } 5 \mid (q-1), \\ 0, & \textit{if } 5 \mid (q+1) \textit{ and } 5 \nmid w, \\ q+1, & \textit{if } 5 \mid w. \end{cases}$$

Also,

$$N = \begin{cases} 2 + \dfrac{q-16}{60} + \dfrac{q}{4} \cdot \dfrac{q-1}{15} \cdot \dfrac{q+1}{w}, & \textit{if } 5 \mid (q-1), \\ 1 + \dfrac{q-4}{60} + \dfrac{q}{4} \cdot \dfrac{q-1}{3} \cdot \dfrac{q+1}{5w}, & \textit{if } 5 \mid (q+1) \textit{ and } 5 \nmid w, \\ 1 + \dfrac{q-4}{60} + \dfrac{q+1}{w} \cdot \left(\dfrac{q^2-q-12}{60} + 1 \right), & \textit{if } 5 \mid w. \end{cases}$$

Proof. The genus $g_{\bar{L}}$ was already computed in [6, Proposition 4.7]. From its proof the action of $\bar{L}$ on $\bar{O}_1 \cup \bar{O}_2$ is depending on whether $5 \mid (q-1)$, or $5 \mid (q+1)$ but $5 \nmid |\bar{L}_Z| = w$ or $5 \mid |\bar{L}_Z|$.

- Let $5 \mid (q-1)$. $\bar{L}$ has 5 Sylow 2-subgroups of order 4 each fixing a point on $\bar{O}_1$. This gives an orbit of $\bar{L}/\bar{L}_Z$ of length 5. The remaining 12 elements of order 5 in $\bar{L}/\bar{L}_Z$ fix another point in $\bar{O}_1$ since they are of type $(B2)$ from Lemma 3.1. The remaining $(q+1)-17$ points in $\bar{O}_1$ are fixed just by $\bar{L}_Z$ in $\bar{L}$, yielding that $\bar{L}$ acts on the remaining points in $\bar{O}_1$ with orbits of length 60. Since no elements in $\bar{L}$ fix points in $\bar{O}_2$, $\bar{L}$ acts with long orbits on $\bar{O}_2$. This gives that $N_1 = 2 + \frac{q-16}{60}$, and $N_2 = \frac{q^3-q}{|\bar{L}|} = \frac{q}{4} \cdot \frac{q-1}{15} \cdot \frac{q+1}{w}$.

- Let $5 \mid (q+1)$ but $5 \nmid |\bar{L}_Z|$. As before, $\bar{L}$ has one orbit of length 5 in $\bar{O}_1$ given by the fixed points of its Sylow 2-subgroups and no other elements in $\bar{L}$ apart from the ones in $\bar{L}_Z$ fix other points in $\bar{O}_1$ or in $\bar{O}_2$. Hence $N_1 = 1 + \frac{(q+1)-5}{60}$, and $N_2 = \frac{q^3-q}{|\bar{L}|} = \frac{q}{4} \cdot \frac{q-1}{3} \cdot \frac{q+1}{5w}$.

- Let $5 \mid |\bar{L}_Z|$. The action on $\bar{O}_1$ is the same as for the previous case since again $5 \mid (q+1)$ and the elements of $\mathrm{SL}(2,q)$ are characterized just by their orders from Lemma 3.1 and the fact that $\mathrm{SL}(2,q)$ contains no elements of type (A). Now the 24 elements of order 5 in $\bar{L} \cap \mathrm{SL}(2,q)$ are of type $(B1)$ and hence fix pointwise 6 distinct self-polar triangles $T_1, \ldots, T_6$ having ℓ as a common side. From the proof of [6, Proposition 4.7], $\bar{L}$ contains other 2 subgroups (and hence 8 elements) of order 5 which are of type (A) and fix distinct sides of $T_1, \ldots, T_6$ respectively, and these sides are all different from ℓ. This implies that $\bar{O}_2$ contains a set of $12(q+1)$ points, the points of intersection of the 2 sides of T_i with $\mathcal{H}_q(\mathbb{F}_{q^2})$ for every $i = 1, \ldots, 6$, on which $\bar{L}$ acts with stabilizer of order 5, and hence with orbits of length $12|\bar{L}_Z|$. Moreover $\bar{L}$ acts with long orbits on the remaining $q^3 - q - 12(q+1)$ points of $\bar{O}_2$. This gives that $N_2 = \frac{12(q+1)}{12|\bar{L}_Z|} + \frac{q^3-q-12(q+1)}{|\bar{L}|} = \frac{q+1}{w}\left(1 + \frac{q^2-q-12}{60}\right)$.

□

Lemma 4.6. *Let h be even and $L \leq Aut(\mathcal{X}_n)$ and let $\bar{L} = \mathbf{A}_4 \times C_w$, where $C_w = \bar{L}_Z$ and h is even. Then*

$$g_{\bar{L}} = \frac{q^2 - qw + 4w - 3q - 4}{24w}, \quad \textit{and} \quad N = \frac{q+20}{12} + \frac{q}{4} \cdot \frac{q-1}{3} \cdot \frac{q+1}{w}.$$

Proof. The genus $g_{\bar{L}}$ was already computed in [6, Proposition 4.6]. From its proof the action of $\bar{L}$ on $\bar{O}_1 \cup \bar{O}_2$ can be described as follows. Since $\bar{L}$ has a unique Sylow 2-subgroup, $\bar{L}$ fixes a point in $\bar{O}_1$. Also the 4 subgroups of $\bar{L}/\bar{L}_Z$ of order 3 are of type (B2) from Lemma 3.1 and each of them fix another point on $\bar{O}_1$. This shows that $\bar{L}$ has a fixed point and one orbit of length 4 on $\bar{O}_1$ and since the unique subgroup of $\bar{L}$ fixing at least another point in the remaining $(q+1)-1-4$ points of $\bar{O}_1$ is $\bar{L}_Z$, we get that $\bar{L}$ acts with orbits of length 12 on the set of the remaining points of $\bar{O}_1$. Since $\bar{L}$ has no other elements fixing points in $\mathcal{H}_q$, it acts semiregularly on $\bar{O}_2$. Hence $N_1 = 2 + \frac{(q+1)-1-4}{12} = \frac{q+20}{12}$, and $N_2 = \frac{q^3-q}{|\bar{L}|} = \frac{q^3-q}{12|\bar{L}_Z|} = \frac{q}{4} \cdot \frac{q-1}{3} \cdot \frac{q+1}{w}$. □

Lemma 4.7. *Let $L \leq Aut(\mathcal{X}_n)$ and let $\bar{L} = (E_{2^f} \rtimes C_d) \times C_w$, where $f \leq h$, E_{2^f} is elementary abelian of order 2^f, $C_w = \bar{L}_Z$ and $d \mid \gcd(2^f - 1, q-1)$. Then*

$$g_{\bar{L}} = \frac{(q+1)(q-w-2^f) + w(2^f+1)}{2^{f+1}dw}, \quad \text{and} \quad N = \frac{q-2^f}{2^f d} + 2 + \frac{q}{2^f} \cdot \frac{q^2-1}{dw}.$$

Proof. The computation of $g_{\bar{L}}$ was given in [6, Proposition 4.8]. Here $\bar{L}$ fixes exactly one point $\bar{P}_1 \in \bar{O}_1$, and the elements of order d in $\bar{L}$ have exactly another fixed point in $\bar{O}_1$ since they are of type (B2) from Lemma 3.1. This implies that $\bar{L}$ has an orbit of length 1 in $\bar{O}_1$ and from the Orbit Stabilizer Theorem it has another orbit of length $|\bar{L}|/d|\bar{L}_Z|$, while it acts on the remaining $(q+1) - 1 - 2^f$ elements in $\bar{O}_1$ with orbits of length $2^k d$. Also $\bar{L}$ acts with long orbits on $\bar{O}_2$ as no elements in $\bar{L}$ fix points in $\bar{O}_2$. This shows that $N_1 = 2 + \frac{(q+1)-1-2^k}{2^k d} = \frac{q-2^k}{2^k d} + 2$, while $N_2 = \frac{|O_2|}{|\bar{L}|} = \frac{q^3-q}{2^k d|\bar{L}_Z|} = \frac{q}{2^k} \cdot \frac{q^2-1}{dw}$. □

From Lemma 3.3 to complete this section we need to analyze the case $\bar{L}$ fixes a self-polar triangle $T = \{P_1, P_2, P_3\} \subseteq \mathbb{P}^2(\mathbb{F}_{q^2}) \setminus \mathcal{H}_q(\mathbb{F}_{q^2})$ either fixing $P = P_1$ and acts transitively on $T \setminus \{P_1\}$ or fixing T pointwise. We recall that the stabilizer of T in $\mathrm{PGU}(3,q)$ is isomorphic to $(C_{q+1} \times C_{q+1}) \rtimes \mathbf{S}_3$, where $C_{q+1} \times C_{q+1}$ fixes T pointwise while $\mathbf{S}_3$ acts faithfully on T, see [16] and [20]. For $\bar{L} \leq (C_{q+1} \times C_{q+1}) \rtimes \mathbf{S}_3$ let $\bar{L}_T$ be the subgroup of $\bar{L}$ fixing T pointwise. In Case 10 of Lemma 3.3 clearly $\bar{L}_T$ has index 2 in $\bar{L}$.

Proposition 4.8. (see [6, Proposition 3.3]) *Let q be even. Let $T = \{P, P_1, P_2\}$ be a self-polar triangle in $\mathbb{P}^2(\mathbb{F}_{q^2}) \setminus \mathcal{H}_q(\mathbb{F}_{q^2})$.*

(i) Let a, w, and e be positive integers satisfying $e \mid (q+1)^2$, $w \mid (q+1)$, $a \mid w$, $aw \mid e$, $\frac{e}{a} \mid (q+1)$, and $\gcd\left(\frac{e}{aw}, \frac{w}{a}\right) = 1$. Then there exists a subgroup $\bar{L} \leq ((C_{q+1} \times C_{q+1}) \rtimes \mathbf{S}_3) \cap M_\ell$ of order $2e$ such that $|\bar{L}_T| = e$ and

$$g_{\bar{L}} = \frac{(q+1)\left(q - 2a - w - \frac{e}{w} + 1\right) + 3e}{4e}. \tag{1}$$

(ii) Conversely, let $\bar{L} \leq ((C_{q+1} \times C_{q+1}) \rtimes \mathbf{S}_3) \cap M_\ell$ and $\bar{L}_T$ has index 2 in $\bar{L}$. Define $e = |\bar{L}|/2$, a to be the order of the subgroup of homologies of $\bar{L}$ with center P_1, which is equal to the order of the subgroup of homologies in $\bar{L}$ with center P_2, and $w = |\bar{L}_Z|$. Then a, w and e satisfy the numerical assumptions in point (i) and the genus $g_{\bar{L}}$ is given by Equation (1).

Remark 4.9. *Let t and w be divisors of $q+1$ and define $a = \gcd(t,w)$ and $e = tw$. It is not hard to see that these numbers satisfy the numerical conditions in (i) Proposition 4.8. Conversely any triple a, w, e is obtained in this way by choosing $t = e/w$. Equation* (1) *reads,*

$$g_{\bar{L}} = \frac{(q+1)(q - 2\gcd(t,w) - w - t + 1) + 3tw}{4tw}.$$

Lemma 4.10. *Let $\bar{L} \leq (C_{q+1} \times C_{q+1}) \rtimes \mathbf{S}_3$ such that $|\bar{L}| = 2e = 2tw$ and $\bar{L}_T$ has index 2 in $\bar{L}$ and $w = |\bar{L}_Z|$. Then $\bar{L}/\bar{L}_Z$ is a dihedral group of order $2t$.*

Proof. Since $\bar{L}_T$ has index 2 in $\bar{L}$, $\bar{L}$ fixes a vertex $P \in T$ and acts transitively on $T \setminus \{P\}$. In particular $\bar{L}$ is a subgroup of $(C_{q+1} \times C_{q+1}) \rtimes C_2$. Hence $\bar{L}/\bar{L}_Z \leq ((C_{q+1} \times C_{q+1}) \rtimes C_2)/Z \cong C_{q+1} \rtimes C_2 = D_{2(q+1)}$ which is a dihedral group of order $2(q+1)$. Since $\bar{L}/\bar{L}_Z$ is not abelian, it is a dihedral group of order $2t$. □

Lemma 4.11. *Let $\bar{L}$ be as in Proposition 4.8 and define $t = e/w$. Then*

$$N = 1 + \frac{q-t+1}{2t} + \frac{(q+1)\gcd(w,t)}{tw} + \frac{(q+1)^2(q-2)}{2tw}.$$

Proof. From Lemma 4.10 $\bar{L}/\bar{L}_Z$ is a dihedral group of order $2t$. Hence $\bar{L}/\bar{L}_Z$ contains exactly t involutions and it acts on the subset of $\bar{O}_1$ given by their fixed points. From Proposition [6, Proposition 3.3] $\bar{L}$ acts with orbits of length $2t$ on the remaining points of $\bar{O}_1$. This shows that $N_1 = 1 + \frac{q+1-t}{2t}$. The only elements in $\bar{L}$ that fix points in $\bar{O}_2$ are the ones contained in the two groups of homologies of order $\gcd(w,t)$ and they fix a set of $q+1$ points respectively on which $\bar{L}$ (from the Orbit Stabilizer Theorem) acts with orbits of length $2tw/\gcd(w,t)$. Hence $\bar{L}$ is semiregular on the remaining $q^3 - q - 2(q+1)$ points in $\bar{O}_2$. Hence,

$$N_2 = \frac{2(q+1)\gcd(w,t)}{2tw} + \frac{(q^3-q)-2(q+1)}{2tw} = \frac{(q+1)\gcd(w,t)}{tw} + \frac{(q+1)^2(q-2)}{2tw}.$$

□

5 The case $q \equiv 1 \pmod 4$: determination of $\bar{L}$, $g_{\bar{L}}$ and N

In this case another description of M_ℓ is given in [23, Section 3]. Let β be any involution of M_ℓ different from $\iota = [-1, 0, 1]$, for instance $\beta = [-1, 0, -1]$; obviously, β normalizes both S_ℓ and Z and it does not commute with S_ℓ in general. Then

$$M_\ell = (S_\ell \rtimes \langle\beta\rangle) \times Z_1 \cong (\mathrm{SL}(2,q) \rtimes C_2) \times C_{\frac{q+1}{2}}\,.$$

With the notation of [12, Section 9] the subgroup $S_\ell \rtimes \langle\beta\rangle$ is also denoted by $\mathrm{SU}^{\pm}(2,q)$, meaning that $S_\ell \rtimes \langle\beta\rangle$ consists of the elements of M_ℓ with determinant 1 or -1; here, the determinant of an element $\alpha \in M_\ell$ is the determinant of the representative matrix of α having entry 1 in the third row and column.

In this section, for any $\bar{L} \leq M_\ell$, we will use the notation $\bar{L}_{Z_1} = \bar{L} \cap Z_1$ and $w = |\bar{L}_{Z_1}|$.

The complete list of subgroups $\bar{L} \leq M_\ell$ is given in Lemma 3.4. However, in the cases in which $\bar{L}$ is tame the genus g_L can be computed directly from $g_{\bar{L}}$ without having to compute N. The values of $g_{\bar{L}}$ can be found in [23] and will not be reproduced here. We proceed by computing N in the remaining, non-tame cases. That is to say, in Cases 1 with $p = 3$, 7, 8, 12, and 15 from Lemma 3.4.

Lemma 5.1. *Let $p = 3$ and $L \leq Aut(\mathcal{X}_n)$ be such that $\bar{L} = \mathrm{SL}(2,5) \times C_w$, where $C_w = \bar{L}_{Z_1}$ and $q^2 \equiv 1 \pmod 5$. Then*

$$g_{\bar{L}} = \frac{(q+1)(q-21-2w) + 140w - 48s}{240w},$$

where

$$s = \begin{cases} 2w & \text{if } 5 \mid (q-1), \\ 0 & \text{if } 5 \mid (q+1),\ 5 \nmid w, \\ q+1 & \text{if } 5 \mid w. \end{cases}$$

Also,

$$N = \begin{cases} \dfrac{q+99}{60} + \dfrac{q}{3} \cdot \dfrac{q-1}{5} \cdot \dfrac{q+1}{w}, & \text{if } 5 \mid (q-1), \\ \dfrac{q+51}{60} + \dfrac{q(q-1)}{3} \cdot \dfrac{q+1}{5w}, & \text{if } 5 \mid (q+1) \text{ and } 5 \nmid w, \\ \dfrac{q+51}{60} + \dfrac{q+1}{2w} + \dfrac{(q^2-q-12)(q+1)}{120w}, & \text{if } 5 \mid w. \end{cases}$$

Proof. The genus $g_{\bar{L}}$ is computed in [23, Proposition 3.4]. According to its proof we can describe the short-orbits structure of $\bar{L}$ in its natural action on $\mathcal{H}_q(\mathbb{F}_{q^2})$.

- Let $5 \mid (q-1)$. Since $\mathrm{SL}(2,5)$ contains 10 cyclic subgroups of order $p=3$, $\bar{L}$ contains a short orbit of length 10 in $\bar{O}_1$ given by the corresponding fixed points. Also $\bar{L}$ contains 6 cyclic subgroups C_5 and the order of the normalizer in $\mathrm{SL}(2,5)$ of C_5 is 20. From Lemma 3.1 each element in C_5 fixes exactly 2 points in $\bar{O}_1$ and the set of the corresponding fixed points is disjoint from the set of 10 points counted before, since the normalizer of an element of order 3 has order coprime with 5. Hence elements of order 4 and of order 5 fixes distinct points on $\bar{O}_1$ implying that there is another short orbit of $\mathrm{SL}(2,5)$ on $\bar{O}_1$ of length 12 because the corresponding stabilizer in $\mathrm{SL}(2,5)$ has order 10. $\mathrm{SL}(2,5)$ acts with orbits of length 60 elsewhere since its unique involution is central and hence fixes $\bar{O}_1$ pointwise. Hence $N_1 = 1 + 1 + \frac{q+1-10-12}{60} = \frac{q+99}{60}$, and $N_2 = \frac{q^3-q}{|\bar{L}|} = \frac{q^3-q}{120|\bar{L}_{Z_1}|} = \frac{q}{3} \cdot \frac{q-1}{5} \cdot \frac{q+1}{w}$.

- Let $5 \mid (q+1)$ but $5 \nmid w$. As before, since $\mathrm{SL}(2,5)$ contains 10 cyclic groups of order $p=3$, $\bar{L}$ contains a short orbit of length 10 in $\bar{O}_1$ given by the corresponding fixed points. Now the cyclic groups of order 5 acts semiregularly on $\mathcal{H}_q(\mathbb{F}_{q^2})$ as they are of type (B1) from Lemma 3.1. Hence $\bar{L}$ has exactly one short orbit on $\bar{O}_1$ of length 10 and acts with orbits of length 60 elsewhere as its unique involution fixes $\bar{O}_1$ pointwise. $\mathrm{SL}(2,5)$ acts semiregularly on $\bar{O}_2$. Hence $N_1 = 1 + \frac{q+1-10}{60} = \frac{q+51}{60}$, and $N_2 = \frac{q^3-q}{|\bar{L}|} = \frac{q^3-q}{120|\bar{L}_{Z_1}|} = \frac{q(q-1)}{3} \cdot \frac{q+1}{5w}$.

- Let $5 \mid w$. As before, since $\mathrm{SL}(2,5)$ contains 10 cyclic groups of order $p=3$, $\bar{L}$ contains a short orbit of length 10 in $\bar{O}_1$ given by the corresponding fixed points. Now the cyclic groups of order 5 acts semiregularly on $\mathcal{H}_q(\mathbb{F}_{q^2})$ as they are of type (B1) from Lemma 3.1. Hence $\bar{L}$ has exactly one short orbit on $\bar{O}_1$ of length 10 and acts with orbits of length 60 elsewhere as its unique involution fixes $\bar{O}_1$ pointwise. $\mathrm{SL}(2,5)$ acts semiregularly on $\bar{O}_2$. From the proof of [23, Proposition 3,4], $\bar{L}$ contains 12 cyclic subgroups of order 5 which are of type (A), that is, that fix $q+1$ distinct points in $\bar{O}_2$. This implies that O_2 contains a set of $12(q+1)$ points on which $\bar{L}$ acts with stabilizer of order 5, and hence with orbits of length $24|\bar{L}_Z|$ and acts with long orbits elsewhere. Hence, $N_1 = 1 + \frac{q+1-10}{60} = \frac{q+51}{60}$, and $N_2 = \frac{12(q+1)}{24|\bar{L}_{Z_1}|} + \frac{q^3-q-12(q+1)}{120|\bar{L}_{Z_1}|} = \frac{q+1}{2w} + \frac{(q^2-q-12)(q+1)}{120w}$.

□

Lemma 5.2. *Let $L \leq Aut(\mathcal{X}_n)$ and let $\bar{L} = \mathrm{SL}(2,p^k) \times C_w$ where $k \mid h$. Let $r = h/k$. Then*

$$g_{\bar{L}} = 1 + \frac{q^2-q-2-\Delta}{2p^k(p^{2k}-1)w},$$

where

$$\Delta = (p^{2k}-1)(q+2)+p^{2k}-1+q+1+p^k(p^k+1)(p^k-3)w+p^k(p^k-1)^2(\gcd(r,2)-1)+2(p^{2k}-1)(w-1)$$
$$+2(w-1)(q+1)+p^k(p^k-1)^2(w-1)(\gcd(r,2)-1)+(\gcd(w,p^k+1)-1)p^k(p^k-1)(q+1)(2-\gcd(r,2)).$$

Also,

$$N=\begin{cases}2+\dfrac{2(q-p^{2k})}{p^k(p^k-1)(p^k+1)}+\dfrac{q}{p^k}\cdot\dfrac{q-1}{(p^{2k}-1)}\cdot\dfrac{q+1}{w}, & \text{if } r \text{ is even,}\\[2ex] 1+\dfrac{2(q-p^k)}{p^k(p^{2k}-1)}+\dfrac{(q+1)\gcd(p^k+1,w)}{(p^k+1)w}+\dfrac{(q^2-q-p^k(p^k-1))(q+1)}{p^k(p^k-1)(p^k+1)w}, & \text{if } r \text{ is odd.}\end{cases}$$

Proof. The genus $g_{\bar{L}}$ was computed in [23, Proposition 3.9]. From its proof we can describe the short-orbits structure of the group $\bar{L}$. We will distinguish two cases.

- Assume that r is even. Then $p^{2k}-1$ divides $q-1$ and hence every element of order dividing $p^{2k}-1$ in $\mathrm{SL}(2,p^k)$ is of type (B2) from Lemma 3.1. Since $\mathrm{SL}(2,p^k)$ contains exactly p^k+1 Sylow p-subgroups, $\bar{L}$ has a short orbit of length p^k+1 contained in $\bar{O}_1$. Since every cyclic subgroup of $\mathrm{SL}(2,p^k)$ is of type (B2), and $\mathrm{SL}(2,p^k)$ contains exactly $p^k(p^k-1)/2$ subgroups of order p^k+1, we get that $\bar{O}_1$ contains another short orbit of $\bar{L}$ given by the corresponding $p^k(p^k-1)$ fixed points. No other elements in $\bar{L}$ other than the central involution and the elements in $\bar{L}_{Z_1}$ fix other points in $\bar{O}_1$ and hence $\bar{L}$ acts with orbits of length $p^k(p^k+1)(p^k-1)/2$ on the remaining points in $\bar{O}_1$. Also $\bar{L}$ acts semiregularly on $\bar{O}_2$. Hence $N_1 = 1+1+2\frac{q+1-(p^k+1)-p^k(p^k-1)}{p^k(p^k-1)(p^k+1)} = 2+\frac{2(q-p^{2k})}{p^k(p^k-1)(p^k+1)}$ and $N_2 = \frac{q^3-q}{|\bar{L}|} = \frac{q}{p^k}\cdot\frac{q-1}{(p^{2k}-1)}\cdot\frac{q+1}{w}$.
- Let r be odd. Then p^k+1 divides $q+1$. Since $\mathrm{SL}(2,p^k)$ contains exactly p^k+1 Sylow p-subgroups, $\bar{L}$ has a short orbit of length p^k+1 contained in $\bar{O}_1$. No other elements other than the unique involution of $\mathrm{SL}(2,p^k)$ (which is central) and $\bar{L}_{Z_1}$ fix other elements in $\bar{O}_1$. This implies that $\bar{L}$ acts with orbits of length $p^k(p^k+1)(p^k-1)/2$ on the remaining points in $\bar{O}_1$. Since p^k+1 divides $q+1$ it might be that $\gcd(p^k+1,|\bar{L}_Z|)$ is not trivial. From [23, Proposition 3.9] if this happens then $\bar{O}_2$ contains a subset of $p^k(p^k-1)(q+1)$ points whose stabilizer in $\bar{L}$ has order $\gcd(p^k+1,w)$, and hence on which $\bar{L}$ acts with orbits of length $|\bar{L}|/\gcd(p^f+1,w)$. Also $\bar{L}$ acts with long orbits on the remaining $q^3-q-p^f(p^f-1)(q+1)$ points in $\bar{O}_2$. Hence $N_1 = 1+2\frac{q+1-(p^k+1)}{p^k(p^{2k}-1)} = 1+\frac{2(q-p^k)}{p^k(p^{2k}-1)}$, and $N_2 = \frac{p^k(p^k-1)(q+1)\gcd(p^k+1,|\bar{L}_{Z_1}|)}{|\bar{L}|}+\frac{q^3-q-p^k(p^k-1)(q+1)}{|\bar{L}|} = \frac{(q+1)\gcd(p^k+1,w)}{(p^k+1)w}+\frac{(q^2-q-p^k(p^k-1))(q+1)}{p^k(p^k-1)(p^k+1)w}$.

□

Lemma 5.3. *Let $L \le Aut(\mathcal{X}_n)$ and let $\bar{L} = \mathrm{TL}(2,p^k)\times C_w$ where $k \mid h$ and $r = h/k$ is even. Then*

$$g_{\bar{L}} = 1+\frac{q^2-q-2-\Delta}{4p^k(p^{2k}-1)w},$$

where

$$\Delta = (p^{2k}-1)(q+2)+p^{2k}-1+q+1+p^k(p^k+1)(p^k-3)w+p^k(p^k-1)^2+2(p^{2k}-1)(w-1)$$
$$+2(w-1)(q+1)+p^k(p^k-1)^2(w-1)+2p^k(p^{2k}-1)w,$$

and

$$N = 2+\frac{q-p^{2k}}{p^k(p^{2k}-1)}+\frac{q}{p^k}\cdot\frac{q-1}{(p^{2k}-1)}\cdot\frac{q+1}{2w}.$$

Proof. The genus $g_{\bar{L}}$ is computed in [23, Proposition 3.10] and from its proof the short orbit structure of $\bar{L}$ on $\mathcal{H}_q(\mathbb{F}_{q^2})$ can be described. The short orbit structure of the subgroup $\mathrm{SL}(2,p^k)\times \bar{L}_{Z_1}$ was already described in the proof of Lemma 5.2 and every element in $\mathrm{TL}(2,p^k)\setminus \mathrm{SL}(2,p^k)$ is of type (B2) from [22, Proposition 4.4]. Hence the action of $\bar{L}$ on $\bar{O}_2$ is semiregular as $\mathrm{SL}(2,p^k)$ acts semiregularly on $\bar{O}_2$ and elements of type (B2) fix just points on $\bar{O}_1$. Since $\mathrm{SL}(2,p^k)$ has exactly two short orbits of distinct lengths on $\bar{O}_1$ then they are also short orbits of $\mathrm{TL}(2,p^k)$.

Since $\mathrm{SL}(2,p^k)$ has index 2 in $\mathrm{TL}(2,p^k)$ either there exists a point R in an orbit of cardinality $p^k(p^{2k}-1)/2$ of $\mathrm{SL}(2,p^k)$ with a stabilizer of order 4, or all remaining orbits under the action of $\mathrm{TL}(2,p^k)$ have cardinality $p^k(p^{2k}-1)$. From the proof of [22, Proposition 4.4], an element $\alpha\in \mathrm{TL}(2,p^k)\setminus \mathrm{SL}(2,p^k)$ has order at least 5. Therefore α cannot occur in the stabilizer of R implying that the order of such a stabilizer remains two. Thus, $N_1 = 2+\frac{q+1-(p^k+1)-p^k(p^k-1)}{p^k(p^{2k}-1)} = 2+\frac{q-p^{2k}}{p^k(p^{2k}-1)}$, and $N_2 = \frac{q^3-q}{|\bar{L}|} = \frac{q}{p^k}\cdot\frac{q-1}{(p^{2k}-1)}\cdot\frac{q+1}{2w}$. □

Lemma 5.4. *Let $L\le Aut(\mathcal{X}_n)$ and let $\bar{L}=\mathrm{SU}^{\pm}(2,p^k)\times C_w \cong (\mathrm{SL}(2,p^k)\rtimes C_2)\times C_w$, where $k\mid h$, h/k is odd and $C_w=\bar{L}_{Z_1}$. Then*

$$g_{\bar{L}} = 1+\frac{q^2-q-2-\Delta}{4p^k(p^{2k}-1)w},$$

where

$$\Delta = (q+1)+p^k(p^k+1)(p^k-3)+(p^{2k}-1)(q+3)+p^k(p^k-1)(q+1)+p^k(p^{2k}-1)+(2w-2)(q+1)$$
$$+2(p^{2k}-1)(w-1)+2p^k(p^k+1)(p^k-2)(w-1)+2p^k(p^k-1)(q+1)(\gcd(p^k+1,w)-1).$$

Moreover

$$N = 1+\frac{q-p^k}{p^k(p^k-1)(p^k+1)}+\frac{(q+1)\gcd(p^k+1,w)}{w}+\frac{[q^2-q-p^k(p^k-1)]}{p^k(p^k+1)(p^k-1)}\cdot\frac{(q+1)}{2w}.$$

Proof. The genus $g_{\bar{L}}$ is computed in [23, Proposition 3.15]. From its proof and the proof of Lemma 5.2 the short orbits structure of $\bar{L}$ on $\mathcal{H}_q$ can be described.

The number of Sylow p-subgroups of $\mathrm{SU}^{\pm}(2,q)$ is the same as the number of Sylow p-subgroups of $\mathrm{SL}(2,p^k)$, hence $\bar{L}$ has a short orbit θ of length p^k+1 contained in $\bar{O}_1$. The stabilizer of a point $\bar{R}\in\bar{O}_1\setminus\theta$ in $\mathrm{SL}(2,p^k)$ has order 2. The order of the stabilizer of $\bar{R}$ in $\mathrm{SU}^{\pm}(2,p^k)$ can grow if and only if there exists an element $\alpha\in\mathrm{SU}^{\pm}(2,p^k)\setminus\mathrm{SL}(2,p^k)$ fixing $\bar{R}$. If α is of type (B2) or (E) then α^2, which is in $\mathrm{SL}(2,p^k)$, fixes exactly two points in θ. If α is of type (B1) then it acts without fixed points on $\bar{O}_1$. If α is of type (A) then it has no fixed points on $\bar{O}_1$ unless α is central and hence in $\mathrm{SL}(2,p^k)$, a contradiction. This shows that $\mathrm{SU}^{\pm}(2,p^k)$ acts with orbits of length $|\mathrm{SU}^{\pm}(2,q)|/2 = |\mathrm{SL}(2,p^k)|$ on $\bar{O}_1\setminus\theta$. Since $\bar{L}_{Z_1}$ acts trivially on $\bar{O}_1$ the length of the orbits of $\bar{L}$ on $\bar{O}_1$ is the same as the length of the orbits of $\mathrm{SU}^{\pm}(2,p^k)$. Hence $N_1 = 1+\frac{q+1-(p^k+1)}{|\mathrm{SL}(2,p^k)|} = 1+\frac{q-p^k}{p^k(p^k-1)(p^k+1)}$.

From the proof of [23, Proposition 3.15] we have that, even though $\mathrm{SL}(2,p^k)$ acts semiregularly on $\bar{O}_2$, $\mathrm{SU}^{\pm}(2,p^k)$ contains $p^k(p^k-1)$ elements of type (A) and order 2 fixing $q+1$ distinct points on $\bar{O}_2$. Also, combining this with the proof of Lemma 5.2, this set of points can have a non-trivial stabilizer in $\mathrm{SL}(2,p^k)\times\bar{L}_{Z_1}$ of order $\gcd(p^k+1,w)$ given by elements of type (A) having the same axis and center as the described elements of order 2 in $\mathrm{SU}^{\pm}(2,p^k)$. Hence the stabilizer has order $2\gcd(p^k+1,w)$ in this case.

Therefore $\bar{O}_2$ contains a set of $p^k(p^k-1)(q+1)$ points on which $\bar{L}$ acts with orbits of length $|\bar{L}|/2\gcd(p^k+1,w) = |\mathrm{SU}^{\pm}(2,p^k)|w/2\gcd(p^k+1,w) = |\mathrm{SL}(2,p^k)|w/\gcd(p^k+1,w)$. Moreover, $\bar{L}$ acts semiregularly elsewhere in $\bar{O}_2$. Hence,

$N_2 = \frac{p^k(p^k-1)(q+1)\gcd(p^k+1,w)}{p^k(p^k-1)(p^k+1)w}+\frac{q^3-q-p^k(p^k-1)(q+1)}{|\bar{L}|} = \frac{(q+1)\gcd(p^k+1,w)}{w}+\frac{[q^2-q-p^k(p^k-1)]}{p^k(p^k+1)(p^k-1)}\cdot\frac{(q+1)}{2w}$. □

At this point we are left with Case 15 from Lemma 3.4. In this case the genus $g_{\bar{L}}$ is computed in [10] and [3].

The following lemma is a consequence of Corollary 4.5 in [10] and the subsequent observations.

Lemma 5.5. [10, Corollary 4.5] *Let $q = p^h$, $m \mid (q^2-1)$ and $u \leq h$. Let $R \in \mathcal{H}_q(\mathbb{F}_{q^2})$. If $\bar{L}$ is a subgroup of* $\mathrm{PGU}(3,q)$ *fixing R, such that $|\bar{L}| = mp^u$ and $\bar{L}$ has a (unique) elementary abelian Sylow p-subgroup, then*

$$g_{\bar{L}} = \frac{1}{2m}(q+1-d)(p^{h-u}-1),$$

where $d = \gcd(q+1, m)$. Finally,

$$N = \frac{q(q^2-1)}{p^u m} + 2 + \frac{d(q-p^u)}{p^u m}.$$

Proof. Since $\bar{L}$ fixes $\bar{R}$ it has the short orbit $\{\bar{R}\}$ of length 1 in $\bar{O}_1$. From the proof of [10, Theorem 4.4] one can derive directly that the sum of the number of fixed points of the elements in $\bar{L}$ when acting on the remaining q^3 points in $\bar{O}_1 \cup \bar{O}_2$ is equal to $q^3 + |\bar{L}| + d(q-p^u) - q$. Using Burnside's lemma we obtain

$$N = 1 + \frac{q^3 - q + |\bar{L}| + d(q-p^u)}{|\bar{L}|} = \frac{q(q^2-1)}{p^u m} + 2 + \frac{d(q-p^u)}{p^u m}.$$

□

Remark 5.6. *Note that it is not true that for any $m \mid (q^2-1)$ and $u \leq h$, there exists a subgroup of* $\mathrm{PGU}(3,q)$ *fixing R of order mp^u. A full classification of the possible subgroups has been carried out in [3]. However, the genera one would obtain using such subgroups and Theorem 2.1 are already obtained in [2].*

6 New genera for maximal function fields

In this section, we give several examples of new genera of maximal function fields. New means that for the indicated finite fields, these genera cannot be constructed using methods or results from [1, 2, 3, 5, 6, 7, 8, 10, 13, 14, 15, 19, 22, 23]. Note that for $q \equiv 1 \pmod 4$, a complete list of subgroups of the automorphism group of the Hermitian curve is known as well as the corresponding genera. Therefore all new genera correspond to function fields that cannot be Galois covered by the Hermitian curve.

$\mathbb{F}_{q^{2n}}$	new genera
$\mathbb{F}_{2^{20}}$	$72, 200, 204, 302, 702, 1532, 3572$
$\mathbb{F}_{2^{28}}$	$140, 492, 560, 1962, 57332$
$\mathbb{F}_{5^6}$	$80, 160, 482$
$\mathbb{F}_{5^{10}}$	$2340, 4160, 4680, 6241, 12484$
$\mathbb{F}_{5^{12}}$	19500
$\mathbb{F}_{5^{14}}$	$337, 338, 676, 2016, 3584, 4032, 5377, 5378, 10756, 58590, 117180, 156241, 156242, 312484$
$\mathbb{F}_{9^{14}}$	$84, 210, 350, 420, 448, 658, 700, 1122, 1124, 1402, 2248, 49476, 123690, 206150, 247380, 263872, 387562,$ $412300, 659682, 659684, 824602, 1319368, 1434888, 3587220, 5978700, 7174440, 7652736, 11239956,$ $11957400, 19131842, 19131844, 23914802, 38263688$
$\mathbb{F}_{13^{10}}$	$240, 245, 281, 490, 738, 843, 846, 983, 1476, 1692, 1970, 57840, 59045, 67481, 118090, 177138, 202443,$ $202446, 236183, 354276, 404892, 472370, 636480, 649740, 742561, 1299480, 1949223, 2227683,$ $2227686, 2598963, 3898446, 4455372, 5197930$

Acknowledgments

The first author would like to acknowledge the support from The Danish Council for Independent Research (DFF-FNU) for the project *Correcting on a Curve*, Grant No. 8021-00030B. The second author would like to thank the Italian Ministry MIUR, Strutture Geometriche, Combinatoria e loro Applicazioni, Prin 2012 prot. 2012XZE22K and GNSAGA of the Italian INDAM.

References

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

[2] N. Anbar, A. Bassa and P. Beelen, *A complete characterization of Galois subfields of the generalized Giulietti-Korchmáros function field*, Finite Fields Appl. **48**, 318–330, (2017).

[3] A. Bassa, L. Ma, C. Xing and S.L. Yeo, *Towards a characterization of subfields of the Deligne-Lusztig function fields*, J. Combin. Theory Ser. A **120** (7), 1351–1371, (2013).

[4] P. Beelen and M. Montanucci, *A new family of maximal curves*, Journal of the London Math. Soc., appeared online. DOI: 10.1112/jlms.12144.

[5] A. Cossidente, G. Korchmáros and F. Torres, *Curves of large genus covered by the Hermitian curve*, Comm. Algebra **28** (10), 4707–4728, (2000).

[6] F. Dalla Volta, M. Montanucci and G. Zini, *On the classification problem for the genera of quotients of the Hermitian curve*, preprint, arXiv:1805.09118.

[7] Y. Danişman and M. Özdemir, *On the genus spectrum of maximal curves over finite fields*, J. Discr. Math. Sc. and Crypt. **18** (5), 513–529, (2015).

[8] S. Fanali and M. Giulietti, *Quotient curves of the GK curve*, Adv. Geom. **12** (2), 239–268, (2012).

[9] A. Garcia, C. Güneri and H. Stichtenoth, *A generalization of the Giulietti-Korchmáros maximal curve*, Adv. Geom. **10** (3), 427–434, (2010).

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

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

[12] M. Giulietti and G. Korchmáros, *Algebraic curves with many automorphisms*, preprint, arXiv:1702.08812.

[13] M. Giulietti, G. Korchmáros and F. Torres, *Quotient curves of the Suzuki curve*, Acta Arithmetica **122** (3), 245–274, (2006).

[14] M. Giulietti, M. Montanucci, L. Quoos and G. Zini, *On some Galois covers of the Suzuki and Ree curves*, Journal of Number Theory **189**, 220–254, (2018).

[15] C. Güneri, M. Özdemir and H. Stichtenoth, *The automorphism group of the generalized GiuliettiKorchmáros function field*, Adv. Geom. **13**, 369–380, (2013).

[16] R.W. Hartley, *Determination of the ternary collineation groups whose coefficients lie in the $GF(2^n)$*, Ann. of Math. Second Series **27** (2), 140–158, (1925).

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

[18] 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), 729–732, (1987).

[19] L. Ma and C. Xing, *On subfields of the Hermitian function fields involving the involution automorphism*, preprint, arXiv:1707.07314.

[20] H.H. Mitchell, *Determination of the ordinary and modular ternary linear groups*, Trans. Amer. Math. Soc. **12** (2), 207–242, (1911).

[21] M. Montanucci and G. Zini, *Some Ree and Suzuki curves are not Galois covered by the Hermitian curve*, Finite Fields Appl. **48**, 175–195, (2017).

[22] M. Montanucci and G. Zini, *On the spectrum of genera of quotients of the Hermitian curve*, Comm. Algebra **46** (11), 4739–4776, (2018).

[23] M. Montanucci and G. Zini, *The complete list of genera of quotients of the $\mathbb{F}_{q^2}$-maximal Hermitian curve for $q \equiv 1 \pmod 4$*, preprint, arXiv:1806.04546.

Peter Beelen
Technical University of Denmark,
Department of Applied Mathematics and Computer Science,
Matematiktorvet 303B,
2800 Kgs. Lyngby,
Denmark,
pabe@dtu.dk

Maria Montanucci
Universitá degli Studi della Basilicata,
Dipartimento di Matematica, Informatica ed Economia,
Campus di Macchia Romana,
Viale dell' Ateneo Lucano 10,
85100 Potenza,
Italy,
maria.montanucci@unibas.it